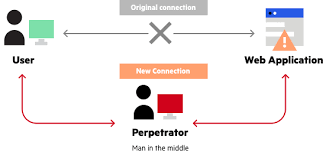
**Project Security Individueel Product 23-24**

**SSL Checker Tool (SCT)**

t.b.h man-in-the-middle attacks



Klas: IC201

Naam: Daan Rook

Studentnummer: 500903570

Datum: 02/10/2023 – 19/11/2023

Versie: 1.0

# Doel

* 1. Problematiek, vereisten en doel

Het man-in-the-middle (MITM) aanvalsscenario is een ernstige bedreiging voor de vertrouwelijkheid en integriteit van gegevens tijdens communicatie via onbeveiligde kanalen.

Voor het waarborgen van deze veiligheid tijdens communicatie worden er certificaten uitgedeeld door een CA. Dat is een vertrouwelijke third-party die certificaten genereerd en uitdeelt. Tegelijkertijd ondertekenen ze ook het certificaat, dit wordt gedaan zodat andere apparaten in staat zijn om het certificaat te verifiëren.

Ook vind er op de achtergrond, tijdens communicatie, een “handshake” plaats. Dit betekent dat er door een reeks aanvragen van jou apparaat en die van de andere partij een overeenkomst word vastgesteld. Nu weten beide partijen dat er een veilige communicatie bestaat.

Deze 2 voorgelegde technieken zijn van belang bij het aanvliegen van het MITM aanvalsscenario.

Het doel van dit project is het leveren van een: ssl-checker-tool. Deze tool bevat de 2 bovengenoemde technieken om zo te bepalen dat er een veilige communicatie bestaat.

* 1. Context of situatie van de problematiek

TechGuard innovations is een middelgroot technologiebedrijf en brengen innovatieve softwaretoepassingen op de markt. Omdat ze onlangs veel te maken hebben gehad met beveiligingsincidenten zijn ze opzoek naar een cybersecuritypartner. Het bedrijf bestaat uit zo ongeveer 150 man waaronder ontwikkelaars, professionals en sinds kort beveiligingsexperts.

Het bedrijf heeft een serie aan aanvallen waargenomen. Na het inschakelen van een derde

partij, is er achterhaald dat het in de meeste gevallen ging om een zogenaamde man-in-the-

middle attack.

Om deze aanvallen te voorkomen maak ik een ssl-checker-tool zodat het bedrijf zelf instaat is

om te observeren en reageren op dergelijke scenario’s

* 1. Gekozen aanpak

Waarom heb ik gekozen voor een tool in plaats van een toepassing die dit probleem kan voorkomen?

Bij het maken van een systeem dat deze aanvallen volledig zou kunnen voorkomen kan het zo zijn dat het bedrijf als potentieel doelwit word beschouwd. Dat komt doordat het dan een uitdaging word voor kwaadwillende. Dit moeten we voorkomen.

Vandaar is er gekozen voor een tool die fungeert als een observatie en reactie mogelijkheid voor het bedrijf.

* 1. Security aspecten en kwaliteitscriteria

Tijdens dit project zijn een paar security aspecten aanwezig, de belangrijkste staan hieronder beschreven:

1. **SSL/TLS security:** Er zal rekening gehouden moeten worden met het up-to-date houden van de applicaties met de laatste versie van SSL/TLS, zodat er geen zwakheden ontstaan door verouderde versies.
2. **Certificate validation/pinning:** Het is in de praktijk van belang dat er alleen geautoriseerde certificaten worden toegestaan.
3. **Veilige opslag van certificaten:** Als er lokaal certificaten worden opgeslagen is het van belang dat deze files veilig worden bewaard.

Deze aspecten moeten worden nageleefd. Maar worden tijdens dit project en product (proof-of-concept) niet altijd gebruikt zodat er een goede simulatie gevormd kan worden.

# Oplossing

* 1. Mogelijke oplossingen

Andere oplossingen voor dit project hadden kunnen zijn:

1. **HSTS(HTTP strict Transport Security):** De browser in kwestie mag alleen maar communiceren d.m.v veilige connecties.
2. **PKI(Public Key Infrastructure):** Deze infrastructure deelt en onderhoud zelf veilige certificaten.
3. **Network Monitoring:** Gebruik bekende netwerk tools om te zoeken naar bekende aanvalspatronen.
   1. Gekozen oplossing

We gaan gebruik maken van een ssl-checker-tool. Zoals beschreven in hoofdstuk 1 bewaakt

deze tool het toestaan van geautoriseerde certificaten en wordt er een check gedaan op de

handshake die aangeeft of een verbinding wel of niet veilig is.

* 1. Netwerk en Systeem diagrammen.

Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving

* 1. Kwaliteitscriteria en risicomitigaties.

Er zijn een aantal risico’s waar we mee te maken hebben, de belangrijkste staan hieronder beschreven:

**Risico:** Data word onderschept tijdens communicatie

**Mitigatie:** Maak gebruik van HTTPS voor een veilige, versleutelde, communicatie.

**Risico:** Misbruik van bekende zwakheden in verouderde third-party libraries/applicaties.

**Mitigatie:** Hou alle afhankelijkheden up-to-date, zodat er gebruik kan worden gemaakt van security patches en fixes.

**Risico:** Ongeautoriseerde toegang tot opgeslagen certificaten.

**Mitigatie:** Zorg ervoor dat opgeslagen certificaten op een veilige manier worden weggezeten voor verder gebruik.

# Proof of Concept

* 1. Gebruikte tools en ontwerp

Dit project is gemaakt in **Python** met de volgende libraries:

* requests
* ssl
* urllib.parse
* pyOpenSSL

Onderdelen die nodig zijn voor een correcte werking van het programma zijn in

requirements.txt beschreven en daarom ook makkelijk te downloaden.

3.2 Proces flows, software diagrammen, dialoog diagrammen

MITM-aanvalsscenario:

Afbeelding met tekst, schermopname, diagram, Lettertype

Automatisch gegenereerde beschrijving

MITM-aanvalsscenario met ssl-checker-tool

Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving

* 1. Gerealiseerde componenten

De componenten van het project:

**SSLChecker.py:** Het stuk code wat de ssl-handshake en certificate pinning checkt.

**createServerCertificate.py:** (Voor het simuleren) Genereerd dit stuk code de server certificate

in een pem file, zodat deze later kan worden gebruikt om te bepalen dat de opgevraagde

certificate correct is.

**server\_certificate.pem:** Een file, die normaal gesproken goed beveiligd is, waarin de

certificate(s) van de webserver(s) staan opgeslagen.

**requirements.txt:** Een file met de correcte versies van gebruikte afhankelijkheden.

**README.md**: Een markdown file met de uitleg hoe het programma geïnstalleerd moet

Worden.

* 1. Test

Voor de 2 gebruikte technieken willen we allebei één test hebben:

**SSL-handshake:** We weten dat het programma een “succesfull” teruggeeft bij de handshake omdat we site gebruiken in de code die geldige certificaten bevatten. We kunnen testen of de code een “fail” teruggeeft, dat is belangrijk in een situatie waarin er daadwerkelijk een MITM-aanval plaats vind, door een site aan het programma te geven die geen ondertekend certificaat bevat. Dat kan d.m.v een localhost server.



Waarop volgt:



Voor de certificate pinning gebruiken we een .py test bestand:

testGetServerCertificate.py

Afbeelding met tekst, schermopname, software

Automatisch gegenereerde beschrijving

In het voorbeeld word er een adres gegeven. Deze word omgezet in een domain, dat is zodat ssl het goed kan lezen, en dan kan ssl het certificaat ophalen en uitprinten.

Dit is wat we terugkrijgen (en verwachten):

This printed certificate comes from: tesselaarbv.nl.

-----BEGIN CERTIFICATE-----

MIIGAzCCBOugAwIBAgISBGy5xwvRSuwyf28OFqAT+4iLMA0GCSqGSIb3DQEBCwUA

MDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQD

EwJSMzAeFw0yMzEwMTIwNDIzMjZaFw0yNDAxMTAwNDIzMjVaMCExHzAdBgNVBAMT

Fmx1bmNoZW5iaWp0ZXNzZWxhYXIubmwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw

ggEKAoIBAQD3aS0aEYeB+OxznqZ2do99obKcspl8a6WcO0CAhuXcsxm8XQz+Dux4

Hv40Sl7tG4PAVmwwnKMm0frHCVZFF+k63D/Ips79zpMV0CVm2/0jfDIaJNGw5arn

eStb6xee4q4XIJTwWGeMxHsODy4ZVIy01zSwIr75mdrm+lyDyvPFTwMaVUG7XO0a

XF0IAUvVI7jj0wfnAZJC6BDsPIARB0CVTJmNMSz8gSZNHBBV7NhmIuEfjGr0tXDF

mNVLmWZevEWzbjNXy9YGlrqDKZu6FIquuWHJA2rAeoZzwO7oN9L0/gTm+Rakagrc

yyZ+1VfSHOxxwCzdD/bcBL+AAv0NvYo/AgMBAAGjggMiMIIDHjAOBgNVHQ8BAf8E

BAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMAwGA1UdEwEB/wQC

MAAwHQYDVR0OBBYEFHPLR/kOsZNKyGU16btvj9iSWgQ1MB8GA1UdIwQYMBaAFBQu

sxe3WFbLrlAJQOYfr52LFMLGMFUGCCsGAQUFBwEBBEkwRzAhBggrBgEFBQcwAYYV

aHR0cDovL3IzLm8ubGVuY3Iub3JnMCIGCCsGAQUFBzAChhZodHRwOi8vcjMuaS5s

ZW5jci5vcmcvMIIBKgYDVR0RBIIBITCCAR2CFWNwYW5lbC50ZXNzZWxhYXJidi5u

bIIaY3BjYWxlbmRhcnMudGVzc2VsYWFyYnYubmyCGWNwY29udGFjdHMudGVzc2Vs

YWFyYnYubmyCE2lwdjYudGVzc2VsYWFyYnYubmyCFmx1bmNoZW5iaWp0ZXNzZWxh

YXIubmyCG21haWwubHVuY2hlbmJpanRlc3NlbGFhci5ubIITbWFpbC50ZXNzZWxh

YXJidi5ubIIOdGVzc2VsYWFyYnYubmyCFndlYmRpc2sudGVzc2VsYWFyYnYubmyC

FndlYm1haWwudGVzc2VsYWFyYnYubmyCGnd3dy5sdW5jaGVuYmlqdGVzc2VsYWFy

Lm5sghJ3d3cudGVzc2VsYWFyYnYubmwwEwYDVR0gBAwwCjAIBgZngQwBAgEwggED

BgorBgEEAdZ5AgQCBIH0BIHxAO8AdQDatr9rP7W2Ip+bwrtca+hwkXFsu1GEhTS9

pD0wSNf7qwAAAYsiVvibAAAEAwBGMEQCIEZ9B7to/VaMq8ryy0K3LXTbAwVf712d

65+xDzTYGqeAAiA6Cahd890E1WIFj5UJNZFeBQiv1PFOxr7TwNAoPQDJCQB2AO7N

0GTV2xrOxVy3nbTNE6Iyh0Z8vOzew1FIWUZxH7WbAAABiyJW+IMAAAQDAEcwRQIh

AOwpVKvc9ltE6DDrUkDuYrAGhnMotyCrDjI0gHkiSiqkAiBcqXhmzHnHVm3Jdcww

HmfwOkIgNlGlkfP9fCig3Y4XuTANBgkqhkiG9w0BAQsFAAOCAQEAl7VP4++VwXVy

kW+OE3v9VtqkH2bOwNLIG7cVnr6F5S0vxDR9b8Sz8UWwqbcINh6w5yf/9y2Jyd3A

+shGnPvuJ+K9J/a7ewR2oLLlyq/l/nnn0s1Fgup+VwuGYpugKAnP6hQg219XFYuz

ULThMkym15SDOqhcjl2lenYT41oKBkEam4HCEf6ctJCYLvoEPjCA59su8cDkFWZU

CsQDlnZebu5OsrBsZ2j1b3J5pUOnKPnFMjlsJukqa5Mpq/TBQ51An4yuzRAC3r1P

XWj4/O+5Qffo4I5WML+OhqXKrviWRQ649t31XH0TzJuzMdIhA6Gc9oHNwR+FihR0

spW1fY3hMg==

-----END CERTIFICATE-----

* 1. Proof of Concept conclusie.

Voor een proof of concept is het aangeleverde programma een goede oplossing. Deze tool is ontworpen om de beveiligingsstatus van een website te controleren door zowel de SSL-handshake even als de certificaatpinning te valideren.

*Functionaliteiten:*

1. **SSL-handshake controle:**

* Het programma voert een SSL -handshake uit met de opgegeven URL.
* Het waarschuwt voor mislukte SSL-handshakes en geeft de errors.

1. **Certificaatpinning:**

* Het programma maakt gebruik van “certificaatpinning” om te valideren of de servercertificaten geldig zijn.
* Een vooraf gespecificeerd certificaat (opgeslagen in een bestand) wordt gebruikt voor de vergelijking.

*Gebruik:*

* De gebruiker verstrekt een URL aan het programma voor de analyse.
* Het programma voert een SLL-handshake uit en waarschuwt voor problemen.
* Certificaatpinning wordt toegepast om te verifiëren of de overeenkomst tussen de 2 servercertificaten kloppend is.

*Installatie:*

* Gebruik de README.md en requirements.txt voor de installatie van het programma en de benodigde afhankelijkheden.
* Voor een overzicht van het project: <https://github.com/DaanRook/ProjectIP1>

# Eindconclusie

* 1. Conclusie

Het product is af en kan worden geïmplementeerd voor gebruik. Voor vragen of opmerkingen rondom het product dient u contact op te nemen met:

Daan Rook, email: [daan.rook@hva.nl](mailto:daan.rook@hva.nl), tel: 06 26756727

De SSL-Checker-Tool is een preventief middel tegen man-in-the-middle attacks en dient alleen gebruikt te worden voor deze doeleinden!

* 1. Advies en aanbevelingen.

*Toekomstige Ontwikkelingen:*

Het bedrijf kan overwegen om geavanceerde functies te integreren zoals het controleren van de certificaatvervaldatum en hoe het programma moet omgaan met serveromleidingen.

Ook is het belangrijk dat er een begrijpelijke gebruikersinterface word ontworpen. Dit bevorderd meer intuïtief gebruik.

*Opmerking:*

Het programma is in de proof-of-conceptfase en verdere ontwikkeling en verfijning zijn mogelijk op basis van vereisten en gebruikersfeedback. (gelieve binnen het bedrijf)

# Bijlage A, Logboek en reflectie

***Logboek:***

|  |  |
| --- | --- |
| Datum/Datum week | Wat heb ik gedaan? |
| 01/10/2023 | Voorbereiden/uitdenken van IPposter |
| 02/10/2023 | Presentatie IPposter |
| Week van 9 Oktober | Doel en probleem vastgesteld en uitgewerkt |
| Week van 23 Oktober | Aanpak en security aspecten beschreven. Begonnen aan gebruik van ssl library en inlezen op servercertificaten. |
| Week van 30 Oktober | Hoofdstuk 2 uitgetypt en een simpele certificaat test gemaakt. Ook begonnen aan het ophalen van de (initiële) server certificaat en deze opslaan. |
| Week van 6 Oktober | Hoofdstuk 3 voor de helft uitgetypt en testen gespecificeerd. Verder gegaan aan SSL-handshake en certificaatpinning. |
| Week van 13 Oktober | Hoofdstuk 3 voor de helft en hoofdstuk 4 uitgetypt. Voor de zekerheid ook een github aangemaakt waar de code instaat voor het naslagwerk. SSL-handshake en certificaatpinning volledig uitgewerkt. |

***Reflectie:***

Dit was voor mij vooral een informatief product dan dat het heel technisch is geweest. Ik heb

een hele hoop nieuwe dingen geleerd over servercertificaten, hoe dit afgehandeld wordt en

hoe het eruit ziet.

Tijdens dit project vond ik het vooral fijn dat je enorm de vrijheid had om je tijd zelf in te delen.

Dat maakt het dan ook makkelijk om aan het project te werken omdat je er op elk moment aan

kan zitten en als je tegen problemen aan liep dit niet hoefde te bespreken met teamleden.

Daarentegen betekende dit ook dat je geen stok achter de deur hebt en dat je zelf goed moet

opletten dat je op schema loopt. Hier ben ik mijzelf wel een paar keer tegengekomen.