From: "5.1.2.e "
Sent: Mon, 10 Jul 2023 11:19:12 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Pentesten

Hoi,

Onderstaand de link:

Externe Toetsen en pentesten - Kiesraad Wiki - SSC-ICT - Confluence (rijksweb.nl)

Volgens mij is Hackdefense nu aan de beurt.

Met vriendelijke groet,

5.1.2.e
5.1.2.e

.....
KIESRAAD
Bezoekadres: Zürichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
5.1.2.e @kiesraad.nl
www.kiesraad.nl
.....
Afwezig op vrijdag

From: "5.1.2.e "
Sent: Tue, 11 Jul 2023 14:37:30 +0200
To: "5.1.2.e @hackdefense.nl" <5.1.2.e @hackdefense.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Verlenging raamovereenkomst: Pentesten en Beveiligingsonderzoeken met kenmerk 201865007.433 - Pl-HackDefense
Attachments: Verlengingsbrieven Beveiligingsonderzoeken en pentesten 1.pdf

Beste 5.1.2.e

Dank voor het prettige gesprek van vandaag.
En dank ook voor de melding met betrekking tot de verlenging, ik heb de brieven en de correspondentie getraceerd en het schijnt dat deze begin februari per post verstuurd zijn aan de leveranciers.
Wellicht is het aan de aandacht ontsnapt of is er iets mis gegaan met de bezorging.

Maar in ieder geval, alsnog een exemplaar in de bijlage.

Met vriendelijke groet,

5.1.2.e
5.1.2.e

.....
KIESRAAD
Bezoekadres: Zürichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
5.1.2.e @kiesraad.nl
www.kiesraad.nl
.....
Afwezig op vrijdag

> Retouradres Postbus 20011 2500 EA Den Haag

HackDefense B.V.
T.a.v. 5.1.2.e
Zijlbaan 28
2352 BN Leiderdorp

Rijksinkoopsamenwerking (RIS)

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag
Postbus 20011
2500 EA Den Haag

Contactpersoon
5.1.2.e

E-mailadres
5.1.2.e @rijksoverheid.nl

Kenmerk
1_201865007.433-P1-HackDefense

Datum 3 februari 2023

Betreft Verlenging Raamovereenkomst "Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software" met kenmerk 201865007.433 – P1-HackDefense

Geachte 5.1.2.e

Uw overeenkomst
De Kiesraad heeft een Raamovereenkomst met u gesloten inzake "Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software", welke is ingegaan per 27 juli 2020.

Gewenste verlenging
Overeenkomstig het gestelde in artikel 4.3 bericht ik u dat deze Raamovereenkomst onder gelijkblijvende voorwaarden met één (1) jaar wordt verlengd. Dit betreft de eerste en tevens laatste verlenging voor de periode van 27 juli 2023 tot en met 26 juli 2024.

Wij hopen dat u hiermee voldoende bent geïnformeerd en kijken uit naar een prettige voortzetting van de samenwerking.

Hoogachtend,

De Kiesraad,
namens deze,
de secretaris-directeur,

5.1.2.e

From: "5.1.2.e "
Sent: Tue, 11 Jul 2023 15:37:28 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: opdrachtbrief Hackdefense
Attachments: Opdrachtbevestiging Pentest OSV2020 Module PP Hack Defense_def.docx

Met vriendelijke groet,

5.1.2.e
Adviseur bedrijfsvoering
.....
KIESRAAD
Bezoekadres: Zürichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
5.1.2.e @kiesraad.nl
www.kiesraad.nl
.....
Afwezig op donderdag

KIESRAAD

Aan: 5.1.2.e

KIESRAAD

Datum
11 juli 2023

Onderwerp
Pentest OSV2020 TK Module PP Hack Defense

Bezoekadres
Zurichtoren, 14 etage
Muzenstraat 85
2511 WB Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Internetadres
www.kiesraad.nl

Geachte 5.1.2.e

N.a.v. de raamovereenkomst tussen de Kiesraad en Hackdefense van 26 juli 2020 inzake "Het uitvoeren van pentesten, veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software", verstrek ik u hierbij een opdracht voor de pentest en code review OSV2020 TK Module PP.

Voorwaarden opdracht
Op deze opdracht zijn de Algemene voorwaarden voor het verstrekken van opdrachten tot het verlenen van diensten ARBIT 2022 van toepassing. De voorwaarden van de Leverancier zijn uitdrukkelijk uitgesloten.

Voorwerp van de opdracht
De navolgende documenten vormen gezamenlijk de opdracht. Voor zover deze stukken met elkaar in tegenspraak zij, prevaleert het eerder genoemde stuk boven het later genoemde:

1. Dit document, inclusief de bijlage;
2. De Raamovereenkomst.

Prestatie
Het uitvoeren van de Opdracht met betrekking tot de pentest en code review OSV2020 TK Module PP, vindt plaats conform de planning en procedure als vermeld in de bijlage.

Acceptatie van de hiervoor genoemde Prestatie vindt plaats in overleg met Opdrachtgever, uiterlijk 30 dagen na Oplevering (ARBIT 11.1).

Kosten
De totale kosten voor de opdracht bedragen maximaal € 5.1.2.f excl. btw

(€ 5.1.2.f incl. btw).

De opdracht vangt aan op <datum/na ondertekening van deze opdrachtbrief> en eindigt op uiterlijk <datum>.
Meerwerk kan pas na akkoord worden gerealiseerd. Dit wordt schriftelijk bevestigd.

Facturatie
Ik wil u er op wijzen dat de Rijksoverheid e-factureren voor alle bestellingen en contracten verplicht heeft gesteld. Papieren facturen of pdf-facturen per mail worden helaas niet in behandeling genomen. Ter informatie is een bijsluiter e-factureren bijgevoegd.

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van **BUDGETCODERING H2B 401002 – 11312 – 44011.**

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

De Kiesraad ontvangt voor de eigen financiële afdeling graag een kopie factuur: Bedrijfsvoering@Kiesraad.nl.

Contactpersonen Opdrachtgever en Wederpartij
De personen die de contacten over de uitvoering van de Prestatie onderhouden zijn:

Voor Opdrachtgever:
5.1.2.e
E:
M:

Voor Wederpartij:
5.1.2.e
E:
M:

Alle bovengenoemde documenten zijn in uw en ons bezit.

Met vriendelijke groet,

5.1.2.e
secretaris-directeur Kiesraad

From: "5.1.2.e "
Sent: Wed, 12 Jul 2023 16:04:50 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Aangepaste Opdrachtbevestiging en kaders pentest PP door Hack Defense
Attachments: Opdrachtbevestiging Pentest OSV2020 TK 2023 Hack Defense_def.pdf, Kaders pentesten OSV2020 PP TK 2023 1.0.pdf

Hallo allen,

Ik pak hem hier weer even over, want het opstellen van opdrachtbrieven ligt officieel bij Bedrijfsvoering. Ik heb de eerste alinea aangepast o.b.v. onderstaande.

@5.1.2.e indien je zo akkoord bent wil ik je vragen het document van een digitale handtekening te voorzien, waarna die verzonden kan worden. Alvast dank.

Groet, 5.1.2.e

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 12 juli 2023 15:30
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: FW: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Hoi 5.1.2.e

Kan je in de opdrachtverstrekking de geel gearceerde zinsnede opnemen?

Deze opdracht wordt aan [leverancier] gegund op basis van de afgesproken opdrachtverstrekking in de raamovereenkomst, in deze een roulatieschema.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 12 juli 2023 14:57
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Prima zo voor mij.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 12 juli 2023 14:09
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Hallo 5.1.2.e

Dat is prima… dan kunnen we in de opdrachtbevestiging volstaan met de zinsnede dat …deze opdracht aan [leverancier] tot stand komt op basis van de afgesproken opdrachtverstrekking in de raamovereenkomst, in deze een roulatieschema.

Mochten we overigens om wat voor reden dan ook af moeten, of willen wijken van dit schema tot opdrachtverstrekking, dan moeten we dat heel goed vastleggen. Want dan kan de ADR weer gaan zeuren dat we afwijken van wat we in andere gevallen expliciet hebben vastgelegd.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 12 juli 2023 14:00
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Ha 5.1.2.e nog even over nagedacht, maar in de context van dat ik wil vastleggen dat we dit gewoon altijd netjes doen en geen enkele keuzevrijheid hebben en nemen in welke partij welke verkiezing test: fijn als we een 'selectiebeschrijving' vanaf nu opnemen als er meerdere partijen in de rovk zitten.

Groet,
5.1.2.e

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 12 juli 2023 09:40
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Hoi 5.1.2.e

Ik denk dat het dan meer verwarring opwekt, want waarom hebben we dat in een eerder stadium niet gedaan en nu bij een van de laatste opdrachten binnen deze raamovereenkomst wel?

Maar goed als jij het wil dan kan het er in. En dan zullen we het opnemen in de uitvraag template voor bij de volgende raamovereenkomst.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 12 juli 2023 09:36
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Hoi 5.1.2.e

Ik begrijp dat het niet nodig is en overbodig over komt. Maar het is voor mij meer een contextbeschrijving die mij nuttig lijkt bij een evt. Woo-verzoek naar de opdrachtverlening.

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Datum: woensdag 12 jul. 2023 9:20 AM
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Goedemorgen 5.1.2.e en 5.1.2.e

We hebben het hier over een (interne) opdrachtbrief, die we voor het inkoopdossier willen vastleggen, zodat bijvoorbeeld een ADR weet dat we de juiste procedure hebben gevolgd bij de uitnutting van de raamovereenkomst.
In die opdrachtbrief vermelden dat we een aanbesteding hebben gevolgd en welke partijen daar uit zijn gekomen is niet zo heel relevant.
We hebben dit ook bij andere opdrachten binnen deze raamovereenkomst nooit gedaan.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 12 juli 2023 08:21
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Dank, zouden we in het begin nog meer in algemene zin kunnen melden iets als dat we hebben aanbesteed voor de periode van x tot y, dat daar drie partijen uit zijn voortgekomen, die op volgorde per verkiezing worden ingezet, en dat Hack Defensie bij deze verkiezing aan de beurt is?
Goed om dat vast te leggen denk ik.

Verder staat ergens nog ‘ zij’ ipv ‘ zijn’.

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Datum: dinsdag 11 jul. 2023 4:44 PM
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Opdrachtbevestiging en kaders pentest PP door Hack Defense

Beste 5.1.2.e

Wij hebben afgestemd dat Hack Defense een pentest gaat uitvoeren op de PP module van OSV voor de TK 2023.
In de bijlage vind je de Opdrachtsbevestiging en een bijlage met opgestelde en afgestemde kaders.

Zou jij de Opdrachtsbevestiging en de bijlage willen lezen en per email akkoord kunnen geven, bij voorkeur voor vrijdag 14 juli?

De bijlage is wellicht wat technisch. Mocht je daar toelichting op wensen, stel daar dan gerust vragen over aan mij.
Als wij jouw akkoord hebben dan kunnen we de Opdrachtsbevestiging digitaal ondertekenen en verzenden naar Hack Defense, zodat zij op tijd kunnen beginnen met de voorbereidingen.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
W www.kiesraad.nl

From: "5.1.2.e "
Sent: Thu, 13 Jul 2023 11:48:49 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: opdrachtbrief HackDefense
Attachments: Kaders pentesten OSV2020 PP TK 2023 1.0.pdf, Opdrachtbevestiging Pentest OSV2020 TK 2023 Hack Defense_def.pdf

Hoi 5.1.2.e

Wil jij de getekende brief met bijlage naar 5.1.2.e sturen en bedrijfsvoering in de cc meenemen? Ik heb helaas geen mailadres. Alvast dank.

Groet, 5.1.2.e

KIESRAAD

Aan: HackDefense B.V.
t.a.v. 5.1.2.e
Sisalbaan 5
2352 AZ Leiderdorp

KIESRAAD

Datum
12 juli 2023

Blad
1 van 3

Bezoekadres
Zurichtoren, 14 etage
Muzenstraat 85
2511 WB Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Bijlage:
Kaders pentesten OSV 2020 PP TK 2023

Onderwerp
Pentest OSV2020 TK Hack Defense

Geachte 5.1.2.e

Hierbij verstrek ik HackDefense B.V. namens de Kiesraad een opdracht voor de pentest en code review OSV2020 TK.

De opdracht wordt gegund op basis van de afgesproken opdrachtverstrekking in de raamovereenkomst tussen de Kiesraad en HackDefense B.V. van 26 juli 2020 (perceel 1) inzake "Het uitvoeren van pentesten, veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software", in deze een roulatieschema.

Voorwaarden opdracht
Op deze opdracht zijn de Algemene voorwaarden voor het verstrekken van opdrachten tot het verlenen van diensten ARBIT 2018 van toepassing. De voorwaarden van de Leverancier zijn uitdrukkelijk uitgesloten.

Voorwerp van de opdracht
De navolgende documenten vormen gezamenlijk de opdracht. Voor zover deze stukken met elkaar in tegenspraak zij, prevaleert het eerder genoemde stuk boven het later genoemde:

1. Dit document, inclusief de bijlage;
2. De Raamovereenkomst.

Prestatie
Het uitvoeren van de Opdracht met betrekking tot de pentest en code review OSV2020 TK, waar de Kiesraad waarde hecht om snel te kunnen starten met de Module PP. De pentest vindt plaats conform de planning en procedure als vermeld in de bijlage document "Kaders pentest OSV2020 TK – Module PP 2023.

Hack Defense zal worden verzocht een tussenrapportage aan te leveren voor de module PP in verband met oplevering en ingebruikname moment van de software.

Acceptatie van de hiervoor genoemde Prestatie vindt plaats in overleg met Opdrachtgever, uiterlijk 30 dagen na Oplevering van de rapportage (ARBIT 11.1).

Kosten
De totale kosten voor de opdracht bedragen maximaal € 5.1.2.f excl. btw (€ 5.1.2.f incl. btw).

De opdracht vangt aan op 14-07-2023.
Meerwerk kan pas na akkoord worden gerealiseerd. Dit wordt schriftelijk bevestigd.

Het hier genoemde bedrag betreft de pentest op de gehele OSV2020 TK software, inclusief code review van alle relevante modules uit de raamovereenkomst.

Facturatie
Ik wil u er op wijzen dat de Rijksoverheid e-factureren voor alle bestellingen en contracten verplicht heeft gesteld. Papieren facturen of pdf-facturen per mail worden helaas niet in behandeling genomen. Ter informatie is een bijsluiter e-factureren bijgevoegd.

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van **BUDGETCODERING H2B 401002 – 11312 – 44011.**

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

De Kiesraad ontvangt voor de eigen financiële afdeling graag een kopie factuur: Bedrijfsvoering@Kiesraad.nl.

Contactpersonen Opdrachtgever en Wederpartij
De personen die de contacten over de uitvoering van de Prestatie onderhouden zijn:

Voor Opdrachtgever:
5.1.2.e
E: 5.1.2.e @kiesraad.nl
M: 5.1.2.e

Voor Wederpartij:
5.1.2.e
E: 5.1.2.e @hackdefense.nl
M: 5.1.2.e

Alle bovengenoemde documenten zijn in uw en ons bezit.

Met vriendelijke groet,
5.1.2.e
5.1.2.e
secretaris-directeur Kiesraad

From: "5.1.2.e" <5.1.2.e@hackdefense.nl>
Sent: Thu, 13 Jul 2023 13:38:54 +0200
To: "5.1.2.e" <5.1.2.e@kiesraad.nl>; "5.1.2.e" <5.1.2.e@kiesraad.nl>
Cc: "5.1.2.e" <5.1.2.e@kiesraad.nl>; "5.1.2.e" <5.1.2.e@hackdefense.nl>
Subject: Re: FW: opdrachtbrief HackDefense
Attachments: Bijlage C - Beschrijving van de Prestatie v1.0.pdf

Dank voor de opdrachtbevestiging!

Zoals zojuist telefonisch besproken, wij zijn akkoord met de opdracht m.u.v. de code review die volgens Bijlage C van de aanbestedingsdocumenten uit Fase 2 ("Bijlage C - Beschrijving van de prestatie v1.0.pdf", zie bijlage, pagina 15) expliciet buiten de reikwijdte valt.

We zullen voor nu dan van OSV2020-PP geen code review uitvoeren, en voor de andere modules die we daarna gaan doen de code review onder een nader te bespreken vervolg-opdracht uitvoeren.

Dank!

5.1.2.e

On 13/07/2023 11:56, 5.1.2.e wrote:

> 5.1.2.e
>
> Hierbij de opdrachtbevestiging. De definitieve versie van het kaderdocument volgt via secure transfer.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo
> .....
> **KIES**RAAD
> Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
> Postadres: Postbus 20011, 2500 EA Den Haag
> .....
> T 5.1.2.e
> W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Uitvoeringsorganisatie
Bedrijfsvoering Rijk
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bijlage C – Beschrijving van de Prestatie

UBR|HIS

Bezoekadres
Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage C – Beschrijving van de Prestatie

Behorend bij

Europese niet-openbare aanbesteding

Toetsing, testen van en advisering over verkiezing gerelateerde systemen en software

ten behoeve van

de Kiesraad

Datum	Mei 2020
Kenmerk	201850004.213.001
Versie	1.0

Inhoud

Leeswijzer bij deze Bijlage

U leest:

- in hoofdstuk 1 achtergrondinformatie over de (informatie)systemen van de Kiesraad.
- in hoofdstuk 2 en 3 een uitgebreide beschrijving van de Prestaties ten behoeve van perceel 1 en perceel 2.
- in hoofdstuk 4 een beschrijving van de wijze van opdrachtverstrekking onder de Raamovereenkomsten voor perceel 1 en perceel 2.
- in hoofdstuk 5 een toelichting op de standaard pentesten.

1. Achtergrondinformatie over de Overheidsopdracht

In dit hoofdstuk lees u informatie over de informatiesystemen van de Kiesraad.

Achtergrondinformatie over informatiesystemen van de Kiesraad
Hieronder leest u een toelichting op een aantal verkiezing gerelateerde systemen en –software van de Kiesraad. Deze lijst is niet limitatief voor de duur van de Raamovereenkomst. Gedurende de duur van de Raamovereenkomst kunnen nieuwe informatiesystemen worden toegevoegd.

OSV en Vervanging OSV
De Kiesraad heeft in 2009 Ondersteunende Software Verkiezingen (hierna: OSV) laten ontwikkelen. Sinds de Europees Parlementsverkiezing van 2009 wordt OSV gebruikt ter ondersteuning van het verkiezingsproces. OSV bestaat uit vijf (5) afzonderlijke programma's, die verschillende facetten van het verkiezingsproces ondersteunen. De eerste drie programma's zijn bedoeld voor de kandidaatstelling en worden door politieke partijen en centraal stembureaus gebruikt om de kandidatenlijsten op te stellen en deze te controleren. De programma's 4 en 5 worden gebruikt bij de vaststelling van de uitslag en de zetelverdeling. Programma 4 is bedoeld voor gemeenten, hoofdstembureau en centraal stembureau om de uitslag vast te stellen en programma 5 ondersteunt het centraal stembureau bij het vaststellen van de zetelverdeling. Voor meer informatie en de broncode van het huidige OSV van de programma's 4 en 5, zie: https://www.kiesraad.nl/verkiezingen/inhoud/osv-en-eml/ondersteunende-software-verkiezingen-osv.

Recent is besloten om over te gaan op Vervanging OSV waarin, ten opzichte van OSV, verbeteringen zijn doorgevoerd in de softwarekwaliteit (door gebruik te maken van actuelere software-onderdelen/library) en softwarebeveiliging. Met de overgang naar Vervanging OSV wordt het programma als volgt onderverdeeld:

- Kandidaatstellingssoftware voor politieke partijen en het centraal stembureau;
- Software voor de vaststelling van de uitslag en zetelverdeling voor onder andere gemeenten en centraal stembureau.

De Kiesraad laat Vervanging OSV op dit moment ontwikkelen, een indicatie van de opbouw van de programmatuur en de omvang (aantallen regels code) zijn opgenomen in Bijlage N - Lines of code.

Databank verkiezingsuitslagen
De Databank Verkiezingsuitslagen is een website met als doel om de uitslagen van verkiezingen digitaal toegankelijk te maken. De publiekelijk toegankelijke Databank omvat inmiddels de uitslagen van meer dan 700 stemmingen. De Kiesraad heeft de Databank Verkiezingsuitslagen laten ontwikkelen en heeft deze in beheer. Hosting en applicatiebeheer van de website is uitbesteed aan een derde partij.

Nieuwe digitale hulpmiddelen
De nieuwe digitale hulpmiddelen zijn nog nader te ontwikkelen hulpmiddelen voor de kandidaatstelling en het bepalen van de uitslag en de zetelverdeling bij verkiezingen. Dit hulpmiddel wordt nog ontworpen en kan bestaan uit een combinatie van software en hardware. De digitale hulpmiddelen kunnen (web)applicaties, mobiele apps, endpoints, servers en netwerkcomponenten omvatten. Het is de bedoeling dat de nieuwe digitale hulpmiddelen op termijn Vervanging OSV gaan vervangen. Het is nog onzeker op welke termijn dit zal gebeuren.

2. Beschrijving van de Prestatie - perceel 1

De Kiesraad besteedt de onderstaande opdrachtonderdelen aan als onderdeel van perceel 1:

- Advisering over beveiliging van (verkiezings)software;
- Uitvoeren van pentesten en veiligheidsonderzoeken op (verkiezings)software.

U leest een beschrijving van deze opdrachtonderdelen in de eerste twee paragrafen.

In paragraaf 3 leest u een beschrijving van een specifieke pentest Opdracht, die wij direct vanuit deze Aanbesteding verstrekken door middel van een Nadere Overeenkomst. Een indicatie van de omvang van dit perceel leest u terug in paragraaf 4.

2.1. Advisering over beveiliging van (verkiezings)software

De Kiesraad wenst op aanvraag adviesopdrachten af te nemen over informatiebeveiligingsvraagstukken. Met behulp van deze Opdrachten tracht de Kiesraad advies te verkrijgen over uiteenlopende informatiebeveiligingsonderwerpen. De Kiesraad wenst bijvoorbeeld advies in te winnen over vraagstukken met betrekking tot:

- De implementatie van (technische) maatregelen om de weerbaarheid van het verkiezingsproces tegen cyberaanvallen te verhogen;
- Het ontwerp en de architectuur van een informatiesysteem (bijv. veilige overdracht van data, de toepassing van encryptie, beschikbaarheid etc.);
- De implementatie van procedures voor het veilig installeren, configureren en gebruiken van informatiesystemen;
- Informatiebeveiligingsbeleid en -strategie.

De bovenstaande lijst betreft slechts een indicatieve weergave van de vraagstukken en betreft nadrukkelijk geen limitatieve lijst.

In voorkomende gevallen neemt de Kiesraad dergelijke adviesopdrachten af van de gecontracteerde Wederpartijen op basis van een minicompetitie. De Kiesraad wenst dat de Wederpartij de uitkomsten van de advieswerkzaamheden beschrijft in een schriftelijke rapportage, nota of memo. De Kiesraad heeft het recht om Opdrachten met een geraamde waarde onder de € 33.000,- rechtstreeks te gunnen aan een van de gecontracteerde Wederpartijen. De Kiesraad hanteert hiervoor een roulatiesysteem onder gecontracteerde Wederpartijen.

2.2. Uitvoeren van pentesten en veiligheidsonderzoeken op (verkiezings)software;

De Kiesraad wenst verschillende pentesten en veiligheidsonderzoeken af te nemen. De Kiesraad verdeelt deze in twee onderdelen:

1. Standaard pentesten op basis van roulatiesysteem;
2. Pentesten en veiligheidsonderzoeken op aanvraag.

Hieronder gaat de Kiesraad nader in op deze twee onderdelen:

2.2.1. Standaard pentesten op basis van roulatiesysteem

De Kiesraad wenst periodiek standaard pentesten uit te laten voeren op de volgende testobjecten:

a. OSV;
b. Vervanging OSV;
c. Databank Verkiezingsuitslagen;
d. De nader te ontwikkelen digitale hulpmiddelen.

Onder de term 'standaard pentest' verstaat de Kiesraad een pentest met een vooraf gedefinieerde reikwijdte, aanpak en prijs. De tabellen in hoofdstuk 5 specificeren op de reikwijdtes van deze standaard pentesten.

Door het voortdurend wijzigende IT-landschap bestaat de kans dat de Kiesraad in de toekomst in het kader van de Raamovereenkomst standaardtesten wenst af te nemen op andere onderzoeksobjecten dan de hierboven beschreven software. In voorkomende gevallen verzoekt de Kiesraad Wederpartij een standaardprijs en -aanpak te formuleren voor dergelijke onderzoeken.

De prijs van standaard pentesten voor het nader te ontwikkelen digitaal hulpmiddel bepalen we samen met de Wederpartijen tijdens de Raamovereenkomst. De Kiesraad verstrekt de Opdrachten voor de standaard pentest via een roulatiesysteem tussen de geselecteerde Wederpartijen.

Hoofdstuk 5 geeft een extra toelichting op de standaard pentest.

2.2.2. Pentesten en veiligheidsonderzoeken op aanvraag

Naast de bovengenoemde standaard pentesten heeft de Kiesraad behoefte aan pentesten en veiligheidsonderzoeken met een specifieke reikwijdte, periodiciteit, diepgang, aanpak of testwijze.

De Kiesraad is voornemens de volgende varianten van pentesten en veiligheidsonderzoeken aan te vragen:

1. Black-box pentest;
2. Grey-box pentest;
3. White-box pentest;
4. Kwetsbaarhedenscan;
5. Secure Code Review;
6. Een combinatie van de bovengenoemde onderzoeken.

Daarnaast kan de Kiesraad in voorkomende gevallen de volgende varianten van veiligheidsonderzoeken aanvragen:

7. Social Engineering;
8. Configuratiereview;
9. Red Teaming;
10. Een combinatie van alle bovengenoemde onderzoeken.

Deze pentesten en veiligheidsonderzoeken zet de Kiesraad uit via een minicompetitie bij de gecontracteerde Wederpartijen in de Raamovereenkomst.

<u>Resultaat van bovengenoemde pentesten en veiligheidsonderzoeken</u>
Het resultaat van de bovengenoemde 'pentesten en veiligheidsonderzoeken op aanvraag' is een rapportage dat bestemd voor de Kiesraad. Deze rapportage bevat ten minste de volgende onderdelen:

- Managementsamenvatting
- Introductie, met:
    - opdrachtbeschrijving;
    - scopedefinitie;
    - aanpak (methoden en technieken).
- Bevindingen, met per bevinding:
    - observatie;
    - risico-inschatting;
    - CVSS 3.1 score;
    - onderbouwing;
    - aanbeveling.
- Risicomatrix en -correlatie
- Algemene conclusies en aanbevelingen

2.3. Opdrachtbeschrijving direct uit te voeren specifieke pentest

De Kiesraad wil een White-box pentest inclusief Secure Code Review en Configuratiereview laten uitvoeren op de vervangende OSV-software (=Vervanging OSV). Voor de uitvoering van deze pentest levert u een plan van aanpak op, die de Kiesraad als Subgunningscriterium 2 beoordeelt. De prijs voor de uitvoering van deze pentest dient opgegeven te worden in het Prijsopgavenformulier (Bijlage 3). Deze White-box pentest inclusief Secure Code Review en Configuratiereview voert u eind augustus/september 2020 uit.

Daarnaast neemt de Kiesraad in de Nadere Overeenkomst een mogelijkheid op om een hertest af te nemen die op basis van nacalculatie wordt afgerekend. De Kiesraad behoudt zich het recht om een tweede hertest af te nemen.

Doelstelling

De doelstelling van de pentest is om de verschillende onderdelen van de vervangende OSV-software te onderzoeken op kwetsbaarheden teneinde ons in staat te stellen om het beveiligingsniveau van de software te verhogen.

Hieronder zijn de drie hoofdonderzoeksvragen opgenomen. U dient onderstaande hoofdonderzoeksvragen te beantwoorden:

1. Welke kwetsbaarheden en risico's op het gebied van informatiebeveiliging zijn te onderkennen in de vervanging OSV-applicatie?
2. In hoeverre zijn de IT-componenten waar de vervanging OSV-applicatie van gebruikmaken (te weten: de applicatieserversoftware en databaseserver) gehardend conform Industry Best Practices?
3. Welke maatregelen kunnen worden getroffen om de geconstateerde risico's te mitigeren?

De reikwijdte van de Opdracht

De Kiesraad wenst de volgende applicatie te onderzoeken als onderdeel van Vervanging OSV:

- Software voor de vaststelling van de uitslag en zetelverdeling.

Kenmerken (uitgangspunten) van de direct uit te voeren pentest (specifieke pentest):

Kenmerken van de direct uit te voeren pentest	
Boxtype	White-box pentest: De tester krijgt volledige openheid over de werking van de applicatie, systemen, architectuur, infrastructuur en broncode.
Perspectief	Geautoriseerd perspectief: de tester ontvangt representatieve testaccounts om het onderzoeksobject tevens vanuit geautoriseerd perspectief te kunnen testen.
Omgeving	Het testobject wordt op basis van te installeren software beschikbaar gesteld. Wederpartij dient de pentest op een eigen testomgeving uit te voeren.
Secure code review	Onderdeel van deze White-box pentesten is tevens een Secure Code Review. U vindt een indicatie van het aantal *lines of code* in Bijlage N.
Configuratiereview / hardeningsreview	Onderdeel van de pentest is een Configuratiereview ten aanzien van de software waar vervanging OSV gebruik van maakt: - webserver/Applicatieserver (bijv. JEE/Thorntail; - databaseserver (bijv. H2). In de Configuratiereview toetst u in hoeverre de infrastructurele componenten zijn gehardend conform industry best practices of hardeningsrichtlijnen van de softwareleverancier.
Richtlijnen en best practices	Bij de pentest op de applicatie worden minimaal de meest recente versies van de onderstaande richtlijnen en best practices gehanteerd (eventueel door u aan te vullen):

Kenmerken van de direct uit te voeren pentest	
	- OWASP Top 10; - OWASP ASVS; - NCSC ICT-beveiligingsrichtlijnen voor webapplicaties; - NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). In het onderdeel van de pentest waarbij u de configuratie van de web, applicatie- en databaseserver onderzoekt, dient u industry best practices op het gebied van hardening en hardeningsrichtlijnen van de betreffende leveranciers toe te passen.
Hertest	In een hertest dienen de bevindingen uit de initieel door de Wederpartij uitgevoerde pentest opnieuw te worden onderzocht. Indien daartoe aanleiding is, kan een tweede hertest noodzakelijk zijn.

Voor het uitvoeren van de pentest op de software voor de vaststelling van de uitslag dient u te voorzien in een eigen (test)omgeving waarop de software dient te worden geïnstalleerd. De OSV-software wordt als een uitvoerbaar installatiepakket beschikbaar gesteld, welke geïnstalleerd kan worden op een 64bit-systeem met minimaal 2GB-geheugen en is voorzien van een Windows 10 (professional) of Linux (bijvoorbeeld Ubuntu 18.04 of recenter).

De volgende onderdelen vallen expliciet buiten de scope van deze Opdracht:
- Testen of reviews met betrekking tot het besturingssysteem (zoals Windows / Linux) waarop de software draait.
- Testen of reviews met betrekking tot de gebruikte hardware (zoals een laptop / desktop).

2.4. Omvang perceel 1

De volgende paragraaf geeft de omvang van perceel 1 weer. De gegevens over de omvang van dit perceel zijn een indicatie. Aan deze gegevens kunt u geen rechten ontlenen.

Vanwege politieke, budgettaire, bestuurlijke of organisatorische ontwikkelingen binnen de Aanbestedende dienst is het mogelijk dat de omvang wijzigt.

Advisering over beveiliging van (verkiezings)software
De omvang van de adviesvraagstukken hangt af van de hoeveelheid vragen en de grootte van het adviesvraagstuk. De Kiesraad maakt onderscheid tussen kleine en grote adviesvragen. Bij kleine adviesvragen kan worden gedacht aan Opdrachten die in een kort tijdsbestek kunnen worden uitgevoerd (tot ongeveer € 10.000 per vraagstuk). Bij grote adviesvragen kan worden gedacht aan Opdrachten die een langere doorlooptijd hebben (vanaf € 10.000 tot ongeveer € 33.000 per vraagstuk). De Kiesraad verwacht jaarlijks twee tot drie kleine adviesopdrachten en één tot twee grote adviesopdrachten af te nemen. De Kiesraad verwacht relatief weinig adviesopdrachten weg te zetten boven de € 33.000.

Uitvoeren van pentesten en veiligheidsonderzoeken op (verkiezings)software
Standaard pentesten
De Kiesraad is voornemens om voorafgaand aan een verkiezing een standaard pentest af te nemen op het informatiesysteem dat voor de betreffende verkiezing wordt ingezet (OSV/ Vervanging OSV/ digitale hulpmiddelen). Onderstaand is ter illustratie de verkiezingskalender opgenomen. De verkiezingskalender is onder voorbehoud.

Bestuursniveau	Frequentie	Laatste keer	Volgende keer

Tweede Kamerverkiezing	elke 4 jaar[1]	Maart	2017	Maart	2021
Gemeenteraadsverkiezingen	elke 4 jaar[2]	Maart	2018	Maart	2022[3]
Provinciale Statenverkiezingen	elke 4 jaar	Maart	2019	Maart	2023
Waterschapsverkiezingen[4]	elke 4 jaar	Maart	2019	Maart	2023
Eilandsraadsverkiezingen	elke 4 jaar	Maart	2019	Maart	2023
Kiescollegeverkiezingen	elke 4 jaar	Maart	2019	Maart	2023
Eerste Kamerverkiezing[5]	elke 4 jaar	Mei	2019	Mei	2023
Europees Parlementsverkiezing	elke 5 jaar	Mei	2019	Mei	2024

De Kiesraad is daarnaast voornemens om minimaal eenmaal per twee jaar een standaard pentest af te nemen op de Databank Verkiezingsuitslagen.

Pentesten en veiligheidsonderzoeken op aanvraag
De Kiesraad verwacht gedurende de duur van de Raamovereenkomst tussen de twee en drie uitgebreide pentesten of veiligheidsonderzoeken uit te zetten.

Voorbehoud bij de raming van de omvang van dit perceel
Het landschap van de Kiesraad is in transitie: de ontwikkelingen op het gebied van wet- en regelgeving hebben een grote impact op de organisatie en de informatiesystemen. De omvang van de af te nemen diensten kennen hierbij een sterke afhankelijkheid van de ontwikkelingen in het IT-landschap van de Kiesraad. De bovengenoemde ramingen voor dit perceel zijn derhalve indicatief. Het is bijvoorbeeld mogelijk dat de Kiesraad door een onvoorziene ontwikkeling in het IT-landschap een grotere hoeveelheid pentesten of adviesvragen uitvraagt dan initieel geraamd. Een verdubbeling van de aantallen sluit de Kiesraad niet uit.

Tot slot kan de Kiesraad besluiten om een second opinion te laten uitvoeren bij een andere partij in de Raamovereenkomst. Ook dit is onderdeel van de omvang van dit perceel.

[1] Indien er sprake is van ontbinding van het kabinet, kan er een (vervroegde) ontbindingsverkiezing volgen. In dat geval vindt de verkiezing plaats op een ander moment binnen de termijn van 4 jaar.
[2] Indien een gemeente betrokken is bij een gemeentelijke herindelingsprocedure kan van de normale termijn afgeweken worden.
[3] Gewoonlijk worden ieder jaar in november herindelingsverkiezingen gehouden in gemeenten die betrokken zijn bij een herindelingsprocedure die op 1 januari daaropvolgend zijn beslag krijgt.
[4] Vanaf maart 2015 vinden Waterschapsverkiezingen tegelijkertijd plaats met Provinciale Statenverkiezingen.
[5] De Eerste Kamer wordt gekozen door de leden van Provinciale Staten en van de kiescolleges voor de Eerste Kamer.

3. Beschrijving van de Prestatie - perceel 2

De Kiesraad besteedt de onderstaande opdrachtonderdelen aan als onderdeel van perceel 2:

- Uitvoeren toetsing verkiezingssoftware en software-kwaliteitsonderzoek;
- Advisering over kwaliteit van (verkiezings)software.

U leest een beschrijving van deze opdrachtonderdelen in de eerste twee paragrafen.

Een indicatie van de omvang van dit perceel leest u terug in paragraaf 3.

Buiten scope perceel 2
Vraagstukken met betrekking tot softwareveiligheid en/of softwarebeveiliging behoren niet tot de scope van perceel 2, maar tot de scope van perceel 1, tenzij het onderdeel uitmaakt van een softwarekwaliteitstoets op basis van ISO 25010.

3.1. Uitvoeren toetsing verkiezingssoftware en software-kwaliteitsonderzoek

De Kiesraad voorziet voor het uitvoeren van kwaliteitsonderzoek twee soorten Opdrachten:

1. Toetsing verkiezingssoftware aan de wettelijke kaders;
2. Beoordeling van de softwarekwaliteit.

3.1.1. Toetsing verkiezingssoftware aan het wettelijk kader

Bij de toetsing gaat het om een onafhankelijk oordeel over de mate waarin de verkiezingssoftware die gebruikt wordt voor de vaststelling van de uitslag en zetelverdeling, voldoet aan bepaalde (wettelijke) kaders. In de huidige situatie volgt het wettelijk toetsingskader uit art. P 1a Kieswet en de verdere uitwerking daarvan in het Kiesbesluit en Kiesregeling. Voor de toekomst is niet uit te sluiten dat het huidige (wettelijke) kader wordt herzien. Ook een toets op de verkiezingssoftware bij een eventuele herziening van het wettelijke kader valt binnen de reikwijdte van deze Aanbesteding.

Op basis van het huidige wettelijke kader, op grond van art. P 1 lid 4 jo lid 6 van het Kiesbesluit, omvat de toetsingsopdracht de beoordeling van de volgende twee onderdelen:

1. Onderdeel 1: De mate waarin de programmatuur voldoet aan de opgestelde specificatie voor de berekening van de uitslag en zetelverdeling (sub a van bijlage bij art. 2a van de Kiesregeling);
2. Onderdeel 2: De mate waarin de programmatuur voldoet aan de eisen die aan de software worden gesteld volgens bijlage 2 bij art. 2a van de Kiesregeling (sub b t/m m).

De Kiesraad kan de uitvoering van de toetsingsopdracht in verschillende combinaties laten uitvoeren, waarbij enkel onderdeel 1 of onderdeel 2 wordt uitgevraagd, dan wel een combinatie van beiden. Onderdeel 1, de toetsing van de berekening van de uitslag en zetelverdeling, wenst de Kiesraad te kunnen uitvragen per verkiezingstype dan wel voor een combinatie van verkiezingstypen. De verkiezingstypen zijn opgesomd in Bijlage 3 - Prijsopgavenformulier, tabblad 2.

De uitkomst van de toetsingsopdracht dient een rapport te zijn dat, afhankelijk van de uitgevraagde onderdelen, antwoord geeft op de volgende twee onderzoeksvragen:

1. Onderdeel 1: In welke mate voldoet de programmatuur aan de specificaties voor de berekening van de uitslag en zetelverdeling, zoals beschreven in Bijlage P - OSV Specificatie (Formele beschrijving berekening zetelverdeling);
2. Onderdeel 2: In welke mate voldoet de programmatuur aan de eisen (sub b t/m m) die zijn opgenomen in bijlage 2 bij art. 2a van de Kiesregeling.

Het rapport waarin de uitkomsten van de toetsing zijn opgenomen, maakt de Kiesraad openbaar. Het is daarbij van belang dat het rapport een gedegen onderbouwing en juiste context bevat.

Daarnaast dient het rapport te worden voorzien van een heldere samenvatting, waarin de (technische) resultaten op een hoger abstractieniveau worden beschreven in de vorm van conclusies.

De Kiesraad neemt de toetsingsopdrachten af op basis van de vooraf gedefinieerde onderzoeksvragen die leiden tot een vooraf bepaalde aanpak en prijs. De Kiesraad zal voorafgaand aan de uitvoering van een toetsingsopdracht bepalen welke onderdelen in de Opdracht worden meegenomen. De gekozen combinatie van onderdelen bepaalt de prijs voor een specifieke toetsingsopdracht. Indien wijzigingen in het wettelijk kader aanleiding geven tot aanpassingen van de vragen (dan wel de omvang van de toetsing), dan vindt een nieuwe uitvraag plaats op basis van de nieuwe gedefinieerde onderzoeksvragen.

Op grond van art. 2a van de Kiesregeling dient te worden beoordeeld of de programmatuur die wordt gebruikt voor de vaststelling van de verkiezingsuitslag en zetelverdeling aan de volgende eisen voldoet:

a. de programmatuur bevat de functionaliteiten die overeenkomstig de specificatie, bedoeld in artikel P 1, tweede lid, van het Kiesbesluit nodig zijn voor de berekening van de uitslag van de verkiezingen en de zetelverdeling;
b. de programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn;
c. de kritische functies voor de berekening van de uitslag van de verkiezingen en de zetelverdeling zijn in de programmatuur herkenbaar en van elkaar gescheiden;
d. de programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen;
e. toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen;
f. de programmatuur ondersteunt voor de vermelding van de aanduidingen van de politieke groeperingen en de namen van de kandidaten in ieder geval de diakritische tekens van de tekenset die op grond van artikel 3, eerste lid, van het Besluit basisregistratie personen voor de basisregistratie personen is vastgesteld;
g. de programmatuur wordt als open source ontwikkeld en maakt gebruik van open standaarden. Indien dit aantoonbaar niet mogelijk is wordt technologie toegepast waarvan de doeltreffendheid in de praktijk is aangetoond en die direct toepasbaar is. Voor verkiezingsgegevens zoals kandidatenlijsten en zetelverdeling wordt de EML_NL standaard toegepast;
h. de standaard programmatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar;
i. het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau;
j. de programmatuur is geschreven in een programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler, onderscheidenlijk interpreter beschikbaar is;
k. de programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem;
l. het is mogelijk de authenticiteit van de programmatuur vast te stellen; en
m. bij het inlezen van verkiezingsgegevens in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.

3.1.2. Beoordeling softwarekwaliteit

De Kiesraad wenst inzicht te hebben in de softwarekwaliteit van de software die in opdracht van de Kiesraad wordt ontwikkeld. Dit geldt voornamelijk voor specifieke ontwikkelde software. Voor de beoordeling van softwarekwaliteit sluit u aan bij de ISO-25010[6] norm.

[6] *De ISO-25010 norm onderscheidt de volgende Productkwaliteit (Product quality) onderwerpen: Functionele geschiktheid (Functional suitability), Prestatie-efficiëntie (Performance efficiency), Uitwisselbaarheid*

De uitgangspunten uit de ISO-25010 norm dienen dan terug te komen in beoordelings- en waarderingssystematiek die wordt toegepast voor de beoordeling van de software. De waardering van de kwaliteitseigenschappen dient door middel van een representatieve beoordelingsindex te worden weergeven en zo mogelijk te worden afgezet tegen een representatieve marktindex.

De Kiesraad formuleert een beoordelingsvraag waarin onderwerpen ten aanzien van 'Product quality' en/of 'Quality in use', of een subset daarvan, worden uitgevraagd. Het resultaat van de beoordeling geeft, in de vorm van een beoordelingsrapport, inzicht in:

- De meest relevante verbeterpunten voor de verschillende onderwerpen, waarbij zoveel mogelijk de verbeterpunten geconcretiseerd worden naar broncodeniveau;
- De gemaakte keuzes (afweging) die door u dan wel ons zijn gemaakt en een minder gunstige uitwerking hebben op de beoordelingssystematiek. In voorkomende situatie hecht de Kiesraad eraan dat het rapport de context bevat die weloverwogen heeft geleid tot een bepaalde (minder gunstige) beoordeling;
- De resultaten, die inzichtelijk worden gemaakt door middel van een representatieve beoordelingsindex.

De Kiesraad heeft het recht om het beoordelingsrapport (of een gedeelte daarvan) openbaar te maken.

Deze Opdrachten verstrekt de Kiesraad via een minicompetitie onder de gecontracteerde Wederpartijen. Voor een minicompetitie stelt de Kiesraad de exacte opdrachtformulering vast.

3.2. Advisering over kwaliteit van (verkiezings)software

Naast de beoordeling van de softwarekwaliteit wenst de Kiesraad op aanvraag adviesopdrachten af te nemen met betrekking tot dit onderwerp. Met behulp van deze Opdrachten tracht de Kiesraad advies te verkrijgen over uiteenlopende software-kwaliteitsonderwerpen. De Kiesraad wenst bijvoorbeeld advies in te winnen over vraagstukken met betrekking tot:

- Het bepalen van impact bij het al dan niet doorvoeren van software technische wijzigingen, zoals het upgraden van de standaardsoftware-componenten;
- Het opstellen van kwaliteitscriteria voor (nieuw) te ontwikkelen software;
- Het implementeren van softwarekwaliteit verbeteringsvoorstellen.

De bovenstaande lijst betreft slechts een indicatieve weergave van de vraagstukken en betreft nadrukkelijk geen limitatieve lijst.

In voorkomende gevallen neemt de Kiesraad dergelijke adviesopdrachten af van de gecontracteerde Wederpartijen op basis van een minicompetitie. De Kiesraad wenst dat de Wederpartij de uitkomsten van de advieswerkzaamheden beschrijft in een schriftelijke rapportage, nota of memo. De Kiesraad heeft het recht om Opdrachten (Prestaties) met een geraamde waarde onder de € 33.000,- rechtstreeks te gunnen aan een van de gecontracteerde Wederpartijen. De Kiesraad hanteert hiervoor een roulatiesysteem onder gecontracteerde Wederpartijen.

3.3. Omvang perceel 2

De volgende paragraaf geeft de omvang voor perceel 2 weer. De gegevens over de omvang van dit perceel zijn een indicatie. Aan deze gegevens kunt u geen rechten ontlenen.

Vanwege politieke, budgettaire, bestuurlijke of organisatorische ontwikkelingen binnen de Aanbestedende dienst is het mogelijk dat de omvang wijzigt.

Uitvoeren softwarekwaliteitsmeting op (verkiezings)software

(Compatibility), Bruikbaarheid (Usability), Betrouwbaarheid (Reliability), Beveiligbaarheid (Security), Onderhoudbaarheid (Maintainability), Overdraagbaarheid (Portability). Daarnaast onderscheidt de norm verschillende Geschiktheid voor gebruik (Quality in use) onderwerpen.

Toetsing verkiezingssoftware aan het wettelijk kader
De Kiesraad verwacht gedurende de duur van de Raamovereenkomst drie toetsingen van de verkiezingssoftware aan het wettelijke kader weg te zetten.

Beoordeling softwarekwaliteit
De Kiesraad verwacht gedurende de duur van de Raamovereenkomst tussen de vijf tot zeven beoordelingen van softwarekwaliteit uit te zetten.

Advisering over kwaliteit van (verkiezings)software.
De omvang van adviesvraagstukken hangen af van de hoeveelheid vragen en de grootte van het adviesvraagstuk. De Kiesraad maakt onderscheid tussen kleine en grote adviesvragen. Bij kleine adviesvragen kan worden gedacht aan Opdrachten die in een kort tijdsbestek kunnen worden uitgevoerd (tot ongeveer € 10.000 per vraagstuk). Bij grote adviesvragen kan worden gedacht aan Opdrachten die een langere doorlooptijd hebben (vanaf € 10.000 tot ongeveer € 33.000 per vraagstuk). De Kiesraad verwacht jaarlijks een tot twee kleine adviesopdrachten en één grote adviesopdrachten af te nemen. De Kiesraad verwacht relatief weinig adviesopdrachten weg te zetten boven de € 33.000.

Voorbehoud bij de raming van de omvang van de Overheidsopdracht
Het landschap van de Kiesraad is in transitie: de ontwikkelingen op het gebied van wet- en regelgeving hebben een grote impact op de organisatie en de informatiesystemen. De omvang van de af te nemen diensten kennen hierbij een sterke afhankelijkheid met de ontwikkelingen in het IT-landschap van de Kiesraad. De bovengenoemde ramingen voor dit perceel zijn derhalve indicatief. Het is bijvoorbeeld mogelijk dat de Kiesraad door een onvoorziene ontwikkeling in het IT-landschap een grotere hoeveelheid pentesten of adviesvragen uitvraagt dan initieel geraamd. Een verdubbeling van de aantallen sluit de Kiesraad niet uit.

Tot slot kan de Kiesraad besluiten om een second opinion te laten uitvoeren bij een andere partij in de Raamovereenkomst. Ook dit is onderdeel van de omvang.

4. Wijze van opdrachtverstrekking onder de Raamovereenkomsten

Hieronder leest u de wijze van verstrekking van Opdrachten onder de Raamovereenkomsten.

Raamovereenkomst perceel 1

Type opdracht	Wijze van opdrachtverstrekking
Standaard pentest op basis van roulatiesysteem	Op basis van roulatiesysteem tussen de Wederpartijen, waarbij de eerste Opdracht aan de partij wordt verstrekt die in de Aanbesteding het hoogste is geëindigd, gevolgd door de tweede partij in ranking van de Aanbesteding etc.
Pentesten en veiligheidsonderzoeken op aanvraag	Op basis van een minicompetitie bij de drie gecontracteerde Wederpartijen.

Advisering over beveiliging van (verkiezings)software)	• Geraamde opdrachtwaarde < € 33.000,- (excl. btw):
	  ○ roulatiesysteem (zie wijze opdrachtverstrekking bij type opdracht "standaard pentest"). Hierbij geldt dat wij het voornemen hebben om deze opdrachten weg te zetten via het roulatiesysteem, maar niet de plicht. Wij kunnen deze opdrachten ook via een minicompetitie tussen de drie raamcontractantanten uitzetten.
	• Geraamde opdrachtwaarde > € 33.000,- (excl. btw):
	  ○ minicompetitie bij de drie raamcontractanten.

Gedeeltelijke of volledige Second opinion – bij standaard pentest	Een second opinion laat de Kiesraad uitvoeren door de volgende Wederpartij in het roulatiesysteem. Het uitvoeren van een volledige second opinion (dit wil zeggen dat volledige Opdracht nogmaals wordt uitgevoerd) geldt als het uitvoeren van een roulatieopdracht, waarbij de volgende roulatieopdracht door de volgende wederpartij in het roulatiesysteem wordt uitgevoerd.

Gedeeltelijke of volledige Second opinion – in overige situaties.	• Indien vooraf bekend is dat de Kiesraad een second opinion wil laten uitvoeren:
	  ○ Bij het uitvoeren van een minicompetitie, gunt de Kiesraad de opdracht voor de second opinion aan de nummer twee in de ranking van de minicompetitie.
	• Indien niet vooraf bekend is dat de Kiesraad een second opinion wil laten uitvoeren:
	  ○ De Kiesraad voert een nieuwe minicompetitie uit waarin zij de opdracht voor de second opinion verstrekt. De Wederpartij die de initiële opdracht uitvoert, neemt geen deel aan deze minicompetitie.

Raamovereenkomst perceel 2

Type opdracht	Wijze van opdrachtverstrekking
Toetsing verkiezingssoftware aan het wettelijk kader	Op basis van roulatiesysteem tussen de Wederpartijen, waarbij de eerste opdracht aan de partij wordt verstrekt die in de Aanbesteding het hoogste is geëindigd, gevolgd door de tweede partij in ranking van de Aanbesteding, etc. De Kiesraad bepaalt de exacte scope (lees welke onderdelen en/of verkiezingstype er worden uitgevraagd) van de Opdracht.
Beoordeling van softwarekwaliteit	Op basis van een minicompetitie bij de twee gecontracteerde Wederpartijen.

Advisering over kwaliteit van (verkiezings)software	• Geraamde opdrachtwaarde < € 33.000,- (excl. btw): o roulatiesysteem (zie wijze opdrachtverstrekking bij type opdracht "Toetsing verkiezingssoftware aan het wettelijk kader"). Hierbij geldt dat wij het voornemen hebben om deze opdrachten weg te zetten via het roulatiesysteem, maar niet de plicht. Wij kunnen deze opdrachten ook via een minicompetitie tussen de twee raamcontractantanten uitzetten. • Geraamde opdrachtwaarde > € 33.000,- (excl. btw): o minicompetitie bij de twee raamcontractanten.
Gedeeltelijke of volledige Second opinion – Toetsing verkiezingssoftware aan het wettelijk kader	Een second opinion laat de Kiesraad uitvoeren door de volgende Wederpartij in het roulatiesysteem. Het uitvoeren van een volledige second opinion (dit wil zeggen dat volledige Opdracht nogmaals wordt uitgevoerd) geldt als het uitvoeren van een roulatieopdracht, waarbij de volgende roulatieopdracht door de volgende wederpartij in het roulatiesysteem wordt uitgevoerd.
Gedeeltelijke of volledige Second opinion –in overige situaties.	• Indien vooraf bekend is dat de Kiesraad een second opinion wil laten uitvoeren: o Bij het uitvoeren van een minicompetitie, gunt de Kiesraad de opdracht voor de second opinion aan de nummer twee in de ranking van de minicompetitie. • Indien niet vooraf bekend is dat de Kiesraad een second opinion wil laten uitvoeren: o De Kiesraad zet de Opdracht uit bij de andere gecontracteerde Wederpartij,

Opdrachten die we direct aan een Wederpartij verstrekken.
Dit zijn bijvoorbeeld Opdrachten die via het roulatiesysteem worden weggezet of onder een bepaald bedrag vallen. Hiervoor stellen we een Nadere Overeenkomst op om tot verstrekking van de Opdracht over te gaan.

Nadere informatie over minicompetities
In gevallen waarvoor we een minicompetitie uitvoeren, gaan we uit van het volgende:
- We beoordelen de Nadere Offertes op basis van de economisch meest voordelige inschrijving ("EMVI") en in het bijzonder de beste prijs-kwaliteit verhouding;
- De nadere uitwerking van de gunningscriteria en de mate waarin genoemde criteria meewegen in de beoordeling vermelden we vooraf in de betreffende Nadere oproep tot mededinging;
- In het voorkomende geval dat de Nadere Offertes van de Wederpartij(en) niet voldoet(n) aan de gestelde eisen of wanneer de Nadere Offertes anderszins tekortschieten, zijn wij gerechtigd Nadere oproep tot mededinging buiten de Raamovereenkomst te starten.

De duur van de Nadere Overeenkomsten die onder de Raamovereenkomsten worden gesloten wordt in de betreffende Nadere Overeenkomsten vastgelegd. De looptijd van de Nadere Overeenkomsten kan de looptijd van de af te sluiten Raamovereenkomst overschrijden. In beginsel lopen de Nadere Overeenkomsten niet door na 31 december 2024.

5. Toelichting standaard pentesten op basis van roulatiesysteem

Dit hoofdstuk geeft een toelichting op de standaard pentesten, zoals beschreven in hoofdstuk 2.

Standaard pentest – OSV	
Beschrijving en doelstelling	Het uitvoeren van een pentest op verschillende onderdelen van OSV. De test bestaat ten minste uit geautomatiseerde kwetsbaarhedenscans en handmatige testactiviteiten. Bij een standaard pentest hoeft geen Secure Code Review uitgevoerd te worden. Een hertest, waarbij de bevindingen uit de initiële pentest opnieuw worden onderzocht, vindt plaats op basis van nacalculatie.
Reikwijdte	De onderstaande testobjecten vallen binnen de reikwijdte van deze Opdracht: - Software ten behoeve van de kandidaatstelling (zie voor meer informatie ook de website); - Software ten behoeve van de vaststelling van de uitslag (zie voor meer informatie ook de website).
Technische informatie testobject	- OSV is geschreven in Java; - De software wordt voorafgaand aan de test ter beschikking gesteld; - Het betreft software die op Windows, MacOS en Linux distributies kan worden geïnstalleerd.
Tenminste te beantwoorden onderzoeksvragen	1. Welke kwetsbaarheden en risico's op het gebied van informatiebeveiliging zijn te onderkennen in het testobject? 2. Welke maatregelen kunnen worden getroffen om de geconstateerde risico's te mitigeren?
Buiten de reikwijdte	• De infrastructuur waarop deze software is geïnstalleerd. • Het uitvoeren van een Secure Code Review.
Omgeving	U krijgt de software aangeleverd en voert de testen zodoende op eigen apparatuur uit.

Standaard pentest – Vervanging OSV	
Beschrijving en doelstelling	Het uitvoeren van een pentest op verschillende onderdelen van Vervanging OSV, inclusief de onderliggende infrastructuur van de centrale componenten. De test bestaat ten minste uit geautomatiseerde kwetsbaarhedenscans en handmatige testactiviteiten. Bij een standaard pentest hoeft geen Secure Code Review uitgevoerd te worden. Een hertest, waarbij de bevindingen uit de initiële pentest opnieuw worden onderzocht, vindt plaats op basis van nacalculatie..
Reikwijdte	De Kiesraad wenst de volgende applicaties te onderzoeken als onderdeel van vervanging OSV: - Software voor de vaststelling van de uitslag en zetelverdeling. - Kandidaatstellingssoftware voor politieke partijen; - Kandidaatstellingssoftware voor het centraal stembureau.
Technische informatie testobject	Vervanging OSV is deels nog in ontwikkeling. Derhalve is nog niet alle technische informatie bekend, of kan deze informatie nog wijzigen. De onderstaande informatie is op het moment van schrijven bekend bij de Kiesraad.

	Code - de software is geschreven in Java; - de software wordt ofwel gehost, ofwel voorafgaand aan de test ter beschikking gesteld; - het betreft software die op Windows, MacOS en Linux distributies kan worden geïnstalleerd; - u vindt een indicatie van het aantal *lines of code* in Bijlage N. **Platform** Vervanging OSV maakt gebruik van diverse standaardsoftwarecomponenten. Op het moment van schrijven is de volgende informatie beschikbaar: - webserver/Applicatieserver (JEE/Thorntail); - databaseserver (standaard H2).
Tenminste te beantwoorden onderzoeksvragen	1. Welke kwetsbaarheden en risico's op het gebied van informatiebeveiliging zijn te onderkennen in het testobject? 2. Welke maatregelen kunnen worden getroffen om de geconstateerde risico's te mitigeren?
Buiten de reikwijdte	• Het uitvoeren van een Secure Code Review.
Omgeving	**Software ten behoeve van de kandidaatstelling voor politieke partijen en het centraal stembureau** Indien de software wordt gehost, dan wordt in een representatieve acceptatieomgeving getest. In voorkomende gevallen kan de Kiesraad u vragen om geïdentificeerde bevindingen met een risicoclassificatie 'kritiek' of 'hoog' te verifiëren in de productieomgeving. **Software ten behoeve van de vaststelling van de uitslag** U krijgt de software aangeleverd en voert de testen zodoende op eigen apparatuur uit.

Standaard pentest – Databank Verkiezingsuitslagen	
Beschrijving en doelstelling	Het uitvoeren van een pentest op de Databank Verkiezingsuitslagen webapplicatie inclusief de onderliggende internet-facing infrastructuur. De test bestaat ten minste uit geautomatiseerde kwetsbaarhedenscans en handmatige testactiviteiten. Bij een standaard pentest hoeft geen Secure Code Review uitgevoerd te worden. Een hertest, waarbij de bevindingen uit de initiële pentest opnieuw worden onderzocht, vindt plaats op basis van nacalculatie.
Reikwijdte	De onderstaande testobjecten vallen binnen de reikwijdte van deze Opdracht: - Databank Verkiezingsuitslagen webapplicatie (zie ook de website en beheermodule); - Onderliggende internet-facing infrastructuur.
Technische informatie testobject	Voor meer informatie over dit testobject kan de betreffende website en beheermodule worden benaderd.
Tenminste te beantwoorden onderzoeksvragen	1. Welke kwetsbaarheden en risico's op het gebied van informatiebeveiliging zijn te onderkennen in het testobject? 2. Welke maatregelen kunnen worden getroffen om de geconstateerde risico's te mitigeren?
Buiten de reikwijdte	• Het uitvoeren van een Secure Code Review.
Omgeving	Acceptatieomgeving

	In voorkomende gevallen kan de Kiesraad u vragen om geïdentificeerde bevindingen met een risicoclassificatie 'kritiek' of 'hoog' te verifiëren in de productieomgeving.

Standaard pentest – digitale hulpmiddelen	
Beschrijving en doelstelling	Het uitvoeren van een pentest op de digitale hulpmiddelen. De test bestaat ten minste uit geautomatiseerde kwetsbaarhedenscans en handmatige testactiviteiten. Bij een standaard pentest hoeft geen Secure Code Review uitgevoerd te worden. Een hertest, waarbij de bevindingen uit de initiële pentest opnieuw worden onderzocht, vindt plaats op basis van nacalculatie.
Reikwijdte	De onderstaande testobjecten vallen binnen de reikwijdte van deze Opdracht: - Nader te bepalen.
Technische informatie testobject	Nader te bepalen.
Tenminste te beantwoorden onderzoeksvragen	1. Welke kwetsbaarheden en risico's op het gebied van informatiebeveiliging zijn te onderkennen in het testobject? 2. Welke maatregelen kunnen worden getroffen om de geconstateerde risico's te mitigeren?
Buiten de reikwijdte	Nader te bepalen.
Omgeving	Nader te bepalen.

Bij ieder van de vier (4) bovengenoemde standaard pentesten zijn de volgende kenmerken minimaal van toepassing:

Kenmerken standaard pentesten	
Boxtype	**White-box pentest:** De tester krijgt volledige openheid over de werking van de applicatie, systemen, architectuur, infrastructuur en broncode.
Perspectief	**Geautoriseerd perspectief:** de tester ontvangt representatieve testaccounts om het onderzoeksobject tevens vanuit geautoriseerd perspectief te kunnen testen.
Richtlijnen en best practices	Bij de pentest worden minimaal de meest recente versies van de onderstaande richtlijnen en best practices gehanteerd (eventueel door u aan te vullen): - OWASP Top 10; - OWASP ASVS; - NCSC ICT-beveiligingsrichtlijnen voor webapplicaties; - NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). Indien één van deze vier richtlijnen vervalt of niet meer relevant is, dan treden Wederpartij en Opdrachtgever in onderling overleg over een vervangende richtlijn die minimaal gelijkwaardig is. Opdrachtgever heeft hierin het vetorecht.
Duur	1. De doorlooptijd van de standaard pentest is maximaal tien (10) Werkdagen. 2. Uiterlijk vijf (5) Werkdagen na beëindiging van de testwerkzaamheden dient het concept pentestrapport te worden opgeleverd aan de Kiesraad. 3. Uiterlijk tien (10) Werkdagen na ontvangst van het conceptrapport dient het definitieve rapport, inclusief eventuele opmerkingen van de Kiesraad en/of de leverancier van het product, te worden opgeleverd.

Resultaat	U levert een rapportage op, die ten minste de volgende onderdelen bevat:
	- Managementsamenvatting
	- Introductie, met:
	  o opdrachtbeschrijving;
	  o scopedefinitie;
	  o aanpak (methoden en technieken).
	- Bevindingen, met per bevinding:
	  o observatie;
	  o risico-inschatting;
	  o CVSS 3.1 score;
	  o onderbouwing;
	  o aanbeveling.
	- Risicomatrix en -correlatie
	- Algemene conclusies en aanbevelingen
	-
	Deze rapportage is te allen tijde uitstekend taalkundig opgebouwd en uitstekend leesbaar ivoor zowel technisch ICT-personeel (zoals ontwikkelaars) als voor het management.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Thu, 13 Jul 2023 16:14:45 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: RE: Kick-off Pentest OSV2020

Hi 5.1.2.e

De VOG's zal ik voor de kick-off proberen aan te leveren. Degene die ik nu heb zijn net verlopen en ik had heel toevallig afgelopen maandag nieuwe aangevraagd.

20 juli om 13.00 uur is goed, ik zal je een agenda uitnodiging met URL van de vergaderkamer.

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Thursday, 13 July 2023 15:21
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: RE: Kick-off Pentest OSV2020

Dag 5.1.2.e

Dank voor je mail. Ik zie uit naar de samenwerking met HackDefense!

Belangrijke voorwaarde voor mij voor de kick-off is wel dat alle relevante VOG's met ons gedeeld zijn.

Mogelijkheden voor mij:
20 juli 13.00 – 15.00
21 juli 09.00 – 16.00

Vanaf de 24ste heb ik verlof. Ben ik wel beschikbaar voor noodgevallen, maar niet voor de kick off.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
W www.kiesraad.nl

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: donderdag 13 juli 2023 15:14
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Kick-off Pentest OSV2020

Beste 5.1.2.e

Met veel plezier gaan wij de pentest voor jullie uitvoeren. Graag vooraf een kick-off met alle belanghebbenden. Wanneer zou dit voor jullie schikken? Liefst zo snel mogelijk om alles op tijd in orde te krijgen, ik begrijp dat de test op 24 juli van start moet gaan.

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Fri, 14 Jul 2023 10:43:00 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Re: Code review module U

Hallo 5.1.2.e je bedoelt dat de code review dan afgerond moet zijn op 14 september?

Dat is haalbaar hoor, geen probleem.

5.1.2.e

On 14/07/2023 10:36, 5.1.2.e wrote:

> 5.1.2.e
>
> Wij hebben het gisteren even kort gehad over code review. Voor de PP module gaat dat niet meer lukken, gezien de tijd. Voor de module U zien wij dit echter wel als een belangrijk onderdeel wat wij getest zouden willen hebben. Ik had geloof ik al de voorlopige planning voor de pentest van U gedeeld. Daarin staat ook de uiterste opleverdatum voor module U (14 september uit mijn hoofd).
>
> **Is het mogelijk voor Hack Defense om een code review op module U uit te voeren als wij de broncode aanleveren op 21 juli**?
>
> Hier ontvangen jullie dan uiteraard een separate opdrachtsbevestiging en vergoeding voor. Het gaat mij nu vooral even om de haalbaarheid.
>
> Ik hoor het graag!
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo
> .....
> **KIES**RAAD
> Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
> Postadres: Postbus 20011, 2500 EA Den Haag
> .....
> T 5.1.2.e
> W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e "
Sent: Mon, 17 Jul 2023 11:17:41 +0200
To: "5.1.2.e " <5.1.2.e @hackdefense.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: RE: Offerte code review

Goedemorgen,

Het verkiezingsproces is niet fundamenteel anders dan 3 jaar geleden.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: maandag 17 juli 2023 11:02
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: Offerte code review

Ja duidelijk, maar niet hele nieuwe functies die zijn toegevoegd bedoel ik, of hele significante aanpassingen in het proces.

5.1.2.e

On 17/07/2023 10:59, 5.1.2.e wrote:

> 5.1.2.e
>
> Dat weet ik niet. Er zal wel het een en ander gewijzigd zijn ivm wetgeving. Maar in de basis is de software hetzelfde naar ik aanneem.
>
> Groet,
>
> 5.1.2.e
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Verzonden:** maandag 17 juli 2023 10:59
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Onderwerp:** Re: Offerte code review
>
> Is er t.o.v. 3 jaar geleden veel veranderd aan OSV2020-U?
>
> Zo nee, dan heb ik voldoende info.

5.1.2.e

On 17/07/2023 09:26, 5.1.2.e wrote:

> 5.1.2.e
>
> Zou jij een offerte willen opstellen voor de code review van de module U?
>
> Welke aanvullende informatie heb je daarvoor nodig van mij? Dan zorg ik dat je die krijgt.
>
> Met vriendelijke groet,

5.1.2.e

5.1.2.e

Aanwezig: ma t/m vrij, afwezig wo

.....

KIESRAAD

Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag

Postadres: Postbus 20011, 2500 EA Den Haag

.....

T 5.1.2.e

W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Tue, 18 Jul 2023 09:31:12 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Re: FW: Wijzigingen OSV2020-U

Dank! Als ik dat zo snel lees zal er in OSV2020-U misschien een functie zijn om de nieuwe (optionele) manier van stemmentellen te ondersteunen (optie 2). We zullen daar wat ruimte voor meenemen. Maar het ziet er niet radicaal anders uit.

5.1.2.e

On 17/07/2023 12:15, 5.1.2.e wrote:

> 5.1.2.e
>
> Zie onderstaande uitleg over de voornaamste wijziging mbt de offerte voor de code review.
>
> De grootste wijziging in de laatste 3 jaar in module Uitslagvaststelling van OSV2020 is de NPVV.
> Op 1 januari 2023 is de Wet nieuwe procedure vaststelling verkiezingsuitslagen (NPVV) in werking getreden, waarmee de Kieswet op het punt van de uitslagvaststelling ingrijpend is gewijzigd. Doel van deze wet is het creëren van mogelijkheden om tijdig, voor de vaststelling van de uitslag van een verkiezing, eventuele (tel)fouten te constateren en op een transparante en controleerbare manier te corrigeren. Dit verkleint de kans dat er op het laatste moment nog tot een hertelling moet worden besloten of dat er een uitslag wordt vastgesteld die fouten bevat.
>
> https://open.overheid.nl/documenten/ronl-5fa5d54ceb8d6144d5bea65e4c9f264474bc4edb/pdf.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo
> .....
> **KIES**RAAD
> Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
> Postadres: Postbus 20011, 2500 EA Den Haag
> .....
> T 5.1.2.e
> W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Tue, 18 Jul 2023 11:35:03 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "'5.1.2.e '" <5.1.2.e @hackdefense.nl>
Subject: RE: Reminder: VOG's

Goedemorgen 5.1.2.e

De VOG's zijn aangevraagd, PostNL moet zijn werk doen om deze op tijd in de brievenbus te deponeren.
Ik heb wel de VOG's die ik vorig jaar heb aangevraagd alvast voor je, deze zijn resp. in mei en juni uitgegeven.

Zodra de nieuwe binnengekomen zijn, mail ik je die ook nog.

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Tuesday, 18 July 2023 11:29
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Reminder: VOG's

Goedemorgen,

Ik stuur even een reminder dat de VOG's nog niet binnen zijn. Deze hebben wij uiterlijk vrijdag nodig ivm de test voor PP van volgende week.

Jullie mogen een scan sturen per email of per secure transfer van ODC:

ODCN Secure Transfer (rijkscloud.nl)

Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Tue, 18 Jul 2023 12:02:49 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: RE: Reminder: VOG's

HI 5.1.2.e

Dit zijn alle relevante VOG's, alleen 5.1.2.e en 5.1.2.e zullen bij jullie testen. Omdat deze iets ouder zijn dan 1 jaar, zijn er nieuwe aangevraagd.

Met vriendelijke groet / with kind regards,

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Tuesday, 18 July 2023 11:37
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; '5.1.2.e ' <5.1.2.e @hackdefense.nl>
Onderwerp: RE: Reminder: VOG's

Dag 5.1.2.e

Dankjewel voor het doorsturen. Hopelijk lukt het nog de rest ook op tijd binnen te krijgen!

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 18 juli 2023 11:35
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; '5.1.2.e ' <5.1.2.e @hackdefense.nl>
Onderwerp: RE: Reminder: VOG's

Goedemorgen 5.1.2.e

De VOG's zijn aangevraagd, PostNL moet zijn werk doen om deze op tijd in de brievenbus te deponeren.
Ik heb wel de VOG's die ik vorig jaar heb aangevraagd alvast voor je, deze zijn resp. in mei en juni uitgegeven.

Zodra de nieuwe binnengekomen zijn, mail ik je die ook nog.

Met vriendelijke groet / with kind regards,

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Tuesday, 18 July 2023 11:29

Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Reminder: VOG's

Goedemorgen,

Ik stuur even een reminder dat de VOG's nog niet binnen zijn. Deze hebben wij uiterlijk vrijdag nodig ivm de test voor PP van volgende week.

Jullie mogen een scan sturen per email of per secure transfer van ODC:

ODCN Secure Transfer (rijkscloud.nl)

Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Thu, 20 Jul 2023 12:33:38 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e @hackdefense.nl" <5.1.2.e @hackdefense.nl>
Subject: VOG 5.1.2.e

Hoi 5.1.2.e goedemiddag,

PostNL zegt vandaag bij 5.1.2.e een VOG te bezorgen, maar omdat hij vandaag op kantoor is, kan deze niet direct naar jullie worden gestuurd.
Hij zal er voor zorgen dat deze direct na ontvangst bij jullie aangeboden wordt!

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

HackDefense
IT security, maar dan begrijpelijk

HackDefense BV
Postbus 3025, 2301 DA Leiden
(071) 204 0101
info@hackdefense.nl
https://hackdefense.nl/

IBAN: NL40 RABO 0337 2727 00
KvK: 69477043
BTW: NL857887270B01

INTAKE-FORMULIER PENTEST
TESTPLAN

Projectnaam		Pentest OSV2020 PP TK 2023
Opdrachtgever	*Naam rechtspersoon*	De Kiesraad
	KvK-nummer	50200097
	Naam tekenbevoegde	5.1.2.e
	Factuurinstructie	Op de opdrachtbevestiging
Projectnummer		PR23057
Kenmerk raamovereenkomst		201850004.213.001
Projecttaal (Nederlands of Engels)		Nederlands
Primaire contactpersoon (*trusted contact*)	*Naam*	5.1.2.e
	E-mail	5.1.2.e @kiesraad.nl
	Telefoon	5.1.2.e
Technisch contactpersoon *(optioneel)*	*Naam*	5.1.2.e
	E-mail	5.1.2.e @kiesraad.nl
	Telefoon	5.1.2.e
Projectleider HackDefense	*Naam*	5.1.2.e
	E-mail	5.1.2.e @hackdefense.nl
	Telefoon	5.1.2.e
Testtype (black/grey/white box)		White box
Testonderdelen		Webapplicatietest

Rapportage	*Startdatum*	Woensdag - 26/07/2023
	Einddatum	Maandag - 31/07/2023
	Taal (Nederlands of Engels)	Nederlands, technische bevindingen in het Engels.

Webapplicatietest

Benodigdheden:

1. Installatie software/documenten voor de applicaties in Windows, Linux en MacOS.
2. Testdata
3. (Installatie)handleidingen.

Kaders & Vereisten:

- De test wordt uitgevoerd conform de minimale vereisten uit het kaderdocument van de Kiesraad.

Planning & locatie:

- De webapplicatietest wordt uitgevoerd bij HackDefense in Leiderdorp op maandag 24 juli 2023 t/m vrijdag 28 juli 2023.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Thu, 20 Jul 2023 15:29:15 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e @hackdefense.nl" <5.1.2.e @hackdefense.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: Module PP

Ha 5.1.2.e offerte komt er zo aan!

On 20/07/2023 15:27, 5.1.2.e wrote:

> Goedemiddag,
>
> Ik heb met akkoord van onze directeur alvast de software verzonden voor de pentest PP. Ik heb de offerte nodig voor de code review om daar de source code van te mogen sturen.
>
> **Hou er rekening mee dat ik na morgen twee weken met vakantie ben en het dan dus niet kan regelen wat betreft opdrachtbrief etc.**
>
> Ik heb de software voor PP alleen naar 5.1.2.e gestuurd, omdat ik daar een telefoonnummer voor nodig heb en die van 5.1.2.e heb ik niet, vandaar. Als jullie het via het eigen netwerk intern met elkaar kunnen delen, graag.
>
> Kijk bij voorkeur voor maandag alvast of installeren lukt ivm mijn afwezigheid volgende week.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo
> .....
> **KIES**RAAD
> Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
> Postadres: Postbus 20011, 2500 EA Den Haag
> .....
> T 5.1.2.e
> W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Thu, 20 Jul 2023 16:37:31 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: RE: Intakeformulier pentest OSV2020 PP TK 2023

Hi 5.1.2.e

Super, bedankt voor het controleren!

From: 5.1.2.e <5.1.2.e @kiesraad.nl>
Sent: 5.1.2.e 20, 2023 4:36 PM
To: 5.1.2.e <5.1.2.e @hackdefense.nl>
Subject: RE: Intakeformulier pentest OSV2020 PP TK 2023

5.1.2.e

Ik heb naar het intakeformulier gekeken. Geen opmerkingen wat mij betreft, anders dan dat de Kiesraad formeel geen rechtspersoon is. Maar daar vloeit geen bloed uit denk ik.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
W www.kiesraad.nl

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: donderdag 20 juli 2023 15:29
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Intakeformulier pentest OSV2020 PP TK 2023

Hi 5.1.2.e

Zoals besproken staat ons intakeformulier in de bijlage. Zou jij deze controleren/verbeteren en terug kunnen sturen?

Ik zie in het kader document ook nog een ander e-mailadres staan dan 5.1.2.e @kiesraad.nl, namelijk 5.1.2.e @kiesraad.nl. Via welk e-mailadres heb jij liever contact?

Met vriendelijke groet / With kind regards,

HackDefense

5.1.2.e
5.1.2.e

M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

HackDefense

Voorstel

Pentest OSV2020-U

Kiesraad

O23077

versie 2.0 - definitief

20 juli 2023

Copyright © 2023 HackDefense BV

Alle rechten voorbehouden. We verzoeken u om dit document vertrouwelijk te behandelen en niet te delen buiten uw organisatie.

HackDefense BV

Postbus 3025
2301 DA Leiden

(071) 204 0101

`https://hackdefense.nl/`

Offerte

Projectnaam	Pentest OSV2020-U
Opdrachtgever	5.1.2.e
KvK-nummer	50200097
Offertenummer	O23077

Documentgeschiedenis

Versie	*Datum*	*Auteur*	*Omschrijving*
1.0	20 juli 2023	5.1.2.e 5.1.2.e	eerste concept
2.0	20 juli 2023	5.1.2.e	wijzigingen na interne review

Managementsamenvatting

Binnen het kader van de raamovereenkomst voor pentesten heeft de Kiesraad aan HackDefense gevraagd om een voorstel te doen voor het testen op *security vulnerabilities* van OSV2020-U, en het adviseren van mitigerende maatregelen daaromtrent.

In dit document vindt u de aanpak, rapportage, en planning die HackDefense voorstelt voor het uitvoeren van deze test.

Het project zal resulteren in een gedegen rapport. Het rapport geeft onze bevindingen en aanbevelingen in technisch detail, en een managementsamenvatting voor de niet technisch onderlegde lezer.

Kosten voor het onderzoek en rapportage bedragen **€** 5.1.2.f (exclusief BTW).

Keurmerk Pentesting

HackDefense is gecertificeerd onder het ”Keurmerk Pentesten”, de Nederlandse pentest-standaard. Dit merk wordt onafhankelijk beheerd door het CCV (Centrum voor Criminaliteitspreventie en Veiligheid). We voeren het keurmerk in al onze beveiligingstestrapporten. Jaarlijks wordt onze kwaliteit door KIWA getoetst aan het keurmerk.

Meer informatie over dit keurmerk vindt u op `https://hetccv.nl/keurmerken/expert/keurmerk-pentesten/`.

Inhoudsopgave

Hoofdstuk 1

Uw vraag

1.1 Achtergrond

1.1.1 Organisatie

De Kiesraad treedt bij verschillende verkiezingen op als centraal stembureau. Verder is de Raad adviesorgaan en informatiecentrum op het gebied van kiesrecht en verkiezingen. Het belang van ICT-beveiliging is evident: de integriteit van het verkiezingsproces is van vitaal belang voor de Nederlandse democratie.

1.1.2 Testobject

OSV2020 is de naam voor een aantal applicaties die worden gebruikt in het verkiezingsproces. Vanzelfsprekend is de veiligheid van deze applicaties van groot belang.

OSV2020-U is de deelapplicatie die zal worden gebruikt om uitslagen en zetelverdelingen vast te stellen. OSV2020-U wordt door de Kiesraad ter beschikking gesteld aan (centraal) stembureaus in gemeenten en kieskringen.

Deze applicatie is gebouwd als webapplicatie in Java, waarbij de gebruikende organisatie (veelal gemeenten) de software installeren op een computer die los staat van het netwerk.

Het installatieprogramma zet een lokale webserver op deze computer, en een Java *runtime*. Daarin draait de applicatie. Uitvoer wordt fysiek overgebracht naar het centraal stembureau.

Genoemd installatieprogramma is nadrukkelijk ook in scope van het onderzoek. OSV2020-U wordt geleverd voor Windows, Mac OS en Linux, waarbij het onderzoek zich dient te richten op de Windows-variant. De installieprogramma's en -procedures voor Mac OS en Linux worden echter ook meegenomen.

In 2020 heeft HackDefense ook een test op OSV2020-U uitgevoerd. Nieuw is nu dat er een tweede, optionele wijze van vaststellen van de uitslag bij is gekomen (de "nieuwe procedure vaststelling verkiezingsuitslagen" ofwel NPVV), waarbij gemeenten ook de keuze hebben om voorkeurstemmen op een later moment te tellen.

1.1.3 Aanleiding testvraag

De Kiesraad wil graag inzicht hebben in de vraag of de integriteit en vertrouwelijkheid van OSV2020-U voldoende gewaarborgd is. Een pentest is daarbij een belangrijk middel.

1.2 Scope

In scope is de applicatie OSV2020-U zoals de Kiesraad deze voor aanvang aan HackDefense zal aanleveren, inclusief installatieprogramma. We installeren de applicatie in onze eigen lab-omgeving.

Ook de broncode is onderdeel van de scope. Deze zal t.z.t. (voor aanvang) worden aangeleverd, exact overeenkomend met de *live* versie van de applicatie die we testen.

1.2.1 Aanvalsperspectief

De beveiliging moet getest worden vanuit de volgende perspectieven:

1. perspectief van de *outsider*, d.w.z. zonder login-gegevens
2. perspectief van de kwaadwillende *insider* met login-gegevens (of kwaadwillende outsider die login-gegevens heeft weten te verkrijgen)

1.2.2 Testvorm

De beoogde testvorm is *white box*, dat wil zeggen dat alle informatie voor de testers beschikbaar is.

Code review is ook onderdeel van de test.

Social engineering of *Denial-of-Service attacks* (DoS of DDoS) zijn niet aan de orde en moeten op geen enkele wijze worden uitgevoerd.

Een hertest maakt geen deel uit van de opdracht. Deze is, als dit nodig of wenselijk blijkt te zijn, uiteraard wel als meerwerk uit te voeren.

1.3 Onderzoeksvraag

De in dit onderzoek te beantwoorden onderzoeksvraag luidt als volgt:

Kunnen – binnen het overeengekomen tijdsbestek – kwetsbaarheden worden gevonden in de beveiliging van OSV2020-U, waardoor ongeautoriseerden toegang tot OSV2020-U of de daarin verwerkte data zouden kunnen verkrijgen?

Beveiligingsissues die niet direct tot ongeautoriseerde toegang leiden maar die wel zouden kunnen helpen bij een inbraak, m.a.w. waarvan de oplossing tot een robuustere beveiliging leiden, moeten uiteraard ook worden gerapporteerd.

1.4 Overige randvoorwaarden

- Het rapport wordt in het Nederlands opgeleverd, met uitzondering van de individuele technische bevindingen; deze zullen in het Engels worden geschreven.
- Het onderzoek wordt uitgevoerd onder de voorwaarden van de raamovereenkomst met contractnummer 201865007.433 - P1 - HackDefense BV.

Hoofdstuk 2

Ons voorstel

Dit hoofdstuk geeft aan hoe wij voorstellen om de onderzoeksvraag te beantwoorden.

2.1 Team

Al onze pentesters zijn hbo- of wo-opgeleid en hebben tenminste het OSCP- en eWPT-certificaat.

Een van onze gecertificeerde Ethical Hackers voert de test uit. Al het werk wordt diepgaand gereviewed door onze Principal Consultant voor we u ons conceptrapport sturen.

2.2 Aanpak

We beginnen het project met een kick-off (via videoconferencing). Daarbij spreken we de praktische zaken af, zoals het vaststellen van het ”trusted contact” (welke contactpersoon is primair), een eventuele communicatiesleutel, en het aanleveren van de applicatie en broncode.

Het testobject is een webapplicatie gebouwd op een web-, applicatie- en databaseserver. Het gehele samenstel van server en applicatie, waaronder configuratie en broncode, zijn onderdeel van het onderzoek.

Ook het installatieprogramma is onderwerp van het onderzoek.

Wij voeren dit onderzoek uit met drie ervaren onderzoekers (allemaal met hbo-/wo-diploma Informatica en relevant certificaat als pentester). De code- en configuratiereview zien we niet los van de pentest van de applicatie. Deze beide onderzoeken versterken elkaar. De onderzoekers leggen wel elk hun focus bij een onderdeel: de ene onderzoeker installeert de applicatie in de lab-omgeving, en leert zo de configuratie kennen. Deze zal zich ook verdiepen in de code. De andere onderzoeker onderwerpt de draaiende applicatie aan een grondige webapplicatie-pentest (inclusief eventuele andere services die de software aan het netwerk blootstelt). De derde onderzoeker neemt de review-rol: hij kijkt regelmatig mee, stelt kritische vragen, en fungeert als klankbord.

In de eerste fase gaan de onderzoekers de applicatie in detail leren kennen. Ze nemen de documentatie door, uiteraard, en starten daarna de test. Onderzoeker 1 benadert de applicatie in de testopstelling, via een intercepting proxy (BurpSuite Pro). Onderzoeker 2 gaat de code en configuraties reviewen. De onderzoekers zitten samen in één ruimte en leren in samenspraak de applicatie en de werking volledig begrijpen. Dit gaat beter dan wanneer dit los van elkaar gebeurt: begrip van de code en begrip van de werking van de applicatie als gebruiker versterken elkaar.

Nadat we op basis van ons begrip van de applicatie onze bevindingen hebben gedaan zullen we de normenkaders (OWASP Top 10 en NCSC-richtlijnen webapplicaties) erbij nemen en nagaan of daar nog controls in staan waar we wellicht nog zinvol aanvullend op kunnen checken. Als daar nog bevindingen uitkomen worden deze meegenomen. Alle controls die we checken worden in het rapport gedocumenteerd, ook als er geen bevindingen uit voortkomen.

Code review

Vanuit onze ervaring als security testers kijken we de code na op veel voorkomende security bugs in Java. Met name deserialization-aanvallen zijn hierbij interessant, maar alle mogelijke vormen van injectie worden onder de loep genomen. Het belangrijkste daarbij is dat de onderzoeker de code begrijpt, ziet wat deze doet, en daar eventuele foutjes uithaalt, in samenspraak met de onderzoeker die de applicatie test. De output van tools voor statische code-analyse kunnen daarbij een startpunt zijn.

De basisbenadering van code reviewing is dat de onderzoeker de plaatsen in de code vindt waar invoer van buiten de applicatie binnenkomt, en deze stapsgewijs door de programmacode volgt. Kennis van en ervaring met securitylekken zorgt er vervolgens voor dat de reviewer ziet waar het eventueel kan misgaan. De onderzoeker die de applicatie live test kan het op deze manier gevonden issue wellicht in de draaiende applicatie verifiëren. Maar er zijn ook issues die zich niet direct openbaren in de draaiende applicatie, maar die mogelijk later een risico zouden kunnen gaan vormen. Daarom rapporteren we ook niet-exploiteerbare, alleen potentiële, issues in de broncode.

2.2.1 Tooling

In het algemeen geldt voor de onderzoeken en tests van HackDefense dat uitvoer van tooling voor ons niet leidend is. Tooling is een hulpmiddel, het is het gereedschap van de vakman. Conclusies worden getrokken door de vakmensen zelf, voor wie een goed begrip van de werking van het te testen object het belangrijkste element van een beveiligingstoets is.

De uitvoer van de tooling wordt daarom altijd handmatig geverifieerd. Ook worden tests die niet geautomatiseerd uitvoerbaar zijn met de hand uitgevoerd. Daarbij telt onze jarenlange kennis en ervaring in computer- en netwerkbeveiliging en ons begrip van de context van de applicatie.

De tools die zullen worden gebruikt zijn in elk geval *Nmap*, *Nessus*, *Nikto* en *BurpSuite Pro*, aangevuld met specifieke tooling zoals *SQLMap* waar dit nodig blijkt.

2.2.2 Projectfasering

Elke beveiligingstest van HackDefense bestaat uit de volgende fasen:

- *Planning*

  Na akkoord op het voorstel plannen we in overleg de beveiligingstest in. Afhankelijk van de omvang van de opdracht kan de uitvoering snel starten, vaak al binnen twee weken.

- *Kick-off*

  Voor aanvang van de test houden we een kickoff-bijeenkomst. Bij deze kickoff wordt met de security officer en andere betrokken stakeholders nagegaan of alle benodigdheden voor de test aanwezig zijn: alle contactgegevens[1], adressen/URL's, toegang tot locaties, etc. Doel is dat alles klaar is om de uitvoer te kunnen starten.

- *Uitvoering test*

  In de afgesproken periode voeren we de test uit zoals afgesproken in dit voorstel. Tijdens de test worden belangrijke bevindingen met de Kiesraad gedeeld zodat waar nodig direct actie kan worden ondernomen.

- *Rapportagefase*

  Na afloop van de test schrijven we ons rapport in concept. Het eerste concept wordt intern gereviewed door een Principal Consultant. Het definitieve conceptrapport bieden we aan de Kiesraad aan voor review.

- *Rapportbespreking en definitieve oplevering*

  We bespreken het rapport en op basis van de feedback vanuit de Kiesraad maken we het rapport definitief.

- *Evaluatie*

  Na oplevering van het definitieve rapport vragen we u om ons te beoordelen met een cijfer tussen 0 en 10. Waar nodig bespreken we na wat er goed ging en waar er eventueel verbeterpunten liggen, zodat we de volgende test nog beter kunnen uitvoeren.

2.2.3 Rapportage

Het rapport geeft in de eerste plaats antwoord op de onderzoeksvraag en bestaat uit de volgende hoofdstukken:

- *Managementsamenvatting* – samenvatting in twee of drie alinea's zonder technische terminologie.
- *Uw vraag* – weergave van de onderzoeksvraag en de scope; dit hoofdstuk omschrijft wat er precies is getest.
- *Onze bevindingen* – verslag van de werkzaamheden: de aanpak, en onze analyse.

[1] we vinden het heel belangrijk dat de penetratietesters en beheerders van elkaars directe telefoonnummers op de hoogte zijn om snel te kunnen schakelen indien nodig

- *Conclusies en aanbevelingen* – het antwoord op de onderzoeksvraag, en een solide advies voor de weg voorwaarts.
- *Bijlage: technische bevindingen* – alle individuele bevindingen, in technisch detail, bestaand uit de onderdelen:
  - *Omschrijving* - korte samenvatting van het issue
  - *Risico-inschatting* - een inschatting van het risico op basis van kans (hoe moeilijk is dit issue te misbruiken) en impact (wat kan een aanvaller doen), inclusief de CVSS-score [2]
  - *Betreft de systemen* of *Betreft de pagina's* - concrete opsomming van IP-adressen, systeemnamen of componenten van een applicatie waarop het omschreven issue van toepassing is
  - *Waarneming* - precieze waarneming, wat hebben we gezien en hoe is dit reproduceerbaar. Waar mogelijk met technische commando's en/of screenshots.
  - *Aanbeveling* - zo exact mogelijk technisch advies hoe dit issue op te lossen is

Als er vragen zijn bij lezing van het rapport of concrete technische hulp nodig is bij het implementeren van onze aanbevelingen dan verlenen we deze hulp - binnen de grenzen van het redelijke - kostenloos.

Naast individuele bevindingen geeft het rapport inzicht in de algemene situatie van de beveiliging van het onderzoeksobject. Daartoe geeft het een heldere samenvatting van hetgeen geconstateerd is, en hoe zich dat verhoudt tot het te verwachten beveiligingsniveau in vergelijkbare toepassingen.

Het rapport wordt u eerst in concept aangeboden. Op basis van uw reactie worden eventueel aanpassingen gedaan. In het (zeldzame) geval dat we uw feedback niet in ons rapport kunnen overnemen zullen we uw reactie als zodanig letterlijk vermelden in het definitieve rapport.

Ernstige bevindingen worden uiteraard direct gemeld en niet pas bij de rapportage. Ook ontvangt u aan het eind van elke testdag een korte samenvatting.

2.3 Planning

We denken de volgende hoeveelheid inzet nodig te hebben:

[2] `https://first.org/cvss/`

testsoort	*uren inzet*
voorbereiden white box, document review	8
installatie testobject in lab-omgeving	8
webapplicatietest	64
code review	64
configuratie-review	16
extra: NPVV	8
totaal tests	168
rapportage	40
QA/review	4
projectmanagement	4
totaal project	216

2.4 Kosten

In de vorige paragraaf heeft u gelezen dat we 216 uur (27 mensdagen) benodigde inzet verwachten.

Het binnen de raamovereenkomst afgesproken dagtarief is € 5.1.2.f Totale kosten komen daardoor uit op **€** 5.1.2.f

(alle bedragen zijn exclusief BTW)

Binnen redelijke grenzen vallen alle uit te voeren werkzaamheden binnen deze vaste prijs; voor onderling schriftelijk nader overeengekomen meerwerk rekenen wij het genoemde tarief.

2.5 Overig

Deze opdracht zal worden uitgevoerd conform de in 2020 gesloten raamovereenkomst voor pentesting (kenmerk 201865007.433 - P1 - HackDefense BV).

Hoofdstuk 3

Tot slot

We zien ernaar uit u bij deze belangrijke opdracht te kunnen ondersteunen. Heeft u nog vragen of opmerkingen, aarzel niet om te bellen met 5.1.2.e of 5.1.2.e bereikbaar via (071) 204 0101.

Als u akkoord bent met dit voorstel verzoek ik u om een getekend exemplaar te retourneren.

Voor akkoord:

Naam:	_____
Functie:	_____
Datum:	_____
Namens:	Kiesraad *KvK-nummer 50200097*
Offertenummer:	O23077 v2.0
Handtekening:	_____

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Fri, 21 Jul 2023 09:21:55 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: offerte pentest en code review OSV2020-U

O sorry, ik had begrepen dat 14 september het concept er moest zijn, maar dat is dus 4 september.

Dan ga ik nog even schuiven & puzzelen met de planning. Moet ik denk ik even met een andere klant overleggen.

Pentest en code review doen we sowieso tegelijkertijd, met je eens dat het onnodig complex wordt om die uit elkaar te trekken. Werkt ook beter om dat samen te doen.

5.1.2.e

On 20/07/2023 17:00, 5.1.2.e wrote:

> 5.1.2.e
>
> Dank voor je toelichting.
>
> @5.1.2.e jij bent morgen (vrijdag) vrij en ik ben vanaf maandag met vakantie. Zou jij hier naar willen kijken en met bedrijfsvoering een opdrachtbrief willen maken in mijn afwezigheid?
>
> @5.1.2.e Akkoord wat betreft OWASP Top 10.
> Wat betreft de planning hadden we het telefonisch erover dat de pentest en code review gelijk zouden lopen voor module U. In dat geval zou de testperiode zijn van 29-08 tot en met 04-09 (zie planning hieronder):
> Dat heeft mijn voorkeur, omdat ik anders met drie verschillende planningen moet werken (PP, U pentest en U code review).

Actie	Start	Afgerond
Eerste concept kaderdocument	07-08	18-08
Afstemmen intern en met Hack Defense	18-08	22-08
Finale versie kaderdocument	23-08	28-08
Oplevering versie 2 Module U door Elect	28-08	-
Pentest	29-08	04-09
Eerste concept rapportage pentest	04-09	07-09
Review	08-09	11-09
Finale versie rapport pentest	11-09	14-09

Oplossen issues door Elect	14-09	18-09
Laatste versie module U	18-09	-
Openbaar maken source code en pentest en code review	18-09	30-09

Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
W www.kiesraad.nl

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: donderdag 20 juli 2023 16:54
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: offerte pentest en code review OSV2020-U

Goedemiddag 5.1.2.e

Hierbij onze offerte voor pentest en code review van OSV2020-U.

Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.

Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:

- we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
- we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)

Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).

Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.

Dank! En fijne vakantie,

5.1.2.e

5.1.2.e

5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Fri, 21 Jul 2023 09:25:43 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: offerte pentest en code review OSV2020-U

Ha 5.1.2.e

Snap ik. Teksten in de offerte zijn ongeveer hetzelfde als in het plan van aanpak in de aanbesteding uit 2020, bijgewerkt met dingen die we toen nog niet wisten.

Geen probleem om de aanpak een stuk globaler te maken en in plaats daarvan naar het nog te maken kaderdocument te verwijzen - maar dan moet ik wel een voorbehoud maken op de ureninschatting, want als in het kaderdocument significant nieuwe dingen komen dan verandert ook de uren- en daarmee de kostenschatting. Op zich geen probleem want de raamovereenkomst voorziet ook wel in een stuk flexibiliteit, dus daar zit ik niet mee.

Ik zal e.e.a. aanpassen. Momentje.

5.1.2.e

On 20/07/2023 17:11, 5.1.2.e wrote:

> Goedemiddag,
>
> Ik heb nu ook inhoudelijk even snel door de offerte gekeken. Ik zou graag nog willen laten toevoegen dat het kaderdocument (hier komt een apart document voor) leidend zal zijn. Het is wat lastig dat deze voor een deel gaat overlappen met wat al in de offerte staat. Deze offerte is al een driekwart plan van aanpak eigenlijk 😊.
>
> Dat kan handig zijn, maar ik ben gewend dat aan onze kant te regelen (zoals je hebt gezien met de pentest voor PP).
>
> Dingen die hier genoemd zijn, zijn wat mij betreft inhoudelijk nog niet compleet. Maar het kaderdocument volgt conform de planning die ik net stuurde half augustus en is in samenspraak met jullie. Dus mijn voorstel is een offerte op te stellen met het aantal uren en eventueel een globalere plan van aanpak.
>
> Dingen die ik graag in samenspraak in het kaderdocument zet en niet in deze offerte, zijn dingen als de scope, onderzoeksvraag, opbouw van de rapportage en overige randvoorwaarden.
>
> Groet,
>
> 5.1.2.e
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Verzonden:** donderdag 20 juli 2023 16:54
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Onderwerp:** offerte pentest en code review OSV2020-U
>
> Goedemiddag 5.1.2.e

Hierbij onze offerte voor pentest en code review van OSV2020-U.

Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.

Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:

- we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
- we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)

Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).

Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.

Dank! En fijne vakantie,

5.1.2.e

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

HackDefense

Voorstel

Pentest OSV2020-U

Kiesraad

O23077

versie 3.0 - definitief

21 juli 2023

Copyright © 2023 HackDefense BV

Alle rechten voorbehouden. We verzoeken u om dit document vertrouwelijk te behandelen en niet te delen buiten uw organisatie.

HackDefense BV

Postbus 3025
2301 DA Leiden

(071) 204 0101

`https://hackdefense.nl/`

Offerte

Projectnaam	Pentest OSV2020-U
Opdrachtgever	5.1.2.e
KvK-nummer	50200097
Offertenummer	O23077

Documentgeschiedenis

Versie	*Datum*	*Auteur*	*Omschrijving*
1.0	20 juli 2023	5.1.2.e 5.1.2.e	eerste concept
2.0	20 juli 2023	5.1.2.e	wijzigingen na interne review
3.0	21 juli 2023	5.1.2.e	wijzigingen na review opdrachtgever

Managementsamenvatting

Binnen het kader van de raamovereenkomst voor pentesten heeft de Kiesraad aan HackDefense gevraagd om een voorstel te doen voor het testen op *security vulnerabilities* van OSV2020-U, en het adviseren van mitigerende maatregelen daaromtrent.

In dit document vindt u de aanpak, rapportage, en planning die HackDefense voorstelt voor het uitvoeren van deze test.

Het project zal resulteren in een gedegen rapport. Het rapport geeft onze bevindingen en aanbevelingen in technisch detail, en een managementsamenvatting voor de niet technisch onderlegde lezer.

Kosten voor het onderzoek en rapportage bedragen **€** 5.1.2.f (exclusief BTW).

Keurmerk Pentesting

HackDefense is gecertificeerd onder het ”Keurmerk Pentesten”, de Nederlandse pentest-standaard. Dit merk wordt onafhankelijk beheerd door het CCV (Centrum voor Criminaliteitspreventie en Veiligheid). We voeren het keurmerk in al onze beveiligingstestrapporten. Jaarlijks wordt onze kwaliteit door KIWA getoetst aan het keurmerk.

Meer informatie over dit keurmerk vindt u op `https://hetccv.nl/keurmerken/expert/keurmerk-pentesten/`.

Inhoudsopgave

Hoofdstuk 1

Uw vraag

1.1 Achtergrond

1.1.1 Organisatie

De Kiesraad treedt bij verschillende verkiezingen op als centraal stembureau. Verder is de Raad adviesorgaan en informatiecentrum op het gebied van kiesrecht en verkiezingen. Het belang van ICT-beveiliging is evident: de integriteit van het verkiezingsproces is van vitaal belang voor de Nederlandse democratie.

1.1.2 Testobject

OSV2020 is de naam voor een aantal applicaties die worden gebruikt in het verkiezingsproces. Vanzelfsprekend is de veiligheid van deze applicaties van groot belang.

OSV2020-U is de deelapplicatie die zal worden gebruikt om uitslagen en zetelverdelingen vast te stellen. OSV2020-U wordt door de Kiesraad ter beschikking gesteld aan (centraal) stembureaus in gemeenten en kieskringen.

Deze applicatie is gebouwd als webapplicatie in Java, waarbij de gebruikende organisatie (veelal gemeenten) de software installeren op een computer die los staat van het netwerk.

Het installatieprogramma zet een lokale webserver op deze computer, en een Java *runtime*. Daarin draait de applicatie. Uitvoer wordt fysiek overgebracht naar het centraal stembureau.

Genoemd installatieprogramma is nadrukkelijk ook in scope van het onderzoek. OSV2020-U wordt geleverd voor Windows, Mac OS en Linux, waarbij het onderzoek zich dient te richten op de Windows-variant. De installieprogramma's en -procedures voor Mac OS en Linux worden echter ook meegenomen.

In 2020 heeft HackDefense ook een test op OSV2020-U uitgevoerd. Nieuw is nu dat er een tweede, optionele wijze van vaststellen van de uitslag bij is gekomen (de "nieuwe procedure vaststelling verkiezingsuitslagen" ofwel NPVV), waarbij gemeenten ook de keuze hebben om voorkeurstemmen op een later moment te tellen.

1.1.3 Aanleiding testvraag

De Kiesraad wil graag inzicht hebben in de vraag of de integriteit en vertrouwelijkheid van OSV2020-U voldoende gewaarborgd is. Een pentest is daarbij een belangrijk middel.

1.2 Scope

In scope is de applicatie OSV2020-U zoals de Kiesraad deze voor aanvang aan HackDefense zal aanleveren, inclusief installatieprogramma. We installeren de applicatie in onze eigen lab-omgeving.

Ook de broncode is onderdeel van de scope. Deze zal t.z.t. (voor aanvang) worden aangeleverd, exact overeenkomend met de *live* versie van de applicatie die we testen.

1.2.1 Aanvalsperspectief

De beveiliging moet getest worden vanuit de volgende perspectieven:

1. perspectief van de *outsider*, d.w.z. zonder login-gegevens
2. perspectief van de kwaadwillende *insider* met login-gegevens (of kwaadwillende outsider die login-gegevens heeft weten te verkrijgen)

1.2.2 Testvorm

De beoogde testvorm is *white box*, dat wil zeggen dat alle informatie voor de testers beschikbaar is.

Code review is ook onderdeel van de test.

Social engineering of *Denial-of-Service attacks* (DoS of DDoS) zijn niet aan de orde en moeten op geen enkele wijze worden uitgevoerd.

Een hertest maakt geen deel uit van de opdracht. Deze is, als dit nodig of wenselijk blijkt te zijn, uiteraard wel als meerwerk uit te voeren.

1.3 Onderzoeksvraag

De in dit onderzoek te beantwoorden onderzoeksvraag luidt als volgt:

Kunnen – binnen het overeengekomen tijdsbestek – kwetsbaarheden worden gevonden in de beveiliging van OSV2020-U, waardoor ongeautoriseerden toegang tot OSV2020-U of de daarin verwerkte data zouden kunnen verkrijgen?

Beveiligingsissues die niet direct tot ongeautoriseerde toegang leiden maar die wel zouden kunnen helpen bij een inbraak, m.a.w. waarvan de oplossing tot een robuustere beveiliging leiden, moeten uiteraard ook worden gerapporteerd.

1.4 Overige randvoorwaarden

- Het rapport wordt in het Nederlands opgeleverd, met uitzondering van de individuele technische bevindingen; deze zullen in het Engels worden geschreven.
- Het onderzoek wordt uitgevoerd onder de voorwaarden van de raamovereenkomst met contractnummer 201865007.433 - P1 - HackDefense BV.
- De exacte invulling van de aanpak van de test zal medio augustus in overleg nader worden ingevuld in een kaderstellend document.

Hoofdstuk 2

Ons voorstel

Dit hoofdstuk geeft aan hoe wij voorstellen om de onderzoeksvraag te beantwoorden.

2.1 Team

Al onze pentesters zijn hbo- of wo-opgeleid en hebben tenminste het OSCP- en eWPT-certificaat.

Een van onze gecertificeerde Ethical Hackers voert de test uit. Al het werk wordt diepgaand gereviewed door onze Principal Consultant voor we u ons conceptrapport sturen.

2.2 Aanpak

De inhoudelijke aanpak van de pentest en de code review zal medio augustus in overleg nader worden ingevuld in een kaderstellend document.

2.2.1 Projectfasering

Elke beveiligingstest van HackDefense bestaat uit de volgende fasen:

- *Planning*

  Na akkoord op het voorstel plannen we in overleg de beveiligingstest in. Afhankelijk van de omvang van de opdracht kan de uitvoering snel starten, vaak al binnen twee weken.

- *Kick-off*

  Voor aanvang van de test houden we een kickoff-bijeenkomst. Bij deze kickoff wordt met de security officer en andere betrokken stakeholders nagegaan of alle benodigdheden voor de test aanwezig zijn: alle contactgegevens[1], adressen/URL's, toegang tot locaties, etc. Doel is dat alles klaar is om de uitvoer te kunnen starten.

[1] we vinden het heel belangrijk dat de penetratietesters en beheerders van elkaars directe telefoonnummers op de hoogte zijn om snel te kunnen schakelen indien nodig

- *Uitvoering test*

  In de afgesproken periode voeren we de test uit zoals afgesproken in dit voorstel. Tijdens de test worden belangrijke bevindingen met de Kiesraad gedeeld zodat waar nodig direct actie kan worden ondernomen.

- *Rapportagefase*

  Na afloop van de test schrijven we ons rapport in concept. Het eerste concept wordt intern gereviewed door een Principal Consultant. Het definitieve conceptrapport bieden we aan de Kiesraad aan voor review.

- *Rapportbespreking en definitieve oplevering*

  We bespreken het rapport en op basis van de feedback vanuit de Kiesraad maken we het rapport definitief.

- *Evaluatie*

  Na oplevering van het definitieve rapport vragen we u om ons te beoordelen met een cijfer tussen 0 en 10. Waar nodig bespreken we na wat er goed ging en waar er eventueel verbeterpunten liggen, zodat we de volgende test nog beter kunnen uitvoeren.

2.2.2 Rapportage

Het rapport geeft in de eerste plaats antwoord op de onderzoeksvraag en bestaat uit de volgende hoofdstukken:

- *Managementsamenvatting* – samenvatting in twee of drie alinea's zonder technische terminologie.
- *Uw vraag* – weergave van de onderzoeksvraag en de scope; dit hoofdstuk omschrijft wat er precies is getest.
- *Onze bevindingen* – verslag van de werkzaamheden: de aanpak, en onze analyse.
- *Conclusies en aanbevelingen* – het antwoord op de onderzoeksvraag, en een solide advies voor de weg voorwaarts.
- *Bijlage: technische bevindingen* – alle individuele bevindingen, in technisch detail, bestaand uit de onderdelen:
  - *Omschrijving* - korte samenvatting van het issue
  - *Risico-inschatting* - een inschatting van het risico op basis van kans (hoe moeilijk is dit issue te misbruiken) en impact (wat kan een aanvaller doen), inclusief de CVSS-score [2]
  - *Betreft de systemen* of *Betreft de pagina's* - concrete opsomming van IP-adressen, systeemnamen of componenten van een applicatie waarop het omschreven issue van toepassing is
  - *Waarneming* - precieze waarneming, wat hebben we gezien en hoe is dit reproduceerbaar. Waar mogelijk met technische commando's en/of screenshots.

[2] `https://first.org/cvss/`

- *Aanbeveling* - zo exact mogelijk technisch advies hoe dit issue op te lossen is

Als er vragen zijn bij lezing van het rapport of concrete technische hulp nodig is bij het implementeren van onze aanbevelingen dan verlenen we deze hulp - binnen de grenzen van het redelijke - kostenloos.

Naast individuele bevindingen geeft het rapport inzicht in de algemene situatie van de beveiliging van het onderzoeksobject. Daartoe geeft het een heldere samenvatting van hetgeen geconstateerd is, en hoe zich dat verhoudt tot het te verwachten beveiligingsniveau in vergelijkbare toepassingen.

Het rapport wordt u eerst in concept aangeboden. Op basis van uw reactie worden eventueel aanpassingen gedaan. In het (zeldzame) geval dat we uw feedback niet in ons rapport kunnen overnemen zullen we uw reactie als zodanig letterlijk vermelden in het definitieve rapport.

Ernstige bevindingen worden uiteraard direct gemeld en niet pas bij de rapportage. Ook ontvangt u aan het eind van elke testdag een korte samenvatting.

2.3 Planning

We denken de volgende hoeveelheid inzet nodig te hebben:

testsoort	*uren inzet*
voorbereiden white box, document review	8
installatie testobject in lab-omgeving	8
webapplicatietest	64
code review	64
configuratie-review	16
extra: NPVV	8
totaal tests	168
rapportage	40
QA/review	4
projectmanagement	4
totaal project	216

Medio augustus zullen we in overleg in een kaderstellend document de aanpak nader uitwerken. Mocht daarbij blijken dat bovenstaande inschatting niet voldoende is, dan kan meerwerk worden uitgevoerd (na wederzijdse schriftelijke bevestiging) tegen het bij raamovereenkomst overeengekomen dagtarief (zie onder).

2.4 Kosten

In de vorige paragraaf heeft u gelezen dat we 216 uur (27 mensdagen) benodigde inzet verwachten.

Het binnen de raamovereenkomst afgesproken dagtarief is € 5.1.2.f Totale kosten komen daardoor uit op **€** 5.1.2.f

(alle bedragen zijn exclusief BTW)

Binnen redelijke grenzen vallen alle uit te voeren werkzaamheden binnen deze vaste prijs; voor onderling schriftelijk nader overeengekomen meerwerk rekenen wij het genoemde tarief.

2.5 Overig

Deze opdracht zal worden uitgevoerd conform de in 2020 gesloten raamovereenkomst voor pentesting (kenmerk 201865007.433 - P1 - HackDefense BV).

Hoofdstuk 3

Tot slot

We zien ernaar uit u bij deze belangrijke opdracht te kunnen ondersteunen. Heeft u nog vragen of opmerkingen, aarzel niet om te bellen met 5.1.2.e of 5.1.2.e bereikbaar via (071) 204 0101.

Als u akkoord bent met dit voorstel verzoek ik u om een getekend exemplaar te retourneren.

Voor akkoord:

Naam:	_____
Functie:	_____
Datum:	_____
Namens:	Kiesraad *KvK-nummer 50200097*
Offertenummer:	O23077 v3.0
Handtekening:	_____

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Fri, 21 Jul 2023 11:54:33 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e @hackdefense.nl" <5.1.2.e @hackdefense.nl>
Cc: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: Nieuwe VOG 5.1.2.e

Hij staat hem nu in te scannen!

On 21/07/2023 10:44, 5.1.2.e wrote:

> Goedemorgen,
>
> Is de nieuwe VOG van 5.1.2.e inmiddels binnen? Dan kan ik dat nog rond maken voor mijn vakantie.
>
> Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Fri, 21 Jul 2023 14:39:45 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: offerte pentest en code review OSV2020-U

Thanks. Heb nog even met de planning gepuzzeld & andere klant gesproken. 29 augustus t/m 7 september gaat lukken (7 sep oplevering conceptrapport code review en pentest OSV2020-U, bedoel ik).

Fijne vakantie!

5.1.2.e

On 21/07/2023 10:36, 5.1.2.e wrote:

> 5.1.2.e
>
> Veel dank. Wat mij betreft akkoord zo. 5.1.2.e gaat er komende week mee verder.
>
> Groet,
>
> 5.1.2.e
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Verzonden:** vrijdag 21 juli 2023 09:58
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Onderwerp:** Re: offerte pentest en code review OSV2020-U
>
> Hierbij een nieuwe versie van de offerte. Wijzigingen:
>
> - aan het eind van hoofdstuk 1 is een randvoorwaarde toegevoegd dat de aanpak nader zal worden ingevuld in een kaderstellend document
> - de inhoudelijke aanpak in hoofdstuk 2 is geheel vervangen door een verwijzing naar dit kaderstellend document
> - bij de planning is een zin toegevoegd die aangeeft dat we ervan uitgaan dat hetgeen we in het kaderstellend document vaststellen past binnen de inschatting van het aantal benodigde dagen, en dat het dagtarief uit de raamovereenkomst van toepassing is op eventueel meerwerk, dat we uitsluitend met expliciete wederzijdse instemming uitvoeren uiteraard.
>
> 5.1.2.e
>
> On 20/07/2023 16:53, 5.1.2.e wrote:
>
> > Goedemiddag 5.1.2.e

Hierbij onze offerte voor pentest en code review van OSV2020-U.

Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.

Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:

- we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
- we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)

Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).

Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.

Dank! En fijne vakantie,

5.1.2.e

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Mon, 24 Jul 2023 17:59:39 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "'5.1.2.e '" <5.1.2.e @hackdefense.nl>; "'5.1.2.e '" <5.1.2.e @hackdefense.nl>
Subject: Update pentest OSV2020-PP

Hi 5.1.2.e

Wij hebben vandaag de applicatie geïnstalleerd en een aantal zaken binnen de applicatie getest. Denk hierbij voornamelijk naar het kijken van de aanwezige functionaliteiten en de low-hanging fruit kwetsbaarheden. Wij hebben ook naar de installatiebestanden gekeken voor eventuele wachtwoorden of andere secrets.

De installatie van de applicatie is goed verlopen en werkt goed. We hebben verder geen noemenswaardige bevindingen gedaan en gaan morgen verder met de test.

Met vriendelijke groet / With kind regards,

HackDefense

5.1.2.e
5.1.2.e

M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Tue, 25 Jul 2023 16:57:53 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "'5.1.2.e '" <5.1.2.e @hackdefense.nl>; "'5.1.2.e '" <5.1.2.e @hackdefense.nl>
Subject: RE: Update pentest OSV2020-PP

Hi 5.1.2.e

We zijn vandaag verder gegaan met de test op de applicatie en twee vragen kwamen bij ons omhoog:

1. Waarom mag de applicatie/systeem verbinding maken met het internet?
    a. Is beantwoord via de telefoon
2. Waarom maakt de applicatie geen gebruik van authenticatie?

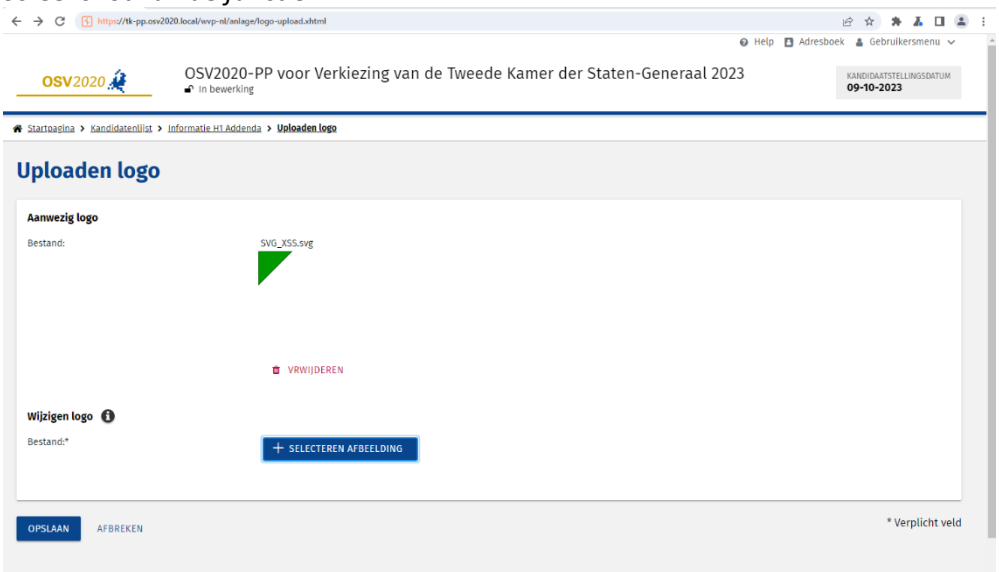
Onbepertke bestandsupload kwetsbaarheid
We hebben daarnaast als noemswaardige bevinding een onbepertke bestandsupload kwetsbaarheid ontdekt. De aanval heeft betrekking op https://tk-pp.osv2020.local/wvp-nl/anlage/logo-upload.xhtml, waarbij het mogelijk is om een logo te uploaden. Wij hebben deze functionaliteit ontdekt na het decompilen van de Java applicatie en het bekijken van de functies. We zijn de functionaliteit niet tegengekomen tijdens de 'normale' flow van de applicatie.

Observatie
Bij het uploaden van een Afbeelding/Logo is het mogelijk om alle soorten bestanden te uploaden zolang de bestandsnaam eindigt op .svg, .png, .jpg of .jpeg. Het is wel mogelijk om de volledige inhoud van het bestand en de content-type te wijzigen. Doordat we functie waarmee het geüploade bestand bekeken kan worden de content-type kopieert van het geüploade bestand, is het mogelijk om alle soorten bestanden te uploaden zoals bijvoorbeeld een Executable (.exe) of een HTML-bestand met daarin JavaScript code. Dit laatste bestand resulteert weer in een Stored Cross-Site Scripting (XSS) aanval.

Impact
Doordat er geen authenticatie of autorisatie aanwezig is in de applicatie, is de impact van een XSS-aanval klein binnen de applicatie. De kwetsbaarheid en een ongebruikte functionaliteit binnen een applicatie staat naar onze mening enkel niet netjes.

Aanbeveling
Verwijder de functionaliteit als deze niet gebruikt wordt of wijzig de functionaliteit door een extra functie aan toe te voegen die het bestand controleert op toegestande extensie, content-type en inhoud.

Screenshot van de functie



From: 5.1.2.e <5.1.2.e @hackdefense.nl>
Sent: 5.1.2.e 24, 2023 6:00 PM
To: '5.1.2.e @kiesraad.nl' <5.1.2.e @kiesraad.nl>
Cc: '5.1.2.e ' <5.1.2.e @hackdefense.nl>; '5.1.2.e ' <5.1.2.e @hackdefense.nl>
Subject: Update pentest OSV2020-PP

Hi 5.1.2.e

Wij hebben vandaag de applicatie geïnstalleerd en een aantal zaken binnen de applicatie getest. Denk hierbij voornamelijk naar het kijken van de aanwezige functionaliteiten en de low-hanging fruit kwetsbaarheden. Wij hebben ook naar de installatiebestanden gekeken voor eventuele wachtwoorden of andere secrets.

De installatie van de applicatie is goed verlopen en werkt goed. We hebben verder geen noemenswaardige bevindingen gedaan en gaan morgen verder met de test.

Met vriendelijke groet / With kind regards,

HackDefense

5.1.2.e
5.1.2.e

M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

HackDefense

Voorstel

Pentest OSV2020-U

Kiesraad

O23077

versie 4.0 - definitief

28 juli 2023

Copyright © 2023 HackDefense BV

Alle rechten voorbehouden. We verzoeken u om dit document vertrouwelijk te behandelen en niet te delen buiten uw organisatie.

HackDefense BV

Postbus 3025
2301 DA Leiden

(071) 204 0101

`https://hackdefense.nl/`

Offerte

Projectnaam	Pentest OSV2020-U
Opdrachtgever	5.1.2.e
KvK-nummer	50200097
Offertenummer	O23077

Documentgeschiedenis

Versie	*Datum*	*Auteur*	*Omschrijving*
1.0	20 juli 2023	5.1.2.e 5.1.2.e	eerste concept
2.0	20 juli 2023	5.1.2.e	wijzigingen na interne review
3.0	21 juli 2023	5.1.2.e	wijzigingen na review opdrachtgever
4.0	28 juli 2023	5.1.2.e	wijzigingen na review opdrachtgever

Managementsamenvatting

Binnen het kader van de raamovereenkomst voor pentesten heeft de Kiesraad aan HackDefense gevraagd om een voorstel te doen voor het testen op *security vulnerabilities* van OSV2020-U, en het adviseren van mitigerende maatregelen daaromtrent.

Dit vormt een uitbreiding op de omschreven aanpak in de ”Standaard Pentest OSV” uit 2020. Er zijn sindsdien enkele zaken aangepast, nieuwe informatie is beschikbaar, en er zijn enkele vragen die buiten de scope van de oorspronkelijke aanbieding vallen.

In dit document vindt u de aanpak, rapportage, en planning die HackDefense voorstelt voor het uitvoeren van deze test.

Het project zal resulteren in een gedegen rapport. Het rapport geeft onze bevindingen en aanbevelingen in technisch detail, en een managementsamenvatting voor de niet technisch onderlegde lezer.

Kosten voor het onderzoek en rapportage bedragen **€** 5.1.2.f (exclusief BTW).

Keurmerk Pentesting

HackDefense is gecertificeerd onder het ”Keurmerk Pentesten”, de Nederlandse pentest-standaard. Dit merk wordt onafhankelijk beheerd door het CCV (Centrum voor Criminaliteitspreventie en Veiligheid). We voeren het keurmerk in al onze beveiligingstestrapporten. Jaarlijks wordt onze kwaliteit door KIWA getoetst aan het keurmerk.

Meer informatie over dit keurmerk vindt u op `https://hetccv.nl/keurmerken/expert/keurmerk-pentesten/`.

Inhoudsopgave

Hoofdstuk 1

Uw vraag

1.1 Achtergrond

1.1.1 Organisatie

De Kiesraad treedt bij verschillende verkiezingen op als centraal stembureau. Verder is de Raad adviesorgaan en informatiecentrum op het gebied van kiesrecht en verkiezingen. Het belang van ICT-beveiliging is evident: de integriteit van het verkiezingsproces is van vitaal belang voor de Nederlandse democratie.

1.1.2 Testobject

OSV2020 is de naam voor een aantal applicaties die worden gebruikt in het verkiezingsproces. Vanzelfsprekend is de veiligheid van deze applicaties van groot belang.

OSV2020-U is de deelapplicatie die zal worden gebruikt om uitslagen en zetelverdelingen vast te stellen. OSV2020-U wordt door de Kiesraad ter beschikking gesteld aan (centraal) stembureaus in gemeenten en kieskringen.

Deze applicatie is gebouwd als webapplicatie in Java, waarbij de gebruikende organisatie (veelal gemeenten) de software installeren op een computer die los staat van het netwerk.

Het installatieprogramma zet een lokale webserver op deze computer, en een Java *runtime*. Daarin draait de applicatie. Uitvoer wordt fysiek overgebracht naar het centraal stembureau.

Genoemd installatieprogramma is nadrukkelijk ook in scope van het onderzoek. OSV2020-U wordt geleverd voor Windows, Mac OS en Linux, waarbij het onderzoek zich dient te richten op de Windows-variant. De installieprogramma's en -procedures voor Mac OS en Linux worden echter ook meegenomen.

In 2020 heeft HackDefense ook een test op OSV2020-U uitgevoerd. Nieuw is nu dat er een tweede, optionele wijze van vaststellen van de uitslag bij is gekomen (de "nieuwe procedure vaststelling verkiezingsuitslagen" ofwel NPVV), waarbij gemeenten ook de keuze hebben om voorkeurstemmen op een later moment te tellen.

1.1.3 Aanleiding testvraag

In 2020 is bij aanbesteding voorzien in een ”Standaard Pentest OSV”, uit te voeren voor elke verkiezing. Voor deze standaard pentest is reeds een opdracht verstrekt. Naast de standaard pentest zijn er enkele extra vragen, waaronder (meest belangrijk) een Secure Code Review.

Dit voorstel beschrijft de gehele opdracht die nader wordt ingevuld via een kaderstellend document.

1.2 Scope

In scope is de applicatie OSV2020-U zoals de Kiesraad deze voor aanvang aan HackDefense zal aanleveren, inclusief installatieprogramma. We installeren de applicatie in onze eigen lab-omgeving.

Ook de broncode is onderdeel van de scope. Deze zal t.z.t. (voor aanvang) worden aangeleverd, exact overeenkomend met de *live* versie van de applicatie die we testen.

1.2.1 Aanvalsperspectief

De beveiliging moet getest worden vanuit de volgende perspectieven:

1. perspectief van de *outsider*, d.w.z. zonder login-gegevens
2. perspectief van de kwaadwillende *insider* met login-gegevens (of kwaadwillende outsider die login-gegevens heeft weten te verkrijgen)

1.2.2 Testvorm

De beoogde testvorm is *white box*, dat wil zeggen dat alle informatie voor de testers beschikbaar is.

Code review is ook onderdeel van de test.

Social engineering of *Denial-of-Service attacks* (DoS of DDoS) zijn niet aan de orde en moeten op geen enkele wijze worden uitgevoerd.

Een hertest maakt geen deel uit van de opdracht. Deze is, als dit nodig of wenselijk blijkt te zijn, uiteraard wel als meerwerk uit te voeren.

1.3 Onderzoeksvraag

De in dit onderzoek te beantwoorden onderzoeksvraag luidt als volgt:

Kunnen – binnen het overeengekomen tijdsbestek – kwetsbaarheden worden gevonden in de beveiliging van OSV2020-U, waardoor ongeautoriseerden toegang tot OSV2020-U of de daarin verwerkte data zouden kunnen verkrijgen?

Beveiligingsissues die niet direct tot ongeautoriseerde toegang leiden maar die wel zouden kunnen helpen bij een inbraak, m.a.w. waarvan de oplossing tot een robuustere beveiliging leiden, moeten uiteraard ook worden gerapporteerd.

1.4 Overige randvoorwaarden

- Het rapport wordt in het Nederlands opgeleverd, met uitzondering van de individuele technische bevindingen; deze zullen in het Engels worden geschreven.
- Het onderzoek wordt uitgevoerd onder de voorwaarden van de raamovereenkomst met contractnummer 201865007.433 - P1 - HackDefense BV.
- De exacte invulling van de aanpak van de test zal medio augustus in overleg nader worden ingevuld in een kaderstellend document.

Hoofdstuk 2

Ons voorstel

Dit hoofdstuk geeft aan hoe wij voorstellen om de onderzoeksvraag te beantwoorden.

2.1 Team

Al onze pentesters zijn hbo- of wo-opgeleid en hebben tenminste het OSCP- en eWPT-certificaat.

Een van onze gecertificeerde Ethical Hackers voert de test uit. Al het werk wordt diepgaand gereviewed door onze Principal Consultant voor we u ons conceptrapport sturen.

2.2 Aanpak

De inhoudelijke aanpak van de pentest en de code review zal medio augustus in overleg nader worden ingevuld in een kaderstellend document.

2.2.1 Projectfasering

Elke beveiligingstest van HackDefense bestaat uit de volgende fasen:

- *Planning*

  Na akkoord op het voorstel plannen we in overleg de beveiligingstest in. Afhankelijk van de omvang van de opdracht kan de uitvoering snel starten, vaak al binnen twee weken.

- *Kick-off*

  Voor aanvang van de test houden we een kickoff-bijeenkomst. Bij deze kickoff wordt met de security officer en andere betrokken stakeholders nagegaan of alle benodigdheden voor de test aanwezig zijn: alle contactgegevens[1], adressen/URL's, toegang tot locaties, etc. Doel is dat alles klaar is om de uitvoer te kunnen starten.

[1] we vinden het heel belangrijk dat de penetratietesters en beheerders van elkaars directe telefoonnummers op de hoogte zijn om snel te kunnen schakelen indien nodig

- *Uitvoering test*

  In de afgesproken periode voeren we de test uit zoals afgesproken in dit voorstel. Tijdens de test worden belangrijke bevindingen met de Kiesraad gedeeld zodat waar nodig direct actie kan worden ondernomen.

- *Rapportagefase*

  Na afloop van de test schrijven we ons rapport in concept. Het eerste concept wordt intern gereviewed door een Principal Consultant. Het definitieve conceptrapport bieden we aan de Kiesraad aan voor review.

- *Rapportbespreking en definitieve oplevering*

  We bespreken het rapport en op basis van de feedback vanuit de Kiesraad maken we het rapport definitief.

- *Evaluatie*

  Na oplevering van het definitieve rapport vragen we u om ons te beoordelen met een cijfer tussen 0 en 10. Waar nodig bespreken we na wat er goed ging en waar er eventueel verbeterpunten liggen, zodat we de volgende test nog beter kunnen uitvoeren.

2.2.2 Rapportage

Het rapport geeft in de eerste plaats antwoord op de onderzoeksvraag en bestaat uit de volgende hoofdstukken:

- *Managementsamenvatting* – samenvatting in twee of drie alinea's zonder technische terminologie.
- *Uw vraag* – weergave van de onderzoeksvraag en de scope; dit hoofdstuk omschrijft wat er precies is getest.
- *Onze bevindingen* – verslag van de werkzaamheden: de aanpak, en onze analyse.
- *Conclusies en aanbevelingen* – het antwoord op de onderzoeksvraag, en een solide advies voor de weg voorwaarts.
- *Bijlage: technische bevindingen* – alle individuele bevindingen, in technisch detail, bestaand uit de onderdelen:
  - *Omschrijving* - korte samenvatting van het issue
  - *Risico-inschatting* - een inschatting van het risico op basis van kans (hoe moeilijk is dit issue te misbruiken) en impact (wat kan een aanvaller doen), inclusief de CVSS-score [2]
  - *Betreft de systemen* of *Betreft de pagina's* - concrete opsomming van IP-adressen, systeemnamen of componenten van een applicatie waarop het omschreven issue van toepassing is
  - *Waarneming* - precieze waarneming, wat hebben we gezien en hoe is dit reproduceerbaar. Waar mogelijk met technische commando's en/of screenshots.

[2] `https://first.org/cvss/`

- *Aanbeveling* - zo exact mogelijk technisch advies hoe dit issue op te lossen is

Als er vragen zijn bij lezing van het rapport of concrete technische hulp nodig is bij het implementeren van onze aanbevelingen dan verlenen we deze hulp - binnen de grenzen van het redelijke - kostenloos.

Naast individuele bevindingen geeft het rapport inzicht in de algemene situatie van de beveiliging van het onderzoeksobject. Daartoe geeft het een heldere samenvatting van hetgeen geconstateerd is, en hoe zich dat verhoudt tot het te verwachten beveiligingsniveau in vergelijkbare toepassingen.

Het rapport wordt u eerst in concept aangeboden. Op basis van uw reactie worden eventueel aanpassingen gedaan. In het (zeldzame) geval dat we uw feedback niet in ons rapport kunnen overnemen zullen we uw reactie als zodanig letterlijk vermelden in het definitieve rapport.

Ernstige bevindingen worden uiteraard direct gemeld en niet pas bij de rapportage. Ook ontvangt u aan het eind van elke testdag een korte samenvatting.

2.3 Planning

We denken de volgende hoeveelheid inzet nodig te hebben:

testsoort	*uren inzet t.o.v. standaardtest*	
	inclusief	*extra*
voorbereiden white box, document review	8	
installatie testobject in lab-omgeving	8	
webapplicatietest	40	24
code review		64
configuratie-review		16
extra: NPVV		8
totaal tests	56	112
rapportage	24	16
QA/review	8	
totaal	88	128

Medio augustus zullen we in overleg in een kaderstellend document de aanpak nader uitwerken. Mocht daarbij blijken dat bovenstaande inschatting niet voldoende is, dan kan meerwerk worden uitgevoerd (na wederzijdse schriftelijke bevestiging) tegen het bij raamovereenkomst overeengekomen dagtarief (zie onder).

2.4 Kosten

In de vorige paragraaf heeft u gelezen dat we 216 uur benodigde inzet verwachten.

Daarvan is 88 uur al inbegrepen in de bestaande opdracht. 128 uur vormt een uitbreiding daarop, voor zover wij dat kunnen overzien vooruitkijkend naar het kaderstellend document.

Het binnen de raamovereenkomst afgesproken dagtarief is € 5.1.2.f Totale kosten komen daardoor uit op **€** 5.1.2.f

(alle bedragen zijn exclusief BTW)

Binnen redelijke grenzen vallen alle uit te voeren werkzaamheden binnen deze vaste prijs; voor onderling schriftelijk nader overeengekomen meerwerk rekenen wij het genoemde tarief.

2.5 Overig

Deze opdracht zal worden uitgevoerd conform de in 2020 gesloten raamovereenkomst voor pentesting (kenmerk 201865007.433 - P1 - HackDefense BV).

Hoofdstuk 3

Tot slot

We zien ernaar uit u bij deze belangrijke opdracht te kunnen ondersteunen. Heeft u nog vragen of opmerkingen, aarzel niet om te bellen met 5.1.2.e of 5.1.2.e bereikbaar via (071) 204 0101.

Als u akkoord bent met dit voorstel verzoek ik u om een getekend exemplaar te retourneren.

Voor akkoord:

Naam:	_____
Functie:	_____
Datum:	_____
Namens:	Kiesraad *KvK-nummer 50200097*
Offertenummer:	O23077 v4.0
Handtekening:	_____

From: "5.1.2.e" <5.1.2.e@hackdefense.nl>
Sent: Tue, 1 Aug 2023 17:14:29 +0200
To: "5.1.2.e" <5.1.2.e@kiesraad.nl>
Subject: RE: Kan rapport niet reviewen, verkeerd mail adres gebruikt

Hi 5.1.2.e

5.1.2.e

Maar de feedback naar 5.1.2.e is ook goed.

From: 5.1.2.e <5.1.2.e@kiesraad.nl>
Sent: 5.1.2.e 1, 2023 4:45 PM
To: 5.1.2.e <5.1.2.e@hackdefense.nl>
Subject: RE: Kan rapport niet reviewen, verkeerd mail adres gebruikt

5.1.2.e

Wat is jouw 06 nr? Anders kan ik de feedback niet sturen via secure transfer.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: dinsdag 1 augustus 2023 16:10
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>; '5.1.2.e' <5.1.2.e@hackdefense.nl>; '5.1.2.e' <5.1.2.e@hackdefense.nl>
Onderwerp: RE: Kan rapport niet reviewen, verkeerd mail adres gebruikt

Hi 5.1.2.e

Als het goed is heb ik nu het rapport naar de juiste e-mail verstuurd.

From: 5.1.2.e <5.1.2.e@kiesraad.nl>
Sent: 5.1.2.e 1, 2023 3:52 PM
To: 5.1.2.e <5.1.2.e@hackdefense.nl>; 5.1.2.e <5.1.2.e@hackdefense.nl>; 5.1.2.e <5.1.2.e@hackdefense.nl>
Subject: Kan rapport niet reviewen, verkeerd mail adres gebruikt

Goedemiddag,

Ik wil nu graag het concept rapport reviewen. Het is alleen verzonden via secure transfer naar het verkeerde mail adres. Daardoor kan ik het niet openen. Ik heb getracht 5.1.2.e en 5.1.2.e telefonisch te bereiken, maar dat lukt helaas niet.

Zouden jullie het zsm naar het juiste mail adres willen sturen via secure transfer? Dat is 5.1.2.e@kiesraad.nl

Met vriendelijke groet,

5.1.2.e
5.1.2.e

Aanwezig: ma t/m vrij, afwezig wo

.....

KIESRAAD

Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag

Postadres: Postbus 20011, 2500 EA Den Haag

.....

T 5.1.2.e

W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Wed, 2 Aug 2023 10:42:44 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>; "'5.1.2.e '" <5.1.2.e @hackdefense.nl>
Subject: Re: Kan rapport niet reviewen, verkeerd mail adres gebruikt

Ha 5.1.2.e heel suf maar ik heb mijn werktelefoon gisteravond bij mijn moeder in Brabant laten liggen... dus kan niet bij het sms'je.

Nummer heb ik doorgeschakeld dus je kan mij er ter verificatie wel op bellen.

Maar kan nu dus niet bij het document want SMS'jes volgen de doorschakeling niet, dacht ik. Is het mogelijk om het document nog een keer te sturen, maar dan met mijn privé-nummer? Dat is 5.1.2.e

Of, andere mogelijkheid, het 06-nummer van 5.1.2.e is 5.1.2.e (mijn werknummer +2).

Excuses voor het ongemak!

5.1.2.e

On 01/08/2023 16:47, 5.1.2.e wrote:

> Goedemiddag,
>
> Dank voor jullie werk en concept rapportage. Jullie hebben er duidelijk goed naar gekeken en het rapport is wat mij betreft helder en begrijpelijk geschreven. Fijn dat de technische bevindingen in het Engels konden!
>
> Ik heb nog een paar kleine suggesties gedaan. Als jullie hier de 1.0 mee kunnen maken, dan zorg ik dat deze begin volgende week naar de Kiesraad stakeholders kan en uiteindelijk op de website.
>
> @5.1.2.e ik stuur de feedback naar jou, omdat ik van 5.1.2.e geen 06nr heb en dat heb ik nodig voor de secure transfer.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo
> .....
> **KIES**RAAD
> Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
> Postadres: Postbus 20011, 2500 EA Den Haag
> .....
> T 5.1.2.e
> W www.kiesraad.nl

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 1 augustus 2023 16:10
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; '5.1.2.e ' <5.1.2.e @hackdefense.nl>; '5.1.2.e '

<5.1.2.e @hackdefense.nl>
Onderwerp: RE: Kan rapport niet reviewen, verkeerd mail adres gebruikt

Hi 5.1.2.e

Als het goed is heb ik nu het rapport naar de juiste e-mail verstuurd.

From: 5.1.2.e <5.1.2.e @kiesraad.nl>
Sent: 5.1.2.e 1, 2023 3:52 PM
To: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>
Subject: Kan rapport niet reviewen, verkeerd mail adres gebruikt

Goedemiddag,

Ik wil nu graag het concept rapport reviewen. Het is alleen verzonden via secure transfer naar het verkeerde mail adres. Daardoor kan ik het niet openen. Ik heb getracht 5.1.2.e en 5.1.2.e telefonisch te bereiken, maar dat lukt helaas niet.

Zouden jullie het zsm naar het juiste mail adres willen sturen via secure transfer? Dat is 5.1.2.e @kiesraad.nl

Met vriendelijke groet,

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e "
Sent: Wed, 2 Aug 2023 15:33:13 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e "
<5.1.2.e @kiesraad.nl>
Subject: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense
Attachments: Aanvullende offerte_[O23077] HackDefense - voorstel pentest OSV2020-U.pdf

Hoi 5.1.2.e

Ik heb een verplichting aangemaakt voor de tweede factuur: nummer **401002-33197.**

Verzoek aan HackDefense om dit ook te vermelden op de e-factuur.

Verder het verzoek om de offerte nog te laten ondertekenen door 5.1.2.e **t.b.v. het inkoopdossier**. Alvast dank. Groet, 5.1.2.e

Nog even hierbij de volledige financiële gegevens:

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van
BUDGETCODERING H2B 401002 – 11312 – 44011.
Verplichtingennummer: 401002-33197

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 31 juli 2023 12:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: 20230731 Offerte Hackdefense_uitbreiding op de pentest

Hoi collega's,

Kunnen jullie een verplichting aanmaken van €5.1.2.f excl btw voor Hackdefense? De opdracht wordt vanuit de raamovereenkomst gegund.

Wie zou dit moeten ondertekenen?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: vrijdag 28 juli 2023 14:59
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hallo 5.1.2.e

Ik zie je punt. Bijgaand aangepast, als uitbreiding op de Standaard Pentest OSV, voor zover wij het meerwerk nu al kunnen overzien (kaderstellend document komt nog).

Let wel dat OSV2020-PP niet echt een 'standalone' Java-applicatie is zoals beschreven in de aanbesteding, waar P0, P1 en P2-3 in één dag testen zouden kunnen worden gedaan. Dat blijkt toch anders (is een webapplicatie net als P4 e.a., zij het lokaal gemaakt door een complete webserver mee te installeren) waardoor ons dat best wat meer tijd kost.

5.1.2.e

On 24/07/2023 19:12, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Ik ben denk ik even afgehaakt in het mailverkeer tussen jou en 5.1.2.e
> De diverse modules van OSV, (PP, KS en U) behoren tot de Standaard pentest OSV. De secure code review niet, ik had dus een offerte verwacht voor de Secure Code Review.
>
> Of heb ik iets gemist?
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e
>
> Afwezig op vrijdag
>
> **Van:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Verzonden:** vrijdag 21 juli 2023 09:58
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Onderwerp:** Re: offerte pentest en code review OSV2020-U
>
> Hierbij een nieuwe versie van de offerte. Wijzigingen:

1. aan het eind van hoofdstuk 1 is een randvoorwaarde toegevoegd dat de aanpak nader zal worden ingevuld in een kaderstellend document
2. de inhoudelijke aanpak in hoofdstuk 2 is geheel vervangen door een verwijzing naar dit kaderstellend document
3. bij de planning is een zin toegevoegd die aangeeft dat we ervan uitgaan dat hetgeen we in het kaderstellend document vaststellen past binnen de inschatting van het aantal benodigde dagen, en dat het dagtarief uit de raamovereenkomst van toepassing is op eventueel meerwerk, dat we uitsluitend met expliciete wederzijdse instemming uitvoeren uiteraard.

5.1.2.e

On 20/07/2023 16:53, 5.1.2.e wrote:

> Goedemiddag 5.1.2.e
>
> Hierbij onze offerte voor pentest en code review van OSV2020-U.
>
> Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.
>
> Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:
>
> 1. we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
> 2. we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)
>
> Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).
>
> Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.
>
> Dank! En fijne vakantie,
>
> 5.1.2.e

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Mon, 7 Aug 2023 09:51:43 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>; "'5.1.2.e '" <5.1.2.e @hackdefense.nl>
Subject: Re: Rapport pentest module PP

Dank je! Leuk om te doen. Wij kijken er ook uit naar de volgende!

5.1.2.e

On 07/08/2023 09:24, 5.1.2.e wrote:

> Goedemorgen,
>
> Ik wilde jullie bedanken voor jullie werk aan de pentest en de rapportage. Bedankt dat jullie zo vlot een mooie test hebben neergezet en goed begrijpelijke rapportage.
>
> Het rapport zal ik vandaag intern delen. Ik weet nog niet wanneer deze openbaar gemaakt zal worden.
>
> Ik zie uit naar onze verdere samenwerking voor de module U!
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo
> .....
> **KIES**RAAD
> Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
> Postadres: Postbus 20011, 2500 EA Den Haag
> .....
> T 5.1.2.e
> W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Mon, 7 Aug 2023 14:52:23 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Re: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

O, dank voor de herinnering, die was er even tussendoor geschoten.

Ik heb zo een afspraak maar zal daarna even kijken.

5.1.2.e

On 07/08/2023 14:51, 5.1.2.e wrote:

> 5.1.2.e
>
> Zie jij kans hier deze week nog naar te kijken? Ik ga donderdag een start maken met het kaderdocument. Zou mooi zijn als we tijdig de offerte en opdrachtbrief klaar hebben.
>
> Groet,
>
> 5.1.2.e
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Verzonden:** donderdag 3 augustus 2023 10:50
> **Aan:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **CC:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Onderwerp:** FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense
>
> Hallo 5.1.2.e
>
> Nog dank voor de offerte. Ik heb inmiddels een nieuwe verplichtingen nummer aan laten maken en de offerte voor akkoord aangeboden.
>
> Nu waren er nog een paar vragen, dan wel opmerkingen over de offerte. Zou jij die kunnen adresseren en eventueel een gewijzigde offerte sturen?
>
> Mochten er nog vragen zijn, dan hoor ik het graag.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e
>
> Afwezig op vrijdag
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Verzonden:** woensdag 2 augustus 2023 21:44
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e

<5.1.2.e @kiesraad.nl>
Onderwerp: RE: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Dank voor de toelichting. Heb het gelezen. Op zich akkoord, maar zou het fijn vinden als in de offerte wat preciezer wordt omschreven:
- dat in de managementsamenvatting wat 'enkele zaken zijn aangepast' concreet wordt omschreven. Ik lees dat ook niet terug in de rest van de offerte.
- ook de omschrijving ' dat er enkele vragen zijn bijgekomen die buiten de scope vallen' zou ik expliciteren dat ' op verzoek van de Kiesraad er enkele onderzoeksvragen zijn bijgekomen..'

Groet,

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Datum: woensdag 02 aug. 2023 4:11 PM
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e
<5.1.2.e @kiesraad.nl>
Onderwerp: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

In de bijlage een aanvullende offerte van Hackdefense voor het secure code onderzoek in OSV2020.

De secure code onderzoek is binnen de scope van de raamovereenkomst, maar valt niet binnen de standaard pentest requirements. Vandaar dat Hackdefense hier een aanvullende offerte voor heeft gemaakt, die voldoet aan de criteria zoals opgenomen in de raamovereenkomst.

Kan jij goedkeuring geven aan deze offerte (laten tekenen) zodat ik dit door kan sturen naar Hackdefense, inclusief het verplichtingen nummer.

Als er nog vragen zijn, dan hoor ik dat graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 15:33
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Ik heb een verplichting aangemaakt voor de tweede factuur: nummer **401002-33197.**

Verzoek aan HackDefense om dit ook te vermelden op de e-factuur.

Verder het verzoek om de offerte nog te laten ondertekenen door 5.1.2.e **t.b.v. het inkoopdossier**. Alvast dank.
Groet, 5.1.2.e

Nog even hierbij de volledige financiële gegevens:

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van **BUDGETCODERING H2B 401002 – 11312 – 44011.**
Verplichtingennummer: 401002-33197

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 31 juli 2023 12:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: 20230731 Offerte Hackdefense_uitbreiding op de pentest

Hoi collega's,

Kunnen jullie een verplichting aanmaken van €5.1.2.f excl btw voor Hackdefense? De opdracht wordt vanuit de raamovereenkomst gegund.

Wie zou dit moeten ondertekenen?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: vrijdag 28 juli 2023 14:59
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hallo 5.1.2.e

Ik zie je punt. Bijgaand aangepast, als uitbreiding op de Standaard Pentest OSV, voor zover wij het meerwerk nu al kunnen overzien (kaderstellend document komt nog).

Let wel dat OSV2020-PP niet echt een 'standalone' Java-applicatie is zoals beschreven in de aanbesteding, waar P0, P1 en P2-3 in één dag testen zouden kunnen worden gedaan. Dat blijkt toch anders (is een webapplicatie net als P4 e.a., zij het lokaal gemaakt door een complete webserver mee te installeren) waardoor ons dat best wat meer tijd kost.

5.1.2.e

On 24/07/2023 19:12, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Ik ben denk ik even afgehaakt in het mailverkeer tussen jou en 5.1.2.e
> De diverse modules van OSV, (PP, KS en U) behoren tot de Standaard pentest OSV. De secure code review niet, ik had dus een offerte verwacht voor de Secure Code Review.
>
> Of heb ik iets gemist?
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e
>
> Afwezig op vrijdag
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e@hackdefense.nl>
> **Verzonden:** vrijdag 21 juli 2023 09:58
> **Aan:** 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e@hackdefense.nl>
> **Onderwerp:** Re: offerte pentest en code review OSV2020-U
>
> Hierbij een nieuwe versie van de offerte. Wijzigingen:
>
> 1. aan het eind van hoofdstuk 1 is een randvoorwaarde toegevoegd dat de aanpak nader zal worden ingevuld in een kaderstellend document
> 2. de inhoudelijke aanpak in hoofdstuk 2 is geheel vervangen door een verwijzing naar dit kaderstellend document
> 3. bij de planning is een zin toegevoegd die aangeeft dat we ervan uitgaan dat hetgeen we in het kaderstellend document vaststellen past binnen de inschatting van het aantal benodigde dagen, en dat het dagtarief uit de raamovereenkomst van toepassing is op eventueel meerwerk, dat we uitsluitend met expliciete wederzijdse instemming uitvoeren uiteraard.

5.1.2.e

On 20/07/2023 16:53, 5.1.2.e wrote:

> Goedemiddag 5.1.2.e
>
> Hierbij onze offerte voor pentest en code review van OSV2020-U.
>
> Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.
>
> Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:
>
> 1. we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
> 2. we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)
>
> Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).
>
> Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.
>
> Dank! En fijne vakantie,
>
> 5.1.2.e

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Tue, 8 Aug 2023 17:16:08 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Re: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense
Attachments: [O23077] HackDefense - voorstel pentest OSV2020-U.pdf

Hallo 5.1.2.e

Bijgaand een aangepaste versie (5.0). Identiek aan 4.0 alleen de tweede alinea van de managementsamenvatting heb ik conform onderstaande als volgt aangepast:

Dit vormt een uitbreiding op de omschreven aanpak in de "Standaard Pentest OSV" uit 2020. Er is een toevoeging in de telsystematiek n.a.v. de nieuwe Wet NPVV en op verzoek van de Kiesraad zijn er enkele onderzoeksvragen bijgekomen waarvan een Secure Code Review de belangrijkste is.

Is dat voldoende helder?

Dank!

5.1.2.e

On 03/08/2023 10:49, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Nog dank voor de offerte. Ik heb inmiddels een nieuwe verplichtingen nummer aan laten maken en de offerte voor akkoord aangeboden.
>
> Nu waren er nog een paar vragen, dan wel opmerkingen over de offerte. Zou jij die kunnen adresseren en eventueel een gewijzigde offerte sturen?
>
> Mochten er nog vragen zijn, dan hoor ik het graag.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e
>
> Afwezig op vrijdag
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Verzonden:** woensdag 2 augustus 2023 21:44
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Onderwerp:** RE: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Dank voor de toelichting. Heb het gelezen. Op zich akkoord, maar zou het fijn vinden als in de offerte wat preciezer wordt omschreven:
- dat in de managementsamenvatting wat ‘enkele zaken zijn aangepast’ concreet wordt omschreven. Ik lees dat ook niet terug in de rest van de offerte.
- ook de omschrijving ‘ dat er enkele vragen zijn bijgekomen die buiten de scope vallen’ zou ik expliciteren dat ‘ op verzoek van de Kiesraad er enkele onderzoeksvragen zijn bijgekomen..’

Groet,

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Datum: woensdag 02 aug. 2023 4:11 PM
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

In de bijlage een aanvullende offerte van Hackdefense voor het secure code onderzoek in OSV2020.

De secure code onderzoek is binnen de scope van de raamovereenkomst, maar valt niet binnen de standaard pentest requirements. Vandaar dat Hackdefense hier een aanvullende offerte voor heeft gemaakt, die voldoet aan de criteria zoals opgenomen in de raamovereenkomst.

Kan jij goedkeuring geven aan deze offerte (laten tekenen) zodat ik dit door kan sturen naar Hackdefense, inclusief het verplichtingen nummer.

Als er nog vragen zijn, dan hoor ik dat graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 15:33
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Ik heb een verplichting aangemaakt voor de tweede factuur: nummer **401002-33197.**

Verzoek aan HackDefense om dit ook te vermelden op de e-factuur.

Verder het verzoek om de offerte nog te laten ondertekenen door 5.1.2.e **t.b.v. het inkoopdossier**. Alvast dank.
Groet, 5.1.2.e

Nog even hierbij de volledige financiële gegevens:

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van **BUDGETCODERING H2B 401002 – 11312 – 44011.**
Verplichtingennummer: 401002-33197

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 31 juli 2023 12:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: 20230731 Offerte Hackdefense_uitbreiding op de pentest

Hoi collega's,

Kunnen jullie een verplichting aanmaken van €5.1.2.f excl btw voor Hackdefense? De opdracht wordt vanuit de raamovereenkomst gegund.

Wie zou dit moeten ondertekenen?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: vrijdag 28 juli 2023 14:59
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hallo 5.1.2.e

Ik zie je punt. Bijgaand aangepast, als uitbreiding op de Standaard Pentest OSV, voor zover wij het meerwerk nu al kunnen overzien (kaderstellend document komt nog).

Let wel dat OSV2020-PP niet echt een 'standalone' Java-applicatie is zoals beschreven in de aanbesteding, waar P0, P1 en P2-3 in één dag testen zouden kunnen worden gedaan. Dat blijkt toch anders (is een webapplicatie net als P4 e.a., zij het lokaal gemaakt door een complete webserver mee te installeren) waardoor ons dat best wat meer tijd kost.

5.1.2.e

On 24/07/2023 19:12, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Ik ben denk ik even afgehaakt in het mailverkeer tussen jou en 5.1.2.e
> De diverse modules van OSV, (PP, KS en U) behoren tot de Standaard pentest OSV. De secure code review niet, ik had dus een offerte verwacht voor de Secure Code Review.
>
> Of heb ik iets gemist?
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e
>
> Afwezig op vrijdag
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e@hackdefense.nl>
> **Verzonden:** vrijdag 21 juli 2023 09:58
> **Aan:** 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e@hackdefense.nl>
> **Onderwerp:** Re: offerte pentest en code review OSV2020-U
>
> Hierbij een nieuwe versie van de offerte. Wijzigingen:
>
> 1. aan het eind van hoofdstuk 1 is een randvoorwaarde toegevoegd dat de aanpak nader zal worden ingevuld in een kaderstellend document
> 2. de inhoudelijke aanpak in hoofdstuk 2 is geheel vervangen door een verwijzing naar dit kaderstellend document
> 3. bij de planning is een zin toegevoegd die aangeeft dat we ervan uitgaan dat hetgeen we in het kaderstellend document vaststellen past binnen de inschatting van het aantal benodigde dagen, en dat het dagtarief uit de raamovereenkomst van toepassing is op eventueel meerwerk, dat we uitsluitend met expliciete wederzijdse instemming uitvoeren uiteraard.
>
> 5.1.2.e

On 20/07/2023 16:53, 5.1.2.e wrote:

Goedemiddag 5.1.2.e

Hierbij onze offerte voor pentest en code review van OSV2020-U.

Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.

Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:

1. we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
2. we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)

Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).

Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.

Dank! En fijne vakantie,

5.1.2.e

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

HackDefense

Voorstel

Pentest OSV2020-U

Kiesraad

O23077

versie 5.0 - definitief

8 augustus 2023

Copyright © 2023 HackDefense BV

Alle rechten voorbehouden. We verzoeken u om dit document vertrouwelijk te behandelen en niet te delen buiten uw organisatie.

HackDefense BV

Postbus 3025
2301 DA Leiden

(071) 204 0101

`https://hackdefense.nl/`

Offerte

Projectnaam	Pentest OSV2020-U
Opdrachtgever	5.1.2.e
KvK-nummer	50200097
Offertenummer	O23077

Documentgeschiedenis

Versie	*Datum*	*Auteur*	*Omschrijving*
1.0	20 juli 2023	5.1.2.e 5.1.2.e	eerste concept
2.0	20 juli 2023	5.1.2.e	wijzigingen na interne review
3.0	21 juli 2023	5.1.2.e	wijzigingen na review opdrachtgever
4.0	28 juli 2023	5.1.2.e	wijzigingen na review opdrachtgever
5.0	8 augustus 2023	5.1.2.e	wijzigingen na review opdrachtgever

Managementsamenvatting

Binnen het kader van de raamovereenkomst voor pentesten heeft de Kiesraad aan HackDefense gevraagd om een voorstel te doen voor het testen op *security vulnerabilities* van OSV2020-U, en het adviseren van mitigerende maatregelen daaromtrent.

Dit vormt een uitbreiding op de omschreven aanpak in de "Standaard Pentest OSV" uit 2020. Er is een toevoeging in de telsystematiek n.a.v. de nieuwe Wet NPVV en op verzoek van de Kiesraad zijn er enkele onderzoeksvragen bijgekomen waarvan een Secure Code Review de belangrijkste is.

In dit document vindt u de aanpak, rapportage, en planning die HackDefense voorstelt voor het uitvoeren van deze test.

Het project zal resulteren in een gedegen rapport. Het rapport geeft onze bevindingen en aanbevelingen in technisch detail, en een managementsamenvatting voor de niet technisch onderlegde lezer.

Kosten voor het onderzoek en rapportage bedragen **€** 5.1.2.f (exclusief BTW).

Keurmerk Pentesting

HackDefense is gecertificeerd onder het "Keurmerk Pentesten", de Nederlandse pentest-standaard. Dit merk wordt onafhankelijk beheerd door het CCV (Centrum voor Criminaliteitspreventie en Veiligheid). We voeren het keurmerk in al onze beveiligingstestrapporten. Jaarlijks wordt onze kwaliteit door KIWA getoetst aan het keurmerk.

Meer informatie over dit keurmerk vindt u op `https://hetccv.nl/keurmerken/expert/keurmerk-pentesten/`.

Inhoudsopgave

Hoofdstuk 1

Uw vraag

1.1 Achtergrond

1.1.1 Organisatie

De Kiesraad treedt bij verschillende verkiezingen op als centraal stembureau. Verder is de Raad adviesorgaan en informatiecentrum op het gebied van kiesrecht en verkiezingen. Het belang van ICT-beveiliging is evident: de integriteit van het verkiezingsproces is van vitaal belang voor de Nederlandse democratie.

1.1.2 Testobject

OSV2020 is de naam voor een aantal applicaties die worden gebruikt in het verkiezingsproces. Vanzelfsprekend is de veiligheid van deze applicaties van groot belang.

OSV2020-U is de deelapplicatie die zal worden gebruikt om uitslagen en zetelverdelingen vast te stellen. OSV2020-U wordt door de Kiesraad ter beschikking gesteld aan (centraal) stembureaus in gemeenten en kieskringen.

Deze applicatie is gebouwd als webapplicatie in Java, waarbij de gebruikende organisatie (veelal gemeenten) de software installeren op een computer die los staat van het netwerk.

Het installatieprogramma zet een lokale webserver op deze computer, en een Java *runtime*. Daarin draait de applicatie. Uitvoer wordt fysiek overgebracht naar het centraal stembureau.

Genoemd installatieprogramma is nadrukkelijk ook in scope van het onderzoek. OSV2020-U wordt geleverd voor Windows, Mac OS en Linux, waarbij het onderzoek zich dient te richten op de Windows-variant. De installieprogramma's en -procedures voor Mac OS en Linux worden echter ook meegenomen.

In 2020 heeft HackDefense ook een test op OSV2020-U uitgevoerd. Nieuw is nu dat er een tweede, optionele wijze van vaststellen van de uitslag bij is gekomen (de "nieuwe procedure vaststelling verkiezingsuitslagen" ofwel NPVV), waarbij gemeenten ook de keuze hebben om voorkeurstemmen op een later moment te tellen.

1.1.3 Aanleiding testvraag

In 2020 is bij aanbesteding voorzien in een ”Standaard Pentest OSV”, uit te voeren voor elke verkiezing. Voor deze standaard pentest is reeds een opdracht verstrekt. Naast de standaard pentest zijn er enkele extra vragen, waaronder (meest belangrijk) een Secure Code Review.

Dit voorstel beschrijft de gehele opdracht die nader wordt ingevuld via een kaderstellend document.

1.2 Scope

In scope is de applicatie OSV2020-U zoals de Kiesraad deze voor aanvang aan HackDefense zal aanleveren, inclusief installatieprogramma. We installeren de applicatie in onze eigen lab-omgeving.

Ook de broncode is onderdeel van de scope. Deze zal t.z.t. (voor aanvang) worden aangeleverd, exact overeenkomend met de *live* versie van de applicatie die we testen.

1.2.1 Aanvalsperspectief

De beveiliging moet getest worden vanuit de volgende perspectieven:

1. perspectief van de *outsider*, d.w.z. zonder login-gegevens
2. perspectief van de kwaadwillende *insider* met login-gegevens (of kwaadwillende outsider die login-gegevens heeft weten te verkrijgen)

1.2.2 Testvorm

De beoogde testvorm is *white box*, dat wil zeggen dat alle informatie voor de testers beschikbaar is.

Code review is ook onderdeel van de test.

Social engineering of *Denial-of-Service attacks* (DoS of DDoS) zijn niet aan de orde en moeten op geen enkele wijze worden uitgevoerd.

Een hertest maakt geen deel uit van de opdracht. Deze is, als dit nodig of wenselijk blijkt te zijn, uiteraard wel als meerwerk uit te voeren.

1.3 Onderzoeksvraag

De in dit onderzoek te beantwoorden onderzoeksvraag luidt als volgt:

Kunnen – binnen het overeengekomen tijdsbestek – kwetsbaarheden worden gevonden in de beveiliging van OSV2020-U, waardoor ongeautoriseerden toegang tot OSV2020-U of de daarin verwerkte data zouden kunnen verkrijgen?

Beveiligingsissues die niet direct tot ongeautoriseerde toegang leiden maar die wel zouden kunnen helpen bij een inbraak, m.a.w. waarvan de oplossing tot een robuustere beveiliging leiden, moeten uiteraard ook worden gerapporteerd.

1.4 Overige randvoorwaarden

- Het rapport wordt in het Nederlands opgeleverd, met uitzondering van de individuele technische bevindingen; deze zullen in het Engels worden geschreven.
- Het onderzoek wordt uitgevoerd onder de voorwaarden van de raamovereenkomst met contractnummer 201865007.433 - P1 - HackDefense BV.
- De exacte invulling van de aanpak van de test zal medio augustus in overleg nader worden ingevuld in een kaderstellend document.

Hoofdstuk 2

Ons voorstel

Dit hoofdstuk geeft aan hoe wij voorstellen om de onderzoeksvraag te beantwoorden.

2.1 Team

Al onze pentesters zijn hbo- of wo-opgeleid en hebben tenminste het OSCP- en eWPT-certificaat.

Een van onze gecertificeerde Ethical Hackers voert de test uit. Al het werk wordt diepgaand gereviewed door onze Principal Consultant voor we u ons conceptrapport sturen.

2.2 Aanpak

De inhoudelijke aanpak van de pentest en de code review zal medio augustus in overleg nader worden ingevuld in een kaderstellend document.

2.2.1 Projectfasering

Elke beveiligingstest van HackDefense bestaat uit de volgende fasen:

- *Planning*

  Na akkoord op het voorstel plannen we in overleg de beveiligingstest in. Afhankelijk van de omvang van de opdracht kan de uitvoering snel starten, vaak al binnen twee weken.

- *Kick-off*

  Voor aanvang van de test houden we een kickoff-bijeenkomst. Bij deze kickoff wordt met de security officer en andere betrokken stakeholders nagegaan of alle benodigdheden voor de test aanwezig zijn: alle contactgegevens[1], adressen/URL's, toegang tot locaties, etc. Doel is dat alles klaar is om de uitvoer te kunnen starten.

[1] we vinden het heel belangrijk dat de penetratietesters en beheerders van elkaars directe telefoonnummers op de hoogte zijn om snel te kunnen schakelen indien nodig

- *Uitvoering test*

  In de afgesproken periode voeren we de test uit zoals afgesproken in dit voorstel. Tijdens de test worden belangrijke bevindingen met de Kiesraad gedeeld zodat waar nodig direct actie kan worden ondernomen.

- *Rapportagefase*

  Na afloop van de test schrijven we ons rapport in concept. Het eerste concept wordt intern gereviewed door een Principal Consultant. Het definitieve conceptrapport bieden we aan de Kiesraad aan voor review.

- *Rapportbespreking en definitieve oplevering*

  We bespreken het rapport en op basis van de feedback vanuit de Kiesraad maken we het rapport definitief.

- *Evaluatie*

  Na oplevering van het definitieve rapport vragen we u om ons te beoordelen met een cijfer tussen 0 en 10. Waar nodig bespreken we na wat er goed ging en waar er eventueel verbeterpunten liggen, zodat we de volgende test nog beter kunnen uitvoeren.

2.2.2 Rapportage

Het rapport geeft in de eerste plaats antwoord op de onderzoeksvraag en bestaat uit de volgende hoofdstukken:

- *Managementsamenvatting* – samenvatting in twee of drie alinea's zonder technische terminologie.
- *Uw vraag* – weergave van de onderzoeksvraag en de scope; dit hoofdstuk omschrijft wat er precies is getest.
- *Onze bevindingen* – verslag van de werkzaamheden: de aanpak, en onze analyse.
- *Conclusies en aanbevelingen* – het antwoord op de onderzoeksvraag, en een solide advies voor de weg voorwaarts.
- *Bijlage: technische bevindingen* – alle individuele bevindingen, in technisch detail, bestaand uit de onderdelen:
  - *Omschrijving* - korte samenvatting van het issue
  - *Risico-inschatting* - een inschatting van het risico op basis van kans (hoe moeilijk is dit issue te misbruiken) en impact (wat kan een aanvaller doen), inclusief de CVSS-score [2]
  - *Betreft de systemen* of *Betreft de pagina's* - concrete opsomming van IP-adressen, systeemnamen of componenten van een applicatie waarop het omschreven issue van toepassing is
  - *Waarneming* - precieze waarneming, wat hebben we gezien en hoe is dit reproduceerbaar. Waar mogelijk met technische commando's en/of screenshots.

[2] `https://first.org/cvss/`

- *Aanbeveling* - zo exact mogelijk technisch advies hoe dit issue op te lossen is

Als er vragen zijn bij lezing van het rapport of concrete technische hulp nodig is bij het implementeren van onze aanbevelingen dan verlenen we deze hulp - binnen de grenzen van het redelijke - kostenloos.

Naast individuele bevindingen geeft het rapport inzicht in de algemene situatie van de beveiliging van het onderzoeksobject. Daartoe geeft het een heldere samenvatting van hetgeen geconstateerd is, en hoe zich dat verhoudt tot het te verwachten beveiligingsniveau in vergelijkbare toepassingen.

Het rapport wordt u eerst in concept aangeboden. Op basis van uw reactie worden eventueel aanpassingen gedaan. In het (zeldzame) geval dat we uw feedback niet in ons rapport kunnen overnemen zullen we uw reactie als zodanig letterlijk vermelden in het definitieve rapport.

Ernstige bevindingen worden uiteraard direct gemeld en niet pas bij de rapportage. Ook ontvangt u aan het eind van elke testdag een korte samenvatting.

2.3 Planning

We denken de volgende hoeveelheid inzet nodig te hebben:

testsoort	*uren inzet t.o.v. standaardtest*	
	inclusief	*extra*
voorbereiden white box, document review	8	
installatie testobject in lab-omgeving	8	
webapplicatietest	40	24
code review		64
configuratie-review		16
extra: NPVV		8
totaal tests	56	112
rapportage	24	16
QA/review	8	
totaal	88	128

Medio augustus zullen we in overleg in een kaderstellend document de aanpak nader uitwerken. Mocht daarbij blijken dat bovenstaande inschatting niet voldoende is, dan kan meerwerk worden uitgevoerd (na wederzijdse schriftelijke bevestiging) tegen het bij raamovereenkomst overeengekomen dagtarief (zie onder).

2.4 Kosten

In de vorige paragraaf heeft u gelezen dat we 216 uur benodigde inzet verwachten.

Daarvan is 88 uur al inbegrepen in de bestaande opdracht. 128 uur vormt een uitbreiding daarop, voor zover wij dat kunnen overzien vooruitkijkend naar het kaderstellend document.

Het binnen de raamovereenkomst afgesproken dagtarief is € 5.1.2.f Totale kosten komen daardoor uit op **€** 5.1.2.f

(alle bedragen zijn exclusief BTW)

Binnen redelijke grenzen vallen alle uit te voeren werkzaamheden binnen deze vaste prijs; voor onderling schriftelijk nader overeengekomen meerwerk rekenen wij het genoemde tarief.

2.5 Overig

Deze opdracht zal worden uitgevoerd conform de in 2020 gesloten raamovereenkomst voor pentesting (kenmerk 201865007.433 - P1 - HackDefense BV).

Hoofdstuk 3

Tot slot

We zien ernaar uit u bij deze belangrijke opdracht te kunnen ondersteunen. Heeft u nog vragen of opmerkingen, aarzel niet om te bellen met 5.1.2.e of 5.1.2.e bereikbaar via (071) 204 0101.

Als u akkoord bent met dit voorstel verzoek ik u om een getekend exemplaar te retourneren.

Voor akkoord:

Naam:	_____
Functie:	_____
Datum:	_____
Namens:	Kiesraad *KvK-nummer 50200097*
Offertenummer:	O23077 v5.0
Handtekening:	_____

From: "5.1.2.e "
Sent: Wed, 9 Aug 2023 10:02:43 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e "
<5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: FW: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense
Attachments: [O23077] HackDefense - voorstel pentest OSV2020-U.pdf

Hallo 5.1.2.e

Op verzoek van 5.1.2.e is de offerte van Hack Defense tekstueel nog aangepast.

In de bijlage tref je de aanvullende offerte van Hack Defense om een code review uit te voeren op de OSV2020 software. Dit type review valt binnen de scope van de raamovereenkomst, maar behoort niet tot de standaard pentest.

Graag een akkoord op de offerte zodat er een verplichtingen nummer aangemaakt kan worden.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 8 augustus 2023 17:16
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

Bijgaand een aangepaste versie (5.0). Identiek aan 4.0 alleen de tweede alinea van de managementsamenvatting heb ik conform onderstaande als volgt aangepast:

Dit vormt een uitbreiding op de omschreven aanpak in de ”Standaard Pentest OSV” uit 2020. Er is een toevoeging in de telsystematiek n.a.v. de nieuwe Wet NPVV en op verzoek van de Kiesraad zijn er enkele onderzoeksvragen bijgekomen waarvan een Secure Code Review de belangrijkste is.

Is dat voldoende helder?

Dank!

5.1.2.e

On 03/08/2023 10:49, 5.1.2.e wrote:

Hallo 5.1.2.e

Nog dank voor de offerte. Ik heb inmiddels een nieuwe verplichtingen nummer aan laten maken en de offerte voor akkoord aangeboden.

Nu waren er nog een paar vragen, dan wel opmerkingen over de offerte. Zou jij die kunnen adresseren en eventueel een gewijzigde offerte sturen?

Mochten er nog vragen zijn, dan hoor ik het graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 21:44
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: RE: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Dank voor de toelichting. Heb het gelezen. Op zich akkoord, maar zou het fijn vinden als in de offerte wat preciezer wordt omschreven:
- dat in de managementsamenvatting wat ‘enkele zaken zijn aangepast’ concreet wordt omschreven. Ik lees dat ook niet terug in de rest van de offerte.
- ook de omschrijving ‘ dat er enkele vragen zijn bijgekomen die buiten de scope vallen’ zou ik expliciteren dat ‘ op verzoek van de Kiesraad er enkele onderzoeksvragen zijn bijgekomen..’

Groet,

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Datum: woensdag 02 aug. 2023 4:11 PM
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e@kiesraad.nl>, 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

In de bijlage een aanvullende offerte van Hackdefense voor het secure code onderzoek in OSV2020.

De secure code onderzoek is binnen de scope van de raamovereenkomst, maar valt niet binnen de standaard pentest requirements. Vandaar dat Hackdefense hier een aanvullende offerte voor heeft gemaakt, die voldoet aan de criteria zoals opgenomen in de raamovereenkomst.

Kan jij goedkeuring geven aan deze offerte (laten tekenen) zodat ik dit door kan sturen naar Hackdefense, inclusief het verplichtingen nummer.

Als er nog vragen zijn, dan hoor ik dat graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 15:33
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Ik heb een verplichting aangemaakt voor de tweede factuur: nummer **401002-33197.**

Verzoek aan HackDefense om dit ook te vermelden op de e-factuur.

Verder het verzoek om de offerte nog te laten ondertekenen door 5.1.2.e **t.b.v. het inkoopdossier**. Alvast dank.
Groet, 5.1.2.e

Nog even hierbij de volledige financiële gegevens:

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van **BUDGETCODERING H2B 401002 – 11312 – 44011.**
Verplichtingennummer: 401002-33197

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 31 juli 2023 12:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: 20230731 Offerte Hackdefense_uitbreiding op de pentest

Hoi collega's,

Kunnen jullie een verplichting aanmaken van €5.1.2.f excl btw voor Hackdefense? De opdracht wordt vanuit de raamovereenkomst gegund.

Wie zou dit moeten ondertekenen?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: vrijdag 28 juli 2023 14:59
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hallo 5.1.2.e

Ik zie je punt. Bijgaand aangepast, als uitbreiding op de Standaard Pentest OSV, voor zover wij het meerwerk nu al kunnen overzien (kaderstellend document komt nog).

Let wel dat OSV2020-PP niet echt een 'standalone' Java-applicatie is zoals beschreven in de aanbesteding, waar P0, P1 en P2-3 in één dag testen zouden kunnen worden gedaan. Dat blijkt toch anders (is een webapplicatie net als P4 e.a., zij het lokaal gemaakt door een complete webserver mee te installeren) waardoor ons dat best wat meer tijd kost.

5.1.2.e

On 24/07/2023 19:12, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Ik ben denk ik even afgehaakt in het mailverkeer tussen jou en 5.1.2.e
> De diverse modules van OSV, (PP, KS en U) behoren tot de Standaard pentest OSV. De secure code review niet, ik had dus een offerte verwacht voor de Secure Code Review.
>
> Of heb ik iets gemist?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: vrijdag 21 juli 2023 09:58
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hierbij een nieuwe versie van de offerte. Wijzigingen:

1. aan het eind van hoofdstuk 1 is een randvoorwaarde toegevoegd dat de aanpak nader zal worden ingevuld in een kaderstellend document
2. de inhoudelijke aanpak in hoofdstuk 2 is geheel vervangen door een verwijzing naar dit kaderstellend document
3. bij de planning is een zin toegevoegd die aangeeft dat we ervan uitgaan dat hetgeen we in het kaderstellend document vaststellen past binnen de inschatting van het aantal benodigde dagen, en dat het dagtarief uit de raamovereenkomst van toepassing is op eventueel meerwerk, dat we uitsluitend met expliciete wederzijdse instemming uitvoeren uiteraard.

5.1.2.e

On 20/07/2023 16:53, 5.1.2.e wrote:

> Goedemiddag 5.1.2.e
>
> Hierbij onze offerte voor pentest en code review van OSV2020-U.
>
> Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.
>
> Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:
>
> 1. we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
> 2. we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)

Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).

Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.

Dank! En fijne vakantie,

5.1.2.e

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e "
Sent: Wed, 9 Aug 2023 10:03:25 +0200
To: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: RE: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Goedemorgen 5.1.2.e

Mij voldoende helder, ik heb hem ter goedkeuring doorgestuurd naar het management.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 8 augustus 2023 17:16
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

Bijgaand een aangepaste versie (5.0). Identiek aan 4.0 alleen de tweede alinea van de managementsamenvatting heb ik conform onderstaande als volgt aangepast:

Dit vormt een uitbreiding op de omschreven aanpak in de "Standaard Pentest OSV" uit 2020. Er is een toevoeging in de telsystematiek n.a.v. de nieuwe Wet NPVV en op verzoek van de Kiesraad zijn er enkele onderzoeksvragen bijgekomen waarvan een Secure Code Review de belangrijkste is.

Is dat voldoende helder?

Dank!

5.1.2.e

On 03/08/2023 10:49, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Nog dank voor de offerte. Ik heb inmiddels een nieuwe verplichtingen nummer aan laten maken en de offerte voor akkoord aangeboden.
>
> Nu waren er nog een paar vragen, dan wel opmerkingen over de offerte. Zou jij die kunnen adresseren en eventueel een gewijzigde offerte sturen?

Mochten er nog vragen zijn, dan hoor ik het graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 21:44
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: RE: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Dank voor de toelichting. Heb het gelezen. Op zich akkoord, maar zou het fijn vinden als in de offerte wat preciezer wordt omschreven:
- dat in de managementsamenvatting wat 'enkele zaken zijn aangepast' concreet wordt omschreven. Ik lees dat ook niet terug in de rest van de offerte.
- ook de omschrijving ' dat er enkele vragen zijn bijgekomen die buiten de scope vallen' zou ik expliciteren dat ' op verzoek van de Kiesraad er enkele onderzoeksvragen zijn bijgekomen..'

Groet,

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Datum: woensdag 02 aug. 2023 4:11 PM
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e@kiesraad.nl>, 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

In de bijlage een aanvullende offerte van Hackdefense voor het secure code onderzoek in OSV2020.

De secure code onderzoek is binnen de scope van de raamovereenkomst, maar valt niet binnen de standaard pentest requirements. Vandaar dat Hackdefense hier een aanvullende offerte voor heeft gemaakt, die voldoet aan de criteria zoals opgenomen in de raamovereenkomst.

Kan jij goedkeuring geven aan deze offerte (laten tekenen) zodat ik dit door kan sturen naar Hackdefense, inclusief het verplichtingen nummer.

Als er nog vragen zijn, dan hoor ik dat graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 15:33
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Ik heb een verplichting aangemaakt voor de tweede factuur: nummer **401002-33197.**

Verzoek aan HackDefense om dit ook te vermelden op de e-factuur.

Verder het verzoek om de offerte nog te laten ondertekenen door 5.1.2.e **t.b.v. het inkoopdossier**. Alvast dank.
Groet, 5.1.2.e

Nog even hierbij de volledige financiële gegevens:

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van **BUDGETCODERING H2B 401002 – 11312 – 44011.**
Verplichtingennummer: 401002-33197

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 31 juli 2023 12:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: 20230731 Offerte Hackdefense_uitbreiding op de pentest

Hoi collega's,

Kunnen jullie een verplichting aanmaken van €5.1.2.f excl btw voor Hackdefense? De opdracht wordt vanuit de raamovereenkomst gegund.

Wie zou dit moeten ondertekenen?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: vrijdag 28 juli 2023 14:59
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hallo 5.1.2.e

Ik zie je punt. Bijgaand aangepast, als uitbreiding op de Standaard Pentest OSV, voor zover wij het meerwerk nu al kunnen overzien (kaderstellend document komt nog).

Let wel dat OSV2020-PP niet echt een 'standalone' Java-applicatie is zoals beschreven in de aanbesteding, waar P0, P1 en P2-3 in één dag testen zouden kunnen worden gedaan. Dat blijkt toch anders (is een webapplicatie net als P4 e.a., zij het lokaal gemaakt door een complete webserver mee te installeren) waardoor ons dat best wat meer tijd kost.

5.1.2.e

On 24/07/2023 19:12, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Ik ben denk ik even afgehaakt in het mailverkeer tussen jou en 5.1.2.e
> De diverse modules van OSV, (PP, KS en U) behoren tot de Standaard pentest OSV. De secure code review niet, ik had dus een offerte verwacht voor de Secure Code Review.
>
> Of heb ik iets gemist?
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: vrijdag 21 juli 2023 09:58
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hierbij een nieuwe versie van de offerte. Wijzigingen:

1. aan het eind van hoofdstuk 1 is een randvoorwaarde toegevoegd dat de aanpak nader zal worden ingevuld in een kaderstellend document
2. de inhoudelijke aanpak in hoofdstuk 2 is geheel vervangen door een verwijzing naar dit kaderstellend document
3. bij de planning is een zin toegevoegd die aangeeft dat we ervan uitgaan dat hetgeen we in het kaderstellend document vaststellen past binnen de inschatting van het aantal benodigde dagen, en dat het dagtarief uit de raamovereenkomst van toepassing is op eventueel meerwerk, dat we uitsluitend met expliciete wederzijdse instemming uitvoeren uiteraard.

5.1.2.e

On 20/07/2023 16:53, 5.1.2.e wrote:

> Goedemiddag 5.1.2.e
>
> Hierbij onze offerte voor pentest en code review van OSV2020-U.
>
> Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.
>
> Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:
>
> 1. we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
> 2. we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)
>
> Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).

Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.

Dank! En fijne vakantie,

5.1.2.e

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e "
Sent: Wed, 9 Aug 2023 11:35:51 +0200
To: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: FW: [JIRA] (ELECTVAPP-2343) Pentest Hackdefense 2023 - Use of insecure random function (A2)

Beste 5.1.2.e

Jullie pentest voor OSV2020 PP heeft een drietal bevindingen opgeleverd met de kwalificaties hoog, midden en laag risico. Hoog en laag zijn volgens Elect iT al opgelost. De bevinding met de kwalificatie midden levert nog discussie op. In onderstaande mail van Elect iT wordt een vraag gesteld aan ons. Zou je ons kunnen adviseren hoe te antwoorden in deze?

Ik vraag dit omdat 5.1.2.e vandaag roostervrij is en wij aanstaande vrijdag een nieuwe release van Elect iT willen ontvangen waarin deze bevinding is opgelost. Ik kopieer 5.1.2.e in zodat zij weet wat de stand van zaken is.

Met vriendelijke groet,

5.1.2.e

5.1.2.e 5.1.2.e
5.1.2.e

.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
E 5.1.2.e @kiesraad.nl
W www.kiesraad.nl

Van: 5.1.2.e <5.1.2.e @elect-it.com>
Verzonden: dinsdag 8 augustus 2023 18:18
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: [JIRA] (ELECTVAPP-2343) Pentest Hackdefense 2023 - Use of insecure random function (A2)

5.1.2.e **commented** on ELECTVAPP-2343

Re: Pentest Hackdefense 2023 - Use of insecure random function (A2)

Hi 5.1.2.e

since the "Local System" account has extensive privileges, which leads to considerable security risks if compromised, we recommend using the "Local Services" account, which is equipped with lower privileges.

What does Hackdefense say about this?

Do you agree with the proposal?

Best regards
5.1.2.e

Add Comment

This message was sent by Atlassian Jira (v8.20.25#820025-sha1:6313616)

From: "5.1.2.e"
Sent: Wed, 9 Aug 2023 13:34:06 +0200
To: "5.1.2.e" <5.1.2.e@kiesraad.nl>
Cc: "5.1.2.e" <5.1.2.e@kiesraad.nl>; "5.1.2.e" <5.1.2.e@kiesraad.nl>
Subject: RE: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense
Attachments: O23077 HackDefense - voorstel pentest OSV2020-U.pdf

Hoi 5.1.2.e

Bijgaand de getekende versie.

Gr 5.1.2.e

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Verzonden: woensdag 9 augustus 2023 12:29
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: FW: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hi collega's van Office,
Zouden jullie ajb bijgevoegde offerte willen ondertekenen met mijn e-handtekening? Zouden jullie de getekende versie willen delen met 5.1.2.e en 5.1.2.e?
Dank en groeten, 5.1.2.e

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Verzonden: woensdag 9 augustus 2023 10:03
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: FW: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

Op verzoek van 5.1.2.e is de offerte van Hack Defense tekstueel nog aangepast.

In de bijlage tref je de aanvullende offerte van Hack Defense om een code review uit te voeren op de OSV2020 software.
Dit type review valt binnen de scope van de raamovereenkomst, maar behoort niet tot de standaard pentest.

Graag een akkoord op de offerte zodat er een verplichtingen nummer aangemaakt kan worden.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: dinsdag 8 augustus 2023 17:16
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>

CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

Bijgaand een aangepaste versie (5.0). Identiek aan 4.0 alleen de tweede alinea van de managementsamenvatting heb ik conform onderstaande als volgt aangepast:

Dit vormt een uitbreiding op de omschreven aanpak in de "Standaard Pentest OSV" uit 2020. Er is een toevoeging in de telsystematiek n.a.v. de nieuwe Wet NPVV en op verzoek van de Kiesraad zijn er enkele onderzoeksvragen bijgekomen waarvan een Secure Code Review de belangrijkste is.

Is dat voldoende helder?

Dank!

5.1.2.e

On 03/08/2023 10:49, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Nog dank voor de offerte. Ik heb inmiddels een nieuwe verplichtingen nummer aan laten maken en de offerte voor akkoord aangeboden.
>
> Nu waren er nog een paar vragen, dan wel opmerkingen over de offerte. Zou jij die kunnen adresseren en eventueel een gewijzigde offerte sturen?
>
> Mochten er nog vragen zijn, dan hoor ik het graag.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e
>
> Afwezig op vrijdag
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Verzonden:** woensdag 2 augustus 2023 21:44
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Onderwerp:** RE: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense
>
> Hoi 5.1.2.e
>
> Dank voor de toelichting. Heb het gelezen. Op zich akkoord, maar zou het fijn vinden als in de offerte wat preciezer wordt omschreven:

- dat in de managementsamenvatting wat ‘enkele zaken zijn aangepast’ concreet wordt omschreven. Ik lees dat ook niet terug in de rest van de offerte.
- ook de omschrijving ‘ dat er enkele vragen zijn bijgekomen die buiten de scope vallen’ zou ik expliciteren dat ‘ op verzoek van de Kiesraad er enkele onderzoeksvragen zijn bijgekomen..’

Groet,

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Datum: woensdag 02 aug. 2023 4:11 PM
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e
<5.1.2.e @kiesraad.nl>
Onderwerp: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

In de bijlage een aanvullende offerte van Hackdefense voor het secure code onderzoek in OSV2020.

De secure code onderzoek is binnen de scope van de raamovereenkomst, maar valt niet binnen de standaard pentest requirements. Vandaar dat Hackdefense hier een aanvullende offerte voor heeft gemaakt, die voldoet aan de criteria zoals opgenomen in de raamovereenkomst.

Kan jij goedkeuring geven aan deze offerte (laten tekenen) zodat ik dit door kan sturen naar Hackdefense, inclusief het verplichtingen nummer.

Als er nog vragen zijn, dan hoor ik dat graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 15:33
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Ik heb een verplichting aangemaakt voor de tweede factuur: nummer **401002-33197.**

Verzoek aan HackDefense om dit ook te vermelden op de e-factuur.

Verder het verzoek om de offerte nog te laten ondertekenen door 5.1.2.e **t.b.v. het inkoopdossier**. Alvast dank.
Groet, 5.1.2.e

Nog even hierbij de volledige financiële gegevens:

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van **BUDGETCODERING H2B 401002 – 11312 – 44011.**
Verplichtingennummer: 401002-33197

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 31 juli 2023 12:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: 20230731 Offerte Hackdefense_uitbreiding op de pentest

Hoi collega's,

Kunnen jullie een verplichting aanmaken van €5.1.2.f excl btw voor Hackdefense? De opdracht wordt vanuit de raamovereenkomst gegund.

Wie zou dit moeten ondertekenen?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: vrijdag 28 juli 2023 14:59
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hallo 5.1.2.e

Ik zie je punt. Bijgaand aangepast, als uitbreiding op de Standaard Pentest OSV, voor zover wij het meerwerk nu al kunnen overzien (kaderstellend document komt nog).

Let wel dat OSV2020-PP niet echt een 'standalone' Java-applicatie is zoals beschreven in de aanbesteding, waar P0, P1 en P2-3 in één dag testen zouden kunnen worden gedaan. Dat blijkt toch anders (is een webapplicatie net als P4 e.a., zij het lokaal gemaakt door een complete webserver mee te installeren) waardoor ons dat best wat meer tijd kost.

5.1.2.e

On 24/07/2023 19:12, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Ik ben denk ik even afgehaakt in het mailverkeer tussen jou en 5.1.2.e
> De diverse modules van OSV, (PP, KS en U) behoren tot de Standaard pentest OSV. De secure code review niet, ik had dus een offerte verwacht voor de Secure Code Review.
>
> Of heb ik iets gemist?
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e
>
> Afwezig op vrijdag
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e@hackdefense.nl>
> **Verzonden:** vrijdag 21 juli 2023 09:58
> **Aan:** 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e@hackdefense.nl>
> **Onderwerp:** Re: offerte pentest en code review OSV2020-U
>
> Hierbij een nieuwe versie van de offerte. Wijzigingen:
>
> 1. aan het eind van hoofdstuk 1 is een randvoorwaarde toegevoegd dat de aanpak nader zal worden ingevuld in een kaderstellend document
> 2. de inhoudelijke aanpak in hoofdstuk 2 is geheel vervangen door een verwijzing naar dit kaderstellend document
> 3. bij de planning is een zin toegevoegd die aangeeft dat we ervan uitgaan dat hetgeen we in het kaderstellend document vaststellen past binnen de inschatting van het aantal benodigde dagen, en dat het dagtarief uit de raamovereenkomst van toepassing is op eventueel meerwerk, dat we uitsluitend met expliciete wederzijdse instemming uitvoeren uiteraard.
>
> 5.1.2.e

On 20/07/2023 16:53, 5.1.2.e wrote:

Goedemiddag 5.1.2.e

Hierbij onze offerte voor pentest en code review van OSV2020-U.

Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.

Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:

1. we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden
2. we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)

Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).

Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.

Dank! En fijne vakantie,

5.1.2.e

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

HackDefense

Voorstel

Pentest OSV2020-U

Kiesraad

O23077

versie 5.0 - definitief

8 augustus 2023

Copyright © 2023 HackDefense BV

Alle rechten voorbehouden. We verzoeken u om dit document vertrouwelijk te behandelen en niet te delen buiten uw organisatie.

HackDefense BV

Postbus 3025
2301 DA Leiden

(071) 204 0101

`https://hackdefense.nl/`

Offerte

Projectnaam	Pentest OSV2020-U
Opdrachtgever	Kiesraad
KvK-nummer	50200097
Offertenummer	O23077

Documentgeschiedenis

Versie	*Datum*	*Auteur*	*Omschrijving*
1.0	20 juli 2023	5.1.2.e 5.1.2.e	eerste concept
2.0	20 juli 2023	5.1.2.e	wijzigingen na interne review
3.0	21 juli 2023	5.1.2.e	wijzigingen na review opdrachtgever
4.0	28 juli 2023	5.1.2.e	wijzigingen na review opdrachtgever
5.0	8 augustus 2023	5.1.2.e	wijzigingen na review opdrachtgever

Managementsamenvatting

Binnen het kader van de raamovereenkomst voor pentesten heeft de Kiesraad aan HackDefense gevraagd om een voorstel te doen voor het testen op *security vulnerabilities* van OSV2020-U, en het adviseren van mitigerende maatregelen daaromtrent.

Dit vormt een uitbreiding op de omschreven aanpak in de "Standaard Pentest OSV" uit 2020. Er is een toevoeging in de telsystematiek n.a.v. de nieuwe Wet NPVV en op verzoek van de Kiesraad zijn er enkele onderzoeksvragen bijgekomen waarvan een Secure Code Review de belangrijkste is.

In dit document vindt u de aanpak, rapportage, en planning die HackDefense voorstelt voor het uitvoeren van deze test.

Het project zal resulteren in een gedegen rapport. Het rapport geeft onze bevindingen en aanbevelingen in technisch detail, en een managementsamenvatting voor de niet technisch onderlegde lezer.

Kosten voor het onderzoek en rapportage bedragen **€** 5.1.2.f (exclusief BTW).

Keurmerk Pentesting

HackDefense is gecertificeerd onder het "Keurmerk Pentesten", de Nederlandse pentest-standaard. Dit merk wordt onafhankelijk beheerd door het CCV (Centrum voor Criminaliteitspreventie en Veiligheid). We voeren het keurmerk in al onze beveiligingstestrapporten. Jaarlijks wordt onze kwaliteit door KIWA getoetst aan het keurmerk.

Meer informatie over dit keurmerk vindt u op `https://hetccv.nl/keurmerken/expert/keurmerk-pentesten/`.

Inhoudsopgave

Hoofdstuk 1

Uw vraag

1.1 Achtergrond

1.1.1 Organisatie

De Kiesraad treedt bij verschillende verkiezingen op als centraal stembureau. Verder is de Raad adviesorgaan en informatiecentrum op het gebied van kiesrecht en verkiezingen. Het belang van ICT-beveiliging is evident: de integriteit van het verkiezingsproces is van vitaal belang voor de Nederlandse democratie.

1.1.2 Testobject

OSV2020 is de naam voor een aantal applicaties die worden gebruikt in het verkiezingsproces. Vanzelfsprekend is de veiligheid van deze applicaties van groot belang.

OSV2020-U is de deelapplicatie die zal worden gebruikt om uitslagen en zetelverdelingen vast te stellen. OSV2020-U wordt door de Kiesraad ter beschikking gesteld aan (centraal) stembureaus in gemeenten en kieskringen.

Deze applicatie is gebouwd als webapplicatie in Java, waarbij de gebruikende organisatie (veelal gemeenten) de software installeren op een computer die los staat van het netwerk.

Het installatieprogramma zet een lokale webserver op deze computer, en een Java *runtime*. Daarin draait de applicatie. Uitvoer wordt fysiek overgebracht naar het centraal stembureau.

Genoemd installatieprogramma is nadrukkelijk ook in scope van het onderzoek. OSV2020-U wordt geleverd voor Windows, Mac OS en Linux, waarbij het onderzoek zich dient te richten op de Windows-variant. De installieprogramma's en -procedures voor Mac OS en Linux worden echter ook meegenomen.

In 2020 heeft HackDefense ook een test op OSV2020-U uitgevoerd. Nieuw is nu dat er een tweede, optionele wijze van vaststellen van de uitslag bij is gekomen (de "nieuwe procedure vaststelling verkiezingsuitslagen" ofwel NPVV), waarbij gemeenten ook de keuze hebben om voorkeurstemmen op een later moment te tellen.

1.1.3 Aanleiding testvraag

In 2020 is bij aanbesteding voorzien in een ”Standaard Pentest OSV”, uit te voeren voor elke verkiezing. Voor deze standaard pentest is reeds een opdracht verstrekt. Naast de standaard pentest zijn er enkele extra vragen, waaronder (meest belangrijk) een Secure Code Review.

Dit voorstel beschrijft de gehele opdracht die nader wordt ingevuld via een kaderstellend document.

1.2 Scope

In scope is de applicatie OSV2020-U zoals de Kiesraad deze voor aanvang aan HackDefense zal aanleveren, inclusief installatieprogramma. We installeren de applicatie in onze eigen lab-omgeving.

Ook de broncode is onderdeel van de scope. Deze zal t.z.t. (voor aanvang) worden aangeleverd, exact overeenkomend met de *live* versie van de applicatie die we testen.

1.2.1 Aanvalsperspectief

De beveiliging moet getest worden vanuit de volgende perspectieven:

1. perspectief van de *outsider*, d.w.z. zonder login-gegevens
2. perspectief van de kwaadwillende *insider* met login-gegevens (of kwaadwillende outsider die login-gegevens heeft weten te verkrijgen)

1.2.2 Testvorm

De beoogde testvorm is *white box*, dat wil zeggen dat alle informatie voor de testers beschikbaar is.

Code review is ook onderdeel van de test.

Social engineering of *Denial-of-Service attacks* (DoS of DDoS) zijn niet aan de orde en moeten op geen enkele wijze worden uitgevoerd.

Een hertest maakt geen deel uit van de opdracht. Deze is, als dit nodig of wenselijk blijkt te zijn, uiteraard wel als meerwerk uit te voeren.

1.3 Onderzoeksvraag

De in dit onderzoek te beantwoorden onderzoeksvraag luidt als volgt:

Kunnen – binnen het overeengekomen tijdsbestek – kwetsbaarheden worden gevonden in de beveiliging van OSV2020-U, waardoor ongeautoriseerden toegang tot OSV2020-U of de daarin verwerkte data zouden kunnen verkrijgen?

Beveiligingsissues die niet direct tot ongeautoriseerde toegang leiden maar die wel zouden kunnen helpen bij een inbraak, m.a.w. waarvan de oplossing tot een robuustere beveiliging leiden, moeten uiteraard ook worden gerapporteerd.

1.4 Overige randvoorwaarden

- Het rapport wordt in het Nederlands opgeleverd, met uitzondering van de individuele technische bevindingen; deze zullen in het Engels worden geschreven.
- Het onderzoek wordt uitgevoerd onder de voorwaarden van de raamovereenkomst met contractnummer 201865007.433 - P1 - HackDefense BV.
- De exacte invulling van de aanpak van de test zal medio augustus in overleg nader worden ingevuld in een kaderstellend document.

Hoofdstuk 2

Ons voorstel

Dit hoofdstuk geeft aan hoe wij voorstellen om de onderzoeksvraag te beantwoorden.

2.1 Team

Al onze pentesters zijn hbo- of wo-opgeleid en hebben tenminste het OSCP- en eWPT-certificaat.

Een van onze gecertificeerde Ethical Hackers voert de test uit. Al het werk wordt diepgaand gereviewed door onze Principal Consultant voor we u ons conceptrapport sturen.

2.2 Aanpak

De inhoudelijke aanpak van de pentest en de code review zal medio augustus in overleg nader worden ingevuld in een kaderstellend document.

2.2.1 Projectfasering

Elke beveiligingstest van HackDefense bestaat uit de volgende fasen:

- *Planning*

  Na akkoord op het voorstel plannen we in overleg de beveiligingstest in. Afhankelijk van de omvang van de opdracht kan de uitvoering snel starten, vaak al binnen twee weken.

- *Kick-off*

  Voor aanvang van de test houden we een kickoff-bijeenkomst. Bij deze kickoff wordt met de security officer en andere betrokken stakeholders nagegaan of alle benodigdheden voor de test aanwezig zijn: alle contactgegevens[1], adressen/URL's, toegang tot locaties, etc. Doel is dat alles klaar is om de uitvoer te kunnen starten.

[1] we vinden het heel belangrijk dat de penetratietesters en beheerders van elkaars directe telefoonnummers op de hoogte zijn om snel te kunnen schakelen indien nodig

- *Uitvoering test*

  In de afgesproken periode voeren we de test uit zoals afgesproken in dit voorstel. Tijdens de test worden belangrijke bevindingen met de Kiesraad gedeeld zodat waar nodig direct actie kan worden ondernomen.

- *Rapportagefase*

  Na afloop van de test schrijven we ons rapport in concept. Het eerste concept wordt intern gereviewed door een Principal Consultant. Het definitieve conceptrapport bieden we aan de Kiesraad aan voor review.

- *Rapportbespreking en definitieve oplevering*

  We bespreken het rapport en op basis van de feedback vanuit de Kiesraad maken we het rapport definitief.

- *Evaluatie*

  Na oplevering van het definitieve rapport vragen we u om ons te beoordelen met een cijfer tussen 0 en 10. Waar nodig bespreken we na wat er goed ging en waar er eventueel verbeterpunten liggen, zodat we de volgende test nog beter kunnen uitvoeren.

2.2.2 Rapportage

Het rapport geeft in de eerste plaats antwoord op de onderzoeksvraag en bestaat uit de volgende hoofdstukken:

- *Managementsamenvatting* – samenvatting in twee of drie alinea's zonder technische terminologie.
- *Uw vraag* – weergave van de onderzoeksvraag en de scope; dit hoofdstuk omschrijft wat er precies is getest.
- *Onze bevindingen* – verslag van de werkzaamheden: de aanpak, en onze analyse.
- *Conclusies en aanbevelingen* – het antwoord op de onderzoeksvraag, en een solide advies voor de weg voorwaarts.
- *Bijlage: technische bevindingen* – alle individuele bevindingen, in technisch detail, bestaand uit de onderdelen:
  - *Omschrijving* - korte samenvatting van het issue
  - *Risico-inschatting* - een inschatting van het risico op basis van kans (hoe moeilijk is dit issue te misbruiken) en impact (wat kan een aanvaller doen), inclusief de CVSS-score [2]
  - *Betreft de systemen* of *Betreft de pagina's* - concrete opsomming van IP-adressen, systeemnamen of componenten van een applicatie waarop het omschreven issue van toepassing is
  - *Waarneming* - precieze waarneming, wat hebben we gezien en hoe is dit reproduceerbaar. Waar mogelijk met technische commando's en/of screenshots.

[2] `https://first.org/cvss/`

- *Aanbeveling* - zo exact mogelijk technisch advies hoe dit issue op te lossen is

Als er vragen zijn bij lezing van het rapport of concrete technische hulp nodig is bij het implementeren van onze aanbevelingen dan verlenen we deze hulp - binnen de grenzen van het redelijke - kostenloos.

Naast individuele bevindingen geeft het rapport inzicht in de algemene situatie van de beveiliging van het onderzoeksobject. Daartoe geeft het een heldere samenvatting van hetgeen geconstateerd is, en hoe zich dat verhoudt tot het te verwachten beveiligingsniveau in vergelijkbare toepassingen.

Het rapport wordt u eerst in concept aangeboden. Op basis van uw reactie worden eventueel aanpassingen gedaan. In het (zeldzame) geval dat we uw feedback niet in ons rapport kunnen overnemen zullen we uw reactie als zodanig letterlijk vermelden in het definitieve rapport.

Ernstige bevindingen worden uiteraard direct gemeld en niet pas bij de rapportage. Ook ontvangt u aan het eind van elke testdag een korte samenvatting.

2.3 Planning

We denken de volgende hoeveelheid inzet nodig te hebben:

testsoort	*uren inzet t.o.v. standaardtest*	
	inclusief	*extra*
voorbereiden white box, document review	8	
installatie testobject in lab-omgeving	8	
webapplicatietest	40	24
code review		64
configuratie-review		16
extra: NPVV		8
totaal tests	56	112
rapportage	24	16
QA/review	8	
totaal	88	128

Medio augustus zullen we in overleg in een kaderstellend document de aanpak nader uitwerken. Mocht daarbij blijken dat bovenstaande inschatting niet voldoende is, dan kan meerwerk worden uitgevoerd (na wederzijdse schriftelijke bevestiging) tegen het bij raamovereenkomst overeengekomen dagtarief (zie onder).

2.4 Kosten

In de vorige paragraaf heeft u gelezen dat we 216 uur benodigde inzet verwachten.

Daarvan is 88 uur al inbegrepen in de bestaande opdracht. 128 uur vormt een uitbreiding daarop, voor zover wij dat kunnen overzien vooruitkijkend naar het kaderstellend document.

Het binnen de raamovereenkomst afgesproken dagtarief is € 5.1.2.f Totale kosten komen daardoor uit op **€** 5.1.2.f

(alle bedragen zijn exclusief BTW)

Binnen redelijke grenzen vallen alle uit te voeren werkzaamheden binnen deze vaste prijs; voor onderling schriftelijk nader overeengekomen meerwerk rekenen wij het genoemde tarief.

2.5 Overig

Deze opdracht zal worden uitgevoerd conform de in 2020 gesloten raamovereenkomst voor pentesting (kenmerk 201865007.433 - P1 - HackDefense BV).

Hoofdstuk 3

Tot slot

We zien ernaar uit u bij deze belangrijke opdracht te kunnen ondersteunen. Heeft u nog vragen of opmerkingen, aarzel niet om te bellen met 5.1.2.e of 5.1.2.e bereikbaar via (071) 204 0101.

Als u akkoord bent met dit voorstel verzoek ik u om een getekend exemplaar te retourneren.

Voor akkoord:

Naam:	5.1.2.e
Functie:	5.1.2.e
Datum:	09-08-2023
Namens:	Kiesraad *KvK-nummer 50200097*
Offertenummer:	O23077 v5.0
Handtekening:	5.1.2.e 

From: "5.1.2.e "
Sent: Wed, 9 Aug 2023 15:08:00 +0200
To: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: RE: FW: [JIRA] (ELECTVAPP-2343) Pentest Hackdefense 2023 - Use of insecure random function (A2)

Hi 5.1.2.e

Veel dank voor je snelle en duidelijke reactie!

Groet, 5.1.2.e

5.1.2.e 5.1.2.e
5.1.2.e

.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
E 5.1.2.e @kiesraad.nl
W www.kiesraad.nl

FOLLOW US ON twitter

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: woensdag 9 augustus 2023 13:48
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: FW: [JIRA] (ELECTVAPP-2343) Pentest Hackdefense 2023 - Use of insecure random function (A2)

Ja, geheel eens, in de bevinding staat ook "Local Service" en niet "Local System".

Dus, ja. :)

5.1.2.e

On 09/08/2023 11:35, 5.1.2.e wrote:

> Beste 5.1.2.e
>
> Jullie pentest voor OSV2020 PP heeft een drietal bevindingen opgeleverd met de kwalificaties hoog, midden en laag risico. Hoog en laag zijn volgens Elect iT al opgelost. De bevinding met de kwalificatie midden levert nog discussie op. In onderstaande mail van Elect iT wordt een vraag gesteld aan ons. Zou je ons kunnen adviseren hoe te antwoorden in deze?
>
> Ik vraag dit omdat 5.1.2.e vandaag roostervrij is en wij aanstaande vrijdag een nieuwe release van Elect iT willen ontvangen waarin deze bevinding is opgelost. Ik kopieer 5.1.2.e in zodat zij weet wat de stand van zaken is.
>
> Met vriendelijke groet,

5.1.2.e

5.1.2.e 5.1.2.e
5.1.2.e

.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
E 5.1.2.e @kiesraad.nl
W www.kiesraad.nl

FOLLOW US ON twitter

Van: 5.1.2.e <5.1.2.e @elect-it.com>
Verzonden: dinsdag 8 augustus 2023 18:18
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: [JIRA] (ELECTVAPP-2343) Pentest Hackdefense 2023 - Use of insecure random function (A2)

5.1.2.e **commented** on ELECTVAPP-2343

Re: Pentest Hackdefense 2023 - Use of insecure random function (A2)

Hi 5.1.2.e

since the "Local System" account has extensive privileges, which leads to considerable security risks if compromised, we recommend using the "Local Services" account, which is equipped with lower privileges.

What does Hackdefense say about this?

Do you agree with the proposal?

Best regards
5.1.2.e

Add Comment

This message was sent by Atlassian Jira (v8.20.25#820025-sha1:6313616)

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Wed, 9 Aug 2023 16:04:03 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Veel dank!

Ik cc mijn collega 5.1.2.e die e.e.a. afhandelt v.w.b. facturatie/administratie.

Voor de uitvoering hebben wij als ik het goed heb volgende week een overleg staan met 5.1.2.e over het kaderdocument.

5.1.2.e

On 09/08/2023 16:00, 5.1.2.e wrote:

> Beste 5.1.2.e
>
> Onderstaand het verplichtingennummer en de voorwaarden met betrekking tot e-facturatie. Dit nummer geldt voor zowel de pen-test als de aanvullende opdracht met betrekking tot de secure code onderzoek.
>
> Mochten er nog vragen zijn, laat het weten
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> .....
> **T** 5.1.2.e
>
> Afwezig op vrijdag
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Verzonden:** woensdag 9 augustus 2023 15:21
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Onderwerp:** RE: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense
>
> Bij deze (nogmaals) de e-facturatiegegevens:
>
> Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van
>
> **BUDGETCODERING H2B 401002 – 11312 – 44011.**
> **Verplichtingennummer: 401002-33197**
>
> Geadresseerd aan:
>
> *Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad*
> *T.a.v. het Financieel Dienstencentrum (FDC)*

Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 9 augustus 2023 10:03
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e
<5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: FW: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

Op verzoek van 5.1.2.e is de offerte van Hack Defense tekstueel nog aangepast.

In de bijlage tref je de aanvullende offerte van Hack Defense om een code review uit te voeren op de OSV2020 software.
Dit type review valt binnen de scope van de raamovereenkomst, maar behoort niet tot de standaard pentest.

Graag een akkoord op de offerte zodat er een verplichtingen nummer aangemaakt kan worden.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 8 augustus 2023 17:16
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

Bijgaand een aangepaste versie (5.0). Identiek aan 4.0 alleen de tweede alinea van de managementsamenvatting heb ik conform onderstaande als volgt aangepast:

Dit vormt een uitbreiding op de omschreven aanpak in de "Standaard Pentest OSV" uit 2020. Er is een toevoeging in de telsystematiek n.a.v. de nieuwe Wet NPVV en op verzoek van de Kiesraad zijn er enkele onderzoeksvragen bijgekomen waarvan een Secure Code Review de belangrijkste is.

Is dat voldoende helder?

Dank!

5.1.2.e

On 03/08/2023 10:49, 5.1.2.e wrote:

Hallo 5.1.2.e

Nog dank voor de offerte. Ik heb inmiddels een nieuwe verplichtingen nummer aan laten maken en de offerte voor akkoord aangeboden.

Nu waren er nog een paar vragen, dan wel opmerkingen over de offerte. Zou jij die kunnen adresseren en eventueel een gewijzigde offerte sturen?

Mochten er nog vragen zijn, dan hoor ik het graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 21:44
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: RE: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Dank voor de toelichting. Heb het gelezen. Op zich akkoord, maar zou het fijn vinden als in de offerte wat preciezer wordt omschreven:
- dat in de managementsamenvatting wat ‘enkele zaken zijn aangepast’ concreet wordt omschreven. Ik lees dat ook niet terug in de rest van de offerte.
- ook de omschrijving ‘ dat er enkele vragen zijn bijgekomen die buiten de scope vallen’ zou ik expliciteren dat ‘ op verzoek van de Kiesraad er enkele onderzoeksvragen zijn bijgekomen..’

Groet,

5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Datum: woensdag 02 aug. 2023 4:11 PM
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e@kiesraad.nl>, 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: FW: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hallo 5.1.2.e

In de bijlage een aanvullende offerte van Hackdefense voor het secure code onderzoek in OSV2020.

De secure code onderzoek is binnen de scope van de raamovereenkomst, maar valt niet binnen de standaard pentest requirements. Vandaar dat Hackdefense hier een aanvullende offerte voor heeft gemaakt, die voldoet aan de criteria zoals opgenomen in de raamovereenkomst.

Kan jij goedkeuring geven aan deze offerte (laten tekenen) zodat ik dit door kan sturen naar Hackdefense, inclusief het verplichtingen nummer.

Als er nog vragen zijn, dan hoor ik dat graag.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: woensdag 2 augustus 2023 15:33
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Verplichtingnr. en verzoek ondertekening Offerte Hackdefense

Hoi 5.1.2.e

Ik heb een verplichting aangemaakt voor de tweede factuur: nummer **401002-33197.**

Verzoek aan HackDefense om dit ook te vermelden op de e-factuur.

Verder het verzoek om de offerte nog te laten ondertekenen door 5.1.2.e **t.b.v. het inkoopdossier**.
Alvast dank. Groet, 5.1.2.e

Nog even hierbij de volledige financiële gegevens:

Uw e-factuur kan worden aangeleverd aan het centrale aanleverpunt voor facturen Digipoort onder vermelding van **BUDGETCODERING H2B 401002 – 11312 – 44011.**
Verplichtingennummer: 401002-33197

Geadresseerd aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties / Kiesraad
T.a.v. het Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED Den Haag

Het voor uw factuur benodigde OIN-nummer: 00000001003214345000.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 31 juli 2023 12:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: 20230731 Offerte Hackdefense_uitbreiding op de pentest

Hoi collega's,

Kunnen jullie een verplichting aanmaken van €5.1.2.f excl btw voor Hackdefense? De opdracht wordt vanuit de raamovereenkomst gegund.

Wie zou dit moeten ondertekenen?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: vrijdag 28 juli 2023 14:59
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hallo 5.1.2.e

Ik zie je punt. Bijgaand aangepast, als uitbreiding op de Standaard Pentest OSV, voor zover wij het meerwerk nu al kunnen overzien (kaderstellend document komt nog).

Let wel dat OSV2020-PP niet echt een 'standalone' Java-applicatie is zoals beschreven in de aanbesteding, waar P0, P1 en P2-3 in één dag testen zouden kunnen worden gedaan. Dat blijkt toch anders (is een webapplicatie net als P4 e.a., zij het lokaal gemaakt door een complete webserver mee te installeren) waardoor ons dat best wat meer tijd kost.

5.1.2.e

On 24/07/2023 19:12, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Ik ben denk ik even afgehaakt in het mailverkeer tussen jou en 5.1.2.e
> De diverse modules van OSV, (PP, KS en U) behoren tot de Standaard pentest OSV. De secure code review niet, ik had dus een offerte verwacht voor de Secure Code Review.

Of heb ik iets gemist?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: vrijdag 21 juli 2023 09:58
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: offerte pentest en code review OSV2020-U

Hierbij een nieuwe versie van de offerte. Wijzigingen:

1. aan het eind van hoofdstuk 1 is een randvoorwaarde toegevoegd dat de aanpak nader zal worden ingevuld in een kaderstellend document
2. de inhoudelijke aanpak in hoofdstuk 2 is geheel vervangen door een verwijzing naar dit kaderstellend document
3. bij de planning is een zin toegevoegd die aangeeft dat we ervan uitgaan dat hetgeen we in het kaderstellend document vaststellen past binnen de inschatting van het aantal benodigde dagen, en dat het dagtarief uit de raamovereenkomst van toepassing is op eventueel meerwerk, dat we uitsluitend met expliciete wederzijdse instemming uitvoeren uiteraard.

5.1.2.e

On 20/07/2023 16:53, 5.1.2.e wrote:

> Goedemiddag 5.1.2.e
>
> Hierbij onze offerte voor pentest en code review van OSV2020-U.
>
> Na veel uitzoekwerk bleek de vraag behoorlijk gelijk aan de "specifieke pentest" uit de uitvraag in 2020. Die ging toch alleen over een pentest inclusief security code review van het "tweede deel van Vervanging OSV", wat voorzien was om het equivalent te zijn van OSV2020-U.
>
> Wij hebben toen (voor eigen rekening) wel wat meer tijd besteed door allerlei omstandigheden, maar we verwachten dat dat nu wel binnen de perken blijft. We hebben daarom hetzelfde voorgesteld als in 2020 qua urenbudget en prijs, met enkele verschillen:
>
> 1. we hebben 1 dag toegevoegd voor NPVV, de nieuwe optionele telmethode waarover we eerder mailden

2. we hebben de OWASP ASVS vervangen door de OWASP Top 10, omdat de ASVS in 2020 erg veel meerwerk kostte (bijv. interviews met de developers) waar eigenlijk heel weinig uitkwam (en omdat jij in ons gesprek al aangaf de ASVS niet zo nodig te vinden)

Het dagtarief is ook behoorlijk lager dan waar wij inmiddels 3 jaar later zitten, maar uiteraard blijft het tarief uit 2020 gelden zoals bepaald in de raamovereenkomst (€5.1.2.f per dag), ook voor eventueel meerwerk in een later stadium (zoals een mogelijke hertest).

Zoals besproken staat deze opdracht (gecombineerde pentest/code review) nu bij ons gepland van 31 augustus tot en met 14 september.

Dank! En fijne vakantie,

5.1.2.e

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | https://hackdefense.nl/
HackDefense BV | Postbus 3025 | 2301 DA Leiden

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Mon, 14 Aug 2023 16:11:12 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: kun jij prestatie verklaren op de factuur van hackdefense? Afgelopen vrijdag opnieuw naar je gestuurd. Verplichting is opgehoogd. Dank alvast

Ja, zo heb ik hem inmiddels begrepen, maar was mij aanvankelijk niet helemaal duidelijk. Deze factuur is tijdens mijn vakantie verstuurd omdat PP was afgerond, denkende dat deze opdracht alleen op PP betrekking had. Maar die opdracht omvat dus inderdaad meer.

Geen probleem om de betaling "on hold" te zetten tot na de test van -U.

5.1.2.e

On 14/08/2023 15:21, 5.1.2.e wrote:

> In aanvulling op 5.1.2.e
>
> De pentesten van zowel PP als U zijn nu als 1 opdracht geformuleerd. Dus de factuur voor de beide *pentesten* is 1 factuur voor beide (PP en U).
>
> De *code review* van module U is een aparte opdracht met een aparte factuur. Ook al is het eindresultaat gebundeld in dezelfde rapportage als de pentest van U.
>
> Hoop dat dit helpt.
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Verzonden:** maandag 14 augustus 2023 15:19
> **Aan:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **CC:** 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
> **Onderwerp:** FW: kun jij prestatie verklaren op de factuur van hackdefense? Afgelopen vrijdag opnieuw naar je gestuurd. Verplichting is opgehoogd. Dank alvast
>
> Beste 5.1.2.e
>
> Ik begrijp van onze bedrijfsvoering dat er reeds een factuur ontvangen was voor de pentest van de OSV applicatie.
>
> Nu is het gewoon binnen de overheid, dat een factuur binnen 30 dagen betaald wordt, maar wel nadat de dienstverlening is afgerond.
> Nu hadden wij deze factuur verwacht nadat de prestatie is afgerond, in dit geval de oplevering van de definitieve eindraportage, dit staat als het goed werkt op 14 september gepland.
>
> Wij zullen dan ook de betaling on-hold zetten totdat dit gebeurt is.
> Kan jij jullie financiële afdeling hiervan op de hoogte stellen?
>
> Alvast bedankt.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e

.....
T 5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 14 augustus 2023 15:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: kun jij prestatie verklaren op de factuur van hackdefense? Afgelopen vrijdag opnieuw naar je gestuurd. Verplichting is opgehoogd. Dank alvast

Met vriendelijke groet,

5.1.2.e
Adviseur bedrijfsvoering
.....
KIESRAAD
Bezoekadres: Zürichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
T 5.1.2.e
5.1.2.e @kiesraad.nl
www.kiesraad.nl
.....
Afwezig op donderdag

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Tue, 15 Aug 2023 13:31:41 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Re: Bevestigen verwijderen testdata module PP

Ha 5.1.2.e ja is goed, om het helemaal zeker te weten heb ik 5.1.2.e nodig en die is maandag weer terug van vakantie. Voor ik dat verklaar wil ik weten dat hij niks meer op zijn laptop heeft.

(kan op zich niks mee gebeuren want staat uit & encrypted, maar als ik zeg dat het weg is, wil ik ook zeker weten dat het weg is :))

5.1.2.e

On 11/08/2023 13:56, 5.1.2.e wrote:

> 5.1.2.e
>
> Zou je mij als je tijd hebt van de week nog een bevestiging kunnen sturen dat alle testdata voor de module PP van jullie infra is verwijderd? Dit is conform het kaderdocument de afspraak 😊. Formeel mag het uiterlijk een maand na de test, maar ik denk dat jullie het nu toch niet meer gaan gebruiken. Dus ik vraag het even voor de zekerheid.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo
> .....
> **KIES**RAAD
> Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
> Postadres: Postbus 20011, 2500 EA Den Haag
> .....
> T 5.1.2.e
> W www.kiesraad.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e "
Sent: Tue, 22 Aug 2023 15:15:06 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>; "5.1.2.e 5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: RE: Modules van U voor pentest en code review

Hallo 5.1.2.e

Dank voor de indicatie van het extra werk.
Kan je dit op basis van een fixed price aanvulling voor ons in een offerte gieten?
Dan kunnen we dit na intern akkoord toevoegen aan de reeds aangemaakte financiële verplichting.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: dinsdag 22 augustus 2023 14:13
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Modules van U voor pentest en code review

5.1.2.e

Dank voor je mail. Zoals besproken goed om onderstaande even af te stemmen met 5.1.2.e

Ik heb de definitieve versie van de kaders zojuist per secure transfer naar je gestuurd. Belangrijkste aanpassing zit onder het kopje “opzet”. Zou je deze voor de zekerheid nog even willen dubbelchecken dat we hetzelfde beeld hebben?

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 22 augustus 2023 14:04
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: Modules van U voor pentest en code review

Ha 5.1.2.e en 5.1.2.e

Na dit besproken te hebben met ons team en gisteren nogmaals met 5.1.2.e denk ik dat het wijs is om voor deze test een extra ethisch hacker in te zetten. Op basis van het onderstaande kan ik best denken dat het wel meevalt, maar in termen van 'lines of code' e.d. weten we het gewoon nog niet, omdat pas a.s. maandag de code komt en we dan direct moeten beginnen.

Om het risico van uitloop dus minimaal te houden zal ik voor de zekerheid een extra tester erbij trekken van dinsdag 29/8 tot en met donderdag 7/9. Dan heb je het dus over 8 dagen meerwerk, tegen afgesproken tarief van €5.1.2.f is dat dan €5.1.2.f

Indien dat akkoord is voor jullie zal ik dat zo organiseren, en van de extra persoon (waarschijnlijk 5.1.2.e 5.1.2.e een VOG laten sturen.

5.1.2.e

On 18/08/2023 11:36, 5.1.2.e wrote:

> Hi 5.1.2.e
>
> Hieronder een korte uitleg voor de Tweede Kamer verkiezing (wijzigt namelijk per verkiezingstype):
>
> 1. De de happy flow was GSB > HSB > CSB. Daar is het Nationaal Briefstembureau (NBSB) bijgekomen. In 2021 bij jullie eerdere test zat briefstemmen voor Nederlanders in het buitenland in de GSB module voor de gemeente Den Haag. Den Haag vond dit ongewenst omdat niet duidelijk was wat nu het resultaat van de gemeente Den Haag was en wat het resultaat van het briefstemmen voor Nederlanders in het buitenland was. Daarom is het NBSB met 4 briefstembureaus (Curacao, Aruba, Sint Maarten en Den Haag zelf – apart loket) ingesteld. Het NBSB totaliseert de resultaten van de vier briefstembureaus, net als het GSB van stembureaus. Daardoor lijkt het voor een groot gedeelte op een GSB met dezelfde optelfunctionaliteit. Alleen zijn enkele functionaliteiten iets anders, zoals de typering van sommige velden, geen keuze tussen centraal en decentraal tellen, aantal kiesgerechtigden op totaal niveau (bij GSB mogelijk op stembureau niveau). En natuurlijk documenten die niet spreken van een gemeentelijk stembureau maar van een nationaal briefstembureau
> 2. Daarnaast heeft de wetgever vanaf 1 januari 2023 het centraal stembureau (Kiesraad voor Tweede Kamer verkiezing) de mogelijkheid gegeven om het GSB een opdracht te geven om een onderzoek te doen als er vermoedens zijn dat er fouten zitten in het proces-verbaal van een stembureau of van het GSB zelf. Het GSB doet een onderzoek en voert eventueel een correctie door in het GSB resultaat. Deze correctie gaat in één keer door naar het CSB en niet naar het HSB zoals in de happy flow. Verder heeft de wetgever bepaald dat het CSB dan een correctie moet doorvoeren voor het HSB (nieuw document en nieuw bestand). Daarom moet de Kiesraad ook over een HSB-c module beschikken die voor een groot gedeelte op de reguliere HSB module lijkt maar andere output genereert. Het CSB moet het resultaat van GSB's kunnen aanpassen en daarmee ook het totaal resultaat van het HSB
> 3. Zoals hierboven beschreven gaat het ook bij het NBSB. CSB geeft opdracht rechtstreeks aan briefstembureau (maakt geen gebruik van OSV2020, net als een stembureau) voor onderzoek, ontvangt eventueel correctie retour (papieren document) en moet dan het resultaat van het NBSB gaan aanpassen. Uit de NBSB-c module komt dan, net als uit de HSB-c module, een corrigendum en een nieuw digitaal bestand
> 4. En dan de laatste module HSBB. De CSB module van OSV2020 kan niet omgaan met subtotalen. Voor kieskring 12 (Den Haag) bestaat het totaal resultaat uit het resultaat van het GSB Den Haag en het NBSB. Het resultaat van het GSB Den Haag gaat naar het HSB Den Haag. Maar het resultaat van het NBSB gaat rechtstreeks naar het CSB. Daarom is er een extra module (eigenlijk een reguliere HSB module) die alleen voor intern gebruik van de Kiesraad is. Deze module telt het resultaat van het GSB Den Haag en het resultaat van het NBSB bij elkaar op om zo het totaalresultaat voor kieskring 12 te berekenen. Het resultaat daarvan moet vervolgens worden ingevoerd in de CSB module.
>
> Ik heb de opzet zo kort en duidelijk mogelijk proberen te verwoorden maar kan mij voorstellen dat je hierover nog vragen hebt. Het belangrijkste is dat de happy flow vanaf 1 januari 2023 is doorbroken omdat ook teruggegaan kan worden in het proces en dan dus ook correcties mogelijk moeten zijn. Dan verandert de uitvoerende instantie (van HSB en NBSB naar CSB) en heeft die uitvoerende instantie ook modules nodig om die correctie door te voeren (HSB-c en NBSB-c). Ik ben graag bereid om een en ander verder toe te lichten.

Groet, 5.1.2.e

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: donderdag 17 augustus 2023 14:01
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Modules van U voor pentest en code review

5.1.2.e

Van wat ik begrijp lijken ze wel sterk op elkaar wat betreft, maar zijn er kleine verschillen in functionaliteit en ook relevantie/belang in het verkiezingsproces.

@5.1.2.e kan jij hier wellicht iets meer over toelichten?

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: donderdag 17 augustus 2023 13:57
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: Modules van U voor pentest en code review

Ha 5.1.2.e

We gaan ons best doen. Hebben jullie al een indicatie van de omvang van die nieuwe modules?

> Op 17 aug. 2023 om 13:19 heeft 5.1.2.e <5.1.2.e @kiesraad.nl> het volgende geschreven:
>
> 5.1.2.e
>
> We begrijpen dat een en ander kort dag is en dat het meer werk gaat opleveren, maar zouden jullie de mogelijkheid hebben om de volgende modules in dezelfde week te testen en de code review te doen?

Modules OSV2020 uitslagvaststelling Tweede Kamer verkiezing		
Voorheen tot 1 januari 2023		
GSB	Totaliseren van stembureau resultaten op gemeentelijk niveau	Beheerd door Gemeentelijk Stembureau
HSB	Totaliseren van gemeentelijke resultaten op kieskring niveau	Beheerd door Hoofd stembureau (bijvoorbeeld of Den Helder)
CSB	Totaliseren van kieskring resultaten tot nationaal niveau en zetelberekening	Beheerd door Centraal Stembureau (kiesraa
Vanaf 1 januari 2023		
GSB	Totaliseren van stembureau resultaten op gemeentelijk niveau	Beheerd door Gemeentelijk Stembureau

HSB	Totaliseren van gemeentelijke resultaten op kieskring niveau	Beheerd door Hoofd stembureau (bijvoorbeeld of Den Helder)
CSB	Totaliseren van kieskring resultaten tot nationaal niveau en zetelberekening	Beheerd door Centraal Stembureau (kiesraa
NBSB	Totaliseren van briefstemmen (Nederlanders in het buitenland)	Beheerd door het Nationaal Brief Stembure (gevestigd in Den Haag)
NBSB-c	Correctie doorvoeren voor Nationaal Brief Stembureau (NBSB module met output corrigendum en nieuw bestand)	Beheerd door Centraal stembureau (kiesraa
HSB-c	Correctie doorvoeren voor Hoofdstembureau (HSB module met output corrigendum en nieuw bestand)	Beheerd door Centraal stembureau (kiesraa
HSBB	Totaliseren resultaat gemeente Den Haag + briefstemmen voor kieskring 12 (HSB module die resultaat gemeente Den Haag en resultaat briefstemmen bij elkaar optelt)	Beheerd door Centraal stembureau (kiesraa

Uit de vorige rapportage haal ik dat jullie de vorige keer hebben getest (zie bijlage) haal ik niet welke van de drie modules (of alle drie) zijn getest. Daarin lijken jullie modules te hebben getest van twee verschillende verkiezingen (TK en GR?). Zou je dat nog kunnen nagaan voor ons?

Kan je mij vertellen of het überhaupt mogelijk is om alle bovenstaande modules in dezelfde week te testen en mee te nemen in het rapport? En wat zouden daarvoor de kosten zijn aan meer werk? Dan gaan we dat alsnog intern zsm proberen te regelen.

Excuses dat dit zo last minute naar boven is gekomen.

Met vriendelijke groet,

5.1.2.e
5.1.2.e

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo

<image003.png>
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by

mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

<Rapport+beveiligingstest+OSV2020-U+TK.pdf>

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Wed, 23 Aug 2023 15:20:05 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Schriftelijke bevestiging vernietiging aangeleverde data OSV2020-PP
Attachments: Bevestiging_vernietiging.pdf

Hi 5.1.2.e

In de bijlage staat een schriftelijke bevestiging over de vernietiging van de aangeleverde data.

Met vriendelijke groet / With kind regards,

HackDefense

5.1.2.e
5.1.2.e

M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

HackDefense

IT security, maar dan begrijpelijk

HackDefense BV
Postbus 3025, 2301 DA Leiden
(071) 204 0101
info@hackdefense.nl
https://hackdefense.nl/

IBAN: NL40 RABO 0337 2727 00
KvK: 69477043
BTW: NL857887270B01

Kiesraad
t.a.v. mw van 5.1.2.e
Per e-mail: 5.1.2.e @kiesraad.nl

Leiden, 23-08-2023

Geachte 5.1.2.e

Hierbij bevestigen wij dat HackDefense op 23 augustus 2023 alle ontvangen data van de Kiesraad over *"OSV2020-PP 2023"* heeft verwijderd. Dit houdt in dat de geïnstalleerde applicaties en het ZIP-bestand, bestaande uit de installatiebestanden en handleidingen verwijderd zijn.

Met vriendelijke groet,

5.1.2.e

5.1.2.e

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Mon, 28 Aug 2023 11:14:41 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "'5.1.2.e '" <5.1.2.e @hackdefense.nl>
Subject: Offerte
Attachments: Offerte O2061x Raamovereenkomst 201865007.433-P1.pdf

Beste 5.1.2.e en 5.1.2.e

Hierbij de offerte voor de extra inzet Ethisch Hacker van HackDefense.
Ik zal de VOG direct van 5.1.2.e zsm naar jullie toesturen.

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e 5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

HackDefense

IT security, maar dan begrijpelijk

HackDefense BV
PO Box 3025, 2301 DA Leiden
(071) 204 0101
info@hackdefense.com
www.hackdefense.com

IBAN: NL40 RABO 0337 2727 00
KvK: 69477043
BTW: NL857887270B01

Kiesraad

t.a.v. 5.1.2.e & 5.1.2.e

5.1.2.e @kiesraad.nl

5.1.2.e @kiesraad.nl

Offerte: Inzet extra ethisch hacker

Geachte 5.1.2.e en 5.1.2.e beste 5.1.2.e en 5.1.2.e

Naar aanleiding van ons gesprek van vorige week, bevestigen we de inzet van een extra ethisch hacker (5.1.2.e) door HackDefense bij de Kiesraad op de pentest/ secure code review van OSV2020-U.

Inzet;

Dinsdag 29 augustus 2023 tot en met donderdag 7 september 2023

8 dagen meerwerk

Geldend dagtarief: €5.1.2.f

Totaal extra kosten (vaste prijs) €5.1.2.f

Deze hertest zal plaatsvinden onder de voorwaarden van onze raamovereenkomst met nummer 201865007.433–P1 en nadere overeenkomst 201865007.433.001

Als u akkoord bent met dit voorstel of vragen/ opmerkingen heeft, dan gelieve dit schriftelijk aan mij mee te delen via 5.1.2.e @hackdefense.nl.

We danken u nogmaals voor het in ons gestelde vertrouwen en zien uit naar de voorzetting van onze plezierige samenwerking.

Met vriendelijke groet,

5.1.2.e

HackDefense BV

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Thu, 31 Aug 2023 11:10:02 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @hackdefense.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: Broncode OSV2020-U

Hoi 5.1.2.e

Super! Dank voor de moeite.

Excuses wat betreft de samenvatting, ik was dat inderdaad vergeten te doen. Bij deze:

- We hebben een XXE gevonden in de XML upload. Het lijkt mee te vallen want we kunnen de server er enkel een request mee naar ons laten maken. Wij zijn nog bezig om te kijken of we dit uit kunnen breiden naar Local File Inclusion.
- We hebben een aantal issues met de airgap
    - Als we een delay van iets meer dan twee seconde introduceren in het netwerk en ICMP requests blokkeren. Dan denkt de applicatie dat hij niet verbonden is met internet terwijl dit wel het geval is.
    - De airgap checkt d.m.v. webrequests en pings naar verschillende servers of er een netwerk beschikbaar is. Bij webrequests denkt de airgap enkel dat er een netwerk verbinding is als de target server een 200 OK status teruggeeft. Iedere andere statuscode lijkt gezien te worden als een gefaalde request. Indien alle servers iets anders dan een 200 status code teruggeven denkt de airgap dat er geen internet is.
    - Als de client-side (in de browser) airgap vasttelt dat er internet beschikbaar is, dan geeft de applicatie wel een melding maar blokkeert niet.
- Als de applicatie wordt geïnstalleerd met de optie om je eigen MariaDB/MySQL database te gebruiken, heeft deze last van transaction/commit issues waardoor de applicatie niet opstart. (De meegeleverde interne database doet het wel).

Met vriendelijke groet,

5.1.2.e

On 8/31/23 9:13 AM, 5.1.2.e wrote:

> 5.1.2.e
>
> Ik was gisteren vrij en lees daarom jouw bericht nu. Ik ga erachteraan en hoop vandaag nog de maven files te kunnen leveren.
>
> Hoe staat het met de pentest? Ik zou daar als het goed is nog een samenvatting/bullets van krijgen aan het einde van elke dag, toch?
>
> Groet,
>
> 5.1.2.e
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Verzonden:** woensdag 30 augustus 2023 10:38
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Onderwerp:** Re: Broncode OSV2020-U
>
> Hoi 5.1.2.e

Ik kom een heel eind verder met de nieuwe bestanden. Maar het zou toch fijn zijn om de broncode te hebben zoals de developers er mee werken. Dat wil zeggen: zij hebben waarschijnlijk een git (of andere versiebeheer software) repository met de code. Daar zullen ook maven files (bestanden die helpen bij het compilen van de applicatie) in staan. Als ik een zip bestand zou kunnen krijgen van de code op de manier waarop de developers daar mee werken dan zou dat enorm helpen!

Met vriendelijke groet,

5.1.2.e

On 8/28/23 3:24 PM, 5.1.2.e wrote:

> Lol, ingewikkeld voor mij. 😃 smh
>
> Ga het fixen!
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e@hackdefense.nl>
> **Verzonden:** maandag 28 augustus 2023 15:24
> **Aan:** 5.1.2.e <5.1.2.e@kiesraad.nl>
> **CC:** 5.1.2.e <5.1.2.e@hackdefense.nl>; 5.1.2.e <5.1.2.e@hackdefense.nl>
> **Onderwerp:** Re: Broncode OSV2020-U
>
> Het is nu naar "5.1.2.e@hackdefense.nl" gestuurd denk ik? Het zou "5.1.2.e@hackdefense.nl" moeten zijn.
>
> Groetjes,
>
> 5.1.2.e
>
> On 8/28/23 3:21 PM, 5.1.2.e wrote:
>
> > Moet nu goed zijn gegaan. Excuus dat het vorige keer fout was gegaan.
> >
> > 
> >
> >
> > ---
> >
> > **Van:** 5.1.2.e <5.1.2.e@hackdefense.nl>
> > **Verzonden:** maandag 28 augustus 2023 15:20
> > **Aan:** 5.1.2.e <5.1.2.e@kiesraad.nl>

CC: 5.1.2.e <5.1.2.e@hackdefense.nl>; 5.1.2.e <5.1.2.e@hackdefense.nl>
Onderwerp: Re: Broncode OSV2020-U

Dankjewel!

Zou je kunnen checken dat het naar 5.1.2.e@hackdefense.nl gestuurd wordt? De vorige was geloof ik bij 5.1.2.e@hackdefense.nl terechtgekomen.

Groetjes,

5.1.2.e

On 8/28/23 3:13 PM, 5.1.2.e wrote:

> 5.1.2.e
>
> Dank voor je mail. Ik stuur je via secure transfer even de rest van alle bestanden die ik heb. Als daar niet bij zit wat je nodig hebt, laat het mij dan nog even weten. Dan gaan we de leverancier vragen om de bestanden die jullie wel nodig hebben.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: maandag 28 augustus 2023 15:05
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@hackdefense.nl>; 5.1.2.e <5.1.2.e@hackdefense.nl>
Onderwerp: Broncode OSV2020-U

Hoi 5.1.2.e

Ik heb de broncode van jullie ontvangen. Echter is dit een zipfile met een hoop .jar files. Dit is in principe al gecompilede code (hoewel vrijwel in z'n geheel terug te brengen naar de bron).

We kunnen de applicatie echter niet bouwen/testen en het is onduidelijk wat de flow van de applicatie is. We missen een aantal libraries, en ik vermoed ook het framework dat om de applicatie heen zit. Het werkt voor ons fijner als we alle code daaromheen ook hebben.

Is het mogelijk voor ons om de volledige broncode, met unit tests (indien die er zijn), dependencies en build instructies te krijgen? Dan kunnen wij de code review veel effectiever uitvoeren.

--
Met vriendelijke groet / With kind regards,

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

--
Met vriendelijke groet / With kind regards,

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

--
Met vriendelijke groet / With kind regards,

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

--
Met vriendelijke groet / With kind regards,

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

--
Met vriendelijke groet / With kind regards,

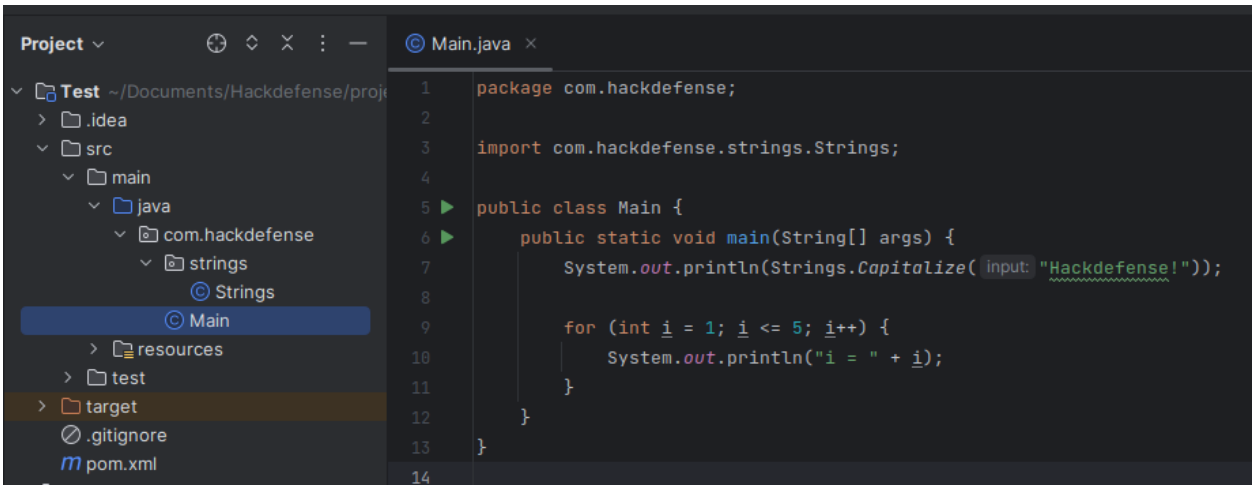
5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

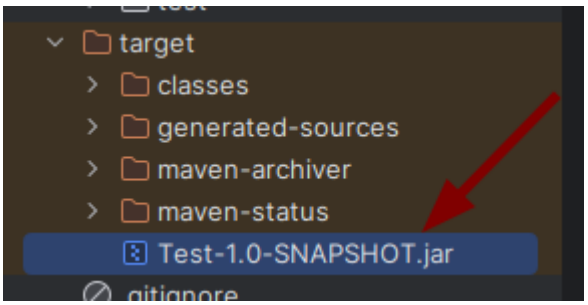
From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Thu, 31 Aug 2023 23:06:01 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @hackdefense.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: Broncode OSV2020-U

Hoi 5.1.2.e

Ik ben bang dat ik mezelf slecht verstaanbaar kan maken in het Duits ;). Jenkins zou heel goed de buildserver kunnen zijn. Die buildserver heeft dan een project nodig om te builden, en ik ben opzoek naar het project dat gebouwd wordt door hun buildserver. Als ik in mijn eigen IDE (software ontwikkelomgeving) een Java project maak dan ziet dat er als volgt uit:



Ik heb een hoofdmap met een src map, daaronder leven alle packages. Een belangrijk ding is dat alle code en classes hier de .java extensie hebben. Mijn IDE laat de extensie weg van deze files, maar de naam van de "Main" file die gehighlight is in de screenshot is dus eigenlijk "Main.java". Als ik dit compile krijg ik de 'target' directory een .jar file:



Wij hebben nu dus een zip bestand met alle .jar files ná de compile stap. En wij willen graag het hele project met alle .java classes vóór de compile stap. Dat zou in dit geval dus een zipfile zijn met een src map en een pom.xml file die omschrijft hoe het compilen in z'n werk gaat. Jenkins zou deze hele map ook krijgen en dan vervolgens zelf de compile stap uitvoeren. Het kan zijn dat het bij hen op een heel andere manier werkt (het Java landschap is helaas enorm complex met uiteenlopende standaarden). Maar zij moeten linksom of rechtsom ontwikkelen en code schrijven in .java files. Uiteraard zal hun src map een stuk groter zijn aangezien het project veel groter is.

Wellicht dat dit verhaal en de screenshots het nog duidelijker maken. Mocht ik nog ergens mee kunnen helpen in het contact, dan hoor ik dat graag. Ik weet niet hoe hun Engels is, maar anders wil ik ook wel proberen om direct met iemand daar te schakelen als dat beter werkt.

Met vriendelijke groet,

5.1.2.e

On 8/31/23 7:25 PM, 5.1.2.e wrote:

5.1.2.e

Dank voor de uitgebreide informatie. Ik ga morgen proberen met Elect te schakelen.

Ik was al een beetje bang dat dit niet de juiste file was. Voor zover ik weet gebruikt Elect Jenkins als buildserver. Kun je daar wat meer mee?

Ze spreken zelf Duits, dus we moeten dingen altijd echt heel duidelijk uitleggen, anders rake dingen soms lost in translation.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl<5.1.2.e @hackdefense.nl>>
Datum: donderdag 31 aug. 2023 5:29 PM
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl<5.1.2.e @kiesraad.nl>>
Onderwerp: Re: FW: Broncode OSV2020-U

Hoi 5.1.2.e

Ik zal morgen een exacte error proberen te krijgen voor de MariaDB issue. We hebben de meest up-to-date versie geprobeerd en verder niet heel veel tijd aan besteed omdat de interne database wel werkt. Ik vermoed ook dat dat de variant is die de meeste mensen zullen draaien. Wat ik nog wel weet is dat alle migraties netjes gedraaid werden en dat hij daarna in de problemen liep.

Wat betreft de broncode, dit is volgens mij dezelfde file die in de OSV2020-U alles.zip zat. Dit is een structuur die alle losse componenten lijkt te verzamelen en daar de uiteindelijke java file van maakt. Dat is inderdaad hoe de uiteindelijke gedistribueerde versie gebouwd wordt. Maar ik ben opzoek naar de bestandsstructuur zoals deze gebruikt wordt tijdens het ontwikkelen. Ik denk iets als "De bestanden zoals die in jullie IDE's staan tijdens het ontwikkelen en hoe deze wordt ingecheckt op jullie versiebeheersysteem (indien dat gebruikt wordt)". Het doel is dat ik graag een volledig project heb draaien, waardoor mijn code analyse tools de code veel beter begrijpen. Ik moet de code kunnen builden, maar het hoeft dan vervolgens niet te werken. Aan enkel de build stap heb ik voldoende. Ik weet niet welk build systeem zij gebruiken, ik zie veel verwijzingen naar Maven dus ik gok dat dat het is. Het zou ook kunnen dat ik iets over het hoofd zie hier, dus als dat het geval is wellicht een klein documentje met hoe zij deze files gebruiken om te developen zou ook enorm helpen.

Vandaag geen nieuwe dingen gevonden, we zijn nu vooral bezig met het uitlopen van de dingen die we tot nu toe hebben gevonden.

Met vriendelijke groet,

5.1.2.e

On 8/31/23 1:22 PM, 5.1.2.e wrote:
5.1.2.e

Heb jij meer informatie over de MariaDB issue? De leverancier zegt het niet te kunnen reproduceren. Als je zegt: vloeit geen bloed uit, kan ook nadat het rapport eruit is, dan is dat ook prima.

De airgap issue vind ik wel dermate serieus dat ik wil dat ze daar wel alvast naar kijken, vandaar de tickets.

Groet,

5.1.2.e

Van: 5.1.2.e
<5.1.2.e @kiesraad.nl><5.1.2.e @kiesraad.nl>
Verzonden: donderdag 31 augustus 2023 13:17
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl><5.1.2.e @kiesraad.nl>
Onderwerp: RE: Broncode OSV2020-U

Hoi 5.1.2.e

Elect iT heeft graag meer informatie over het MariaDB/MySQL database issue. Volgens Elect iT werkt deze functionaliteit namelijk naar behoren.

Wie vraagt de informatie op?

Groet, 5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 31 augustus 2023 12:55
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl<5.1.2.e @kiesraad.nl>>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl<5.1.2.e @kiesraad.nl>>
Onderwerp: RE: Broncode OSV2020-U

Hoi 5.1.2.e

Ik heb in JIRA de volgende tickets aangemaakt:
MySQL database => JIRA ticket 2367
Airgap issue => JIRA ticket 2368

Groet, 5.1.2.e

Van: 5.1.2.e <5.1.2.e @kiesraad.nl<5.1.2.e @kiesraad.nl>>
Verzonden: donderdag 31 augustus 2023 11:32
Aan: 5.1.2.e
<5.1.2.e @kiesraad.nl<5.1.2.e @kiesraad.nl>>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl<5.1.2.e @kiesraad.nl>>
Onderwerp: FW: Broncode OSV2020-U

5.1.2.e

Zou jij alvast tickets willen aanmaken voor Elect omtrent de airgap issues? Deze moeten echt opgelost worden namelijk voor de release. De XXE moeten ze eerst nog verder onderzoeken.

Daarnaast ook maar alvast een ticket voor de MariaDB issues.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl<5.1.2.e @hackdefense.nl>>
Verzonden: donderdag 31 augustus 2023 11:10
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl<5.1.2.e @kiesraad.nl>>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl<5.1.2.e @hackdefense.nl>>; 5.1.2.e
<5.1.2.e @hackdefense.nl<5.1.2.e @hackdefense.nl>>
Onderwerp: Re: Broncode OSV2020-U

Hoi 5.1.2.e

Super! Dank voor de moeite.

Excuses wat betreft de samenvatting, ik was dat inderdaad vergeten te doen. Bij deze:

* We hebben een XXE gevonden in de XML upload. Het lijkt mee te vallen want we kunnen de server er enkel een request mee naar ons laten maken. Wij zijn nog bezig om te kijken of we dit uit kunnen breiden naar Local File Inclusion.
* We hebben een aantal issues met de airgap
    * Als we een delay van iets meer dan twee seconde introduceren in het netwerk en ICMP requests blokkeren. Dan denkt de applicatie dat hij niet verbonden is met internet terwijl dit wel het geval is.
    * De airgap checkt d.m.v. webrequests en pings naar verschillende servers of er een netwerk beschikbaar is. Bij webrequests denkt de airgap enkel dat er een netwerk verbinding is als de target server een 200 OK status teruggeeft. Iedere andere statuscode lijkt gezien te worden als een gefaalde request. Indien alle servers iets anders dan een 200 status code teruggeven denkt de airgap dat er geen internet is.
    * Als de client-side (in de browser) airgap vasttelt dat er internet beschikbaar is, dan geeft de applicatie wel een melding maar blokkeert niet.
* Als de applicatie wordt geïnstalleerd met de optie om je eigen MariaDB/MySQL database te gebruiken, heeft deze last van transaction/commit issues waardoor de applicatie niet opstart. (De meegeleverde interne database doet het wel).

Met vriendelijke groet,

5.1.2.e

_____
Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.
--
Met vriendelijke groet / With kind regards,
[HackDefense] <http://www.hackdefense.com> 5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl<5.1.2.e @hackdefense.nl> |
www.hackdefense.com<https://www.hackdefense.com>
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

--
Met vriendelijke groet / With kind regards,

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Fri, 1 Sep 2023 17:08:01 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @hackdefense.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Update OSV2020-U

Hoi 5.1.2.e

Voor vandaag zijn is de belangrijkste bevinding dat we 'vars' en 'dynvars' files hebben gevonden in de installers. Ze bevatten wachtwoorden met namen als "INITIAL_SERVICE_PASSWORD". Ik vermoed dat de wachtwoorden die in deze file staan gebruikt worden als initiële waardes en later veranderd worden, maar ik zou dat in de broncode moeten verifiëren. Dus we kunnen nog niet zeggen wat de impact van deze bevinding is.

Had jij nog gehoord van Elect IT? Fijn weekend alvast!

--
Met vriendelijke groet / With kind regards,

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Mon, 4 Sep 2023 15:38:41 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Re: Code review module U source code format

Hoi 5.1.2.e

Wat betreft de codereview lopen wij nu tegen het probleem aan dat we niet alle code hebben ontvangen die gebruikt wordt tijdens het draaien van de applicatie. De ontwikkelaar maakt gebruik van een webframework. Dat framework laadt de code die voor jullie geschreven is in als een module. Als we de zip file die we van jullie gekregen hebben uitpakken, dan missen we informatie om de code uit te voeren, te debuggen en te laten analyseren door onze tooling. De enige optie de we hebben op dit moment is handmatig door alle code zoeken en conclusies maken op de informatie de we kunnen zien.

In een ideaal scenario hebben we de volledige codebase, zodat we deze zelf kunnen builden en uitvoeren. Als er dan een webrequest wordt gemaakt naar de server, dan kunnen wij vanaf het moment dat zo'n request binnenkomt, tot het moment dat de request de server verlaat zien wat er gebeurt. Soms als je naar een stukje code kijkt, dan worden stukjes code uit andere libraries aangeroepen. Het helpt voor het begrijpen van de code enorm als we de code uit die libraries kunnen bekijken. Momenteel is het zo dat we niet alle achterliggende code kunnen bekijken, omdat die mist.

Uiteraard hebben we wel de uiteindelijke installatie die we kunnen decompilen. Alleen hebben we dan nog steeds te weinig informatie om goed gebruik te kunnen maken van onze analyse tools. Dit is niet om te zeggen dat we helemaal geen code review hebben kunnen doen. De broncode van de module die voor de Kiesraad geschreven is, is gewoon te lezen. Daar hebben we naar kunnen kijken en hebben we ook bevindingen over. We kunnen die bevindingen alleen niet in de context plaatsen van de hele software omdat we niet weten wat er allemaal nog meer bij komt kijken. Een analogie die in m'n hoofd rondspeelt is: "We moeten een puzzel maken, maar alle stukjes liggen door het huis verspreid en het voorbeeldplaatje ontbreekt." Met genoeg tijd valt er uiteindelijk wel een werkbare situatie van te maken. In de tijd die voor dit project staat hebben we ons gefocust op het beoordelen van de aangeleverde code, maar niet op de wisselwerking tussen die code en de rest van de applicatie.

We doen een zinvolle review, maar het had beter gekund als we de volledige broncode hadden gehad. We nemen hierover een voorbehoud op in het rapport over de code die we niet hebben kunnen reviewen en het feit dat we een deel van onze analyse tools niet hebben kunnen toepassen.

Met vriendelijke groet,

5.1.2.e

On 9/4/23 1:03 PM, 5.1.2.e wrote:

> 5.1.2.e
>
> Klopt inderdaad. Ik ga onze kant hierover informeren en vragen wat we ermee willen. Ik wacht even verder op de mail met uitleg van 5.1.2.e
>
> Groet,
>
> 5.1.2.e
>
> ---
>
> **Van:** 5.1.2.e <5.1.2.e @hackdefense.nl>
> **Verzonden:** maandag 4 september 2023 13:01
> **Aan:** 5.1.2.e <5.1.2.e @kiesraad.nl>

CC: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: Code review module U source code format

Inmiddels had jij 5.1.2.e gesproken begreep ik?

Het gaat inderdaad wat langzamer hierdoor, het is op deze manier beduidend minder makkelijk om door de code heen te gaan. Gaat wel, maar duurt langer en je kunt minder analyse-tooling gebruiken.

Belangrijke implicatie is ook wel dat de broncode niet alle onderliggende functies bevat omdat Elect dat niet allemaal wil delen vanuit een gedeelde codebase met andere applicaties die zij maken. Wij kunnen die wel bekijken in de binary (Java is vrij goed te herleiden tot broncode), maar ook weer op een ingewikkelde manier.

5.1.2.e

On 04/09/2023 12:14, 5.1.2.e wrote:

> Goedemiddag,
>
> Elect kan de source code helaas niet aanleveren in het gewenste format. Kunnen jullie aangeven wat hiervan de implicatie is voor jullie code review?
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

--
Met vriendelijke groet / With kind regards,

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Thu, 7 Sep 2023 13:01:12 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Subject: Re: Concept rapportage pentest en code review

We zijn er druk mee!

On 07/09/2023 12:59, 5.1.2.e wrote:

> Goedemiddag,
>
> Gentle reminder: conform planning ontvang ik graag vandaag het conceptrapport voor de pentest en code review van U. Dan kan ik deze morgen reviewen en kunnen jullie hem volgende week nog aanpassen, waar nodig.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Fri, 8 Sep 2023 14:49:08 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @hackdefense.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Re: Concept rapportage pentest en code review U

5.1.2.e ! We gaan er mee aan de slag.

5.1.2.e

On 08/09/2023 11:35, 5.1.2.e wrote:

> Goedemorgen,
>
> Dank voor jullie mooie rapportage voor de pentest en code review van U. In de secure transfer heb ik een paar minimale opmerkingen geplaatst om in de definitieve versie te verwerken.
>
> Al met al wil ik jullie complimenten geven voor jullie professionele werk en de kwaliteit van de test en de rapportage. Veel andere organisaties kunnen hier nog een voorbeeld aan nemen wat mij betreft.
>
> Fijn weekend!
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Tue, 12 Sep 2023 10:36:02 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "'5.1.2.e '" <5.1.2.e @hackdefense.nl>; "'5.1.2.e 5.1.2.e '" <5.1.2.e @hackdefense.nl>
Cc: "'5.1.2.e '" <5.1.2.e @hackdefense.nl>
Subject: RE: Hertest hoofdlijnen OSV U

Hoi 5.1.2.e

Ik heb het in onze planning gezet, 5.1.2.e zal nog even contact met je opnemen per mail om alles in gereedheid te brengen.

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Tuesday, 12 September 2023 10:32
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; '5.1.2.e ' <5.1.2.e @hackdefense.nl>
CC: '5.1.2.e ' <5.1.2.e @hackdefense.nl>
Onderwerp: RE: Hertest hoofdlijnen OSV U

Dag 5.1.2.e

Dankjewel. Dat is prima!

We zouden graag dezelfde week nog een rapport ontvangen van de hertest.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 12 september 2023 10:11
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; '5.1.2.e ' <5.1.2.e @hackdefense.nl>
CC: '5.1.2.e ' <5.1.2.e @hackdefense.nl>
Onderwerp: RE: Hertest hoofdlijnen OSV U

Hoi 5.1.2.e

Dat gaat lukken. Zal ik dit plannen voor maandag 18 september? Ik vraag 5.1.2.e om dit te doen.

Akkoord?

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e 5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Tuesday, 12 September 2023 09:34
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: RE: Hertest hoofdlijnen OSV U

5.1.2.e

Een en ander is inmiddels intern afgestemd. We zouden graag een hertest van de 4 genoemde bevindingen krijgen in de week van 18 september.

In tegenstelling tot mijn eerdere bericht is de bedoeling dat ook de rapportage van de hertest openbaar gaat worden gemaakt. Mag nogsteeds een paar A4tjes zijn.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: maandag 11 september 2023 14:24
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: Re: Hertest hoofdlijnen OSV U

Hallo 5.1.2.e ja hoor hier is voldoende ruimte voor binnen de opdracht. Hertest is zo gebeurd. Dus geen aanvullende opdracht voor nodig.

5.1.2.e

On 11/09/2023 14:19, 5.1.2.e wrote:

> Goedemorgen 5.1.2.e
>
> Gezien twee bevindingen al eerder opgelost hadden moeten zijn door Elect, overwegen wij jullie een aantal van de bevindingen te laten hertesten. Met name:
>
> 1. XXE bevinding
> 2. Niet randomized wachtwoorden genereren
> 3. Credentials in de installer
> 4. Upload restricties
>
> Na de hertest is in principe een simpel verslag 1 a 2 A4tjes voldoende met bevindingen. Deze gaan we dan **niet** publiceren. Zouden jullie hier tijd voor hebben in de week van 18 september om in elk geval deze punten te hertesten? En zouden daar kosten aan gebonden zijn, zoja, wat bedragen de kosten dan ongeveer?
>
> Ik hoor het graag.
>
> Met vriendelijke groet,

5.1.2.e
5.1.2.e

5.1.2.e
5.1.2.e

Aanwezig: ma t/m vrij, afwezig wo

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e" <5.1.2.e@hackdefense.nl>
Sent: Thu, 14 Sep 2023 13:14:23 +0200
To: "5.1.2.e" <5.1.2.e@kiesraad.nl>
Cc: "5.1.2.e@hackdefense.nl" <5.1.2.e@hackdefense.nl>; "5.1.2.e" <5.1.2.e@kiesraad.nl>
Subject: Re: Hertest OSV U

5.1.2.e

Nog even ter bevestiging, ik heb je zojuist de definitieve versie van het rapport gestuurd via secure transfer (naar 5.1.2.e@kiesraad.nl).

Ik hoor graag of het goed is aangekomen.

Met vriendelijke groet / with kind regards,

HackDefense
5.1.2.e
5.1.2.e
T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

On 12-9-2023 14:08, 5.1.2.e wrote:

> 5.1.2.e
>
> Prima om de dinsdag te starten. Ik zou graag een apart rapport ontvangen en dan deze week de defintieve versie van het eerdere rapport.
>
> Dat is omdat ik het graag formeel wil kunnen delen met de Raad en directeuren.
>
> De hertest mag meteen een definitieve versie zijn. Als ik daar hele rare dingen zie dan geef ik het alsnog wel aan, maar verwacht ik niet.
>
> Groet,
>
> 5.1.2.e

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: dinsdag 12 september 2023 13:16
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e@hackdefense.nl; 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: Re: Hertest OSV U

Hoi 5.1.2.e

Geen probleem!

Als we de maandagmiddag alle bestanden ontvangen, beginnen we waarschijnlijk op dinsdag (19 sept.) met de hertest.

Het zou prima moeten gaan met de broncode van na het buildproces. Ik neem aan er geen hele grote veranderingen zijn vergeleken met de oude broncode.

Qua rapportage, vinden jullie het goed als de resultaten van de hertest worden toegevoegd als een extra onderdeel van het volledige testrapport, of hebben jullie dit liever in een los document?

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

On 12-9-2023 11:28, 5.1.2.e wrote:

> 5.1.2.e
>
> Veel dank dat je op korte termijn de test nog kunt uitvoeren.
>
> Het gaat inderdaad om de genoemde punten. Ik kan je de 18e in de middag pas (medische afspraak helaas in de ochtend) de software geven. Je krijgt dan inderdaad de nieuwe installer. Ik stuur je de broncode zoals wij die krijgen van de leverancier. Dus helaas niet zoals jullie die graag hebben (van voor de build). Ik vrees dat ik daar niks aan kan veranderen.
>
> Met vriendelijke groet,
>
> 5.1.2.e
> 5.1.2.e
>
> 5.1.2.e
> 5.1.2.e
> Aanwezig: ma t/m vrij, afwezig wo

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 12 september 2023 11:15
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e @hackdefense.nl
Onderwerp: Hertest OSV U

Hoi 5.1.2.e

Ik kan aankomende maandag (18 sept.) beginnen met de hertest van OSV-U.

Ik heb begrepen dat het alleen om de volgende 4 bevindingen gaat, zoals ze in het rapport worden genoemd:

1. XML External Entity vulnerability
2. Hard coded default passwords in installer
3. Use of insecure random function
4. Insufficient upload restrictions

Klopt dit?

Voor de hertest heb ik in ieder geval de geüpdate installers nodig. Verder kan het ook nuttig zijn om de geüpdate broncode te hebben, zodat we ook kunnen kijken naar de manier waarop de aanpassingen zijn gedaan.

Als je nog vragen hebt, ben ik uiteraard gewoon op dit e-mailadres te bereiken.

--
Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

e-Factuur

Leverancier

Identificatienummer	
Naam	Hackdefense B.V.
Adres	Sisalbaan 5A Leiderdorp 2352AZ NL
Telefoon	5.1.2.e
Email	5.1.2.e hackdefense.nl
KvK	69477043
BTW	NL857887270B01 VAT
IBAN	NL40RABO0337272700

Afnemer

OIN	00000001003214345000
Naam	Binnenlandse Zaken en Koninkrijksrelaties Kerndepartement
Postbus	Turfmarkt 147 Den Haag 2511 DP NL
Contactpersoon	5.1.2.e
Telefoon	
E-mail	

Factuurnummer	23010138	Factuurdatum	2023-09-11	Vervaldatum	2023-10-11
Datum levering	-	Factuur type	380	Indicatie kopie	-
Valuta	EUR	Contractnummer	-	Ordernummer afnemer	H2B 401002 – 11312 – 44011 verplichtingennummer 40
Ordernummer leverancier	-			Boekingscode	-

Omschrijving: Pentest OSV2020-U
BUDGETCODERING
H2B 40,

RegelNr	Omschrijving	Aantal	Basisprijs	Korting (%)	Prijs incl. korting	Tot.excl. BTW	BTW %
1	Pentest OSV2020-U Pentest OSV2020-U	1.00	5.1.2.f		5.1.2.f	5.1.2.f	21
	Ordernummer afnemer **Artikel nr afnemer** - **Artikel nr leverancier** - **Jobnummer**				**Valuta**	EUR	

Betalingscondities

Betalingsconditie	Betaling binnen 30 dagen
PaymentID	23010138
PaymentMeansCode	58
Percentage korting	-
Omschrijving kortingstermijn	-

Totaal

BTW %	Tot. grondslag	Bedrag BTW
21	5.1.2.f	5.1.2.f
	Totaal te betalen	5.1.2.f

HackDefense B.V.
Postbus 3025
2301 DA Leiden

Telefoon (071) 204 0101
E-mail 5.1.5 @hackdefense.nl
Website https://hackdefense.nl
IBAN NL40RABO0337272700
BIC RABONL2U
KvK 69477043
BTW nummer NL857887270B01

Ministerie van BZK / Kiesraad
T.a.v. Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED 's-Gravenhage

Factuur 23010138

Factuurdatum 11-09-2023
Vervaldatum 25-09-2023
H2B 401002-11312-44011

Omschrijving	Prijs	BTW %	Bedrag excl. BTW	BTW bedrag	Bedrag incl. BTW
WAM Pentesten, Web Applicatie Pentesting Pentest OSV2020-U BUDGETCODERING H2B 401002 – 11312 – 44011. Verplichtingennummer: 401002-33197 50% volgens offerte na oplevering concept rapport	€ 5.1.2.f	21 %	€ 5.1.2.f	€ 5.1.2.f	€ 5.1.2.f
	Totaal exclusief BTW		€ 5.1.2.f		
	Te betalen BTW 21%		€ 5.1.2.f	€ 5.1.2.f	
	Totaal te voldoen				€ 5.1.2.f

Wij verzoeken u om bovenstaand bedrag uiterlijk per de vervaldatum over te maken op bankrekeningnummer NL40 RABO 0337 2727 00 ten name van HackDefense B.V., onder vermelding van factuurnummer 23010138

e-Factuur

Leverancier

Identificatienummer	
Naam	Hackdefense B.V.
Adres	Sisalbaan 5A Leiderdorp 2352AZ NL
Telefoon	5.1.2.e
Email	5.1.2.e @hackdefense.nl
KvK	69477043
BTW	NL857887270B01 VAT
IBAN	NL40RABO0337272700

Afnemer

OIN	00000001003214345000
Naam	Binnenlandse Zaken en Koninkrijksrelaties Kerndepartement
Postbus	Turfmarkt 147 Den Haag 2511 DP NL
Contactpersoon	Kiesraad, 5.1.2.e
Telefoon	
E-mail	

Factuurnummer	23010106	Factuurdatum	2023-07-31	Vervaldatum	2023-08-30
Datum levering	-	Factuur type	380	Indicatie kopie	-
Valuta	EUR	Contractnummer	-	Ordernummer afnemer	201865007.433.001
Ordernummer leverancier	-			Boekingscode	-

Omschrijving: Pentest OSV2020 TK,

Regelnr	Omschrijving	Aantal	Basisprijs	Korting (%)	Prijs incl. korting	Tot.excl. BTW	BTW %
1	Verplichtingennummer 401002 Contractnummer 201865007.433.001 BUDGETCODERING H2B 401002 – 11312 – Verplichtingennummer 401002 Contractnummer 201865007.433.001 BUDGETCODERING H2B 401002 – 11312 –	1.00	5.1.2.f		5.1.2.f	5.1.2.f	21

Ordernummer afnemer
Artikel nr afnemer -
Artikel nr leverancier -
Jobnummer

Valuta EUR

Betalingscondities

Betalingsconditie	Betaling binnen 30 dagen
PaymentID	23010106
PaymentMeansCode	58
Percentage korting	-
Omschrijving kortingstermijn	-

Totaal

BTW %	Tot. grondslag	Bedrag BTW
21	5.1.2.f	5.1.2.f

Totaal te betalen 5.1.2.f

e-Factuur

Leverancier

Identificatienummer	
Naam	Hackdefense B.V.
Adres	Sisalbaan 5A Leiderdorp 2352AZ NL
Telefoon	5.1.2.e
Email	5.1.2.e hackdefense.nl
KvK	69477043
BTW	NL857887270B01 VAT
IBAN	NL40RABO0337272700

Afnemer

OIN	00000001003214345000
Naam	Binnenlandse Zaken en Koninkrijksrelaties Kerndepartement
Postbus	Turfmarkt 147 Den Haag 2511 DP NL
Contactpersoon	5.1.2.e
Telefoon	
E-mail	

Factuurnummer	23010127	Factuurdatum	2023-08-30	Vervaldatum	2023-09-29
Datum levering	-	Factuur type	380	Indicatie kopie	-
Valuta	EUR	Contractnummer	-	Ordernummer afnemer	BUDGETCODERING H2B 401002 – 11312 – 44011 Verplich
Ordernummer leverancier	-			Boekingscode	-
Omschrijving	Pentest OSV2020-U,				

Regelnr	Omschrijving	Aantal	Basisprijs	Korting (%)	Prijs incl. korting	Tot.excl. BTW	BTW %
1	Invoice Pentest Kiesraad OSV2020-U 50% na start project Invoice Pentest Kiesraad OSV2020-U 50% na start project	1.00	5.1.2.f		5.1.2.f	5.1.2.f	21
	Ordernummer afnemer **Artikel nr afnemer** - **Artikel nr leverancier** - **Jobnummer**				**Valuta**	EUR	

Betalingscondities

Betalingsconditie	Betaling binnen 30 dagen
PaymentID	23010127
PaymentMeansCode	58
Percentage korting	-
Omschrijving kortingstermijn	-

Totaal

BTW %	Tot. grondslag	Bedrag BTW
21	5.1.2.f	5.1.2.f
	Totaal te betalen	5.1.2.f

HackDefense B.V.
Postbus 3025
2301 DA Leiden

Telefoon (071) 204 0101
E-mail 5.1.5 @hackdefense.nl
Website https://hackdefense.nl
IBAN NL40RABO0337272700
BIC RABONL2U
KvK 69477043
BTW nummer NL857887270B01

Ministerie van BZK / Kiesraad
T.a.v. Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED 's-Gravenhage

Factuur 23010127

Factuurdatum 30-08-2023
Vervaldatum 13-09-2023
H2B 401002-11312-44011

Omschrijving	Prijs	BTW %	Bedrag excl. BTW	BTW bedrag	Bedrag incl. BTW
WAM Pentesten, Web Applicatie Pentesting Pentest OSV2020-U BUDGETCODERING H2B 401002 – 11312 – 44011. Verplichtingennummer: 401002-33197 50% volgens offerte	€ 5.1.2.f	21 %	€ 5.1.2.f	€ 5.1.2.f	€ 5.1.2.f
	Totaal exclusief BTW		€ 5.1.2.f		
	Te betalen BTW 21%		€ 5.1.2.f	€ 5.1.2.f	
	Totaal te voldoen				€ 5.1.2.f

Wij verzoeken u om bovenstaand bedrag uiterlijk per de vervaldatum over te maken op bankrekeningnummer NL40 RABO 0337 2727 00 ten name van HackDefense B.V., onder vermelding van factuurnummer 23010127

From: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Sent: Mon, 18 Sep 2023 12:19:30 +0200 (CET)
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: Advies mbt fact 5.1.2.e - Hackdefense B.V.
Attachments: Bijlage.PDF
Importance: Normal

Onderstaande mail is automatisch gegenereerd. Indien deze niet voor u is graag kiezen voor "Terugsturen met advies". LET OP: NIET doorsturen i.v.m. verdere verwerking.

Beste Collega,

Graag bijgaande factuur beoordelen. U kunt uw keuze kenbaar maken door op één van onderstaande links te drukken. Een nieuwe mail wordt geopend waar u uw keuze kunt beargumenteren.

Akkoord:	de leverancier heeft conform opdracht geleverd
Niet Akkoord:	de leverancier heeft niet conform opdracht geleverd **Verplichte toelichting**
Terugsturen met advies:	u kunt advies geven of aangeven dat de factuur niet voor u is **Verplichte toelichting**

Toelichting van 5.1.2.e

Goedemiddag 5.1.2.e jouw akkoord voor prestatie voor bijgaande fac tuur. Met vriendelijke groet, 5.1.2.e

Met vriendelijke groet,
5.1.2.e

Factuur detail informatie

Factuurnummer	2280003377
Documenttype	Factuur
Relatienummer	8012500
Bedrijfsnummer	2B
Boekjaar	2023

Positie	Budgetplaats	Budgetpositie	Fonds	Grootboek	Bestedingsmarkering	Documentpositie	Referentie	Totaalbedrag
002	401002	11312	2B	44011		000	401002-11312-44011	5.1.2.f

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e "
Sent: Mon, 18 Sep 2023 16:50:10 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: FW: Factuur context
Attachments: Creditnota 23010145 (106).pdf, Creditnota 23010144 (127).pdf, Creditnota 23010143 (138).pdf

TI, zie dat jij niet bent meegenomen

Wil jij de facturen afkeuren met de mededeling dat deze worden gecrediteerd. Thx!

Met vriendelijke groet,

5.1.2.e
5.1.2.e

5.1.2.e
5.1.2.e
Aanwezig: ma, di, woe, do.

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

www.kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: maandag 18 september 2023 16:36
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Factuur context

Hoi 5.1.2.e

Bijgevoegd de creditnota's. Deze zijn ook via het portaal ingediend.
Ik zal morgen een nieuwe totaal factuur opmaken met daarin de drie onderdelen.
Fijne avond!

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e 5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Monday, 18 September 2023 15:42
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: FW: Factuur context

Hoi 5.1.2.e

Moeten de credit facturen ook via het leverancierspportaal?

Met vriendelijke groet,

5.1.2.e
5.1.2.e
5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: maandag 18 september 2023 15:41
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Factuur context

Ha 5.1.2.e

Is het de bedoeling dat de creditfacturen ook weer via het leverancierspportaal worden ingediend?

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e 5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Monday, 18 September 2023 15:26
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>; '5.1.2.e '
<5.1.2.e @hackdefense.nl>
Onderwerp: RE: Factuur context

Hallo 5.1.2.e

Ja graag alle facturen crediteren en één factuur met de drie onderdelen plus omschrijving.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: maandag 18 september 2023 15:24
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; '5.1.2.e ' <5.1.2.e @hackdefense.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Factuur context

Ha 5.1.2.e

Wil je alle 3 de facturen gecrediteerd hebben?

Met vriendelijke groet / with kind regards,

5.1.2.e
5.1.2.e 5.1.2.e
T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Verzonden: Monday, 18 September 2023 12:55
Aan: 5.1.2.e <5.1.2.e@hackdefense.nl>; 5.1.2.e <5.1.2.e@hackdefense.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: RE: Factuur context

5.1.2.e

Dank voor de uitleg. Zouden jullie deze facturen kunnen crediteren/intrekken en opnieuw de juiste willen sturen? Dan kan ik ze goedkeuren.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: maandag 18 september 2023 12:17
Aan: 5.1.2.e <5.1.2.e@hackdefense.nl>; 5.1.2.e <5.1.2.e@kiesraad.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: Re: Factuur context

Sorry, het is echt ingewikkeld geworden mede door mijn toedoen (ik had het eerst mis). Er zijn 3 dingen:

- De eerste factuur was het basisbedrag dat we in 2020 in de aanbesteding hadden staan voor heel OSV (de 'standaard pentest', €5.1.2.f). Omdat deze al in 2020 is omschreven en geaccordeerd was hiervoor geen offerte nodig, er is direct opdracht verstrekt door de Kiesraad.
  Wij hebben deze gefactureerd na de pentest OSV2020-PP eind juli. Dat was een vergissing want hij gaat ook over OSV2020-U. We hebben afgesproken dat de Kiesraad de betaling zou aanhouden tot na de uitvoering van de pentest op OSV2020-U.
- De tweede zou moeten gaan over meerwerk nummer 1: o.a. de secure code review op OSV2020-U die niet was inbegrepen in de "standaard pentest" uit de aanbesteding. Dit is onze offerte O23077 (finale versie: 5.0). Het meerwerk zou 128 uur zijn (16 dagen) tegen het dagtarief uit 2020 (€5.1.2.f) dus zou €5.1.2.f moeten zijn. Ik denk dat hier per ongeluk het verkeerde bedrag is gefactureerd.
- De derde factuur zou moeten gaan over de extra inzet doordat OSV2020-U bij nader inzien toch een behoorlijke set extra modules had. Dat hebben we gezien de korte tijdslijnen snel per mail in een briefje bevestigd. Gaat om 8 dagen a €5.1.2.f = €5.1.2.f

In totaal zou het dus moeten gaan om 5.1.2.f = €5.1.2.f (ex BTW) voor 36 dagen inzet.

5.1.2.e

On 18/09/2023 11:13, 5.1.2.e wrote:

Hoi 5.1.2.e

Factuur 23010106 is voor de werkzaamheden in juli 2023.

Met vriendelijke groet / with kind regards,

5.1.2.e
5.1.2.e 5.1.2.e
T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Verzonden: Monday, 18 September 2023 11:06
Aan: 5.1.2.e@hackdefense.nl; 5.1.2.e <5.1.2.e@hackdefense.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: Factuur context

Goedemorgen,

Wij hebben van jullie drie facturen ontvangen. Twee daarvan kan ik plaatsen en worden goedgekeurd. De derde heb ik even hulp bij nodig.

Kunnen jullie aangeven waar de factuur in de bijlage precies voor is?

Met vriendelijke groet,

5.1.2.e
5.1.2.e

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

HackDefense B.V.
Postbus 3025
2301 DA Leiden

Telefoon (071) 204 0101
E-mail 5.1.5 @hackdefense.nl
Website https://hackdefense.nl
IBAN NL40RABO0337272700
BIC RABONL2U
KvK 69477043
BTW nummer NL857887270B01

Ministerie van BZK / Kiesraad
T.a.v. Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED 's-Gravenhage

Creditnota 23010145

Factuurdatum 18-09-2023
Vervaldatum 02-10-2023
H2B 401002-11312-44011

Omschrijving	Prijs	BTW %	Bedrag excl. BTW	BTW bedrag	Bedrag incl. BTW
WAM Pentesten, Web Applicatie Pentesting Pentest OSV2020 TK Verplichtingennummer 401002 Contractnummer 201865007.433.001	€ 5.1.2.f	21 %	€ 5.1.2.f	€ 5.1.2.f	€ 5.1.2.f
	Totaal exclusief BTW		€ 5.1.2.f		
	Te betalen BTW 21%		€ 5.1.2.f	€ 5.1.2.f	
	Totaal te voldoen				**€** 5.1.2.f

Wij verzoeken u om bovenstaand bedrag uiterlijk per de vervaldatum over te maken op bankrekeningnummer NL40 RABO 0337 2727 00 ten name van HackDefense B.V., onder vermelding van factuurnummer 23010145

HackDefense B.V.
Postbus 3025
2301 DA Leiden

Telefoon (071) 204 0101
E-mail 5.1.5 @hackdefense.nl
Website https://hackdefense.nl
IBAN NL40RABO0337272700
BIC RABONL2U
KvK 69477043
BTW nummer NL857887270B01

Ministerie van BZK / Kiesraad
T.a.v. Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED 's-Gravenhage

Creditnota 23010144

Factuurdatum 18-09-2023
Vervaldatum 02-10-2023
H2B 401002-11312-44011

Omschrijving	Prijs	BTW %	Bedrag excl. BTW	BTW bedrag	Bedrag incl. BTW
WAM Pentesten, Web Applicatie Pentesting Pentest OSV2020-U BUDGETCODERING H2B 401002 – 11312 – 44011. Verplichtingennummer: 401002-33197 50% volgens offerte	€ 5.1.2.f	21 %	€ 5.1.2.f	€ 5.1.2.f	€ 5.1.2.f
	Totaal exclusief BTW		€ 5.1.2.f		
	Te betalen BTW 21%		€ 5.1.2.f	€ 5.1.2.f	
	Totaal te voldoen				**€** 5.1.2.f

Wij verzoeken u om bovenstaand bedrag uiterlijk per de vervaldatum over te maken op bankrekeningnummer NL40 RABO 0337 2727 00 ten name van HackDefense B.V., onder vermelding van factuurnummer 23010144

HackDefense B.V.
Postbus 3025
2301 DA Leiden

Telefoon (071) 204 0101
E-mail 5.1.5 @hackdefense.nl
Website https://hackdefense.nl
IBAN NL40RABO0337272700
BIC RABONL2U
KvK 69477043
BTW nummer NL857887270B01

Ministerie van BZK / Kiesraad
T.a.v. Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED 's-Gravenhage

Creditnota 23010143

Factuurdatum 18-09-2023
Vervaldatum 02-10-2023
H2B 401002-11312-44011

Omschrijving	Prijs	BTW %	Bedrag excl. BTW	BTW bedrag	Bedrag incl. BTW
WAM Pentesten, Web Applicatie Pentesting Pentest OSV2020-U BUDGETCODERING H2B 401002 – 11312 – 44011. Verplichtingennummer: 401002-33197 50% volgens offerte na oplevering concept rapport	€ 5.1.2.f	21 %	€ 5.1.2.f	€ 5.1.2.f	€ 5.1.2.f
	Totaal exclusief BTW		€ 5.1.2.f		
	Te betalen BTW 21%		€ 5.1.2.f	€ 5.1.2.f	
	Totaal te voldoen				**€** 5.1.2.f

Wij verzoeken u om bovenstaand bedrag uiterlijk per de vervaldatum over te maken op bankrekeningnummer NL40 RABO 0337 2727 00 ten name van HackDefense B.V., onder vermelding van factuurnummer 23010143

From: "5.1.2.e "
Sent: Tue, 19 Sep 2023 15:31:02 +0200
To: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e "
<5.1.2.e @kiesraad.nl>
Subject: RE: Factuur context

Hallo 5.1.2.e

Volgens mij klopt de factuur zo.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 19 september 2023 15:14
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Factuur context

Hi 5.1.2.e

In de bijlage de factuur, deze is nog niet verstuurd, wil jij kijken of deze zo klopt voordat ik de factuur in het leverancierssportaal zet?

Dank!

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e 5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Monday, 18 September 2023 15:42
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: FW: Factuur context

Hoi 5.1.2.e

Moeten de credit facturen ook via het leverancierssportaal?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: maandag 18 september 2023 15:41
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Factuur context

Ha 5.1.2.e

Is het de bedoeling dat de creditfacturen ook weer via het leveranciersportaal worden ingediend?

Met vriendelijke groet / with kind regards,

5.1.2.e
5.1.2.e 5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Monday, 18 September 2023 15:26
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>; '5.1.2.e '
<5.1.2.e @hackdefense.nl>
Onderwerp: RE: Factuur context

Hallo 5.1.2.e

Ja graag alle facturen crediteren en één factuur met de drie onderdelen plus omschrijving.

Met vriendelijke groet,

5.1.2.e
5.1.2.e
5.1.2.e

Afwezig op vrijdag

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: maandag 18 september 2023 15:24
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; '5.1.2.e ' <5.1.2.e @hackdefense.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Factuur context

Ha 5.1.2.e

Wil je alle 3 de facturen gecrediteerd hebben?

Met vriendelijke groet / with kind regards,

5.1.2.e
5.1.2.e 5.1.2.e
T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Monday, 18 September 2023 12:55
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @hackdefense.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Factuur context

5.1.2.e

Dank voor de uitleg. Zouden jullie deze facturen kunnen crediteren/intrekken en opnieuw de juiste willen sturen? Dan kan ik ze goedkeuren.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: maandag 18 september 2023 12:17
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Re: Factuur context

Sorry, het is echt ingewikkeld geworden mede door mijn toedoen (ik had het eerst mis). Er zijn 3 dingen:

- De eerste factuur was het basisbedrag dat we in 2020 in de aanbesteding hadden staan voor heel OSV (de 'standaard pentest', €5.1.2.f). Omdat deze al in 2020 is omschreven en geaccordeerd was hiervoor geen offerte nodig, er is direct opdracht verstrekt door de Kiesraad.
  Wij hebben deze gefactureerd na de pentest OSV2020-PP eind juli. Dat was een vergissing want hij gaat ook over OSV2020-U. We hebben afgesproken dat de Kiesraad de betaling zou aanhouden tot na de uitvoering van de pentest op OSV2020-U.
- De tweede zou moeten gaan over meerwerk nummer 1: o.a. de secure code review op OSV2020-U die niet was inbegrepen in de "standaard pentest" uit de aanbesteding. Dit is onze offerte O23077 (finale versie: 5.0). Het meerwerk zou 128 uur zijn (16 dagen) tegen het dagtarief uit 2020 (€5.1.2.f) dus zou €5.1.2.f moeten zijn. Ik denk dat hier per ongeluk het verkeerde bedrag is gefactureerd.
- De derde factuur zou moeten gaan over de extra inzet doordat OSV2020-U bij nader inzien toch een behoorlijke set extra modules had. Dat hebben we gezien de korte tijdslijnen snel per mail in een briefje bevestigd. Gaat om 8 dagen a €5.1.2.f = €5.1.2.f

In totaal zou het dus moeten gaan om 5.1.2.f = €5.1.2.f (ex BTW) voor 36 dagen inzet.

5.1.2.e

On 18/09/2023 11:13, 5.1.2.e wrote:

> Hoi 5.1.2.e

Factuur 23010106 is voor de werkzaamheden in juli 2023.

Met vriendelijke groet / with kind regards,

5.1.2.e
5.1.2.e 5.1.2.e
T: (5.1.2.e | M: 5.1.2.e
5.1.2.e@hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e@kiesraad.nl>
Verzonden: Monday, 18 September 2023 11:06
Aan: 5.1.2.e@hackdefense.nl; 5.1.2.e <5.1.2.e@hackdefense.nl>
CC: 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: Factuur context

Goedemorgen,

Wij hebben van jullie drie facturen ontvangen. Twee daarvan kan ik plaatsen en worden goedgekeurd. De derde heb ik even hulp bij nodig.

Kunnen jullie aangeven waar de factuur in de bijlage precies voor is?

Met vriendelijke groet,

5.1.2.e
5.1.2.e

5.1.2.e
5.1.2.e
Aanwezig: ma t/m vrij, afwezig wo

Kiesraad
Zurichtoren 14e etage – Muzenstraat 85 – 2511 WB Den Haag
Postbus 20011 – 2500 EA Den Haag

kiesraad.nl

Verkiezingen waar de samenleving op kan vertrouwen

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

From: "5.1.2.e " <5.1.2.e @hackdefense.nl>
Sent: Tue, 26 Sep 2023 11:51:40 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: RE: Factuur context

Prima, dan sluiten wij af.
Dan nog even een korte evaluatie:

Omdat we de kwaliteit van onze dienstverlening scherp in de gaten houden stellen we na afloop van elk project de volgende korte vraag:
Op een schaal van 0-10, hoe tevreden bent u over de manier waarop HackDefense opdracht heeft uitgevoerd?
Als u met een cijfer op deze mail zou willen reageren, dan zijn we u zeer erkentelijk. Eventuele opmerking(en)/toelichting is uiteraard ook welkom, maar optioneel.

De resultaten van de evaluatie zijn voor intern gebruik.

Nogmaals hartelijk dank voor uw opdracht!

Met vriendelijke groet / with kind regards,

HackDefense

5.1.2.e
5.1.2.e 5.1.2.e

T: (5.1.2.e | M: 5.1.2.e
5.1.2.e @hackdefense.nl | www.hackdefense.com
HackDefense BV | Sisalbaan 5a | 2352 AZ Leiderdorp

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: Tuesday, 26 September 2023 11:50
Aan: 5.1.2.e <5.1.2.e @hackdefense.nl>
Onderwerp: RE: Factuur context

Dag 5.1.2.e

Dank voor de mail. Alle werkzaamheden zijn wat ons betreft afgerond wat betreft jullie dienstverlening voor de pentest.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: dinsdag 26 september 2023 11:06
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Factuur context

Ha 5.1.2.e

Ik kreeg van 5.1.2.e degene die de test heeft uitgevoerd bij jullie, de vraag of alles nu afgerond is.
Kun jij mij hierover inlichten?

Hartelijk dank!

Met vriendelijke groet / with kind regards,

e-Factuur

Leverancier

Identificatienummer	
Naam	Fox-IT B.V.
Adres	Olof Palmestraat 6 Delft 2616 LM NL
Telefoon	5.1.2.e
Email	5.1.2.e @fox-it.com
KvK	27301624
BTW	NL818052971B01 VAT
IBAN	NL05INGB0009642118

Afnemer

OIN	00000001003214345000
Naam	Binnenlandse Zaken en Koninkrijksrelaties Kerndepartement
Postbus	Turfmarkt 147 Den Haag 2511 DP NL
Contactpersoon	5.1.2.e
Telefoon	
E-mail	
BTW-nr	

Factuurnummer	00120850	Factuurdatum	2024-03-25	Vervaldatum	2024-04-24
Datum levering	-	Factuur type	380	Indicatie kopie	-
Valuta	EUR	Contractnummer	-	Ordernummer afnemer	401002-35839
Ordernummer leverancier	-			Boekingscode	-

Omschrijving: Standaard Pentest OSV2020 ten behoeve va,

Regelnr	Omschrijving	Aantal	Basisprijs	Korting (%)	Prijs incl. korting	Tot.excl. BTW	BTW %
1	Standaard Pentest OSV2020 ten behoeve van De Kiesraad Budgetcodering: H2B 401002-10024-44011 Standaard Pentest OSV2020 ten behoeve van De Kiesraad Budgetcodering: H2B 401002-10024-44011	1.00	5.1.2.f		5.1.2.f	5.1.2.f	21

Ordernummer afnemer
Artikel nr afnemer -
Artikel nr leverancier -
Jobnummer

Valuta EUR

Betalingscondities

Betalingsconditie	Betaling binnen 30 dagen
PaymentID	00120850
PaymentMeansCode	58
Percentage korting	-
Omschrijving kortingstermijn	-

Totaal

BTW %	Tot. grondslag	Bedrag BTW
21	5.1.2.f	5.1.2.f

Totaal te betalen 5.1.2.f

e-Factuur

Leverancier

Identificatienummer	
Naam	Hackdefense B.V.
Adres	Sisalbaan Leiderdorp 2352 AZ NL
Telefoon	071-2040101
Email	5.1.5 @hackdefense.nl
KvK	-
BTW	
IBAN	NL40RABO0337272700

Afnemer

OIN	
Naam	BZK Kerndepartement
Postbus	Turfmarkt Den Haag 2511 DP NL
Contactpersoon	5.1.2.e @Kiesraad.nl
Telefoon	
E-mail	

Factuurnummer	20200408	Factuurdatum	2020-12-17	Vervaldatum	-
Datum levering	2020-12-17 - 2020-12-17	Factuur type	D	Indicatie kopie	-
Valuta	EUR	Contractnummer	-	Ordernummer afnemer	201865007.433.001
Ordernummer leverancier	-			Boekingscode	-

Omschrijving: hertest pentest OSV2020-U Verplichtingennummer: H2B 401002-18272 Contractnummer: 201865007.433.001 Budgetcodering: H2B 401002-10024-44011

Regelnr	Omschrijving	Aantal	Basisprijs	Korting (%)	Prijs incl. korting	Tot.excl. BTW	BTW %
1	hertest pentest OSV2020-U, zoals overeengekomen hertest pentest OSV2020-U, zoals overeengekomen	5.00	5.1.2.f		5.1.2.f	5.1.2.f	

Ordernummer afnemer
Artikel nr afnemer -
Artikel nr leverancier -
Valuta EUR

Betalingscondities

Betalingsconditie	30 dagen
PaymentID	
PaymentMeansCode	42
Percentage korting	-
Omschrijving kortingstermijn	-

Totaal

BTW %	Tot. grondslag	Bedrag BTW
21	5.1.2.f	5.1.2.f

Totaal te betalen 5.1.2.f

> Dit is een automatisch gegenereerd document op 17-12-2020 15:42:41

Factuur

Wilt u bij correspondentie over deze factuur refereren naar de gegevens bij factuurdetails (2).

Factuur aan
BZK Kerndepartement
Turfmarkt 147 - 2511 DP Den Haag

Afzender
Hackdefense B.V.
Sisalbaan 5-A - 2352 AZ Leiderdorp NL

1 Algemene gegevens

Besteld door	Ministerie van BZK
	Turfmarkt 147
	2511 DP Den Haag
Klant contactpersoon	5.1.2.e @Kiesraad.nl

Leveranciersnr.	7009910
Leveranciersvestiging	000037826298
KvK nummer	69477043
Btw-nummer	NL857887270B01
IBAN	NL40RABO0337272700
BIC	RABONL2U

2 Detaillering factuur

Factuurnummer	20200408
Factuurkenmerk	
Factuurdatum	17-12-2020
Boekstuknummer	80023642
Naam contactpersoon	5.1.2.e
Email contactpersoon	5.1.5 @hackdefense.nl
Tel. contactpersoon	071-2040101

Soort facturatie	E-facturatie
Omschrijving	hertest pentest OSV2020-U Verplichtingennummer: H2B 401002-18272 Contractnummer: 201865007.433.001 Budgetcodering: H2B 401002-10024-44011
(Order) referentie	201865007.433.001

3 Factuurregels

Regel	Onderdeelnummer/-omschrijving	Leverdatum	Aantal	Eenheid	Prijs(EUR)	Btw %	Bedrag(EUR)
1	hertest pentest OSV2020-U, zoals overeengekomen	17-12-2020	5,00		5.1.2.f	21	5.1.2.f

Btw details: Prijs en bedrag zijn exclusief btw, de btw (indien van toepassing) is separaat vermeld in de kolom btw%.
Orderregel referentie:

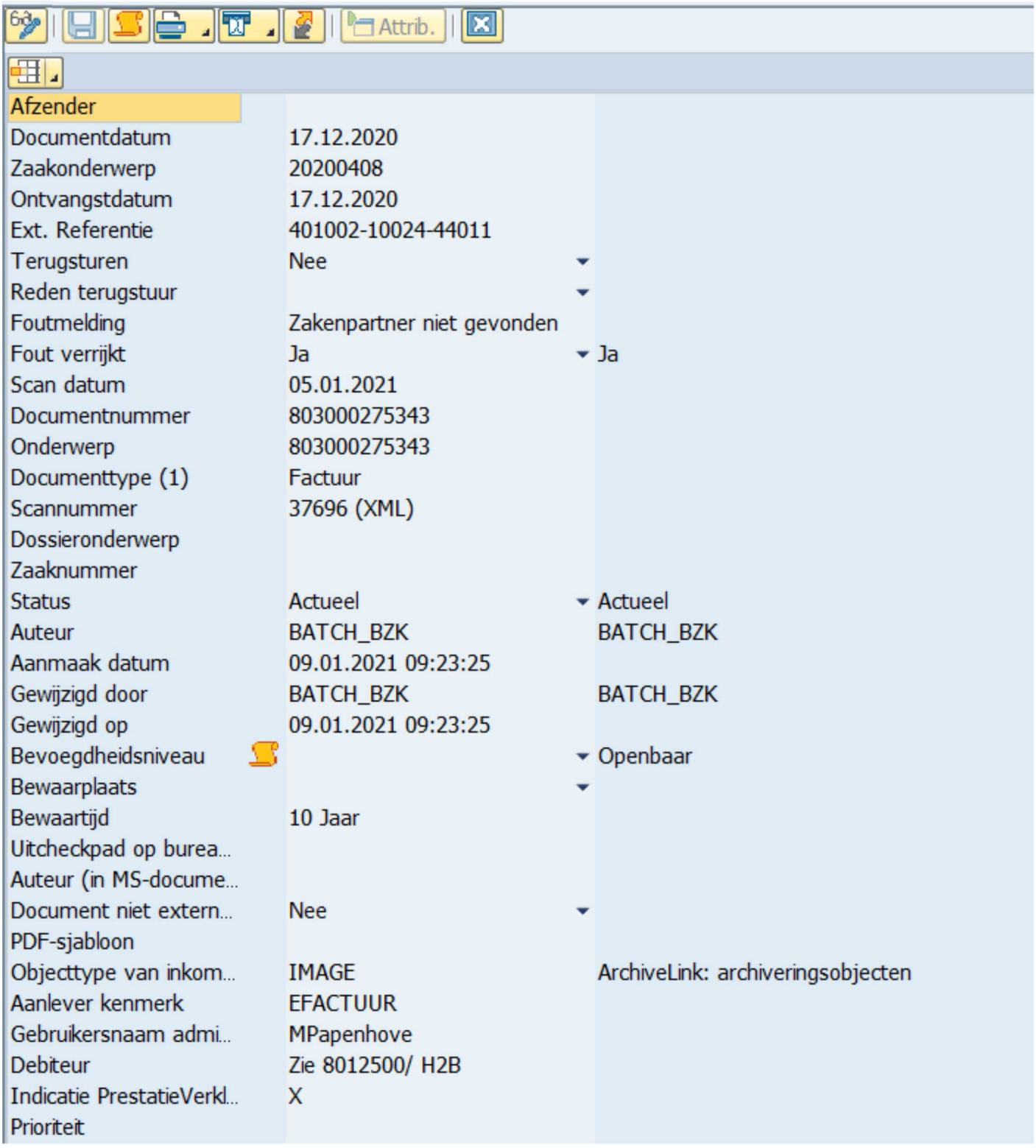
Subtotaal excl. Btw	5.1.2.f
BTW HOOG 21%	5.1.2.f
Totaal inclusief Btw	5.1.2.f

Van: 5.1.2.e @minszw.nl <5.1.2.e @minszw.nl>
Verzonden: Monday, February 22, 2021 8:01:29 AM
Aan: "5.1.2.e @minszw.nl" <5.1.2.e @minszw.nl>
Onderwerp: FW: SPOED e-factuur 20200408 (BZK) FW: status factuur 20200408? (zp 8012500)
Bijlage(n): Factuur 20200408 (BZK).pdf

Van: 5.1.2.e <5.1.2.e @minszw.nl>
Verzonden: vrijdag 19 februari 2021 12:24
Aan: 5.1.2.e @minszw.nl <5.1.2.e @minszw.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: SPOED e-factuur 20200408 (BZK) FW: status factuur 20200408? (zp 8012500)
Urgentie: Hoog

Goedemiddag collega,

Zie mail hieronder van 5.1.2.e
Factuur 20200408 staat niet in SAP maar wel in Scaceps met melding dat zp niet gevonden is (zp 8012500 bestaat wel):



Kunnen jullie deze oude e-factuur (bijlage 2) nogmaals met spoed doorzetten naar KTA?
Ik hoor het graag.
Alvast bedankt.

Met vriendelijke groet,

5.1.2.e
Medewerker Servicedesk Financieel Dienstencentrum
.....
Ministerie van Sociale Zaken en Werkgelegenheid
Directie DSU / Financieel Dienstencentrum
Locatie Hoftoren / 26e etage
Rijnstraat 50 | 2515 XP Den Haag
Postadres: Postbus 90801 | 2509 LV | Den Haag

.....
T 5.1.2.e
Werktijden: maandag t/m vrijdag (8.00 uur - 17.00 uur)

Het Financieel Dienstencentrum (FDC) is het interdepartementale samenwerkingsverband onder verantwoordelijkheid van SZW.
Het FDC voert de financiële administratie en het beheer van het financiële SAP-systeem uit voor de ministeries van BZK, Financiën, OCW, SZW en VWS.

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: vrijdag 19 februari 2021 11:58
Aan: 5.1.2.e <5.1.2.e @minszw.nl>
Onderwerp: FW: status factuur 20200408?

Beste 5.1.2.e 5.1.2.e
Zouden jullie s.v.p. kunnen nagaan of deze factuur bij FDC is aangekomen/wat er mis kan zijn gegaan?
Groet, 5.1.2.e

Van: 5.1.2.e <5.1.2.e @hackdefense.nl>
Verzonden: vrijdag 19 februari 2021 11:52
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e kiesraad.nl>; 5.1.2.e 5.1.2.e <5.1.2.e @Kiesraad.nl>
Onderwerp: Re: status factuur 20200408?

Op onderstaande mail heb ik nog geen reactie mogen ontvangen, evenmin als betaling van de factuur.

Klopt er iets niet, hebben we iets niet goed gedaan bij de indiening?

Bij voorbaat vriendelijk dank voor de beantwoording,

5.1.2.e

On 1/30/21 8:46 PM, 5.1.2.e wrote:

> Op 17-12-2020 heb ik bijgaande factuur ingediend via digiinkoop. We hebben nog geen betaling ontvangen. Is de factuur in goede orde aangekomen? Is er iets dat betaling tegenhoudt?

Dank,

5.1.2.e

HackDefense

e-Factuur

Leverancier

Identificatienummer	
Naam	Hackdefense B.V.
Adres	Sisalbaan 5A Leiderdorp 2352AZ NL
Telefoon	5.1.2.e
Email	5.1.2.e hackdefense.nl
KvK	69477043
BTW	NL857887270B01 VAT
IBAN	NL40RABO0337272700

Afnemer

OIN	00000001003214345000
Naam	Binnenlandse Zaken en Koninkrijksrelaties Kerndepartement
Postbus	Turfmarkt 147 Den Haag 2511 DP NL
Contactpersoon	5.1.2.e
Telefoon	
E-mail	
BTW-nr	

Factuurnummer	23010147	Factuurdatum	2023-09-20	Vervaldatum	2023-10-20
Datum levering	-	Factuur type	380	Indicatie kopie	-
Valuta	EUR	Contractnummer	-	Ordernummer afnemer	BUDGETCODERING H2B 401002 – 11312 – 44011. Verpl
Ordernummer leverancier	-			Boekingscode	-
Omschrijving	Pentest OSV2020-U,				

RegelNr	Omschrijving	Aantal	Basisprijs	Korting (%)	Prijs incl. korting	Tot.excl. BTW	BTW %
1	Pentest OSV2020-U Pentest OSV2020-U	1.00	5.1.2.f		5.1.2.f	5.1.2.f	21
	Ordernummer afnemer **Artikel nr afnemer** - **Artikel nr leverancier** - **Jobnummer**				**Valuta**	EUR	

Betalingscondities

Betalingsconditie	Betaling binnen 30 dagen
PaymentID	23010147
PaymentMeansCode	58
Percentage korting	-
Omschrijving kortingstermijn	-

Totaal

BTW %	Tot. grondslag	Bedrag BTW
21	5.1.2.f	5.1.2.f
	Totaal te betalen	5.1.2.f

HackDefense B.V.
Postbus 3025
2301 DA Leiden

Telefoon (071) 204 0101
E-mail 5.1.5 @hackdefense.nl
Website https://hackdefense.nl
IBAN NL40RABO0337272700
BIC RABONL2U
KvK 69477043
BTW nummer NL857887270B01

Ministerie van BZK / Kiesraad
T.a.v. Financieel Dienstencentrum (FDC)
Postbus 13178
2501 ED 's-Gravenhage

Factuur 23010147

Factuurdatum 20-09-2023
Vervaldatum 04-10-2023
H2B 401002-11312-44011

Omschrijving	Prijs	BTW %	Bedrag excl. BTW	BTW bedrag	Bedrag incl. BTW
WAM Pentesten, Web Applicatie Pentesting Pentest OSV2020 U Verplichtingennummer 401002 Contractnummer 201865007.433.001	€ 5.1.2.f	21 %	€ 5.1.2.f	€ 5.1.2.f	€ 5.1.2.f
WAM Pentesten, Web Applicatie Pentesting Meerwerkt OSV2020-U volgens offerte O23077 5.0 BUDGETCODERING H2B 401002 – 11312 – 44011. Verplichtingennummer: 401002-33197	€ 5.1.2.f	21 %	€ 5.1.2.f	€ 5.1.2.f	€ 5.1.2.f
WAM Pentesten, Web Applicatie Pentesting Extra inzet OSV2020-U 8 dagen a € 5.1.2.f	€ 5.1.2.f	21 %	€ 5.1.2.f	€ 5.1.2.f	€ 5.1.2.f
	Totaal exclusief BTW		€ 5.1.2.f		
	Te betalen BTW 21%		€ 5.1.2.f	€ 5.1.2.f	
	Totaal te voldoen				**€** 5.1.2.f

Wij verzoeken u om bovenstaand bedrag uiterlijk per de vervaldatum over te maken op bankrekeningnummer NL40 RABO 0337 2727 00 ten name van HackDefense B.V., onder vermelding van factuurnummer 23010147

From: "5.1.2.e "
Sent: Mon, 15 Mar 2021 11:40:21 +0100
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>; "5.1.2.e " <5.1.2.e @kiesraad.nl>
Cc: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: RE: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense
Attachments: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense.v4.docx

Hierbij de versie

5.1.2.e
Afwezig: woensdag

T 5.1.2.e / 5.1.2.e (privé)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: maandag 15 maart 2021 10:51
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @Kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Als dit gebeurd is (goed Nederlands) dan graag akkoord met handtekening en verzending.
5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Datum: maandag 15 mrt. 2021 10:47 AM
Aan: 5.1.2.e <5.1.2.e @Kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Hallo 5.1.2.e

Volgens mij heb jij in deze versie de meer taalkundige opmerkingen die 5.1.2.e hieronder had opgemerkt en die al eerder verwerkt waren er weer in terug gedaan. Graag nog even aandacht hiervoor.

Groet,
5.1.2.e

Van: 5.1.2.e <5.1.2.e @Kiesraad.nl>
Verzonden: maandag 15 maart 2021 10:15
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Hoi 5.1.2.e

Hierbij de nieuwe versie, met track changes, deze is ook afgestemd met de HIS.
5.1.2.e (onze inkoopadviseur van de HIS die deze aanbesteding heeft begeleid) adviseert om de zin van de mini competitie helemaal weg te halen, als jij het daarmee eens bent dan verwijder ik deze.

Het is ook lastig om aan te geven dat er "dezelfde gunningscriteria gebruikt worden" aangezien de binnen de aanbestede raamovereenkomst er meerdere soorten opdrachten zijn en dus ook de criteria kunnen afwijken.

5.1.2.e
Afwezig: woensdag

T 5.1.2.e / 5.1.2.e (privé)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: zondag 14 maart 2021 21:47
Aan: 5.1.2.e <5.1.2.e @Kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Hoi 5.1.2.e
1. Neem dan op 'De beantwoording gaat verder in op perceel 1 omdat daarover de Kamervragen zijn gesteld' (dat stond ook in je eerdere concept)
2. Ik zou niet dat hele verhaal opnemen maar de zin (na mini-competitie): 'Daarbij worden dezelfde gunningscriteria gebruikt als bij de aanbestedingsstukken voor de raamovereenkomst'.
5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @Kiesraad.nl>
Datum: zondag 14 mrt. 2021 9:38 PM
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: RE: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Hoi 5.1.2.e

VRAAG WAAROM NIET HIER OVER PERCEEL 2 GERAPPORTEERD??
Omdat er over dat perceel (toetsen van kwaliteit)

1. Er geen vragen zijn gesteld over de levercier(s) van kwaliteitstoetsen (wettelijk toets uitgevoerd door expleo https://www.kiesraad.nl/adviezen-en-publicaties/formulieren/2021/02/01/expleo-toetsingsrapport-osv2020)
2. het compliceert het de antwoorden om daar andere partijen hebben ingeschreven en aan andere partijen zijn gegund (KPMG en Expleo).

Een minicompetitie is een aanbestedingsterm, ik kan daar een verwijzingen naar opnemen:

Plaatsen opdrachten binnen een raamovereenkomst

Voor het daadwerkelijk plaatsen van opdrachten binnen de raamovereenkomst sluit u aparte overeenkomsten (nadere overeenkomsten). Bij raamovereenkomsten met meer dan één ondernemer waarbij nog niet alle voorwaarden vooraf zijn bepaald, wordt voor het plaatsen van deze nadere opdrachten de mededinging opnieuw opengesteld door het organiseren van een zogenaamde **minicompetitie** tussen de betrokken raamovereenkomstpartijen. Partijen worden uitgenodigd een nadere offerte in te dienen op grond van een nadere offerteaanvraag. U moet partijen voldoende tijd geven om in te schrijven, waarbij u inschat hoeveel tijd een contractspartij nodig heeft om een reële inschrijving te doen. De wetgever heeft daar geen nadere regels voor gegeven.
Voor het beoordelen van de nadere inschrijvingen bij de minicompetitie, waarbij het niet meer gaat om de voorwaarden die al in de raamovereenkomst zijn overeengekomen, maar bijvoorbeeld wel gaat om planning, aflevermoment, prijs en cv's van personen die de opdracht gaan uitvoeren, past u de gunningsvoorwaarden toe die u in de aanbestedingsstukken voor de raamovereenkomst hebt opgenomen. U mag dus geen afwijkende gunningscriteria gebruiken bij het plaatsen van de opdracht binnen de raamovereenkomst (let wel, de gunningscriteria voor gunning van de nadere opdrachten binnen de raamovereenkomst kunnen geheel andere zijn dan de gunningscriteria waarop de

raamovereenkomst zelf is gegund). U mag deze voorwaarden bij het plaatsen van een nadere opdracht niet meer wijzigen.

5.1.2.e
Afwezig: woensdag

T 5.1.2.e / 5.1.2.e (privé)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Verzonden: zondag 14 maart 2021 20:50
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
CC: 5.1.2.e <5.1.2.e @Kiesraad.nl>
Onderwerp: RE: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

`Zie onder. Paar aanpassingen in CAPITA vanwege goed Nls. XX is schrappen. En twee vragen.

Hieronder treft u de gevraagde informatie aan.

De Kiesraad heeft in 2020 een Europees aanbesteding traject afgerond met als resultaat raamovereenkomsten met 5 partijen voor hieronder genoemde twee percelen:

1. Perceel 1:
    a. het uitvoeren van pentesten en -veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software.
2. Perceel 2:
    a. het uitvoeren toetsing verkiezingssoftware en software- kwaliteitsonderzoek en Advisering over kwaliteit van (verkiezings)software

Bij de Europese aanbesteding heeft de Kiesraad XXXX (2 x 'heeft') de inkoopregels van het rijk gevolgd. DAARUIT vloeit voort dat UBR|HIS de inkoop heeft begeleidt.

De Europese aanbesteding bestond uit twee rondes; één ronde voor het selecteren van de geïnteresseerde partijen en één ronde voor het selecteren van de beste inschrijving.

Hieronder wordt ingegaan in op perceel 1. VRAAG WAAROM NIET HIER OVER PERCEEL 2 GERAPPORTEERD??

Op perceel 1 hebben ZICH vier partijen XXXX ingeschreven en zijn XX drie partijen geselecteerd. Op 29 juli 2020 is de aankondiging tot een gegunde opdracht gepubliceerd op tendernet. De drie partijen waarmee een raamovereenkomst IS afgesloten zijn Hackdefense, PWC en Fox IT. De duur van de raamovereenkomsten IS twee jaar, met de mogelijkheid om de raamovereenkomsten met tweemaal één jaar te verlengen.

De opdracht tot het uitvoeren van deze beveiligingstest is overeenkomstig de aanbestedingsprocedure gegund aan de partij met de hoogste score. Het gunningscriteriUM was de beste prijs-kwaliteitsverhouding waarbij het subgunningscriteriUM kwaliteit de weging had van 70 en het subgunningscriteriaUM prijs de weging had van 30.

Voor het selecteren van de beste inschrijving is een beoordeling uitgevoerd door een beoordelingsteam dAT bestond uit 4 medewerkers van het secretariaat van de Kiesraad en één adviseur van de UBR|HIS. Ieder lid van het team heeft een individuele beoordeling uitgevoerd op de vooraf aan de geselecteerde partijen bekend gemaakt criteria. Volgende opdrachten gaan via een mini competitie. WAT BEKENT DIT??

De publicatie van de Europese aanbesteding en de bijbehorende stukken zijn te vinden op TenderNed:
https://www.tenderned.nl/tenderned-tap/aankondigingen/182228;section=2

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Datum: zondag 14 mrt. 2021 4:02 PM

Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e @Kiesraad.nl>
Onderwerp: FW: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Hallo 5.1.2.e

Ben jij akkoord dat we jouw digitale handtekening gebruiken voor de afhandeling?

Groet,
5.1.2.e

Van: 5.1.2.e
Verzonden: zondag 14 maart 2021 15:42
Aan: 5.1.2.e <5.1.2.e @hotmail.com>; '5.1.2.e ' <5.1.2.e @planet.nl>; 5.1.2.e <5.1.2.e @rotterdam.nl>; 5.1.2.e <5.1.2.e @uva.nl>; 5.1.2.e <5.1.2.e @5.1.2.e >; 5.1.2.e <5.1.2.e @kiesraad.nl>; 'Prof.dr. 5.1.2.e ' <5.1.2.e @fsw.leidenuniv.nl>
CC: 5.1.2.e <5.1.2.e @Kiesraad.nl>; 5.1.2.e <5.1.2.e @kiesraad.nl>; Hormann, 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Beste leden,

Afgelopen vrijdag heeft BZK de in de bijlage opgenomen Kamervragen ontvangen van het TK-lid Baudet. De vragen gaan over de onafhankelijkheid van Hackdefense, de organisatie die voor ons de beveiliging van OSV2020 heeft onderzocht. Wij zijn door BZK gevraagd om in antwoord op vraag 7 input te verschaffen over de Europese aanbesteding die heeft geleid tot de gunning van de opdracht. In de bijlage de informatie die we met BZK in dit kader zullen delen.
De planning van BZK is om de antwoorden op de Kamervragen morgen naar de Kamer te sturen.

groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl> namens 5.1.2.e <5.1.2.e @minbzk.nl>
Datum: vrijdag 12 mrt. 2021 15:44
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Aan de voorzitter van de Kiesraad, 5.1.2.e
ter attentie van de secretaris-directeur, 5.1.2.e

Vandaag zijn bij het ministerie van BZK schriftelijke vragen ontvangen van het TK-lid Baudet over de onafhankelijkheid van de organisatie die de beveiliging van de verkiezingssoftware heeft onderzocht. De vragen zijn als bijlage bijgevoegd.
De opdracht aan Hackdefense waarop de kamervragen betrekking hebben is door de Kiesraad gegeven. Gelet daarop wil het ministerie van BZK graag een ambtsbericht ontvangen van de Kiesraad waarin de Kiesraad alle relevante informatie verschaft die nodig is voor het beantwoorden van vraag 7.

Graag ontvangt het ministerie van BZK dit ambtsbericht uiterlijk maandag 15 maart vóór 12.00 uur. De planning is er namelijk op gericht om de vragen zsm mogelijk, dat wil zeggen op 15 maart a.s. te beantwoorden.

De minister van Binnenlandse Zaken en Koninkrijksrelaties
Namens deze,

5.1.2.e
5.1.2.e

From: "5.1.2.e "
Sent: Mon, 15 Mar 2021 12:01:53 +0100
To: "5.1.2.e " <5.1.2.e @minbzk.nl>
Cc: "5.1.2.e " <5.1.2.e @minbzk.nl>
Subject: RE: Ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense
Attachments: Ambtsbericht voor de beantwoording van Tweede Kamervragen over HackDefense.pdf

Beste 5.1.2.e

Hierbij de definitieve versie van het Ambtsbericht voor de beantwoording van Tweede Kamervragen over HackDefense, voorzien van een handtekening van onze voorzitter Wim Kuijken.

Met vriendelijke groeten,

5.1.2.e
Officemanager
Aanwezig maandag, dinsdag en woensdag (tot 15:30 uur)
.....
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511 WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
.....
M 5.1.2.e
E 5.1.2.e @kiesraad.nl
W www.kiesraad.nl

Van: 5.1.2.e <5.1.2.e @minbzk.nl> 5.1.2.e <5.1.2.e @minbzk.nl>
Datum: vrijdag 12 mrt. 2021 15:44
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>, 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: ambtsbericht voor de beantwoording van Tweede Kamervragen over Hackdefense

Aan de voorzitter van de Kiesraad, 5.1.2.e
ter attentie van de secretaris-directeur, 5.1.2.e

Vandaag zijn bij het ministerie van BZK schriftelijke vragen ontvangen van het TK-lid Baudet over de onafhankelijkheid van de organisatie die de beveiliging van de verkiezingssoftware heeft onderzocht. De vragen zijn als bijlage bijgevoegd.
De opdracht aan Hackdefense waarop de kamervragen betrekking hebben is door de Kiesraad gegeven. Gelet daarop wil het ministerie van BZK graag een ambtsbericht ontvangen van de Kiesraad waarin de Kiesraad alle relevante informatie verschaft die nodig is voor het beantwoorden van vraag 7.

Graag ontvangt het ministerie van BZK dit ambtsbericht uiterlijk maandag 15 maart vóór 12.00 uur. De planning is er namelijk op gericht om de vragen zsm mogelijk, dat wil zeggen op 15 maart a.s. te beantwoorden.

De minister van Binnenlandse Zaken en Koninkrijksrelaties
Namens deze,

5.1.2.e
5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 17 november 2020 17:49
Aan: 5.1.2.e
Onderwerp: FW: nadere overeenkomst hertest OSV2020-U

Ter info

Van: 5.1.2.e
Verzonden: dinsdag 17 november 2020 17:49
Aan: '5.1.2.e'
CC: 5.1.2.e
Onderwerp: RE: nadere overeenkomst hertest OSV2020-U

Hallo 5.1.2.e

We hebben wat uitdaging bij enkele aanpassingen in OSV2020-U voor de Tweede Kamerverkiezing, waardoor Elect iT nog geen nieuwe versie van OSV2020-U heeft opgeleverd. Ik kan jullie daardoor volgende week nog niet de versie aanleveren voor de hertest. Zoals het er nu voorstaat komt de nieuwe versie van OSV2020-U over 2 weken. Is het voor jullie mogelijk de hertest van OSV2020-U te verplaatsen naar begin december?

Excuses dat het qua planning anders loopt dat we eerder hadden besproken, zodra ik meer duidelijkheid heb over wanneer Elect iT de nieuwe versie oplevert laat ik het je uiteraard weten.

Groet,
5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 12 november 2020 17:05
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Re: nadere overeenkomst hertest OSV2020-U

Hallo 5.1.2.e dat is prima, dan gaan we een update van het bestaande rapport maken.

Mag ik concluderen dat de offerte verder akkoord is? Dan hou ik 23 november e.v. vrij in onze planning.

5.1.2.e

On 11/12/20 3:09 PM, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Dank voor de offerte. In de offerte staat de vraag of we een korte rapportage aangaande de status, of, naar wens, een addendum bij het oorsponkelijke rapport. We hebben de voorkeur voor een addendum op het bestaande rapport zodat we een geüpdatet rapport met de status van OSV2020-U hebben.
>
> Groet,
> 5.1.2.e
>
> ---
>
> **Van:** 5.1.2.e
> **Verzonden:** maandag 9 november 2020 15:15
> **Aan:** 5.1.2.e
> **Onderwerp:** Re: nadere overeenkomst hertest OSV2020-U

Hallo 5.1.2.e

Ik had die tweet inderdaad gezien. En ben het eens met de reacties eronder, dat het feitelijk geen issue is. Maar we kijken ernaar!

Bijgaand een offerte voor de hertest!

5.1.2.e

On 11/6/20 12:32 PM, 5.1.2.e wrote:

> Hallo 5.1.2.e
>
> Op basis van de huidige planning verwacht ik 23/24-11 je de nieuwe versie van OSV2020-U te kunnen sturen voor de hertest. Aangezien de hertest betrekking heeft op de nieuwere versie voor de Tweede Kamer, zouden we je willen vragen om extra te kijken naar de bijgewerkte EML signing implementatie en een check op de kritische broncode wijzingen t.o.v. de vorige door jullie geteste versie. Via twitter werden wij nog gewezen op een onjuiste gebruik van Array.equals, als het goed is is dit door Elect aangepast naar MessageDigest.isEqual. Zouden jullie dit kunnen checken.
>
> We ontvangen inderdaad graag een offerte. Ik neem aan dat hertest binnen offerte opgave gaat plaatvinden, mocht echter blijken dat dat niet mogelijk is zal er voor eventuele aanvullende uren eerst goedkeuring moeten komen van onze zijde.
>
> Groet,
> 5.1.2.e

Van: 5.1.2.e <5.1.2.e@hackdefense.nl>
Verzonden: woensdag 28 oktober 2020 10:13
Aan: 5.1.2.e <5.1.2.e@kiesraad.nl>
Onderwerp: Re: nadere overeenkomst

Ha 5.1.2.e

Ik ben met onze planning voor november bezig en heb nog in potlood een hertest OSV2020-U staan.

Heb jij daar al meer nieuws over? M.n. wanneer we hem kunnen inplannen.

Zal ik er ook een offerte voor sturen trouwens? Is dat nodig? Hoeft voor mij niet per se maar kan me voorstellen dat dat in het proces noodzakelijk is.

Groet!

5.1.2.e

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was

sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Van: 5.1.2.e
Aan: 5.1.2.e
Cc: 5.1.2.e
Onderwerp: RE: Akkoord hertest Hackdefense OSV2020-U
Datum: dinsdag 10 november 2020 12:57:17

Graag akkoord.

Groet,
5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @kiesraad.nl>
Datum: dinsdag 10 nov. 2020 12:08
Aan: 5.1.2.e <5.1.2.e @kiesraad.nl>
Kopie: 5.1.2.e <5.1.2.e @kiesraad.nl>
Onderwerp: Akkoord hertest Hackdefense OSV2020-U

Hallo 5.1.2.e
We hebben een offerte van Hackdefense ontvangen voor het uitvoeren van de hertest op OSV2020-U. Hackdefense gaat uit van maximaal 5 dagen voor de hertest (€5.1.2.f excl. BTW/5.1.2.f incl. BTW). Graag je akkoord voor het laten uitvoeren van de hertest.
Groet,
5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 7 augustus 2020 15:06
Aan: 5.1.2.e
Onderwerp: RE: Verzoek om je akkoord op het instellen van een verplichting voor de NOK bij de ROK ARBIT inzake Specifieke pentest vervanging OSV met Hackdefense BV

Hallo 5.1.2.e

Dank en graag akkoord.

Groet,
5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 7 augustus 2020 14:33
5.1.2.e
Onderwerp: Verzoek om je akkoord op het instellen van een verplichting voor de NOK bij de ROK ARBIT inzake Specifieke pentest vervanging OSV met Hackdefense BV

5.1.2.e

Tussen de Kiesraad en HackDefense BV is een Raamovereenkomst ARBIT 2018 afgesloten inzake Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software.
Onder deze ROK wordt nu met Hackdefense BV (1e in de gunning van deze EA voor perceel 1) een Nadere Overeenkomst bij de Raamovereenkomst ARBIT inzake Specifieke pentest vervanging OSV afgesloten.

Voor de Nadere **Overeenkomst tussen Kiesraad en Hackdefense BV inzake Specifieke pentest vervanging OSV** dient een verplichting te worden ingesteld.

Vervolgens zal het systeem vragen om een goedkeuring van de geregistreerde voorlopige middelenbesteding. Doorgaans zou de collega bedrijfsvoering die goedkeuring dienen te geven; nu die functie vacant is, is dat niet mogelijk.
Via deze mail wil ik je akkoord/goedkeuring vragen op het ophogen van de verplichting; goedkeuring niet in het financiële systeem 3F maar op deze mail + bijlage. Je akkoord graag via een replay op deze mail, waarna ik het akkoord toevoeg aan het dossier in 3F en ik vervolgens zelf de goedkeuring kan uitvoeren, immers er is dan voldaan aan het vierogen-principe.

Relevante gegevens
De opdracht omvat:
- White-box pentest inclusief Secure Code Review en Configuratiereview op Vervanging OSV voor de software van de vaststelling van de uitslag en zetelverdeling.
- **Optioneel** Hertesten op de Opdracht

De NOK treedt in werking op het moment waarop deze door beide partijen is getekend; 30 juli 2020.
De NOK gaat in op 17 augustus 2020 en eindigt op 31 december 2020.

Opdrachtwaarde
-De Vergoeding voor de White-box pentest inclusief Secure Code Review en Configuratiereview op Vervanging OSV voor de software van de vaststelling van de uitslag en zetelverdeling bedraagt: **€** 5.1.2.f **excl. BTW, €** 5.1.2.f **incl. BTW**
-De vergoeding voor de optionele hertest is € 5.1.2.f excl. BTW, € 5.1.2.f incl. BTW per dag.
De optionele hertest wordt nu niet afgenomen. Zonodig wordt daarvoor door de Kiesraad schriftelijk aan Hackdefense een voorstel voor de hertest gevraagd. Zowel voorstel opdrachtnemer als akkoord opdrachtgever wordt schriftelijk vastgelegd.

Samengevat komt dat neer op:

Verplichting instellen voor NO met Hackdefense BV inzake Specifieke pentest vervanging OSV voor een totaalbedrag van € 5.1.2.f **incl. BTW.**
Verzoek om je akkoord op het instellen van de verplichting zoals hiervoor beschreven.
Bijgevoegd:
- Raamovereenkomst ARBIT 2018 inzake Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software.
- Nadere Overeenkomst bij de Raamovereenkomst ARBIT inzake Specifieke pentest vervanging OSV

Vriendelijke groet,
5.1.2.e

HackDefense

IT security, maar dan begrijpelijk

HackDefense BV
PO Box 3025, 2301 DA Leiden
(071) 204 0101
info@hackdefense.nl
https://hackdefense.nl/

IBAN: NL40 RABO 0337 2727 00
KvK: 69477043
BTW: NL857887270B01

Kiesraad
t.a.v. 5.1.2.e
5.1.2.e @kiesraad.nl

Leiden, 9 november 2020

Offerte hertest OSV2020-U [O20611]

Geachte 5.1.2.e beste 5.1.2.e

Zoals besproken ontvangt u hierbij ons voorstel om een hertest uit te voeren op OSV2020-U, op de bevindingen zoals beschreven in ons rapport van 13 oktober jl. met nummer PR20042.

Deze hertest zal plaatsvinden onder de voorwaarden van onze raamovereenkomst met nummer 201865007.433–P1 en nadere overeenkomst 201865007.433.001 (activiteit B2). Deze overeenkomsten bepalen een dagtarief van € 5.1.2.f en dat eventuele hertests op nacalculatiebasis worden uitgevoerd.

We verwachten voor een goede hertest maximaal 5 mensdagen inzet nodig te hebben en bieden deze hertest conform bovengenoemde overeenkomsten daarom aan op basis van nacalculatie van werkelijk gemaakte uren a € 5.1.2.f (exclusief BTW) per uur met een maximum van € 5.1.2.f

De hertest zal vanaf 23 november a.s. worden uitgevoerd en binnen 5 dagen worden afgerond met een korte rapportage aangaande de status, of, naar wens, een addendum bij het oorsponkelijke rapport.

De hertest zal de status bepalen van een nieuw aan te leveren versie van OSV2020-U ten aanzien van de bevindingen uit ons rapport d.d. 13 oktober, en daarbij extra aandacht besteden aan de bijgewerkte implementatie van *EML signing.* Ook zal een check worden gedaan op de kritische

broncode-wijzingen t.o.v. de vorige door ons geteste versie., en een via Twitter[1] gemelde wijziging in de code waarbij bij de vergelijking van twee hash-waaden de functie `Array.equals` is aangepast naar `MessageDigest.isEqual`.

Als u akkoord bent met dit voorstel, of vragen/opmerkingen heeft, dan gelieve dit schriftelijk aan mij mee te delen via 5.1.2.e `.nl`.

We danken u nogmaals voor het in ons gestelde vertrouwen en zien uit naar de voortzetting van onze plezierige samenwerking!

Met vriendelijke groet,

HackDefense BV

1 https://twitter.com/ProgrammerDude/status/1318498151876231168

Bijlage 3 - Dossier Financiële Afspraken

behorend bij

Raamovereenkomst ARBIT-2018

tussen

de Kiesraad

en

Fox-IT B.V.

inzake

Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software

met kenmerk

201865007.433 – P1 – Fox-IT B.V.

Inhoud

1. Inleiding

1.1. Doelstelling en positionering van dit document

In dit Dossier Financiële Afspraken (hierna "DFA") zijn, als onderdeel van de Raamovereenkomst, alle financiële afspraken opgenomen ten aanzien van de Raamovereenkomst inzake uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software. Het DFA is opgebouwd uit drie hoofdstukken. U leest:

- in hoofdstuk 1 een inleiding van dit DFA;
- in hoofdstuk 2 de prijsstelling c.q. tarieven van de Opdrachten, andere voorwaarden omtrent de prijsstelling c.q. tarieven;
- in hoofdstuk 3 de regels met betrekking tot de wijze van facturatie.

De voorwaarden van de Raamovereenkomst zijn van toepassing op hetgeen in dit DFA is vastgelegd waarbij de voorwaarden van de Raamovereenkomst prevaleren boven de voorwaarden in deze DFA. Begrippen die met een hoofdletter zijn geschreven zijn gedefinieerd in de Raamovereenkomst. De DFA is een Bijlage bij de Raamovereenkomst.

1.2. Looptijd DFA

De looptijd van het DFA is gelijk aan de looptijd van de Raamovereenkomst.

1.3. Documentbeheer

Dit document kan alleen worden gewijzigd na instemming van de daartoe gerechtigde contactpersonen van de Opdrachtgever en dient te voldoen aan de kaders van de wet- en regelgeving, waaronder ten minste de Aanbestedingswet 2012 wordt verstaan. Indien gedurende de looptijd aanpassingen worden overeengekomen, dan worden deze wijzigingen opgenomen in een op te stellen wijziging op de Raamovereenkomst. Wanneer er gedurende het jaar iets wijzigt, bijv. de contactpersoon of het factuuradres, dan kan er wel al gewerkt worden met bijv. de/het nieuw(e) CP/factuuradres en wordt dit in juli van het betreffende jaar vastgelegd in een nieuwe versie van het DFA. De verantwoordelijkheid voor het opstellen en onderhouden van het DFA ligt bij de Opdrachtgever.

2. Prijsaanbieding

2.1. Inleiding

De Wederpartij heeft naar aanleiding van het Bestek d.d. 1 mei 2020 een prijsaanbieding uitgebracht die is weergegeven in paragraaf 2.3 Prijzenblad.

2.2. Volledigheid prijsaanbieding en prijsontwikkeling

Wederpartij garandeert dat alle tijdens de looptijd van de Raamovereenkomst voorkomende kosten in de door hem geoffreerde Vergoedingen zijn opgenomen. Wederpartij is niet gerechtigd om andere Vergoedingen, kosten en/of prijzen in rekening te brengen dan de Vergoedingen (kosten en tarieven) die op grond van dit DFA en de Raamovereenkomst zijn afgesproken.

Bij uitbreidingen op de overeengekomen Prestatie en/of bij het afnemen van nieuwe Prestaties dient Wederpartij marktconforme Vergoedingen aan te blijven bieden.

2.3. Prijzenblad

De op het moment van ondertekening vastgestelde maximale Vergoedingen zijn in onderstaand prijzenblad vastgelegd. Deze Vergoedingen en tarieven zijn inclusief alle overige kosten (waaronder ook tenminste wordt verstaan administratie- reis-, verblijf- en verwerkingskosten) en in euro's (€).

Tarieven Standaard pentesten

Tarieven standaard pentest	Vaste Vergoeding exclusief btw	Vaste Vergoeding inclusief btw
Standaard pentest OSV	€ 5.1.2.f	€ 5.1.2.f
Standaard pentest Vervanging OSV	€ 5.1.2.f	€ 5.1.2.f
Standaard pentest Databank verkiezingsuitslagen	€ 5.1.2.f	€ 5.1.2.f
Standaard pentest nieuw digitaal hulpmiddel	N.o.t.k. op basis van het hieronder genoemde maximum dagtarief.	

Tarieven overige Opdrachten
Het maximale dagtarief voor overige Opdrachten bedraagt € 5.1.2.f exclusief btw en € 5.1.2.f inclusief btw.

De Vergoedingen voor Opdrachten worden uiteindelijk door Opdrachtgever vastgelegd in een Nadere Overeenkomst of bestelopdracht, conform de bepaalde procedures in artikel 5 en 6 van de Raamovereenkomst

2.4. Afspraken omtrent prijzen, tarieven en Vergoedingen

Let op: De volgende eisen zijn relevant voor beide Partijen:
1. Wederpartij offreert in Nadere Offertes geen hogere tarieven dan de hierboven opgenomen tarieven.
2. Wederpartij voert hertesten op standaard pentesten uit op basis van nacalculatie conform de tarieven (in casu € 5.1.2.f exclusief btw) die voor de standaard pentesten gelden. Wederpartij geeft voorafgaand aan een hertest een onderbouwing van de kosten en de duur van de hertest aan en voert die hertesten pas uit na akkoord van Opdrachtgever.

Deze eisen zijn overgenomen uit Bijlage 1 bij het Bestek.

2.5. Indexering

De overeengekomen tarieven kunnen gedurende de looptijd van de Raamovereenkomst niet worden geïndexeerd.

3. Regels met betrekking tot facturatie

3.1. Factuurspecificatie

Een factuur bevat tenminste de volgende gegevens:
- factuurdatum
- beschrijving van de verrichtte Opdracht
- hoogte van de Vergoeding
- verschuldigde btw
- contractnummer
- verplichtingennummer

Daarnaast gelden in beginsel altijd alle voorwaarden met betrekking tot facturering, betaling etc. uit de ARBIT-2018.

Zonder bovenstaande informatie kan een factuur niet in behandeling worden genomen. Wederpartij dient bij onvolledige facturering een creditfactuur uit te reiken en een nieuwe factuur in te dienen met de juiste en volledige informatie.

3.2. Wijze van factureren

De wijze van factureren dient te voldoen aan de volgende uitgangspuntenten tenzij anders overeengekomen in een gesloten Nadere Overeenkomst of bestelopdracht.

Wijze van facturatie
Wederpartij zendt de facturen onder vermelding van contractnummer en verplichtingennummer aan het centrale aanleverpunt voor e-facturen bij de Rijksoverheid:

- Factuuradres/OIN nummer: 00000001003214345000
- Ministerie/afdeling:
  Ministerie van Binnenlandse Zaken en Koninkrijksrelaties/Kiesraad
  T.a.v. het Financieel Dienstencentrum (FDC)
  Postbus 13178
  2501 ED Den Haag
- Budgetcodering: H2B 401002-10024-44011
- Verplichtingnummer: Staat in Nadere Overeenkomst of bestelopdracht
- Afschrift factuur: 5.1.2.e @Kiesraad.nl

Raamovereenkomst ARBIT-2018

tussen

de Kiesraad

en

Fox-IT B.V.

inzake

Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software

met kenmerk

201865007.433 – P1 – Fox-IT B.V.

Raamovereenkomst ARBIT-2018 inzake het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software
Contractnummer: 201865007.433 – P1 – Fox-IT B.V.

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Kiesraad,
namens deze,
de secretaris-directeur van de Kiesraad, 5.1.2.e
hierna te noemen: Opdrachtgever,

en

2. Fox-IT B.V.,
(statutair) gevestigd te Delft,
te dezen vertegenwoordigd door,
de directeur Managed Services, 5.1.2.e
hierna te noemen: Wederpartij,

Hierna gezamenlijk te noemen: Partijen.

Overwegende dat:

a. Opdrachtgever verantwoordelijk is voor een goed verloop van de kandidaatstelling en een correcte vaststelling van de uitslag van landelijke verkiezingen. Opdrachtgever gebruikt in het kader van de uitoefening van zijn taak software die de processen van kandidaatstelling, de vaststelling van de verkiezingsuitslag en de toewijzing van zetels aan kandidaten ondersteunt;
b. Opdrachtgever in het kader van de uitoefening van zijn taak behoefte heeft aan het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software;
c. Opdrachtgever in verband met hetgeen hiervoor onder a en b is overwogen, tot aanbesteding van het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software door middel van een niet-openbare Europese aanbestedingsprocedure is overgegaan;
d. Op 24 januari 2020 door of namens Opdrachtgever een aankondiging naar het Supplement op het Publicatieblad van de Europese Unie (hierna: Publicatieblad) is verzonden en dat deze aankondiging is gepubliceerd onder nummer 2020/S 020-044550;
e. Wederpartij een verzoek tot deelname heeft ingediend;
f. Opdrachtgever dit verzoek tot deelname heeft beoordeeld en het resultaat op 24 maart 2020 kenbaar heeft gemaakt aan de geselecteerden;
g. Opdrachtgever op 1 mei 2020 drie (3) geselecteerden, waaronder Wederpartij, heeft uitgenodigd om een inschrijving in te dienen;
h. Wederpartij op 4 juni 2020 een Inschrijving heeft uitgebracht;
i. Opdrachtgever de opdracht op 1 juli 2020 voorlopig heeft gegund aan drie (3) inschrijvers waaronder Wederpartij;
j. Opdrachtgever op basis van deze Raamovereenkomst Wederpartij opnieuw kan oproepen tot mededinging met het oog op het sluiten van een Nadere Overeenkomst.

Inhoud

Komen overeen:

1. Begrippen

In de Raamovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan is gegeven in de Voorwaarden. In aanvulling daarop wordt onder de navolgende begrippen indien met een beginhoofdletter gebruikt, verstaan:

#	Begrip	Definitie
1.1	Nadere Overeenkomst	De schriftelijke overeenkomst tussen Opdrachtgever en Wederpartij, waarmee nadere opdrachten worden verstrekt onder de gesloten Raamovereenkomst. Het format concept Nadere Overeenkomst is bijgevoegd als Bijlage 7.
1.2	Raamovereenkomst	Deze overeenkomst.
1.3	Nadere Offerte	Een aanbieding voor een opdracht tot het verrichten van een Prestatie die Wederpartij naar aanleiding van een Nadere oproep tot mededinging uitbrengt aan Opdrachtgever onder de Raamovereenkomst.
1.4	Nadere oproep tot mededinging	Een uitnodiging door Opdrachtgever onder de Raamovereenkomst aan de geselecteerde Wederpartijen tot het uitbrengen van een Nadere Offerte voor een opdracht tot het verrichten van een Prestatie.
1.5	Inschrijving	Het aanbod d.d. 4 juni 2020 van Wederpartij aan Opdrachtgever op basis van het Bestek, zoals aangevuld op d.d. 12 juni 2020 en 18 juni 2020.

2. Voorwerp van de Raamovereenkomst

2.1. Partijen sluiten hierbij een Raamovereenkomst op grond waarvan Opdrachtgever gerechtigd is Wederpartij op te roepen tot mededinging via een Nadere oproep tot mededinging. Op basis van de door Wederpartij uitgebrachte Nadere Offerte kan Opdrachtgever met Wederpartij Nadere Overeenkomsten sluiten. Daarnaast heeft Opdrachtgever de mogelijkheid om Opdrachten voor standaard pentesten weg te zetten via het roulatiesysteem, zoals beschreven in artikel 6.

2.2. Nadere Overeenkomsten worden op basis van een Nadere oproep tot mededinging afgesloten op basis van de als Bijlage 7 opgenomen Format Nadere Overeenkomst. Opdrachten voor Standaard pentesten worden afgesloten, middels het roulatiesysteem zoals beschreven in artikel 6, op basis van het als Bijlage 8 opgenomen format bestelopdracht.

2.3. De navolgende stukken vormen gezamenlijk de Raamovereenkomst. Voor zover deze stukken met elkaar in tegenspraak zijn, prevaleert het eerdergenoemde stuk boven het later genoemde:
1) dit document;
2) de ARBIT-2018;
3) de nota van inlichtingen d.d. 22 mei 2020 (perceel 1);
4) de nota van inlichtingen d.d. 7 mei 2020 (perceel 1);
5) het Dossier Financiële Afspraken;
6) het Bestek d.d. 1 mei 2020 met kenmerk 201850004.213.001 inclusief Bijlagen;
7) de door Wederpartij aan Opdrachtgever uitgebrachte Inschrijving inclusief Bijlagen van 4 juni 2020 zonder kenmerk, zoals aangevuld op d.d. 12 juni 2020 en 18 juni 2020.

3. Contactpersonen en rapportage

3.1. De personen die de contacten over de uitvoering van de Raamovereenkomst onderhouden zijn:
Voor Opdrachtgever: 5.1.2.e ;
E: 5.1.2.e @kiesraad.nl
T: 5.1.2.e
M: 5.1.2.e

Voor Wederpartij: Fox-IT B.V.
C: 5.1.2.e
E: 5.1.2.e @fox-it.com
T: 5.1.2.e

4. Inwerkingtreding en duur van de Raamovereenkomst

4.1. De Raamovereenkomst treedt in werking op het moment waarop deze door beide partijen is ondertekend.

4.2. De Raamovereenkomst heeft een looptijd van 27 juli 2020 tot en met 26 juli 2023.

4.3. Opdrachtgever kan de Raamovereenkomst onder gelijkblijvende voorwaarden voor een periode van maximaal twaalf (12) maanden verlengen. Indien Opdrachtgever van dit recht gebruik wenst te maken doet hij hiervan uiterlijk drie (3) maanden voor het einde van de in artikel 4.2 bedoelde looptijd schriftelijk mededeling aan Wederpartij.

5. Minicompetitie

5.1. Opdrachtgever kan Wederpartij opnieuw oproepen tot mededinging via een Nadere oproep tot mededinging voor Opdrachten met betrekking tot pentesten en veiligheidsonderzoeken op aanvraag en advisering over beveiliging van (verkiezings)software.

5.2. In de volgende gevallen is Opdrachtgever niet verplicht om **alle gecontracteerde wederpartijen** uit te nodigen voor een Nadere oproep tot mededinging: indien het gaat over advisering over beveiliging van (verkiezings)software en de geraamde waarde van de Opdracht kleiner is dan € 5.1.2.f exclusief btw. Opdrachtgever vraagt in deze situatie een Nadere Offerte op aan Wederpartij en beoordeelt vervolgens of deze Nadere Offerte voldoet aan de eisen van Opdrachtgever en deze Raamovereenkomst. Opdrachtgever vraagt een Nadere Offerte op bij één van de gecontracteerde wederpartijen op basis van de roulatiemethodiek in artikel 6.2.

5.3. Wederpartij brengt binnen vijftien (15) Werkdagen na dagtekening van de Nadere oproep tot mededinging een Nadere Offerte uit aan Opdrachtgever op het in de Nadere oproep tot mededingen genoemde adres. De hiervoor genoemde termijn is een Fatale termijn. In geval van Spoed kan Opdrachtgever deze termijn terugbrengen tot zeven (7) Werkdagen en motiveert het spoedeisende belang in de Nadere oproep tot mededinging.

5.4. Indien de Nadere Offerte niet binnen de in artikel 5.3 gestelde termijn door Opdrachtgever is ontvangen of deze niet voldoet aan de daaraan gestelde eisen dan wordt Wederpartij geacht geen Nadere Offerte te hebben gedaan.

5.5. Indien Wederpartij twee keer nalaat een Nadere Offerte uit te brengen, kan Opdrachtgever de Raamovereenkomst ontbinden.

5.6. Opdrachtgever beoordeelt de Nadere Offerte op basis van de in de Nadere oproep tot mededinging vastgestelde criteria en informeert Wederpartij met bekwame spoed over de

uitkomst daarvan. Een afwijzing van de Nadere Offerte wordt schriftelijk gemotiveerd. Opdrachtgever sluit met de Wederpartij die de economische meest voordelige Nadere Offerte heeft ingediend een Nadere Overeenkomst af.

5.7. Indien geen van de door Opdrachtgever tot mededinging opgeroepen wederpartijen op een daartoe strekkend verzoek van Opdrachtgever een Nadere Offerte doet mag Opdrachtgever de opdracht bij een derde partij plaatsen, dit wil zeggen een partij buiten deze Raamovereenkomst.

6. Roulatiesysteem

6.1. Opdrachtgever hanteert een roulatiesysteem tussen de gecontracteerde Wederpartijen voor Opdrachten met betrekking tot standaard pentesten op de volgende testobjecten:
   a. OSV;
   b. Vervanging OSV;
   c. Databank Verkiezingsuitslagen;
   d. De nader te ontwikkelen digitale hulpmiddelen.

6.2. Opdrachtgever verstrekt de Opdrachten voor standaard pentesten in roulatie op de volgende wijze, conform de afgesproken tarieven in artikel 7.1 en overige voorwaarden in deze Raamovereenkomst.
   a. De eerste standaard pentest wordt verstrekt aan de wederpartij die als eerste (1e) in de ranking van de Aanbesteding is geëindigd (in casu "HackDefense B.V.");
   b. De tweede standaard pentest wordt verstrekt aan de wederpartij die als tweede (2e) in de ranking van de Aanbesteding is geëindigd (in casu "PricewaterhouseCoopers Advisory N.V.");
   c. De derde standaard pentest wordt verstrekt aan de wederpartij die als derde (3e) in de ranking van de Aanbesteding is geëindigd (in casu "Fox-IT B.V.");
   d. De vierde standaard pentest wordt verstrekt aan de wederpartij die als eerste (1e) in de ranking van de Aanbesteding is geëindigd (in casu "HackDefense B.V.");
   e. Etc.

6.3. Opdrachtgever verstrekt een Opdracht voor een standaard pentest middels Bijlage 8 aan Wederpartij.

6.4. Indien Opdrachtgever een second opinion wil laten uitvoeren dan verstrekt Opdrachtgever deze Opdracht aan de volgende Wederpartij in het roulatiesysteem. Indien deze Opdracht het uitvoeren van een volledige second opinion (dit wil zeggen dat volledige opdracht nogmaals wordt uitgevoerd) betreft, vervalt hiermee voor deze wederpartij het recht op het uitvoeren van de volgende standaard pentest.

6.5. Wederpartij is verplicht om een standaard pentest uit te voeren. Indien een Wederpartij niet in staat is om een standaard pentest uit te voeren, kan de Opdrachtgever besluiten de Raamovereenkomst te ontbinden.

6.6. Opdrachtgever houdt een administratie bij met daarin een overzicht van de verstrekte Opdrachten met betrekking tot standaard pentesten en andere Opdrachten die middels het roulatiesysteem mogen en zijn weggezet. Opdrachtgever deelt dit overzicht op verzoek met Wederpartij.

7. Prijzen en tarieven

7.1. De maximale prijs c.q. tarieven die Wederpartij aan Opdrachtgever mag offreren naar aanleiding van een Nadere oproep tot mededinging als bedoeld in artikel 5 en het roulatiesysteem als bedoeld in artikel 6 zijn vastgelegd in het Bijlage 3 - Dossier Financiële Afspraken.

8. Facturering en betaling

8.1. Afspraken omtrent facturatie zijn vastgelegd in Bijlage 3 - Dossier Financiële Afspraken.

9. Algemene en bijzondere voorwaarden

9.1. De toepasselijkheid van algemene en bijzondere voorwaarden van Wederpartij dan wel van door Wederpartij bij het verrichten van de Prestatie te betrekken derden, is uitgesloten, tenzij daarvan in de Nadere Overeenkomst expliciet wordt afgeweken.

9.2. De voor het gebruik van de Prestatie vereiste acceptatie van algemene of bijzondere voorwaarden, zoals bijvoorbeeld bij "shrink-wrap"- en "click-wrap" licenties, bindt Opdrachtgever niet. Wederpartij vrijwaart Opdrachtgever dat dergelijke acceptaties niet leiden tot enige beperking op het Overeengekomen gebruik.

9.3. Een exemplaar van de ARBIT-2018 is bij de Raamovereenkomst gevoegd als Bijlage 1.

9.4. Wederpartij voert de opdracht uit in overeenstemming met de toepasselijke wet- en (beroeps)regelgeving. Opdrachtnemer is nimmer gehouden tot enig handelen of nalaten dat met de hiervoor bedoelde regels strijdig of onverenigbaar is.

9.5. Artikel 29.3 uit de ARBIT-2018 wordt als volgt aangepast: Wederpartij overlegt op verzoek onverwijld bewijs van premiebetaling aan Opdrachtgever.

9.6. De artikelen 38 tot en met 41, 42 tot en met 47, 57 tot en met 60, 61 tot en met 67 en 68 tot en met 84 uit de ARBIT-2018 zijn niet van toepassing op deze Raamovereenkomst.

10. Social return

10.1 Voor de Wederpartij geldt een inspanningsverplichting tot het inzetten van personeel met een afstand tot de arbeidsmarkt, waarbij wordt gestreefd naar een inzet van circa 5% van de loonsom van de Raamovereenkomst en daaronder vallende Nadere Overeenkomsten en bestelopdrachten te besteden aan extra werk(ervarings)plaatsen voor mensen behorende uit de doelgroep:

- Wet Werk en Bijstand (WWB) gerechtigden, die langer werkloos zijn dan 12 maanden, 50 jaar of ouder zijn en/of die zonder re-integratieondersteuning of andere begeleiding niet zelfstandig aan werk kunnen komen.
- Werkloosheidswet (WW) gerechtigden, die langer werkloos zijn dan 12 maanden, en/of 50 jaar of ouder zijn.
- Wet Werk en Inkomen naar Arbeidsvermogen (WIA) gerechtigden.
- Regeling Werkhervatting Gedeeltelijk Arbeidsgeschikten (WGA) gerechtigden.
- Wet Arbeidsongeschiktheid zelfstandigen (WAZ) gerechtigden.
- Wet Arbeidsongeschiktheidsvoorziening Jonggehandicapten (WAJONG) gerechtigden.
- Wet Inkomensvoorziening Oudere en gedeeltelijk Arbeidsongeschikte Werkloze werknemers (IOAW) gerechtigden.
- De Wet Inkomensvoorziening Oudere en gedeeltelijk Arbeidsongeschikte gewezen Zelfstandigen (IOAZ) gerechtigden.
- Wet Sociale Werkvoorziening (WSW) geïndiceerden.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

- Leer/werkplekken voor niet uitkeringsgerechtigde werkzoekenden (nuggers)
- Leer/werkplekken voor vroegtijdig schoolverlaters en jongeren met onvoldoende kwalificaties.
- Leer/werkplekken in het kader van BOL/BBL-opleidingen, VSO en/of praktijkscholen.

Dan wel een andere wijze waarbij minimaal een vergelijkbare impact wordt behaald m.b.t. het verkleinen van de afstand tot de arbeidsmarkt voor de doelgroep zoals hierboven beschreven. Opdrachtgever bepaalt of de impact minimaal vergelijkbaar is en gaat daarover met Opdrachtnemer in gesprek.

10.2 Als de in artikel 10.1 genoemde wetten vervanging krijgen in nieuwe wetten, dan verwijst dit artikel voortaan naar die nieuwe wetten.

10.3 Wederpartij levert uiterlijk binnen twee (2) maanden na tweezijdige ondertekening van de Raamovereenkomst een plan van aanpak op aan Opdrachtgever, waarin Wederpartij beschrijft hoe Wederpartij social return gaat toepassen bij de uitvoering van de Nadere Overeenkomsten en bestelopdrachten, conform het gestelde in artikel 10.1. Het plan van aanpak bevat tenminste de volgende onderwerpen:
a. De manier waarop u het afgesproken percentage realiseert of een andere manier waarop u een vergelijkbare impact realiseert;
b. De vorm van begeleiding van de social return-medewerkers;
c. Hoe u de kwaliteit van de werkzaamheden waarborgt.

10.4 Wederpartij biedt het plan van aanpak ter Acceptatie aan Opdrachtgever aan. Na Acceptatie door Opdrachtgever maakt het plan van aanpak onderdeel uit van deze Raamovereenkomst.

10.5 Wederpartij rapporteert jaarlijks in juli conform Bijlage 6 aan Opdrachtgever de daadwerkelijke percentages aan (extra) werk(ervarings)plaatsen.

11. Vrijwaringsverklaring

11.1 Opdrachtgever geeft Wederpartij expliciet en uitsluitend toestemming tot het uitvoeren van Opdrachten, zoals pentesten en andere veiligheidsonderzoeken, die binnen de reikwijdte van deze Raamovereenkomst vallen. Opdrachtgever zal bij het aangaan van een Nadere Overeenkomst of het verstrekken van een bestelopdracht nader specificeren waar de toestemming in het concrete geval op ziet. Daarbij geldt een vrijwaring van de aansprakelijkheid volgens de reikwijdte zoals beschreven in artikel 11.2.

11.2 Wederpartij is niet aansprakelijk voor schade die ontstaat als gevolg van het uitvoeren van Opdrachten met betrekking tot pentesten en andere veiligheidsonderzoeken op toegewezen informatiesystemen van Opdrachtgever, mits de betreffende aanspraak betrekking heeft op werkzaamheden die vallen binnen de reikwijdte van de betreffende Opdracht en de betreffende werkzaamheden zijn verricht conform het bepaalde in deze Raamovereenkomst. Opdrachtgever vrijwaart de Wederpartij tegen aansprakelijkheden, waarin een derde zich direct of indirect beroept op de artikelen 161sexies, 161septies, 138ab (computervredebreuk) en 138b (hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden) van het Wetboek van Strafrecht.

11.3 Deze handelingen, zoals genoemd in artikel 11.2, voltrekken zich onder de uitdrukkelijke voorwaarde dat Wederpartij uitsluitend de beveiliging tracht te analyseren, te doorbreken en/of toegang tracht te verwerven tot door de Opdrachtgever aangegeven onderdelen van het informatiesysteem of de informatiesystemen.

11.4 De vrijwaring als omschreven in 11.2 ziet niet op schade die is ontstaan door een toerekenbare tekortkoming bij het uitvoeren van de Raamovereenkomst c.q. Opdrachten door Wederpartij, dan wel bij opzet, bewuste roekeloosheid, ernstige verwijtbaarheid door Wederpartij.

12. Geheimhoudingsverklaring

12.1 In aanvulling op artikel 17 van de ARBIT-2018, leggen Opdrachtgever en Wederpartij de volgende aanvullende afspraken vast ten aanzien van geheimhouding:

a. Wederpartij zal alle informatie, die hem/haar gedurende het verdere verloop van deze Raamovereenkomst en daarmee de uitvoering van de onderhavige overheidsopdrachten / Opdrachten ter kennis komt en waarvan hij/zij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden (hierna: Vertrouwelijk informatie), vertrouwelijk behandelen en op generlei wijze bekendmaken buiten de eigen organisatie, daaronder vallen in het bijzonder alle documenten en informatie welke zowel schriftelijk, als mondeling worden verstrekt, in het kader van de uitvoering van de Raamovereenkomst, behalve voor zover vigerende beroeps- en gedragsregels, enig wettelijk voorschrift of uitspraak van de rechter hem/haar tot bekendmaking verplicht of voor zover Opdrachtgever hiervoor toestemming heeft gegeven. Informatie van algemene bekendheid en/of informatie die door Opdrachtgever openbaar is gemaakt valt buiten de werkingssfeer van de geheimhoudingsplicht.
b. Wederpartij neemt passende technische en organisatorische maatregelen om de Vertrouwelijke informatie te beveiligen en beveiligd te houden tegen verlies of enige vorm van onzorgvuldig, ondeskundig of onrechtmatig handelen;
c. Wederpartij maakt de vertrouwelijke informatie uitsluitend bekend binnen de eigen organisatie aan personen die deze informatie nodig hebben voor het doel waarvoor Opdrachtgever deze informatie heeft verstrekt en verplicht de betreffende personen tot geheimhouding van deze informatie.
d. In geval van schending van de geheimhoudingsplicht heeft Opdrachtgever het recht deze Raamovereenkomst en eventuele lopende Nadere Overeenkomsten of bestelopdrachten onmiddellijk te ontbinden. Opdrachtgever is vervolgens geen kosten meer verschuldigd en op Opdrachtgever kan geen schade worden verhaald.
e. Wederpartij is zich ervan bewust dat schending van de geheimhoudingsplicht kan leiden tot schade bij Opdrachtgever en derden en dat zijn/haar organisatie gehouden is tot niet alleen betaling van de boete maar daarnaast ook tot vergoeding van de schade die is ontstaan als gevolg van een schending van de geheimhoudingsplicht.
f. Wederpartij zal, na afloop van het verrichten van een Prestatie, de documenten (zowel digitaal als in hard copy) met vertrouwelijke informatie direct na Acceptatie van de Prestatie vernietigen en Opdrachtgever hiervan uit eigen beweging op de hoogte stellen, met dien verstande dat Wederpartij voor zover op grond van de wet of beroeps- en gedragsregels vereist – na voorafgaand overleg met de Opdrachtgever één exemplaar van de relevante vertrouwelijke informatie mag bewaren. De geheimhoudingsverplichting uit deze Raamovereenkomst blijft ten alle tijden voortduren, dus ook na afloop of beëindiging van deze Raamovereenkomst
g. Wederpartij garandeert dat (i) ondergetekende bekend is met de relevante wet- en regelgeving in Nederland, (ii) zich er van bewust is dat schending hiervan een strafbaar feit kan zijn en (iii) dat noch ondergetekende, noch een van haar directeuren, functionarissen, medewerkers, werknemers en professionele adviseurs of andere vanwege Wederpartij betrokkenen hoe ook door Wederpartij ingeschakeld of genoemd deze wet- en regelgeving zal overtreden in verband met de voorgenomen Opdracht.

13. Slotbepaling

13.1 Afwijkingen van deze Raamovereenkomst, een Nadere Overeenkomst of een bestelopdracht zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.

13.2 Door ondertekening van deze Raamovereenkomst vervallen alle eventueel eerder door Partijen gemaakte mondelinge en schriftelijke afspraken omtrent het verstrekken van opdrachten tot het verrichten van Diensten, al dan niet onder een Nadere Overeenkomst.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Plaats: Den Haag
Datum: 22-7-2020

De Kiesraad
namens deze,
de secretaris-directeur,

5.1.2.e

5.1.2.e

Plaats: Delft
Datum: 27-7-2020

Fox-IT B.V.
namens deze,
de directeur Managed Services,

5.1.2.e

5.1.2.e

Overzicht bijlagen:
1. de ARBIT-2018;
2. de nota van inlichtingen d.d. 7 mei 2020 en de 2de nota van inlichtingen d.d. 22 mei 2020 (perceel 1);
3. het Dossier Financiële Afspraken;
4. het Bestek d.d. 1 mei 2020 met kenmerk 201850004.213.001;
5. de door Wederpartij aan Opdrachtgever uitgebrachte Inschrijving van 4 juni 2020 zoals aangevuld op d.d. 12 juni 2020 en 18 juni 2020;
6. Verantwoordingsformulier social return;
7. Format Nadere Overeenkomst;
8. Format bestelopdracht;
9. Format Verwerkersovereenkomst.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 1 - ARBIT-2018
Reeds in bezet van beide Partijen, initieel bijgevoegd als Bijlage B bij het Bestek.

Bijlage 2 - Nota van inlichtingen d.d. 7 mei 2020 en de 2de nota van inlichtingen d.d. 22 mei 2020 (perceel 1)

Reeds in bezit van beide Partijen, ten tijde van de aanbesteding beschikbaar gesteld via TenderNed.

Bijlage 3 - Dossier Financiële Afspraken
Bijgevoegd en geparafeerd door beide Partijen.

Bijlage 4 - Bestek d.d. 01 mei 2020 met kenmerk 201850004.213.001
Reeds in bezit van beide Partijen, beschikbaar gesteld op 1 mei 2020 via TenderNed.

Bijlage 5 - Inschrijving van 4 juni 2020 zoals aangevuld op d.d. 12 juni 2020 en 18 juni 2020

Reeds in bezit van beide Partijen.

Bijlage 6 - Verantwoordingsformulier social return

Toelichting
Opdrachtgever controleert de uitvoering van de social return voorwaarde door middel van dit verantwoordingsformulier. Wederpartij overlegt dit formulier jaarlijkse aan Opdrachtgever. Wederpartij dient aan te geven dat hij aan het overeengekomen percentage heeft voldaan en de ingezette arbeidskracht(en) een social return indicatie heeft (hebben).

Over de Rijksbrede en interdepartementale aanbestedingen met social return zal jaarlijks extra worden gecontroleerd middels een steekproef. Op dat moment wordt de Wederpartij verzocht inzage te verlenen in de arbeidsovereenkomsten, die deels moeten worden afgeschermd, van de ingezette social return werknemers. Tevens zal ook gesproken worden over de wijze van begeleiding en uw ervaringen met de inzet van het instrument.

2 Verantwoordingstabel social return artikel 10 uit de Raamovereenkomst

Periode inzet (Datum)	Persoon	Indicatie ingezette arbeidskracht *(bijv. WWB, WSW, WIA, etc.)*	Wervingskanaal *(bijv. gemeente, UWV, etc.)*	Over deze periode gehaalde waarde van de loonsom	Cumulatief	Nog te realiseren
				€/uren	€/uren	€/uren
				€/uren	€/uren	€/uren
				€/uren	€/uren	€/uren
				€/uren	€/uren	€/uren
Totaal				**€/uren**	**€/uren**	**€/uren**

Let op: de kolom "Persoon" mag geen Persoonsgegevens (naam) bevatten. U dient de Persoonsgegevens te anonimiseren door bijvoorbeeld een fictieve naam of nummering toe te kennen aan de ingezette medewerkers.

3 Akkoord
Foxt-IT B.V. verklaart hierbij dat zij voldoet aan haar verplichting voor social return. Deze verplichting staat in artikel 10 en verder in de Raamovereenkomst met als naam: Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software met het kenmerk: 201865007.433 – P1 – Fox-IT B.V.

4 Ondertekening

Naam organisatie	
Naam ondertekening bevoegd persoon	
Datum	
Handtekening	

Bijlage 7 - Format Nadere Overeenkomst
In bezit van beide Partijen, onderdeel van het Bestek, Bijlage H.

Bijlage 8 - Format bestelopdracht
In bezit van beide Partijen, onderdeel van het Bestek, Bijlage J.

Bijlage 9 - Format Verwerkersovereenkomst
In bezit van beide Partijen, onderdeel van het Bestek, Bijlage I.

Bijlage 3 - Dossier Financiële Afspraken

behorend bij

Raamovereenkomst ARBIT-2018

tussen

de Kiesraad

en

HackDefense B.V.

inzake

Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software

met kenmerk

201865007.433 – P1 – HackDefense B.V.

Inhoud

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

1. Inleiding

1.1. Doelstelling en positionering van dit document

In dit Dossier Financiële Afspraken (hierna "DFA") zijn, als onderdeel van de Raamovereenkomst, alle financiële afspraken opgenomen ten aanzien van de Raamovereenkomst inzake uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software. Het DFA is opgebouwd uit drie hoofdstukken. U leest:

- in hoofdstuk 1 een inleiding van dit DFA;
- in hoofdstuk 2 de prijsstelling c.q. tarieven van de Opdrachten andere voorwaarden omtrent de prijsstelling c.q. tarieven;
- in hoofdstuk 3 de regels met betrekking tot de wijze van facturatie.

De voorwaarden van de Raamovereenkomst zijn van toepassing op hetgeen in dit DFA is vastgelegd waarbij de voorwaarden van de Raamovereenkomst prevaleren boven de voorwaarden in deze DFA. Begrippen die met een hoofdletter zijn geschreven zijn gedefinieerd in de Raamovereenkomst. De DFA is een Bijlage bij de Raamovereenkomst.

1.2. Looptijd DFA

De looptijd van het DFA is gelijk aan de looptijd van de Raamovereenkomst.

1.3. Documentbeheer

Dit document kan alleen worden gewijzigd na instemming van de daartoe gerechtigde contactpersonen van de Opdrachtgever en dient te voldoen aan de kaders van de wet- en regelgeving, waaronder ten minste de Aanbestedingswet 2012 wordt verstaan. Indien gedurende de looptijd aanpassingen worden overeengekomen, dan worden deze wijzigingen opgenomen in een op te stellen wijziging op de Raamovereenkomst. Wanneer er gedurende het jaar iets wijzigt, bijv. de contactpersoon of het factuuradres, dan kan er wel al gewerkt worden met bijv. de/het nieuw(e) CP/factuuradres en wordt dit in juli van het betreffende jaar vastgelegd in een nieuwe versie van het DFA. De verantwoordelijkheid voor het opstellen en onderhouden van het DFA ligt bij de Opdrachtgever.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

2. Prijsaanbieding

2.1. Inleiding

De Wederpartij heeft naar aanleiding van het Bestek d.d. 1 mei 2020 een prijsaanbieding uitgebracht die is weergegeven in paragraaf 2.3 Prijzenblad.

2.2. Volledigheid prijsaanbieding en prijsontwikkeling

Wederpartij garandeert dat alle tijdens de looptijd van de Raamovereenkomst voorkomende kosten in de door hem geoffreerde Vergoedingen zijn opgenomen. Wederpartij is niet gerechtigd om andere Vergoedingen, kosten en/of prijzen in rekening te brengen dan de Vergoedingen (kosten en tarieven) die op grond van dit DFA en de Raamovereenkomst zijn afgesproken.

Bij uitbreidingen op de overeengekomen Prestatie en/of bij het afnemen van nieuwe Prestaties dient Wederpartij marktconforme Vergoedingen aan te blijven bieden.

2.3. Prijzenblad

De op het moment van ondertekening vastgestelde maximale Vergoedingen zijn in onderstaand prijzenblad vastgelegd. Deze Vergoedingen en tarieven zijn inclusief alle overige kosten (waaronder ook tenminste wordt verstaan administratie- reis-, verblijf- en verwerkingskosten) en in euro's (€).

Tarieven Standaard pentesten

Tarieven standaard pentest	Vaste Vergoeding exclusief btw	Vaste Vergoeding inclusief btw
Standaard pentest OSV	€ 5.1.2.f	€ 5.1.2.f
Standaard pentest Vervanging OSV	€ 5.1.2.f	€ 5.1.2.f
Standaard pentest Databank verkiezingsuitslagen	€ 5.1.2.f	€ 5.1.2.f
Standaard pentest nieuw digitaal hulpmiddel	N.o.t.k. op basis van het hieronder genoemde maximum dagtarief.	

Tarieven overige Opdrachten
Het maximale dagtarief voor overige Opdrachten bedraagt € 5.1.2.f exclusief btw en € 5.1.2.f inclusief btw.

De Vergoedingen voor Opdrachten worden uiteindelijk door Opdrachtgever vastgelegd in een Nadere Overeenkomst of bestelopdracht, conform de bepaalde procedures in artikel 5 en 6 van de Raamovereenkomst

2.4. Afspraken omtrent prijzen, tarieven en Vergoedingen

Let op: De volgende eisen zijn relevant voor beide Partijen:

1. Wederpartij offreert in Nadere Offertes geen hogere tarieven dan de hierboven opgenomen tarieven.
2. Wederpartij voert hertesten op standaard pentesten uit op basis van nacalculatie conform de tarieven (in casu € 5.1.2.f exclusief btw) die voor de standaard pentesten gelden. Wederpartij geeft voorafgaand aan een hertest een onderbouwing van de kosten en de duur van de hertest aan en voert die hertesten pas uit na akkoord van Opdrachtgever.

Deze eisen zijn overgenomen uit Bijlage 1 bij het Bestek.

2.5. Indexering

De overeengekomen tarieven kunnen gedurende de looptijd van de Raamovereenkomst niet worden geïndexeerd.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

3. Regels met betrekking tot facturatie

3.1. Factuurspecificatie

Een factuur bevat tenminste de volgende gegevens:

- factuurdatum
- beschrijving van de verrichtte Opdracht
- hoogte van de Vergoeding
- verschuldigde btw
- contractnummer
- verplichtingennummer

Daarnaast gelden in beginsel altijd alle voorwaarden met betrekking tot facturering, betaling etc. uit de ARBIT-2018.

Zonder bovenstaande informatie kan een factuur niet in behandeling worden genomen. Wederpartij dient bij onvolledige facturering een creditfactuur uit te reiken en een nieuwe factuur in te dienen met de juiste en volledige informatie.

3.2. Wijze van factureren

De wijze van factureren dient te voldoen aan de volgende uitgangspuntenten tenzij anders overeengekomen in een gesloten Nadere Overeenkomst of bestelopdracht.

Wijze van facturatie
Wederpartij zendt de facturen onder vermelding van contractnummer en verplichtingennummer aan het centrale aanleverpunt voor e-facturen bij de Rijksoverheid:

- Factuuradres/OIN nummer: 00000001003214345000
- Ministerie/afdeling:
  Ministerie van Binnenlandse Zaken en Koninkrijksrelaties/Kiesraad
  T.a.v. het Financieel Dienstencentrum (FDC)
  Postbus 13178
  2501 ED Den Haag
- Budgetcodering: H2B 5.1.2.e
- Verplichtingnummer: Staat in Nadere Overeenkomst of bestelopdracht
- Afschrift factuur: 5.1.2.e @Kiesraad.nl

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Nadere Overeenkomst bij Raamovereenkomst ARBIT inzake het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software

tussen

de Kiesraad

en

HackDefense B.V.

inzake

Specifieke pentest Vervanging OSV

met kenmerk

201865007.433.001

Model Nadere Overeenkomst bij de Raamovereenkomst ARBIT inzake Specifieke pentest vervanging OSV
Contractnummer: 201865007.433.001
Verplichtingennummer: 401002

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Kiesraad,
namens deze,
de secretaris-directeur van de Kiesraad, 5.1.2.e
hierna te noemen: Opdrachtgever,

en

2. HackDefense B.V.,
(statutair) gevestigd te Delft,
te dezen vertegenwoordigd door,
de directeur, 5.1.2.e
hierna te noemen: Wederpartij,

Hierna gezamenlijk te noemen: Partijen.

Overwegende dat:
a. Opdrachtgever verantwoordelijk is voor een goed verloop van de kandidaatstelling en een correcte vaststelling van de uitslag van landelijke verkiezingen. Opdrachtgever gebruikt in het kader van de uitoefening van zijn taak software die de processen van kandidaatstelling, de vaststelling van de verkiezingsuitslag en de toewijzing van zetels aan kandidaten ondersteunt;
b. Opdrachtgever in het kader van de uitoefening van zijn taak behoefte heeft aan een specifieke pentest op vervanging OSV;
c. Opdrachtgever in zijn behoefte wenst te voorzien door met Wederpartij een Nadere Overeenkomst aan te gaan onder de Raamovereenkomst inzake het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software met ingangsdatum 27 juli 2020 met kenmerk 201865007.433 – P1 – HackDefense B.V;
d. Opdrachtgever in verband met hetgeen hiervoor is overwogen, tot aanbesteding van een specifieke pentest op vervanging OSV - eind augustus/september 2020 - door middel van het Bestek d.d. 01 mei 2020 is overgegaan;
e. Wederpartij op 4 juni 2020 een Inschrijving heeft ingediend;
f. Opdrachtgever de opdracht op 1 juli 2020 voorlopig heeft gegund aan Wederpartij.

Inhoud

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Komen overeen:

1. Begrippen

In de Nadere Overeenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan is gegeven in de Voorwaarden en de Raamovereenkomst.

2. Voorwerp van de Nadere Overeenkomst

2.1. Partijen sluiten hierbij op basis van de Raamovereenkomst een Nadere Overeenkomst waarbij Wederpartij zich tegen de in artikel 7 bedoelde Vergoeding verbindt tot het verrichten van de Prestatie zoals beschreven in het Bestek, die in hoofdlijnen bestaat uit:

- het uitvoeren van de Opdracht / de Opdrachten:

Volg nummer	Onderwerp	Aantal
B1	White-box pentest inclusief Secure Code Review en Configuratiereview op Vervanging OSV voor de software van de vaststelling van de uitslag en zetelverdeling conform hetgeen staat beschreven in het Bestek en de Inschrijving van Wederpartij.	*1*
B2	**Optioneel** Hertesten op de Opdracht met volgnummer B1	*Op afroep door Opdrachtgever*

Eén en ander teneinde Opdrachtgever in staat te stellen daarvan het Overeengekomen gebruik te maken.

2.2. De navolgende stukken vormen gezamenlijk de Nadere Overeenkomst. Voor zover deze stukken met elkaar in tegenspraak zijn, prevaleert het eerder genoemde stuk boven het later genoemde:
1) dit document;
2) de Raamovereenkomst met kenmerk 201865007.433 – P1 – HackDefense B.V;
3) het Bestek d.d. 01 mei 2020 inclusief Bijlagen;
4) de Inschrijving d.d. 4 juni 2020 inclusief Bijlagen, zoals aangevuld op d.d. 11 juni 2020.

3. Contactpersonen

3.1. De personen die de contacten over de uitvoering van de Nadere Overeenkomst onderhouden zijn:
Voor Opdrachtgever: 5.1.2.e;
E: 5.1.2.e @kiesraad.nl
T: 5.1.2.e
M: 5.1.2.e

Voor Wederpartij: HackDefense B.V.
C: 5.1.2.e
E: 5.1.2.e @hackdefense.nl
T: 5.1.2.e
M: 5.1.2.e

4. Inwerkingtreding en duur van de Nadere Overeenkomst

4.1. De Nadere Overeenkomst treedt in werking op het moment waarop deze door beide partijen is ondertekend.

4.2. De Nadere Overeenkomst gaat in op 17 augustus 2020 en eindigt op 31 december 2020.

5. Oplevering

5.1. Wederpartij draagt zorg voor Oplevering op de in de onderstaande tabel vermelde wijze, datum en plaats. Genoemde data zijn Fatale termijnen.

Volg-nummer	Onderwerp	Wijze van Oplevering	Adres en datum
B1	White-box pentest inclusief Secure Code Review en Configuratiereview op Vervanging OSV voor de software van de vaststelling van de uitslag en zetelverdeling	*Een definitief rapport conform het gestelde in het Bestek en het aangebodene in de Inschrijving.*	*De Kiesraad* *Muzenstraat 85* *2511 WB Den Haag* *Binnen twintig Werkdagen na opdrachtverstrekking door Opdrachtgever.*
B2	**Optioneel** Hertesten op de Opdracht met volgnummer B1	*Nader te bepalen in overleg met de contactpersoon van Opdrachtgever*	*In overleg met en na afroep door de contactpersoon van Opdrachtgever*

6. Acceptatie

6.1. Acceptatie

Volg-nummer	Onderwerp	Acceptatie	Uiterste datum van mededeling van (non-) Acceptatie
B1	White-box pentest inclusief Secure Code Review en Configuratiereview op Vervanging OSV voor de software van de vaststelling van de uitslag en zetelverdeling	*In overleg met Opdrachtgever.*	30 dagen na Oplevering (11.1 ARBIT)
B2	**Optioneel** Hertesten op de Opdracht met volgnummer B1	*In overleg met Opdrachtgever.*	30 dagen na Oplevering (11.1 ARBIT)

7. Vergoeding

7.1. Partijen komen de navolgende Vergoeding voor volgnummer B1 overeen:

Volg-nummer	Onderwerp	Prijs excl. Btw	Prijs incl. btw
B1	De Vergoeding voor de White-box pentest inclusief Secure Code Review en Configuratiereview op Vervanging OSV voor de software van de vaststelling van de uitslag en zetelverdeling bedraagt:	€ 5.1.2.f	€ 5.1.2.f
De Vergoeding voor de Prestatie bedraagt:		€ 5.1.2.f	€ 5.1.2.f

7.2. Partijen komen de navolgende Vergoeding overeen **op basis van nacalculatie** voor volgnummer B2, indien van **deze optie** gebruik wordt gemaakt. Wederpartij:

Volg-nummer	Onderwerp	Prijs excl. Btw per dag	Prijs incl. btw per dag
B2	Het tarief per dag voor het uitvoeren van een hertest:	€ 5.1.2.f	€ 5.1.2.f

Opdrachtgever vraagt schriftelijk aan Wederpartij een voorstel voor de hertest. Opdrachtgever ontvangt van Wederpartij een voorstel en geeft schriftelijk akkoord op dit voorstel aan Wederpartij. Dit voorstel wordt na akkoord van Opdrachtgever, onderdeel van deze Nadere Overeenkomst en onderliggende voorwaarden.

8. Facturering en betaling

8.1. De Vergoeding is verschuldigd vanaf:

Volg-nummer	Onderwerp	Tijdstip van verschuldigdheid
B1	Whitebox pentest op vervanging OSV, Configuratiereview op vervanging OSV en Secure Code Review op Vervanging OSV	*Na Acceptatie*
B2	**Optioneel** Hertesten op de Opdracht met volgnummer B1.	*Na Acceptatie op basis van nacalculatie (op halve dagen afgerekend).*

8.2 Wederpartij zendt de facturen onder vermelding van bovengenoemd contractnummer en verplichtingennummer conform de wijze zoals beschreven in Bijlage 3 – Dossier Financiële Afspraken van de Raamovereenkomst.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Plaats: Den Haag
Datum: 28-7-2020

De Kiesraad
namens deze,
de secretaris-directeur,

5.1.2.e

5.1.2.e

Plaats: Leiden
Datum: 30-7-2020

HackDefense B.V.
namens deze,
de directeur,

5.1.2.e

5.1.2.e

Overzicht bijlagen:

1. het Bestek d.d. 1 mei 2020 inclusief Bijlagen;
2. de Inschrijving d.d. 4 juni 2020 inclusief Bijlagen, zoals aangevuld op d.d. 11 juni 2020;
3. De Raamovereenkomst met kenmerk 201865007.433 – P1 – HackDefense B.V.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 1 - Bestek d.d. 1 mei 2020 met kenmerk 201850004.213.001
Reeds in bezit van beide Partijen, beschikbaar gesteld op 1 mei 2020 via TenderNed.

Bijlage 2 - Inschrijving van 4 juni 2020 zoals aangevuld op d.d. 11 juni 2020
Reeds in bezit van beide Partijen.

Bijlage 3 – Raamovereenkomst met kenmerk 201865007.433 – P1 – HackDefense B.V.
Reeds in bezit van beide Partijen.

Raamovereenkomst ARBIT-2018

tussen

de Kiesraad

en

HackDefense B.V.

inzake

Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software

met kenmerk

201865007.433 – P1 – HackDefense B.V.

Raamovereenkomst ARBIT-2018 inzake het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software
Contractnummer: 201865007.433 – P1 – HackDefense B.V.

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Kiesraad,
namens deze,
de secretaris-directeur van de Kiesraad, 5.1.2.e
hierna te noemen: Opdrachtgever,

en

2. HackDefense B.V.,
(statutair) gevestigd te Leiden,
te dezen vertegenwoordigd door,
de directeur, 5.1.2.e
hierna te noemen: Wederpartij,

Hierna gezamenlijk te noemen: Partijen.

Overwegende dat:

a. Opdrachtgever verantwoordelijk is voor een goed verloop van de kandidaatstelling en een correcte vaststelling van de uitslag van landelijke verkiezingen. Opdrachtgever gebruikt in het kader van de uitoefening van zijn taak software die de processen van kandidaatstelling, de vaststelling van de verkiezingsuitslag en de toewijzing van zetels aan kandidaten ondersteunt;
b. Opdrachtgever in het kader van de uitoefening van zijn taak behoefte heeft aan het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software;
c. Opdrachtgever in verband met hetgeen hiervoor onder a en b is overwogen, tot aanbesteding van het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software door middel van een niet-openbare Europese aanbestedingsprocedure is overgegaan;
d. Op 24 januari 2020 door of namens Opdrachtgever een aankondiging naar het Supplement op het Publicatieblad van de Europese Unie (hierna: Publicatieblad) is verzonden en dat deze aankondiging is gepubliceerd onder nummer 2020/S 020-044550;
e. Wederpartij een verzoek tot deelname heeft ingediend;
f. Opdrachtgever dit verzoek tot deelname heeft beoordeeld en het resultaat op 24 maart 2020 kenbaar heeft gemaakt aan de geselecteerden;
g. Opdrachtgever op 1 mei 2020 drie (3) geselecteerden, waaronder Wederpartij, heeft uitgenodigd om een inschrijving in te dienen;
h. Wederpartij op 4 juni 2020 een Inschrijving heeft uitgebracht;
i. Opdrachtgever de opdracht op 1 juli 2020 voorlopig heeft gegund aan drie (3) inschrijvers waaronder Wederpartij;
j. Opdrachtgever op basis van deze Raamovereenkomst Wederpartij opnieuw kan oproepen tot mededinging met het oog op het sluiten van een Nadere Overeenkomst.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Inhoud

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Komen overeen:

1. Begrippen

In de Raamovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan is gegeven in de Voorwaarden. In aanvulling daarop wordt onder de navolgende begrippen indien met een beginhoofdletter gebruikt, verstaan:

#	Begrip	Definitie
1.1	Nadere Overeenkomst	De schriftelijke overeenkomst tussen Opdrachtgever en Wederpartij, waarmee nadere opdrachten worden verstrekt onder de gesloten Raamovereenkomst. Het format concept Nadere Overeenkomst is bijgevoegd als Bijlage 7.
1.2	Raamovereenkomst	Deze overeenkomst.
1.3	Nadere Offerte	Een aanbieding voor een opdracht tot het verrichten van een Prestatie die Wederpartij naar aanleiding van een Nadere oproep tot mededinging uitbrengt aan Opdrachtgever onder de Raamovereenkomst.
1.4	Nadere oproep tot mededinging	Een uitnodiging door Opdrachtgever onder de Raamovereenkomst aan de geselecteerde Wederpartijen tot het uitbrengen van een Nadere Offerte voor een opdracht tot het verrichten van een Prestatie.
1.5	Inschrijving	Het aanbod d.d. 4 juni 2020 van Wederpartij aan Opdrachtgever op basis van het Bestek, zoals aangevuld op d.d. 11 juni.

2. Voorwerp van de Raamovereenkomst

2.1. Partijen sluiten hierbij een Raamovereenkomst op grond waarvan Opdrachtgever gerechtigd is Wederpartij op te roepen tot mededinging via een Nadere oproep tot mededinging. Op basis van de door Wederpartij uitgebrachte Nadere Offerte kan Opdrachtgever met Wederpartij Nadere Overeenkomsten sluiten. Daarnaast heeft Opdrachtgever de mogelijkheid om Opdrachten voor standaard pentesten weg te zetten via het roulatiesysteem, zoals beschreven in artikel 6.

2.2. Nadere Overeenkomsten worden op basis van een Nadere oproep tot mededinging afgesloten op basis van de als Bijlage 7 opgenomen Format Nadere Overeenkomst. Opdrachten voor Standaard pentesten worden afgesloten, middels het roulatiesysteem zoals beschreven in artikel 6, op basis van het als Bijlage 8 opgenomen format bestelopdracht.

2.3. De navolgende stukken vormen gezamenlijk de Raamovereenkomst. Voor zover deze stukken met elkaar in tegenspraak zijn, prevaleert het eerdergenoemde stuk boven het later genoemde:

1) dit document;
2) de ARBIT-2018;
3) de nota van inlichtingen d.d. 22 mei 2020 (perceel 1);
4) de nota van inlichtingen d.d. 7 mei 2020 (perceel 1);
5) het Dossier Financiële Afspraken;
6) het Bestek d.d. 1 mei 2020 met kenmerk 201850004.213.001 inclusief Bijlagen;
7) de door Wederpartij aan Opdrachtgever uitgebrachte Inschrijving inclusief Bijlagen van 4 juni 2020 zonder kenmerk, zoals aangevuld op d.d. 11 juni.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

3. Contactpersonen en rapportage

3.1. De personen die de contacten over de uitvoering van de Raamovereenkomst onderhouden zijn:
Voor Opdrachtgever: 5.1.2.e ;
E: 5.1.2.e @kiesraad.nl
T: 5.1.2.e
M: 5.1.2.e

Voor Wederpartij: HackDefense B.V.
Eerste contactpersoon
C: 5.1.2.e
E: 5.1.2.e @hackdefense.nl
T: 5.1.2.e
M: 5.1.2.e

Tweede contactpersoon
C: 5.1.2.e
E: 5.1.2.e @hackdefense.nl
M: 5.1.2.e

4. Inwerkingtreding en duur van de Raamovereenkomst

4.1. De Raamovereenkomst treedt in werking op het moment waarop deze door beide partijen is ondertekend.

4.2. De Raamovereenkomst heeft een looptijd van 27 juli 2020 tot en met 26 juli 2023.

4.3. Opdrachtgever kan de Raamovereenkomst onder gelijkblijvende voorwaarden voor een periode van maximaal twaalf (12) maanden verlengen. Indien Opdrachtgever van dit recht gebruik wenst te maken doet hij hiervan uiterlijk drie (3) maanden voor het einde van de in artikel 4.2 bedoelde looptijd schriftelijk mededeling aan Wederpartij.

5. Minicompetitie

5.1. Opdrachtgever kan Wederpartij opnieuw oproepen tot mededinging via een Nadere oproep tot mededinging voor Opdrachten met betrekking tot pentesten en veiligheidsonderzoeken op aanvraag en advisering over beveiliging van (verkiezings)software.

5.2. In de volgende gevallen is Opdrachtgever niet verplicht om **alle gecontracteerde wederpartijen** uit te nodigen voor een Nadere oproep tot mededinging: indien het gaat over advisering over beveiliging van (verkiezings)software en de geraamde waarde van de Opdracht kleiner is dan € 5.1.2.f exclusief btw. Opdrachtgever vraagt in deze situatie een Nadere Offerte op aan Wederpartij en beoordeelt vervolgens of deze Nadere Offerte voldoet aan de eisen van Opdrachtgever en deze Raamovereenkomst. Opdrachtgever vraagt een Nadere Offerte op bij één van de gecontracteerde wederpartijen op basis van de roulatiemethodiek in artikel 6.2.

5.3. Wederpartij brengt binnen vijftien (15) Werkdagen na dagtekening van de Nadere oproep tot mededinging een Nadere Offerte uit aan Opdrachtgever op het in de Nadere oproep tot mededingen genoemde adres. De hiervoor genoemde termijn is een Fatale termijn. In geval van Spoed kan Opdrachtgever deze termijn terugbrengen tot zeven (7) Werkdagen en motiveert het spoedeisende belang in de Nadere oproep tot mededinging.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

5.4. Indien de Nadere Offerte niet binnen de in artikel 5.3 gestelde termijn door Opdrachtgever is ontvangen of deze niet voldoet aan de daaraan gestelde eisen dan wordt Wederpartij geacht geen Nadere Offerte te hebben gedaan.

5.5. Indien Wederpartij twee keer nalaat een Nadere Offerte uit te brengen, kan Opdrachtgever de Raamovereenkomst ontbinden.

5.6. Opdrachtgever beoordeelt de Nadere Offerte op basis van de in de Nadere oproep tot mededinging vastgestelde criteria en informeert Wederpartij met bekwame spoed over de uitkomst daarvan. Een afwijzing van de Nadere Offerte wordt schriftelijk gemotiveerd. Opdrachtgever sluit met de Wederpartij die de economische meest voordelige Nadere Offerte heeft ingediend een Nadere Overeenkomst af.

5.7. Indien geen van de door Opdrachtgever tot mededinging opgeroepen wederpartijen op een daartoe strekkend verzoek van Opdrachtgever een Nadere Offerte doet mag Opdrachtgever de opdracht bij een derde partij plaatsen, dit wil zeggen een partij buiten deze Raamovereenkomst.

6. Roulatiesysteem

6.1. Opdrachtgever hanteert een roulatiesysteem tussen de gecontracteerde Wederpartijen voor Opdrachten met betrekking tot standaard pentesten op de volgende testobjecten:
   a. OSV;
   b. Vervanging OSV;
   c. Databank Verkiezingsuitslagen;
   d. De nader te ontwikkelen digitale hulpmiddelen.

6.2. Opdrachtgever verstrekt de Opdrachten voor standaard pentesten in roulatie op de volgende wijze, conform de afgesproken tarieven in artikel 7.1 en overige voorwaarden in deze Raamovereenkomst.
   a. De eerste standaard pentest wordt verstrekt aan de wederpartij die als eerste (1e) in de ranking van de Aanbesteding is geëindigd (in casu "HackDefense B.V.");
   b. De tweede standaard pentest wordt verstrekt aan de wederpartij die als tweede (2e) in de ranking van de Aanbesteding is geëindigd (in casu "PricewaterhouseCoopers Advisory N.V.");
   c. De derde standaard pentest wordt verstrekt aan de wederpartij die als derde (3e) in de ranking van de Aanbesteding is geëindigd (in casu "Fox-IT B.V.");
   d. De vierde standaard pentest wordt verstrekt aan de wederpartij die als eerste (1e) in de ranking van de Aanbesteding is geëindigd (in casu "HackDefense B.V.");
   e. Etc.

6.3. Opdrachtgever verstrekt een Opdracht voor een standaard pentest middels Bijlage 8 aan Wederpartij.

6.4. Indien Opdrachtgever een second opinion wil laten uitvoeren dan verstrekt Opdrachtgever deze Opdracht aan de volgende Wederpartij in het roulatiesysteem. Indien deze Opdracht het uitvoeren van een volledige second opinion (dit wil zeggen dat volledige opdracht nogmaals wordt uitgevoerd) betreft, vervalt hiermee voor deze wederpartij het recht op het uitvoeren van de volgende standaard pentest.

6.5. Wederpartij is verplicht om een standaard pentest uit te voeren. Indien een Wederpartij niet in staat is om een standaard pentest uit te voeren, kan de Opdrachtgever besluiten de Raamovereenkomst te ontbinden.

6.6. Opdrachtgever houdt een administratie bij met daarin een overzicht van de verstrekte Opdrachten met betrekking tot standaard pentesten en andere Opdrachten die middels het roulatiesysteem mogen en zijn weggezet. Opdrachtgever deelt dit overzicht op verzoek met Wederpartij.

7. Prijzen en tarieven

7.1. De maximale prijs c.q. tarieven die Wederpartij aan Opdrachtgever mag offreren naar aanleiding van een Nadere oproep tot mededinging als bedoeld in artikel 5 en het roulatiesysteem als bedoeld in artikel 6 zijn vastgelegd in het Bijlage 3 - Dossier Financiële Afspraken.

8. Facturering en betaling

8.1. Afspraken omtrent facturatie zijn vastgelegd in Bijlage 3 - Dossier Financiële Afspraken.

9. Algemene en bijzondere voorwaarden

9.1. De toepasselijkheid van algemene en bijzondere voorwaarden van Wederpartij dan wel van door Wederpartij bij het verrichten van de Prestatie te betrekken derden, is uitgesloten, tenzij daarvan in de Nadere Overeenkomst expliciet wordt afgeweken.

9.2. De voor het gebruik van de Prestatie vereiste acceptatie van algemene of bijzondere voorwaarden, zoals bijvoorbeeld bij "shrink-wrap"- en "click-wrap" licenties, bindt Opdrachtgever niet. Wederpartij vrijwaart Opdrachtgever dat dergelijke acceptaties niet leiden tot enige beperking op het Overeengekomen gebruik.

9.3. Een exemplaar van de ARBIT-2018 is bij de Raamovereenkomst gevoegd als Bijlage 1.

9.4. Wederpartij voert de opdracht uit in overeenstemming met de toepasselijke wet- en (beroeps)regelgeving. Opdrachtnemer is nimmer gehouden tot enig handelen of nalaten dat met de hiervoor bedoelde regels strijdig of onverenigbaar is.

9.5. Artikel 29.3 uit de ARBIT-2018 wordt als volgt aangepast: Wederpartij overlegt op verzoek onverwijld bewijs van premiebetaling aan Opdrachtgever.

9.6. De artikelen 38 tot en met 41, 42 tot en met 47, 57 tot en met 60, 61 tot en met 67 en 68 tot en met 84 uit de ARBIT-2018 zijn niet van toepassing op deze Raamovereenkomst.

10. Social return

10.1 Voor de Wederpartij geldt een inspanningsverplichting tot het inzetten van personeel met een afstand tot de arbeidsmarkt, waarbij wordt gestreefd naar een inzet van circa 5% van de loonsom van de Raamovereenkomst en daaronder vallende Nadere Overeenkomsten en bestelopdrachten te besteden aan extra werk(ervarings)plaatsen voor mensen behorende uit de doelgroep:

- Wet Werk en Bijstand (WWB) gerechtigden, die langer werkloos zijn dan 12 maanden, 50 jaar of ouder zijn en/of die zonder re-integratieondersteuning of andere begeleiding niet zelfstandig aan werk kunnen komen.
- Werkloosheidswet (WW) gerechtigden, die langer werkloos zijn dan 12 maanden, en/of 50 jaar of ouder zijn.
- Wet Werk en Inkomen naar Arbeidsvermogen (WIA) gerechtigden.
- Regeling Werkhervatting Gedeeltelijk Arbeidsgeschikten (WGA) gerechtigden.
- Wet Arbeidsongeschiktheid zelfstandigen (WAZ) gerechtigden.
- Wet Arbeidsongeschiktheidsvoorziening Jonggehandicapten (WAJONG) gerechtigden.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

- Wet Inkomensvoorziening Oudere en gedeeltelijk Arbeidsongeschikte Werkloze werknemers (IOAW) gerechtigden.
- De Wet Inkomensvoorziening Oudere en gedeeltelijk Arbeidsongeschikte gewezen Zelfstandigen (IOAZ) gerechtigden.
- Wet Sociale Werkvoorziening (WSW) geïndiceerden.
- Leer/werkplekken voor niet uitkeringsgerechtigde werkzoekenden (nuggers)
- Leer/werkplekken voor vroegtijdig schoolverlaters en jongeren met onvoldoende kwalificaties.
- Leer/werkplekken in het kader van BOL/BBL-opleidingen, VSO en/of praktijkscholen.

Dan wel een andere wijze waarbij minimaal een vergelijkbare impact wordt behaald m.b.t. het verkleinen van de afstand tot de arbeidsmarkt voor de doelgroep zoals hierboven beschreven. Opdrachtgever bepaalt of de impact minimaal vergelijkbaar is en gaat daarover met Opdrachtnemer in gesprek.

10.2 Als de in artikel 10.1 genoemde wetten vervanging krijgen in nieuwe wetten, dan verwijst dit artikel voortaan naar die nieuwe wetten.

10.3 Wederpartij levert uiterlijk binnen twee (2) maanden na tweezijdige ondertekening van de Raamovereenkomst een plan van aanpak op aan Opdrachtgever, waarin Wederpartij beschrijft hoe Wederpartij social return gaat toepassen bij de uitvoering van de Nadere Overeenkomsten en bestelopdrachten, conform het gestelde in artikel 10.1. Het plan van aanpak bevat tenminste de volgende onderwerpen:

a. De manier waarop u het afgesproken percentage realiseert of een andere manier waarop u een vergelijkbare impact realiseert;
b. De vorm van begeleiding van de social return-medewerkers;
c. Hoe u de kwaliteit van de werkzaamheden waarborgt.

10.4 Wederpartij biedt het plan van aanpak ter Acceptatie aan Opdrachtgever aan. Na Acceptatie door Opdrachtgever maakt het plan van aanpak onderdeel uit van deze Raamovereenkomst.

10.5 Wederpartij rapporteert jaarlijks in juli conform Bijlage 6 aan Opdrachtgever de daadwerkelijke percentages aan (extra) werk(ervarings)plaatsen.

11. Vrijwaringsverklaring

11.1 Opdrachtgever geeft Wederpartij expliciet en uitsluitend toestemming tot het uitvoeren van Opdrachten, zoals pentesten en andere veiligheidsonderzoeken, die binnen de reikwijdte van deze Raamovereenkomst vallen. Opdrachtgever zal bij het aangaan van een Nadere Overeenkomst of het verstrekken van een bestelopdracht nader specificeren waar de toestemming in het concrete geval op ziet. Daarbij geldt een vrijwaring van de aansprakelijkheid volgens de reikwijdte zoals beschreven in artikel 11.2.

11.2 Wederpartij is niet aansprakelijk voor schade die ontstaat als gevolg van het uitvoeren van Opdrachten met betrekking tot pentesten en andere veiligheidsonderzoeken op toegewezen informatiesystemen van Opdrachtgever, mits de betreffende aanspraak betrekking heeft op werkzaamheden die vallen binnen de reikwijdte van de betreffende Opdracht en de betreffende werkzaamheden zijn verricht conform het bepaalde in deze Raamovereenkomst. Opdrachtgever vrijwaart de Wederpartij tegen aansprakelijkheden, waarin een derde zich direct of indirect beroept op de artikelen 161sexies, 161septies, 138ab (computervredebreuk) en 138b (hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden) van het Wetboek van Strafrecht.

11.3 Deze handelingen, zoals genoemd in artikel 11.2, voltrekken zich onder de uitdrukkelijke voorwaarde dat Wederpartij uitsluitend de beveiliging tracht te analyseren, te doorbreken en/of toegang tracht te verwerven tot door de Opdrachtgever aangegeven onderdelen van het informatiesysteem of de informatiesystemen.

11.4 De vrijwaring als omschreven in 11.2 ziet niet op schade die is ontstaan door een toerekenbare tekortkoming bij het uitvoeren van de Raamovereenkomst c.q. Opdrachten door Wederpartij, dan wel bij opzet, bewuste roekeloosheid, ernstige verwijtbaarheid door Wederpartij.

12. Geheimhoudingsverklaring

12.1 In aanvulling op artikel 17 van de ARBIT-2018, leggen Opdrachtgever en Wederpartij de volgende aanvullende afspraken vast ten aanzien van geheimhouding:

a. Wederpartij zal alle informatie, die hem/haar gedurende het verdere verloop van deze Raamovereenkomst en daarmee de uitvoering van de onderhavige overheidsopdrachten / Opdrachten ter kennis komt en waarvan hij/zij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden (hierna: Vertrouwelijk informatie), vertrouwelijk behandelen en op generlei wijze bekendmaken buiten de eigen organisatie, daaronder vallen in het bijzonder alle documenten en informatie welke zowel schriftelijk, als mondeling worden verstrekt, in het kader van de uitvoering van de Raamovereenkomst, behalve voor zover vigerende beroeps- en gedragsregels, enig wettelijk voorschrift of uitspraak van de rechter hem/haar tot bekendmaking verplicht of voor zover Opdrachtgever hiervoor toestemming heeft gegeven. Informatie van algemene bekendheid en/of informatie die door Opdrachtgever openbaar is gemaakt valt buiten de werkingssfeer van de geheimhoudingsplicht.
b. Wederpartij neemt passende technische en organisatorische maatregelen om de Vertrouwelijke informatie te beveiligen en beveiligd te houden tegen verlies of enige vorm van onzorgvuldig, ondeskundig of onrechtmatig handelen;
c. Wederpartij maakt de vertrouwelijke informatie uitsluitend bekend binnen de eigen organisatie aan personen die deze informatie nodig hebben voor het doel waarvoor Opdrachtgever deze informatie heeft verstrekt en verplicht de betreffende personen tot geheimhouding van deze informatie.
d. In geval van schending van de geheimhoudingsplicht heeft Opdrachtgever het recht deze Raamovereenkomst en eventuele lopende Nadere Overeenkomsten of bestelopdrachten onmiddellijk te ontbinden. Opdrachtgever is vervolgens geen kosten meer verschuldigd en op Opdrachtgever kan geen schade worden verhaald.
e. Wederpartij is zich ervan bewust dat schending van de geheimhoudingsplicht kan leiden tot schade bij Opdrachtgever en derden en dat zijn/haar organisatie gehouden is tot niet alleen betaling van de boete maar daarnaast ook tot vergoeding van de schade die is ontstaan als gevolg van een schending van de geheimhoudingsplicht.
f. Wederpartij zal, na afloop van het verrichten van een Prestatie, de documenten (zowel digitaal als in hard copy) met vertrouwelijke informatie direct na Acceptatie van de Prestatie vernietigen en Opdrachtgever hiervan uit eigen beweging op de hoogte stellen, met dien verstande dat Wederpartij voor zover op grond van de wet of beroeps- en gedragsregels vereist – na voorafgaand overleg met de Opdrachtgever één exemplaar van de relevante vertrouwelijke informatie mag bewaren. De geheimhoudingsverplichting uit deze Raamovereenkomst blijft ten alle tijden voortduren, dus ook na afloop of beëindiging van deze Raamovereenkomst
g. Wederpartij garandeert dat (i) ondergetekende bekend is met de relevante wet- en regelgeving in Nederland, (ii) zich er van bewust is dat schending hiervan een strafbaar feit kan zijn en (iii) dat noch ondergetekende, noch een van haar directeuren, functionarissen, medewerkers, werknemers en professionele adviseurs of andere vanwege Wederpartij betrokkenen hoe ook door Wederpartij ingeschakeld of genoemd deze wet- en regelgeving zal overtreden in verband met de voorgenomen Opdracht.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

13. Slotbepaling

13.1 Afwijkingen van deze Raamovereenkomst, een Nadere Overeenkomst of een bestelopdracht zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.

13.2 Door ondertekening van deze Raamovereenkomst vervallen alle eventueel eerder door Partijen gemaakte mondelinge en schriftelijke afspraken omtrent het verstrekken van opdrachten tot het verrichten van Diensten, al dan niet onder een Nadere Overeenkomst.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Plaats: Den Haag
Datum: 22-7-2020

De Kiesraad
namens deze,
de secretaris-directeur,

5.1.2.e

Plaats: Leiden
Datum: 24-7-2020

HackDefense B.V.
namens deze,
de directeur,

5.1.2.e

Overzicht bijlagen:

1. de ARBIT-2018;
2. de nota van inlichtingen d.d. 7 mei 2020 en de 2de nota van inlichtingen d.d. 22 mei 2020 (perceel 1);
3. het Dossier Financiële Afspraken;
4. het Bestek d.d. 1 mei 2020 met kenmerk 201850004.213.001;
5. de door Wederpartij aan Opdrachtgever uitgebrachte Inschrijving van 4 juni 2020, zoals aangevuld d.d. 11 juni 2020;
6. Verantwoordingsformulier social return;
7. Format Nadere Overeenkomst;
8. Format bestelopdracht;
9. Format Verwerkersovereenkomst.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 1 - ARBIT-2018
Reeds in bezet van beide Partijen, initieel bijgevoegd als Bijlage B bij het Bestek.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 2 - Nota van inlichtingen d.d. 7 mei 2020 en de 2de nota van inlichtingen d.d. 22 mei 2020 (perceel 1)
Reeds in bezit van beide Partijen, ten tijde van de aanbesteding beschikbaar gesteld via TenderNed.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 3 - Dossier Financiële Afspraken
Bijgevoegd en geparafeerd door beide Partijen.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 4 - Bestek d.d. 1 mei 2020 met kenmerk 201850004.213.001
Reeds in bezit van beide Partijen, beschikbaar gesteld op 1 mei 2020 via TenderNed .

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 5 - Inschrijving van 4 juni 2020 zoals aangevuld op d.d. 11 juni 2020
Reeds in bezit van beide Partijen.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 6 - Verantwoordingsformulier social return
Toelichting
Opdrachtgever controleert de uitvoering van social return voorwaarde door middel van dit verantwoordingsformulier. Wederpartij overlegt dit formulier jaarlijkse aan Opdrachtgever. Wederpartij dient aan te geven dat hij aan het overeengekomen percentage heeft voldaan en de ingezette arbeidskracht(en) een social return indicatie heeft (hebben).

Over de Rijksbrede en interdepartementale aanbestedingen met social return zal jaarlijks extra worden gecontroleerd middels een steekproef. Op dat moment wordt de Wederpartij verzocht inzage te verlenen in de arbeidsovereenkomsten, die deels moeten worden afgeschermd, van de ingezette social return werknemers. Tevens zal ook gesproken worden over de wijze van begeleiding en uw ervaringen met de inzet van het instrument.

2 Verantwoordingstabel social return artikel 10 uit de Raamovereenkomst

Periode inzet (Datum)	Persoon	Indicatie ingezette arbeidskracht *(bijv. WWB, WSW, WIA, etc.)*	Wervingskanaal *(bijv. gemeente, UWV, etc.)*	Over deze periode gehaalde waarde van de loonsom	Cumulatief	Nog te realiseren
				€/uren	€/uren	€/uren
				€/uren	€/uren	€/uren
				€/uren	€/uren	€/uren
				€/uren	€/uren	€/uren
Totaal				**€/uren**	**€/uren**	**€/uren**

Let op: de kolom "Persoon" mag geen Persoonsgegevens (naam) bevatten. U dient de Persoonsgegevens te anonimiseren door bijvoorbeeld een fictieve naam of nummering toe te kennen aan de ingezette medewerkers.

3 Akkoord
HackDefense B.V. verklaart hierbij dat zij voldoet aan haar verplichting voor social return. Deze verplichting staat in artikel 10 en verder in de Raamovereenkomst met als naam: Het uitvoeren van pentesten en veiligheidsonderzoeken en advisering over beveiliging van (verkiezings)software met het kenmerk: 201865007.433 – P1 – HackDefense B.V.

4 Ondertekening

Naam organisatie	
Naam ondertekening bevoegd persoon	
Datum	
Handtekening	

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 7 - Format Nadere Overeenkomst
In bezit van beide Partijen, onderdeel van het Bestek, Bijlage H.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 8 - Format bestelopdracht
In bezit van beide Partijen, onderdeel van het Bestek, Bijlage J.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e

Bijlage 9 - Format Verwerkersovereenkomst
In bezit van beide Partijen, onderdeel van het Bestek, Bijlage I.

Paraaf Opdrachtgever: 5.1.2.e

Paraaf Wederpartij: 5.1.2.e