

Rapport Banking Website

Red vs Blue team event 2

Fontys ICT

4-1-2021

Colofon

|  |  |
| --- | --- |
| **Label** | **Gegevens** |
| Klant | Alexander Lambooij |
| Auteur | Thomas van Heel en Joel Adams |
| Status | Afgerond |
| Classificatie | Vertrouwelijk |

Versiegeschiedenis

|  |  |  |
| --- | --- | --- |
| **Versie** | **Datum** | **Aanpassingen** |
| 1.0 | 1-1-2021 | Setup en vullen met inhoud |
| 1.1 | 4-1-2021 | Laatste aanpassingen |

## 

## 

# **Hoofdstuk 1**

**Management samenvatting**

Fontys ICT heeft gevraagd, aansluitend op de Red - vs Blue team, een tijd-gelimiteerde pentest uit te voeren op de Internetbankieren applicatie. Dit is gebeurt om de testomgeving in Seclab.

De impressie van de veiligheid van de applicatie is niet erg positief. De maker van de applicatie heeft tijdens het maken van de applicatie, de ‘*hacker mindset*’ niet in gedachte genomen. Zo kan de request aangepast worden waardoor je bijvoorbeeld gebruikers kan aanmaken met slechte wachtwoorden of properties die missen. Ook kan er geld overgemaakt worden naar je eigen bankrekening en zit hier dus ook geen validatie op.

De webapplicatie maakt bovendien ook alleen maar gebruik van HTTP, wat de hacker de mogelijkheid biedt (gevoelig) netwerkverkeer te onderscheppen.

Ondanks dat, kan er wel gezegd worden dat de maker van de applicatie wel een goede toepassing heeft omtrent authenticatie. Echter, moet er wel voor gezorgd worden dat de gebruiker van de applicatie “feedback” krijgt als diegene verkeerde data invoert.

In dit rapport vind je alle details van het onderzoek en bevindingen, dit bevat ook het technische advies.

1.1 Overzicht bevindingen

De bevindingen zijn gesorteerd op basis van de classificatie. Indien er meer informatie benodigd is kan [Bijlage A](#_x9pd8qhgsqbk) ingezien worden.

|  |  |
| --- | --- |
| **Bevinding** | **Risico** |
| Het gebruik van een zwak protocol, dit kan leiden tot o.a. het sniffen van het netwerkverkeer. |  |
| Het gebrek aan meerdere invoer validatie, dit kan leiden tot het aanmaken van gebruikersaccounts zonder valide data. |  |

# Inhoudsopgave

[Hoofdstuk 1](#_762agdplpeq6) **3**

[**Inhoudsopgave**](#_i09huxmtl0sa) **5**

[Hoofdstuk 2](#_9ebguro5h6st) **6**

[**2.1 Onderzoeksvraag**](#_l5zynsppyp6s) **6**

[**2.2 Scope**](#_gm2gnfqavhfj) **6**

[Hoofdstuk 3](#_tvtjn36lv7y3) 7

[**3.1 Aanpak**](#_ubioixhhvus6) **7**

[3.1.1 Algemeen](#_m75qw8rytc2y) 7

[3.1.2 Web](#_kd6p7povjkss) 7

[**3.2 Analyse**](#_vf3fa0h49e3n) **7**

[Hoofdstuk 4](#_l9rj5ydqhqo4) 8

[**4.1 Conclusie**](#_cfnbf0p1jr4l) **8**

[**4.2 Advies**](#_b282lo8radkt) **8**

[Bijlage A](#_v7za36jen881) 9

[**Zwak protocol**](#_k9fcelbe2inm) **9**

[Reproductie](#_6fnaqs95ip8l) 9

[**Risico’s**](#_72kj8fzhnzmr) **9**

[Preventie](#_ty2pu2dkyhms) 9

[**Invoer validatie**](#_t1n954wkhy4w) **10**

[Reproductie](#_jr4feqmb4m6o) 10

[Risico’s](#_s8or11cdq62b) 11

[Preventie](#_aatoxs5bdedz) 11

[**Overige bevindingen**](#_vio998fe03tu) **11**

[Uitlog-functie](#_oaxb2clj2c9u) 11

[Gebruikersfeedback](#_hzf0hyjkksqr) 11

[Geen functionaliteit na inlog](#_v5dsr9e83ga5) 11

[Inloggen onbetrouwbaar](#_om00tnu2yq9d) 11

[Geen Email Check](#_rvgzznoppne2) 11

# **Hoofdstuk 2**

**Aanvraag**

Vandaag de dag is internet een belangrijk aspect in de maatschappij, zo ook het internetbankieren. Deze applicatie vervuld deze functionaliteit, hiermee kan je gemakkelijk je financiële zaken regelen zoals overboeken.

De stakeholders van dit project zijn Alexander Lambooij, Fontys ICT, Joel Adams en Thomas van Heel.

# **2.1 Onderzoeksvraag**

De applicatie die getest getest gaat worden is de internetbankieren app van Alexander Lambooij, deze staat op de Seclab omgeving van Fontys.

De desbetreffende IP-adressen behorend bij de applicatie zijn:

* 10.10.2.128:80 = frontend
* 10.10.2.128:8081 = backend
* 10.10.2.128:3306 = MySQL database

Het doel is om de webapplicatie te testen tegen veiligheidsproblemen.

# **2.2 Scope**

De scope van het project is om te zoeken naar veiligheidsproblemen in de webapplicatie en/of bijbehorende systemen, gehost op Seclab.

## 

## **Hoofdstuk 3**

Bevindingen

# **3.1 Aanpak**

Eerst is er een connectie gemaakt met de VPN voor de Seclab omgeving, zo kon er getest worden. De cyber killchain is gevolg namelijk:

1. Reconnaissance
2. Intrusion
3. Exploitation

Er zijn meer stappen, maar die zijn nu niet van toepassing, omdat ik niet verder kan gaan dan exploitatie. Met deze stappen, was ik bereid om de zwakheden in de applicatie te achterhalen.

## **3.1.1 Algemeen**

Om de webapplicatie te begrijpen zijn er verschillende testen gedaan. Deze testen bevatten scanning en fuzzing. Burp Suite is ook een hele handige tool om HTTP requests mee te onderscheppen en Postman om onze eigen calls te schrijven

## **3.1.2 Web**

Testen is gedaan via Seclab, hier werd de applicatie op gehost. De tools die gebruikt zijn bij de pentest zijn voornamelijk de tools die Kali Linux bevat en die wij gebruiken voor alle pentesten. De tools zijn:

* Burp Suite
* Nmap
* Nikto

# **3.2 Analyse**

Onderstaand is een beschrijving gegeven van elk probleem. De technische uitleg is in de bijlage te vinden om beter te begrijpen wat verkeerd ging en wat beter zou moeten.

1. **Zwak protocol (High)**

De webapplicatie maakt gebruik van HTTP in plaats van HTTPS. Dit biedt hackers de mogelijkheid netwerkverkeer te onderscheppen of een MITM aanval op te zetten. Hier hebben we te maken met gevoelige informatie en dient dit niet gelekt te worden aan de buitenwereld.

1. **Invoer validatie (Medium)**

Een aantal voorbeelden van verkeerde invoervalidatie zijn: een hacker kan geld overmaken naar zichzelf, er kunnen accounts aangemaakt worden met zwakke wachtwoorden of zelfs helemaal geen properties. Dit komt door het gebrek aan invoer validatie, want anders zou dit afgevangen kunnen worden.

## **Hoofdstuk 4**

**Conclusie en advies**

Concluderend uit de pentest, kan worden vastgesteld dat de applicatie niet helemaal veilig is zoals gedacht.

# **4.1 Conclusie**

De applicatie heeft een gebrek aan invoer validatie en checks. Bovendien wordt dit allemaal gedaan via een onveilige verbinding.Dit bij elkaar geeft hackers meer aanvalsvectoren en dat is niet wat je wil, vooral niet in een internetbankieren applicatie.

# **4.2 Advies**

Het beste advies wat gegeven kan worden op basis van de pentest, is om meer te testen voor je de applicatie openbaar maakt. Hiermee voorkom je dat er slordigheidsfouten in de applicatie zitten, zoals een gebrek aan checks en input validatie. Voor nu is het advies om de applicatie te verbeteren op basis van de bevindingen die in dit rapport vermeld staan. In de toekomst dient er een continuïteit omtrent testen te worden toegepast.

## 

## **Bijlage A**

**Technische bevindingen**

## Zwak protocol

**7.5 (High)** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

### Reproductie

Als de pagina geladen wordt, wordt het automatisch HTTP in plaats van HTTPS.

### Risico’s

Alle data die over het netwerk gaat is niet versleuteld, dit kan betekenen dat iedereen op het netwerk de informatie die over de lijn gaat kan lezen. Als er dus wachtwoorden of geheime informatie over dit onveilige netwerk gaat, kan het gestolen en misbruikt worden.

### Preventie

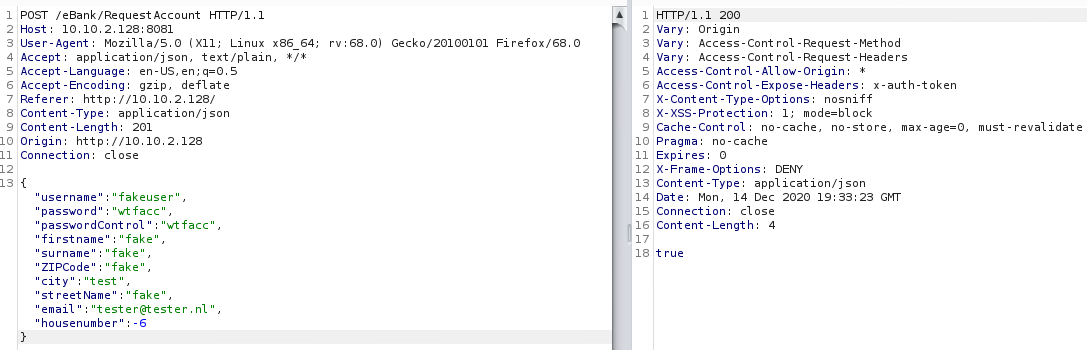
Je hebt een certificaat nodig om je site https te maken. Om deze te krijgen moet je eentje kopen, en vervolgens installeren en activeren op je website.

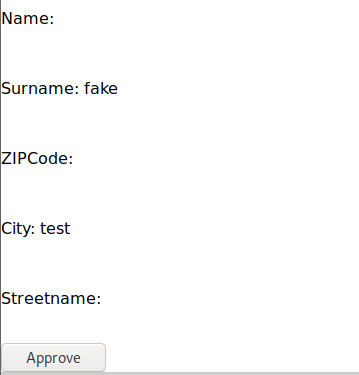
# 

## Invoer validatie

**4.4 (Medium)** CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/RL:O/RC:C/CR:M

### Reproductie

1. Bij het registreren van een account onderschep je het netwerkverkeer. Je ziet dan een request naar ‘/eBank/RequestAccount’.
2. Daarbij zie je de gehele user staan met alle velden. Hier kan je letterlijk alles in aanpassen of verwijderen. In dit geval heb ik een user aangemaakt met een slecht wachtwoord en willekeurige gegevens. Het werkt ook als je velden verwijderd.
3. Verzend de request en je ziet als resultaat ‘true’. Als er via admin wordt ingelogd zie je ook dat dit account goedgekeurd kan worden.



### Risico’s

Zonder invoer validatie is er een mogelijkheid tot het aanmaken van gebruikers zonder valide data. Bovendien kan de gebruiker ook geld overmaken naar zijn eigen rekening.

### Preventie

Alle objecten moeten, ook op de server-side, gecheckt worden. Zo kan het geen niet-valide informatie bevatten en wordt alles goed afgehandeld.

## Overige bevindingen

### Uitlog-functie

Nadat de gebruiker heeft ingelogd, is er geen mogelijkheid meer om uit te loggen.

### Gebruikersfeedback

Als de gebruiker met foute inlog gegevens gebruikt, is daar geen melding van en weet de gebruiker niet of er iets goed of fout is.

### Geen functionaliteit na inlog

Nadat de geregistreerde gebruiker heeft ingelogd kon hij geen functionaliteit gebruiken, ook nadat het account was goedgekeurd.

### Inloggen onbetrouwbaar

De gebruiker kan niet altijd inloggen, ook al zijn de gegevens correct.

### Email check

Bij het registreren checkt de applicatie niet of de ingevoerde e-mail bestaat of niet. Als verbetering op de applicatie zou e-mail verificatie toegepast kunnen worden.