00352

STYCO

Offerte 11042017

PENETRATION HACK TEST REKENTOOL



398329

00352

STYCO

Ondertekening

Bedrijfsnaam	Styco B.V.
Contactpersoon	[redacted]
Functie	Managing Director
Adres	Fluitschipkaai 179
PC & Plaats	2498KW DEN HAAG
Telefoon	[redacted]
E-Mail	[redacted]@styco.nl

Ondertekening

Door opdrachtgever, de gemeente Amsterdam en opdrachtnemer Styco B.V. overeengekomen en ondertekend en akkoord met offerte.

Opdrachtnemer
Styco B.V.
Namens deze
Den Haag, 11 april 2017

[redacted]
Managing Director

Opdrachtgever
Gemeente Amsterdam
Namens deze

398329

Inhoudsopgave

Inhoud	Contactgegevens en Ondertekening	2
1	Inleiding	4
2	Partijen	5
2.1	Opdrachtgever	5
2.2	Opdrachtnemer	5
3	Opdracht	6
3.1	Achtergrond en vraagstelling	6
3.2	Doelstelling van de opdracht	6
4	Verantwoordelijkheden	7
4.1	Verantwoordelijkheden Gemeente Amsterdam	7
4.2	Verantwoordelijkheden van de Pentester	7
5	Beperkingen en Randvoorwaarden	8
	Beperkingen	8
	Randvoorwaarden	8
6	Team en Aanpak	9
6.1	Team	9
	Aanpak Pentest	9
7	Prijs en Facturatie	11
7.1	Prijs en Flexibiliteit	11
7.2	Facturatie	11
7.3	Algemene Inkoopvoorwaarden Gemeente Amsterdam	11

398329

1.1. Inleiding	Naar aanleiding van uw offerteaanvraag, treft u hierbij de offerte voor de Penetration/Hacktest Rekentool (DIGID)voor de Gemeente Amsterdam, Cluster Ruimte en Economie. De Penetration en Hacktest geeft u inzicht in de kwetsbaarheden in betreffende applicatie(s)en adviezen om deze kwetsbaarheden op te lossen. U verkrijgt hiermee zekerheid over opzet en bestaan van de maatregelen en procedures gericht op de ICT Beveiliging van de web-omgeving. Deze offerte gaat onder andere in op de doelstellingen aanpak, te verrichten werkzaamheden en verantwoordelijkheden alsmede de randvoorwaarden en prijs en facturatie van de opdracht.

398329

2. Partijen

2.1 Opdrachtgever	Gemeente Amsterdam gevestigd te Amsterdam, Weesperplein 8, hierna te noemen opdrachtgever.
2.2 Opdrachtnemer	Opdrachtnemer is STYCO B.V. gevestigd te Den Haag. STYCO heeft haar jarenlange ervaring en kennis vertaald in ICT maatwerkoplossingen voor alle branches die we op basis van vergelijkbare klantbehoeften en klantgroutte aanbieden. Op dit moment zijn wij actief in vijf ICT deelgebieden, die onlosmakelijk met elkaar verbonden zijn. Dit zijn de markten; Management-, Infrastructuur-, development-, BI & IT-Security/Audit Solutions. Wij bepalen samen met u het meest passende model. Wij bieden u hierin graag geïntegreerde ICT oplossingen en om uw organisatie van werkdruk te verlichten. De opdrachtgever zijn gebaseerd op een scherpe analyse van uw huidige situatie met een zeer heldere visie op uw toekomstige en huidige bedrijfs- of overheidsbehoeften.

398329

3. Opdracht

3.1 Achtergrond en vraagstelling	Op dit moment is de Gemeente Amsterdam bezig met het maken van een web applicatie, het overstapportaal, ten behoeve van vernieuwde wetgeving met betrekking tot erfpacht. Deze applicatie zal in juli live gaan en zal een DigiD koppeling gaan bevatten, wat de applicatie onderhevig zal maken aan de normen die hier door Logius aan worden gesteld. Daarnaast heeft de Gemeente Amsterdam een Rekentool welke informatie geeft over kosten met betrekking tot deze zelfde regelgeving over erfpacht. Deze tool slaat geen informatie op en heeft geen DigiD koppeling. De Rekentool heeft al eerder online gestaan, maar viel toen niet onder de nieuwe richtlijnen van de Gemeente dat hier een pentest op moest worden uitgevoerd. Dat is in die periode dan ook niet gedaan. Door veranderingen in de wetgeving komt deze Rekentool ten tweede male online en zal nu daarom alsnog onderworpen moeten worden aan een pentest. De Gemeente wil de noodzaak om de Rekentool te laten pentesten gebruiken als een leermoment over hoe een pentest wordt uitgevoerd in het kader van een DigiD audit. Op deze manier kunnen deze bevindingen direct worden teruggebracht naar de ontwikkeling van het overstapportaal om deze met de DigiD normen en manier van testen in het achterhoofd te ontwikkelen. Zo kan het overstapportaal direct op een meer compliant manier worden ontwikkeld. Vraagstelling van de gemeente is, dat er een penetration hack test op de Rekentool uitgevoerd dient te worden.. Hierbij willen zij een zo breed mogelijk inzicht in de kwetsbaarheden die in deze tool zitten, zowel wat betreft infrastructuur als de logica van de applicatie. Behalve voor het in kaart brengen van de kwetsbaarheden moet de test worden uitgevoerd alsof deze ten behoeve is van een DigiD audit. [redacted] bevindingen zullen daarom gekoppeld moeten worden aan de DigiD normen. Dit overzicht moet inzicht geven in de manier waarop een dergelijke pentest wordt uitgevoerd en geïnterpreteerd. Met de termijn waarop de Rekentool online zal worden gebracht in het achterhoofd is het noodzakelijk dat de pentest zo'n afgerond dient te worden. Infrastructuur OS versie Linux Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-81- Generic x86_64) Aantal servers 1 voor de Rekentool. Het Overstapportaal zal minimaal 2 servers met een fail-over bevatten Firewall type Shorewall Applicatie, dbase Wordpress, PH P7.0.0- Fpm nginx, MySQL
3.2 Doelstelling van de opdracht	[redacted] doelstelling van de opdracht was en Hackcentrix geef inzicht in de kwetsbaarheden en relateer bevindingen aan de technisch geraisoneerde beveiligingsrichtlijnen. De Penetration hack test zal uitgevoerd worden op de Rekentool van de Gemeente Amsterdam. De test zal worden uitgevoerd via het internet en een combinatie zijn van geautomatiseerde en handmatige tests. De test zal via het internet (extern) als grey box test worden uitgevoerd. Dit houdt in dat er in beperkte mate informatie wordt verstrekt over de infrastructuur om binnen de beschikbare tijd een zo goed mogelijk beeld te krijgen over de kwetsbaarheden in de applicatie. [redacted] applicatie maakt geen gebruik van authenticatie. Het is dan ook niet nodig (mogelijk) inloggegevens te verstrekken voor de test.

398329

4. Verantwoordelijkheden

4.1 Verantwoordelijkheden Gemeente Amsterdam	Gemeente Amsterdam is verantwoordelijk voor de beschrijving van de activiteiten en beschikbaarheid van de applicatie/s Rekentool. Gemeente Amsterdam heeft aangegeven dat de Overstapportaal per 1 juli 2017 wordt geïmplementeerd. voor nieuwe aansluitingen in 2017 hanteert Logius het volgende: Tot 1 juli 2017 is het huidige normenkader van toepassing. Tussen 1 juli 2017 en 1 november 2017 kunt u kiezen welk normenkader u wilt hanteren, dit zal deels afhankelijk zijn of u gebruik maakt van serviceorganisaties en tegen welke normen zij getoetst zijn; Na 1 november 2017 bent u verplicht uw nieuwe aansluiting te toetsen tegen het normenkader v2.0. Hiervoor geldt dat Pen en Hacktest: Voor aanvang van de Pen en Hacktest dienen de volgende documenten beschikbaar te zijn: Getekende Vrijwaringsverklaring Penetratietest Overzicht van Inlog-codentials voor Penetratietest voor de rollen 'Gebruiker'en 'Beheerder'.
4.2 Verantwoordelijkheden van de Pentester	1. Aan en afmelden van Pen en Hacktest werkzaamheden. 2. Bereikbaarheid tijdens uitvoering van Pen en Hacktest. 3. Zorgvuldig uitvoeren van Pen en Hacktest waarbij kans en impact van mogelijke schade wordt beperkt. 4. De IP-adressen waarvandaan wordt getest worden kenbaar gemaakt aan de opdrachtgever. Dit vereist dat deze voldoet aan de geldende ethische voorschriften en zijn werkzaamheden zodanig plant en uitvoert dat een redelijke mate van zekerheid wordt verkregen over de mate of de interne beheersmaatregelen, in alle van materieel belang zijnde aspecten, zo aldoende ze zijn opgezet en bestaan. Pen & Hacktest werkzaamheden worden alleen uitgevoerd met een getekende vrijwaringsverklaring Penetratietest en overzicht van inlog credentials voor Penetratietest voor de rollen 'Gebruiker'en 'Beheerder'

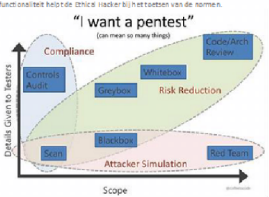
398329

5. Beperkingen en Randvoorwaarden

5.1 Beperkingen	De Rekentool applicatie is niet formeel onderhevig aan de DigiD normen aangezien deze geen gebruik maakt van de DigiD koppelingen. Er zijn dan ook enkele beperkingen met betrekking tot het kunnen testen van deze normen zoals (maar niet beperkt tot): 1. Het testen van authenticatie / autorisatie. 2. Het testen van de infrastructuur binnen het DMZ (applicatie wordt gehost in een cloud omgeving) 3. Diverse normen met betrekking tot processen welke vanuit de Auditor moeten worden beoordeeld.
5.2 Randvoorwaarden	1. Ondertekende vrijwaringsverklaring voor aanvang Penetration Hack test. 2. De doel omgeving (URL's / IP adressen) dienen bij aanvang van de test beschikbaar te zijn. 3. Test credentials en contactgegevens van de Gemeente dienen beschikbaar te zijn voor het geval van problemen of kritische bevindingen. 4. Er zal mogelijk worden getest zowel binnen als buiten standaard kantooruren.

398329

6.1 Team	Penetratie/Hacktesten zal uitgevoerd worden door: [redacted]
6.2 Aanpak Pentest:	De Pen en Hacktest wordt als Greybox test in een timebox uitgevoerd. De mate van voorkennis (verstrekte informatie) heeft invloed op de effectiviteit van de uitvoering. Heldere scope en enige informatie over architectuur, gebruikte technieken en functionaliteit helpt de Ethics Hacker bij het toetsen van de normen.



Per technische norm worden geautomatiseerde scans en handmatige testen uitgevoerd volgens de OWASP Testing Guide v4.

Voor de Pen en Hacktest zijn de volgende 21 technisch gerelateerde normen in scope:

BB-6	Maak gebruik van een hardenings-proces, zodat alle ICT-componenten zijn gehard tegen aanvallen.
BB-7	De laatste (beveiligings-)patches zijn geïnstalleerd en deze worden volgens een patchmanagement proces doorgevoerd.
BB-12	Ontwerp en richt maatregelen in met betrekking tot toegangsbeveiliging / toegangsbeheer.
BB-13	Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.
B1-1	Er moet gebruik worden gemaakt van een Demilitarised Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeerstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke.
B1-2	Beheer- en productieverkeer zijn van elkaar gescheiden.
B1-3	Netwerktoegang tot de webapplicaties is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.
B2-1	Maak gebruik van veilige beheermechanismen.
B3-1	De webapplicatie valideert de inhoud van een HTTP- request voor die wordt gebruikt.
B3-2	De webapplicatie controleert voor elk HTTP verzoek of de initiator geauthenseerd is en de juiste autorisaties heeft.

398329

83-3 De webapplicatie normaliseert invoerdata voor validatie.

83-4 De webapplicatie codeert dynamische onderdelen in de uitvoer.

83-5 Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.

83-6 De webapplicatie valideert alle invoer, gegevens die aan de webapplicatie worden aangeboden, aan de serverzijde.

83-7 De webapplicatie staat geen dynamische file includes toe of beperkt de keuze mogelijkheid (whitelisting).

83-16 Zet de cookie attributen 'HttpOnly' en 'Secure'.

85-1 Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.

85-2 Maak gebruik van versleutelde (HTTPS) verbindingen.

85-3 Sla gevoelige gegevens versleuteld of gehashed op (Voor zover betrekking hebbend op DigID).

85-4 Versleutel cookies.

87-1 Maak gebruik van Intrusion Detection Systemen (IDS).

Naast het toetsen van de normen worden een aantal kwetsbaarheidscans uitgevoerd o.a. Nmap, Nikto en OWASP ZAP om een algeheel beeld van de effectiviteit van de beveiliging beheer processen te verkrijgen.

Een aantal veel voorkomende beveiligingsfouten uit de OWASP top 10 (2013) zijn verwerkt in de bovengenoemde normen. Tijdens de kwetsbaarheidscans en handmatige testen wordt op de overige OWASP top 10 items getest voor zover deze in de OWASP Testing Guide uit zijn opgenomen. Niet alle items zijn met scans of handmatige testen aantoonbaar (zie ook http://www.owasp.org/index.php/ZAP/ptp/TopTop10)

398329

7. Prijs en Facturatie

7.1 Prijs en Flexibiliteit	Het honorarium is gebaseerd op de vereiste expertise, ervaring en tijdsbesteding voor de penetration test. Onze werkwijze binnen uw organisatie is op persoonlijke en vakinhoudelijk vlak gericht om op de meest effectieve en efficiënte wijze resultaten binnen uw organisatie te behalen.

Activiteiten	Uren
1. Opdracht en applicatie informatie	2
2. Penetratietests Scannen en testen infrastructuur Validatie kwetsbaarheden infrastructuur Scannen webapplicatie	12
3. Handmatig tests Handmatig testen en valideren webapplicatie	12
4. Rapportage Analyse en Rapportage	16
5. Beoordeling en review Review rapportage Beoordeling DigiD normen	10
Totaal uren	50
Totaalbedrag	€ 6000,-

Voor bovenstaande prijsstelling geldt het volgende:

- Uitgegaan van de tarieven van de senior pentest consultant;
- Prioriteit van de activiteiten zullen tijdens de opdracht nader afgestemd kunnen worden;
- Indien er overuren worden gemaakt dan zullen die uren worden gefactureerd op basis van het bovengenoemde uurtarief.

Flexibiliteit

- Met betrekking tot ondersteuning in het vervolgtraject en/of ondersteuning bij oplossen van bevindingen, kunnen we de inzet van de pen hack consultant na het project, voortzetten op basis van gemaakt uren. We hanteren een uurtarief van € 120,- exclusief 21% btw, inclusief reiskosten. Zie punt 7.2.

7.2 Facturatie	Wij factureren aan het einde van de maand op basis van feitelijk gewerkte uren aan deze opdracht.
7.3 Algemene Inkoopvoorwaarden Gemeente Amsterdam	De algemene voorwaarden voor leveringen diensten van de gemeente Amsterdam van maart 2010, gedeponeerd bij de Kamer van Koophandel op 12 maart onder nummer 5436886 zijn van toepassing.

398329