Bijlage 12

Penetration Testing

Inhoudsopgave

1 Voorwoord

Dit document wordt gebruikt om de penetratietest efficient te laten uitvoeren. Omdat dit document details bevat over applicaties en personen wordt dit document als vertrouwelijk geklassificeerd.

Vanaf 1 maart 2024 is het veld “verantwoordelijk manager”een verplicht veld. De manager is voor de pentest accounts verantwoordelijk en zorgt voor de accodering van de extra rollen en rechten t.a.v. deze accounts.

Type pentest:	Uitleg:
Blackbox:	Bij een black-box testopdracht wordt de penetratietester in de rol van de gemiddelde hacker geplaatst, zonder interne kennis van het doelsysteem. Testers krijgen geen architectuurdiagrammen of broncode die niet openbaar beschikbaar zijn. Een black-box penetratietest stelt de kwetsbaarheden in een systeem vast die van buiten het netwerk kunnen worden misbruikt.
Greybox:	De volgende stap omhoog van black-box-testen is gray-box-testen. Als een black-box-tester een systeem onderzoekt vanuit het perspectief van een buitenstaander, heeft een grey-box-tester de toegangs- en kennisniveaus van een gebruiker, mogelijk met verhoogde rechten op een systeem. Gray-box-pentesters hebben doorgaans enige kennis van de interne onderdelen van een netwerk, mogelijk inclusief ontwerp- en architectuurdocumentatie en een account intern in het netwerk.
Whitebox:	White-box-testen kennen verschillende namen, waaronder cristal-box. Het valt aan de andere kant van het spectrum van black-box-testen: penetratietesters krijgen volledige toegang tot de broncode, architectuurdocumentatie, enzovoort. De belangrijkste uitdaging bij white-box-testen is het doorzoeken van de enorme hoeveelheid beschikbare gegevens om mogelijke zwakke punten te identificeren, waardoor dit het meest tijdrovende type penetratietest is.

2 Omschrijving van de opdracht en applicatie

Beschijf de opdracht en de applicatie. Wat is het doel van de applicatie en wat voor soort data wordt gebruikt. Door wie wordt de applicatie gebruikt? In dit hoofdstuk dient antwoord te worden gegeven op deze vragen.

Beschrijving:

3 Inventarisatie pentest

3.1 Contactgegevens

Om de aanvraag zo goed mogelijk te laten verlopen is het nodig om contactgegevens op te geven. Deze kunnen benodigd zijn voor de aanvraag van de pentest en/of voor aanvullende vragen/opmerkingen gedurende de pentest.

Verantwoordelijk (operationeel) manager		
Naam:	E-mailadres:	Telefoonnummer:

Team leden / POer			
Naam:	Functie:	E-mailadres:	Telefoonnummer:

3.2 Vragenlijst pentest

Wat voor soort pentest dient er te worden uitgevoerd op de omgeving. Dit kunnen verschillende testen zijn vanuit verschillende actoren.

Vragen over de omgeving / applicatie:	**Antwoorden en toelichting:**
Per wanneer is de omgeving beschikbaar?	Datum: Toelichting:
Per wanneer dient de applicatie getest te worden:	Startdatum: Einddatum: Let op: Wanneer de applicatie wordt gehost in het datacenter van xxxxx, dan dient hiervoor een change te worden aangevraagd.
Welke omgeving wordt getest:	Productie / Acceptatie / Test / Ontwikkel Toelichting:
Is de omgeving gelijk aan productie (wanneer NIET de productieomgeving wordt getest):	Ja / Nee Toelichting:
Betreft dit een hertest: **Zo ja, dienen er bepaalde functionaliteiten te worden hertest:**	~~Ja~~ / **Nee** Toelichting:

	Let op: Het kan voorkomen dat er andere functionaliteiten met kwetsbaarheiden buiten scope vallen.
Is de applicatie volledig:	Ja / Nee Toelichting:
Zijn er werkzaamheden actief die eventueel de test kunnen beïnvloeden?	Ja / Nee Toelichting:
Hoe is de omgeving benaderbaar:	Internet / Locatie Kadaster / Overig Toelichting:
Zijn er toegangsgegevens benodigd	Ja / Nee
Type toegangsgegevens:	Gebruikersnaam en wachtwoord / Certificaten / Tokens / Whitelisting / Single-Sign-On (SSO) Toelichting:
Is er documentatie beschikbaar van de omgeving:	Ja / Nee Toelichting:
Bevat de te testen omgeving vertrouwelijke gegevens, bijvoorbeeld: • **Persoonsgegevens** • **Bijzondere persoonsgegevens** • **Specifieke dienstafhankelijke (vertrouwelijke) gegevens.**	Toelichting:

3.3 Type pentest

Wat voor type pentest dient er worden uitgevoerd:

Type	Informatie	
Blackbox	De aanvaller heeft geen informatie van de applicatie. Inloggegevens zijn in principe niet nodig.	
Greybox	De aanvaller gebruikt beperkte informatie om de applicatie te testen. Dit kan bijvoorbeeld inloggegevens zijn of technische informatie van de applicatie.	
Whitebox	De aanvaller heeft alle benodigde informatie van en over de applicatie. Dit zijn (eventueel) inloggegevens, maar ook toegang tot de broncode van de applicatie.	

Bij Greybox en Whitebox wordt aangeraden om een architectuurplaat van het applicatielandschap mee te leveren.

3.3.1 Gebruikersaccounts

Wanneer er wordt gekozen voor een greybox of whitebox pentest is het mogelijk om de aanvallers c.q. pentesters te voorzien van accounts om in te loggen. Voor een applicatie wordt er vaak gebruik gemaakt van verschillende rollen voor klanten, beheerders, medewerkers en/of managers. Voor iedere rol dient er afzonderlijk 2 accounts te worden gegeven om de applicatie volledig te testen.

Aanvulling: De gebruikersnaam en wachtwoorden dienen door middel van een beveiligd bestand (incl wachtwoord) te worden overgedragen.

Rol/functie 1:	**Beschrijving:**	**Mijn Kadaster** (indien van toepassing) **Dienstcodes-Dienstnamen**

Rol/functie 2:	**Beschrijving:**	**Mijn Kadaster** (indien van toepassing) **Dienstcodes-Dienstnamen**

Rol/functie 3:	**Beschrijving:**	**Mijn Kadaster** (indien van toepassing) **Dienstcodes-Dienstnamen**

Rol/functie 4:	**Beschrijving:**	**Mijn Kadaster** (indien van toepassing) **Dienstcodes-Dienstnamen**

3.3.2 Webservice en/of API's

Wanneer de omgeving ook webservices en/of API's bevat, dan kunnen deze ook worden getest. Wanneer dit niet van toepassing is, dan kunnen deze velden leeg blijven.

Vraag:	**Antwoord:**
Bevat de omgeving een webservice of API?	Ja / Nee Toelichting:

Zijn hier voorbeelden van?	Ja / Nee Zo ja, wat voor type zijn dit? (wsdl, swagger, postman, etc)

3.4 Domeinen en IP-adressen

Geef aan hoe de pentester de applicatie kan benaderen. Daarnaast dient er ook rekening te worden gehouden of de pentester de applicatie van buitenaf de applicatie kan benaderen of dat deze binnen het Kadaster domein moet zitten.

URL	IPv4 / IPv6 adressen:	Intern / Extern

3.5 Wet – regelgeveing en standaarden.

Indien er op de dienst(en) specifieke wet-, regelgeving en/of standaarden van toepassing zijn, dan kunnen deze hieronder worden aangegeven.

Onderstaande wet-, regelgeving en/of standaarden dienen getoets te worden	Aankruisen indien van toepassing.
ICT-beveiligings richtlijnen voor webapplicaties (NCSC)	
PKIoverheid	
Algemene verordening gegevensbescherming (AVG)	
Organisatie	
Interne richtlijnen	
Overige	