



# PENTEST RAPPORTAGE

## Webapplicatie - Voorbeeldrapportage

Opdrachtgever:	Company BV
Project:	99998 - Keflavik
Auteur(s):	M. Kamminga en P. Luijben
Reviewer(s):	N. Theunissen
Document aangemaakt:	11-06-2024



ISO 9001  
Quality  
Management  
Systems  
CERTIFIED

ISO/IEC  
27001  
Information Security  
Management  
CERTIFIED

Dit document mag niet worden verspreid of gekopieerd zonder toestemming van NFIR B.V.

NFIR B.V.  
Laan van Zuid Hoorn 165  
2289 DD Rijswijk

088-323 02 05  
info@nfir.nl  
www.nfir.nl

IBAN NL 81 RABO 0313 7904 93  
KVK 69575347  
BTW 8579.24.953.B01



## Disclaimer

### Vertrouwelijk

Dit document is geclassificeerd als vertrouwelijk. De informatie in dit document en de bijbehorende bijlagen zijn alleen bedoeld voor Company BV. Het gebruik van dit document door een andere partij dan hiervoor genoemd is niet toegestaan, tenzij deze partij uitdrukkelijk is geautoriseerd door Company BV. De informatie in dit document is als vertrouwelijk gemarkeerd en valt onder de bepalingen van een geheimhoudingsovereenkomst.

Als u het gepresenteerde document onbedoeld ontvangt en/of u hebt geen toestemming om het document in uw bezit te hebben, verzoekt NFIR B.V. u om het document onmiddellijk te sluiten en terug te sturen naar NFIR B.V.

Elk misbruik van dit document of de informatie in dit document is niet toegestaan. NFIR B.V. aanvaardt geen aansprakelijkheid voor enig ongeoorloofd gebruik of misbruik van het gepresenteerde document door een derde partij of voor schade veroorzaakt door de inhoud van dit document.

### Disclaimer Penetratietest

NFIR B.V. voert de penetratietest uit volgens de huidige normen en methodologieën. Een beveiligingscontrole is echter een momentopname. NFIR B.V. aanvaardt geen aansprakelijkheid voor kwetsbaarheden die niet (algemeen) bekend waren op het moment van het uitvoeren van de beveiligingsaudit.

### Copyright © 2024 NFIR B.V.

Alle rechten voorbehouden. De inhoud van dit document mag niet worden gedistribueerd, opgeslagen of gepubliceerd in welke vorm dan ook, digitaal, mechanisch, door fotokopie of opnames, zonder schriftelijke toestemming van NFIR B.V. Aanpassingen aan het door NFIR opgesteld rapport zijn op geen enkele wijze toegestaan.

### Handelsnamen

NFIR en het NFIR-logo zijn handelsmerken van NFIR B.V. Alle andere handelsmerken in dit document zijn eigendom van de vermelde partijen.

### Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren, en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

### POB-vergunning

Het ministerie van Justitie en Veiligheid heeft NFIR een vergunning afgegeven, waardoor NFIR haar werkzaamheden mag uitvoeren. Deze vergunning betreft de POB-vergunning. De POB-vergunning dekt het verwerken van strafrechtelijke gegevens, waarmee NFIR in aanraking kan komen bij het uitvoeren van haar diensten. Het POB-licentie nummer van NFIR is: 1672.



## Management Samenvatting

Company BV heeft NFIR verzocht om een penetratietest uit te voeren op de web applicatie. De scope van de penetratietest omvat de OWASP Juice Shop test webapplicatie

De penetratietest vond plaats van 06-06-2024 tot en met 07-06-2024. Deze gehele periode omvat zowel de technische uitvoering van de penetratietest als het samenstellen van dit rapport.

## Gebruikte standaarden bij de uitvoering van deze penetratietest

Bij de penetratietest is gebruikgemaakt van diverse internationale standaarden voor het ontdekken en classificeren van kwetsbaarheden. De volgende standaarden zijn van toepassing op deze opdracht:

- OWASP WSTG: standaard ten behoeve van webapplicatie penetratietesten.
- OWASP Top 10: de 10 meest kritische kwetsbaarheden van webapplicaties.
- Common Vulnerability Scoring System (CVSS): wordt gebruikt om de ernst van de kwetsbaarheden te classificeren.

## Aantal Bevindingen

Categorie	Bevindingen
✗ Bevindingen: OWASP Juice Shop Webapplicatie	<div><b>KRITIEK (10)</b></div> <ul style="list-style-type: none"><li>● Kritiek: 2 bevindingen</li><li>● Hoog: 1 bevinding</li><li>● Gemiddeld: 1 bevinding</li><li>● Laag: 1 bevinding</li><li>● Info: 3 bevindingen</li></ul>

Tabel 1: Een overzicht van bevindingen gesorteerd op onderdeel inclusief classificatie en hoogste CVSS score.

Tijdens het onderzoek zijn in totaal 8 bevindingen aangetroffen waarvan 2 kritiek, 1 hoog, 1 gemiddeld, 1 laag en 3 informatief.

## Belangrijkste bevindingen

Hieronder worden de belangrijkste kwetsbaarheden kort benoemd.

1. **Kritiek:** Een SQL injectie kwetsbaarheid kan gebruikt worden om de webapplicatie authenticatie te passeren.
2. **Kritiek:** Een SQL Injectie kwetsbaarheid geeft toegang tot wachtwoordhashes.
3. **Kritiek:** Directory Listing is ingeschakeld, gevoelige bestanden zijn beschikbaar.



## Adviezen

NFIR adviseert om de gevonden kwetsbaarheden zo spoedig mogelijk op te lossen in volgorde van kritiek naar laag en een hertest uit te voeren om te verifiëren of de gevonden kwetsbaarheden daadwerkelijk zijn opgelost.



# 1. Opdrachtbeschrijving

Company BV heeft NFIR verzocht om een penetratietest uit te voeren en heeft hiervoor de desbetreffende scope onderdelen aangeleverd na de intake meeting. De opdracht is uitgevoerd volgens de getekende offerte:

[Offerte Juice Company.pdf](#) .

## 1.1. Doel

Het doel van een penetratietest is kwetsbaarheden identificeren binnen de webapplicatie volgens de afgesproken scope.

## 1.2. Aanvalsscenario

De penetratietest omvat een White Box, waarbij NFIR 24 uur heeft besteed aan het onderzoek en de rapportage. De volgende aanvalsscenario's zijn uitgevoerd:

### 1.2.1. White Box: Web Applicatie

Vooraf is alle informatie over de functionaliteiten van de webapplicatie verkregen en zijn inloggegevens en de broncode van de webapplicatie door de opdrachtgever verstrekt. In dit aanvalsscenario kan zeer gericht gezocht worden naar kwetsbaarheden en risico's binnen de webapplicatie die mogelijk misbruikt kunnen worden door kwaadwillende hackers. Het is belangrijk om te weten dat een White Box pentest geen code review / audit betreft.

## 1.3. Standaarden en methodieken

Bij de penetratietest is gebruik gemaakt van diverse internationale standaarden voor het ontdekken en classificeren van kwetsbaarheden. De volgende standaarden zijn van toepassing op deze opdracht:

- OWASP WSTG: Standaard ten behoeve van webapplicatie pentesten.
- OWASP Top 10: De 10 meest kritische kwetsbaarheden van webapplicaties.
- Common Vulnerability Scoring System (CVSS): Wordt gebruikt om de ernst van de kwetsbaarheden te classificeren.
  - ◇ Het scoresysteem werkt op basis van acht verschillende basisparameters, die samen de risicoscore bepalen.
  - ◇ Deze parameters vormen zogenaamde vector strings en kunnen gebruikt worden om te herleiden waarop de scores gebaseerd zijn. Dit herleiden kan eenvoudig gereproduceerd worden door op de vector string te klikken.
  - ◇ Informatieve bevindingen zijn afwijkingen van de best practices op het gebied van beveiliging die, hoewel ze een minimaal onmiddellijk risico veroorzaken, in de toekomst een grotere bedreiging kunnen vormen.

Er zijn zeven fasen tijdens een penetratietest. Deze zeven fasen zijn:

ID	Fase	Omschrijving
----	------	--------------



1	Informatie verzamelen	Deze fase bestaat uit het verzamelen van zoveel mogelijk informatie uit openbare bronnen (OSINT) en informatie die wordt aangeleverd door de opdrachtgever, zoals netwerktekeningen en een IP-nummerplan.
2	Informatie analyseren	Gedurende deze fase wordt de informatie gewaardeerd en wordt daarmee vastgesteld welke informatie relevant is voor de penetratietest om bijvoorbeeld een aanvalsmethodiek en mogelijke bedreigingen in kaart te brengen.
3	Kwetsbaarheden analyse	Nadat alle informatie is verzameld, wordt in deze fase gezocht naar kwetsbaarheden in systemen en applicaties. Hierbij wordt zowel met automatische tooling als op creatieve wijze handmatig gezocht naar kwetsbaarheden. Tijdens deze fase wordt gebruik gemaakt van diverse internationale standaarden zoals OWASP Top 10, PTES, en OWASP MASTG.
4	Exploitatie	Tijdens de exploitatie fase is toegang verkrijgen tot het systeem het doel. De verzamelde informatie wordt gebruikt om op een zorgvuldige wijze aanvallen uit te voeren, met als doel de geïdentificeerde kwetsbaarheden te bevestigen.
5	Post-exploitatie	In de post-exploitatie fase wordt vastgesteld wat de waarde is van het gecompromitteerde systeem. Dit is afhankelijk van de gevonden data en of deze bruikbaar is om het netwerk verder te compromitteren.
6	Rapporteren	Alle bevindingen worden samengebracht in een compleet en helder uitgewerkt rapport. Dit rapport bevat een beschrijving van de bevindingen, een scoresysteem (CVSS) waarbij de kwetsbaarheden een classificatie krijgen, de mogelijke impact van de kwetsbaarheden, en aanbevelingen die uw organisatie helpen met het oplossen van de gevonden kwetsbaarheden.
7	Hertest	Op basis van de aanbevelingen kunnen de gevonden kwetsbaarheden door uw eigen organisatie (of externe partij) worden opgelost. Zodra de kwetsbaarheden zijn opgelost, wordt NFIR veelal gevraagd dit te controleren middels een hertest. Er wordt dan onderzocht en gerapporteerd of de kwetsbaarheden daadwerkelijk zijn opgelost. Een hertest kan alleen worden begroot na voltooiing van de initiële penetratietest.

Tabel 1.1: Zeven fasen penetratietest



## 1.4. Onderdelen per bevinding

De kwetsbaarheden die zijn aangetroffen tijdens het uitvoeren van de penetratietest zullen in de bevindingen hoofdstukken worden beschreven. Per kwetsbaarheid worden de volgende onderdelen beschreven:

Onderdeel	Omschrijving
Host(s)	IP-adressen / omgevingen die zijn getroffen door de kwetsbaarheid.
CVSS-Score	CVSS-score die aan de kwetsbaarheid is gekoppeld.
CVSS Vector String	De metriekeken die gebruikt zijn om de CVSS-score van de kwetsbaarheid te berekenen. Deze vector string is aanklikbaar en verwijst naar de online calculator van de CVSS.
Omschrijving	Omschrijving van de kwetsbaarheid, wat deze inhoudt, en wat het gevolg is als deze wordt misbruikt.
Mogelijke Impact	Een omschrijving van de mogelijke impact van de kwetsbaarheid. Wat kan een aanvaller doen en waartoe kan toegang worden verkregen?
Aanbeveling	Advies omtrent hoe de kwetsbaarheid gemitigeerd kan worden
Bevestiging	Procedure die is gebruikt om de kwetsbaarheid vast te stellen.
Referenties	Additionele informatie over de bevinding
Classificaties	Root cause op basis van Common Weakness Enumeration (CWE)

Tabel 1.2: De verschillende onderdelen per bevinding

## 1.5. Scope

In de onderstaande tabellen wordt de scope voor de penetratietest van de uitgevoerde opdracht beschreven.

Scope	Omschrijving
127.0.0.1	Juiceshop Web application

Tabel 1.3:

Er zijn bij de uitvoering geen DDoS-aanvallen uitgevoerd.



## 2. Resultaten penetratietest

De penetratietest vond plaats van 06-06-2024 tot en met 07-06-2024. Deze gehele periode omvat zowel de technische uitvoering van de penetratietest als het samenstellen van dit rapport.

### 2.1. Aantal bevindingen

De onderstaande tabel toont het totale aantal bevindingen van de uitgevoerde penetratietest, gepresenteerd per risicoclassificatie:

Categorie	Bevindingen
✗ <b>Bevindingen: OWASP Juice Shop Webapplicatie</b>	<div><b>KRITIEK (10)</b></div> <ul style="list-style-type: none"><li>● Kritiek: 2 bevindingen</li><li>● Hoog: 1 bevinding</li><li>● Gemiddeld: 1 bevinding</li><li>● Laag: 1 bevinding</li><li>● Info: 3 bevindingen</li></ul>

Tabel 2.1: Een overzicht van bevindingen gesorteerd op onderdeel inclusief classificatie en hoogste CVSS score.

Tijdens het onderzoek zijn in totaal 8 bevindingen aangetroffen.

### 2.2. Verkregen toegang

Door NFIR is tijdens het onderzoek de volgende toegang verkregen. Tot deze systemen heeft een gebruiker normaal geen toegang.

Toegang	Omschrijving
Administrator toegang (lokaal)	Er is toegang verkregen als admin. Het gaat hierbij om het lokaal inloggen op de systemen en inzagen van de lokale database.
Database	De gegevens in de SQL database kunnen worden bekeken. Er is toegang met gebruiker admin.

Tabel 2.2:





## 2.3. Bevindingen overzicht

De onderstaande tabel geeft een overzicht van alle aangetroffen bevindingen inclusief de classificatie.

#	Bevinding	Status	Classificatie	Pagina
001	SQL Injectie – Authenticatie omzeilen	✗ Niet opgelost	KRITIEK (10)	9
002	SQL Injectie – Toegang tot wachtwoordhashes	✗ Niet opgelost	KRITIEK (10)	11
003	Gevoelige bestanden beschikbaar	✗ Niet opgelost	HOOG (8.8)	13
004	Open Redirect – Parameter 'to'	✗ Niet opgelost	GEMIDDELD (5.3)	15
005	Directory Listing is ingeschakeld	✗ Niet opgelost	LAAG (2.3)	16
006	Wachtwoordbeleid onvoldoende	✗ Niet opgelost	INFO (0)	17
007	Geen gebruik van beveiligde https-verbinding	✗ Niet opgelost	INFO (0)	18
008	Stack Trace Error – Information disclosure	✗ Niet opgelost	INFO (0)	19

Tabel 2.3: Bevindingen gesorteerd op classificatie.

In hoofdstuk [Bevindingen: OWASP Juice Shop Webapplicatie](#) zijn de aangetroffen kwetsbaarheden opgenomen, uitgewerkt aan de hand van het bovenstaande overzicht.



### 3. Bevindingen: OWASP Juice Shop Webapplicatie

#### SQL Injectie – Authenticatie omzeilen

**10  
KRITIEK**

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

ID: 99998-NL-001

Target: localhost (127.0.0.1)

##### Omschrijving

Het is mogelijk, door een SQL injectie te gebruiken, in te loggen als de admin gebruiker zonder het wachtwoord te gebruiken.

##### Mogelijke impact

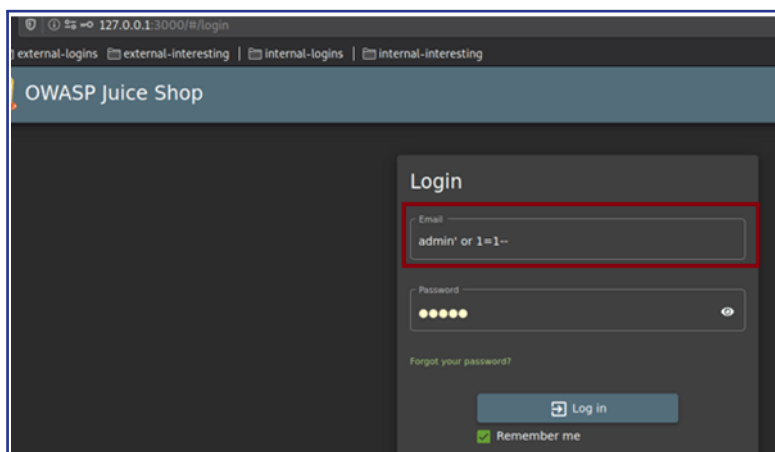
Door gebruik te maken van dit gebruikersaccount is toegang tot de webapplicatie verkregen met het hoogste niveau van rechten.

##### Aanbeveling

Geadviseerd wordt om gebruikt te maken van 'prepared statements' om het risico van SQL injectie te verkleinen. Daarnaast wordt geadviseerd om speciale karakters af te vangen zodat deze alleen geïnterpreteerd worden als strings.

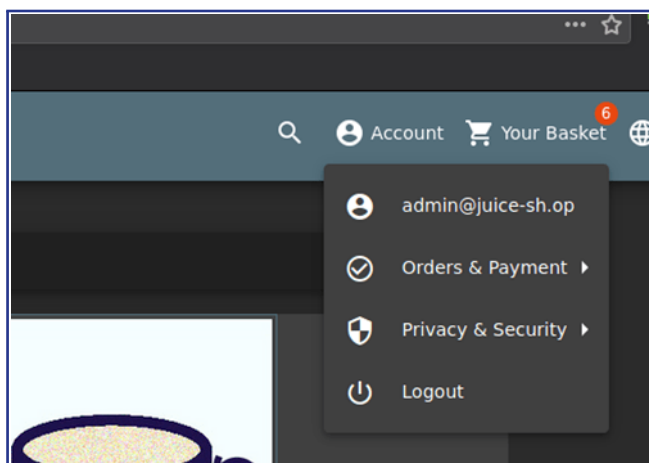
##### Bevestiging

Op de inlogpagina is het mogelijk om in te loggen als admin door ``admin' or 1=1--" in het e-mail veld te plaatsen:



Figuur 3.1: Inlogpagina - Login bypass.

Vervolgens kan worden ingelogd en is te zien dat als admin gebruiker is ingelogd:



Figuur 3.2: Ingelogd als admin gebruiker.

## Referenties

Checklist-ID: WSTG-AHTN-04

## Classificaties

- [CWE-89: Improper Neutralization of Special Elements used in an SQL Command \('SQL Injection'\)](#)



## SQL Injectie – Toegang tot wachtwoordhashes

**10  
KRITIEK**

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

ID: 99998-NL-002

Target: localhost (127.0.0.1)

### Omschrijving

De shop API is kwetsbaar voor een SQL injection. Hiermee is het mogelijk om de database uit te lezen, en wachtwoorden van gebruikers te achterhalen.

Het wachtwoord van de admin gebruiker is achterhaald, en toegang tot de applicatie is verkregen.

### Mogelijke impact

Een aanvaller kan alle informatie in de database achterhalen. Wanneer wachtwoordhashes gekraakt worden, is het mogelijk om in te loggen als die gebruikers met de bijbehorende rechten en mogelijkheden.

### Aanbeveling

Geadviseerd wordt om gebruik te maken van prepared statements om het risico van SQL injection te verkleinen. Ten tweede wordt geadviseerd om speciale karakters af te vangen zodat deze alleen geïnterpreteerd worden als strings. Tot slot wordt geadviseerd om geen gebruik te maken van MD5 om wachtwoorden op te slaan, maar gebruik te maken van PBKDF2.

### Bevestiging

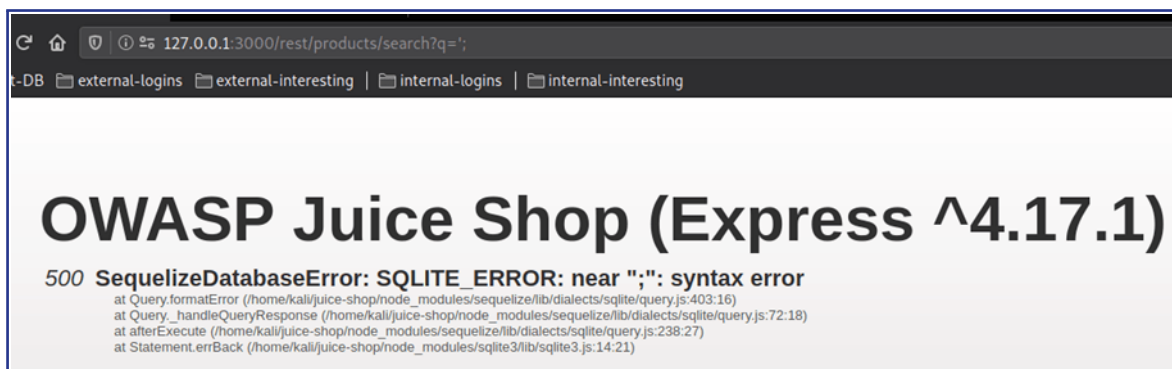
Door met Firefox naar 127.0.0.1:3000/#/search/ te gaan en een zoekopdracht te doen, is te zien dat gebruik wordt gemaakt van een API:

Method	Domain	File	Initiator	Type	Transferred	Size
GET	127.0.0.1:3000	/api/Quantities/	polyfills-es2018...	json	cached	5.85 KB
GET	127.0.0.1:3000	search?q=	polyfills-es2018...	json	cached	13.18 KB
GET	127.0.0.1:3000	fan_facemask.jpg	vendor-es2018.j...	jpeg	cached	26.30 KB

Headers: GET http://127.0.0.1:3000/rest/products/search?q=

Figuur 3.3: SQL Injectie - gebruik van API.

Door `'))--' te plaatsen achter de zoekopdracht in de API, is de volgende foutmelding te zien:



Figuur 3.4: SQL Injectie - foutmelding in sqlite.



Dit geeft aan dat de API kwetsbaar is. Door vervolgens `1')) UNION SELECT password, id, email, username, '5', '6', '7', '8', '9' FROM Users--` achter de zoekopdracht te plaatsen, zijn de MD5 wachtwoordhashes van de gebruikers binnen de applicatie te zien:

```
{
  "status": "success",
  "data": [
    {
      "id": "****",
      "name": 18,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 1,
      "description": "admin@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 11,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 16,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 3,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 14,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 9,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 19,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 4,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 12,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 5,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 13,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 15,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 10,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 8,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 6,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 2,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 20,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 7,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6"
    },
    {
      "id": "****",
      "name": 17,
      "description": "****@juice-sh.op",
      "price": "****",
      "deluxePrice": "5",
      "image": "6",
      "createdAt": "2020-01-01T00:00:00Z"
    }
  ]
}
```

Door gebruik te maken van hashcat, was het mogelijk om het wachtwoord van de volgende gebruikers te achterhalen:

- admin@juice-sh.op
- mc.safesearch@juice-sh.op
- jim@juice-sh.op
- demo@juice-sh.op

## Referenties

Checklist-ID: WSTG-AHTN-04

## Classificaties

- [CWE-89: Improper Neutralization of Special Elements used in an SQL Command \('SQL Injection'\)](#)



## Gevoelige bestanden beschikbaar

**8.8**  
**HOOG**

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:L/SI:L/SA:N

ID: 99998-NL-003

Target: localhost (127.0.0.1)

### Omschrijving

In bevinding 'Directory Listing is ingeschakeld' zijn publiek beschikbare bestanden gevonden. Dit betreft ook gevoelige bestanden.

### Mogelijke impact

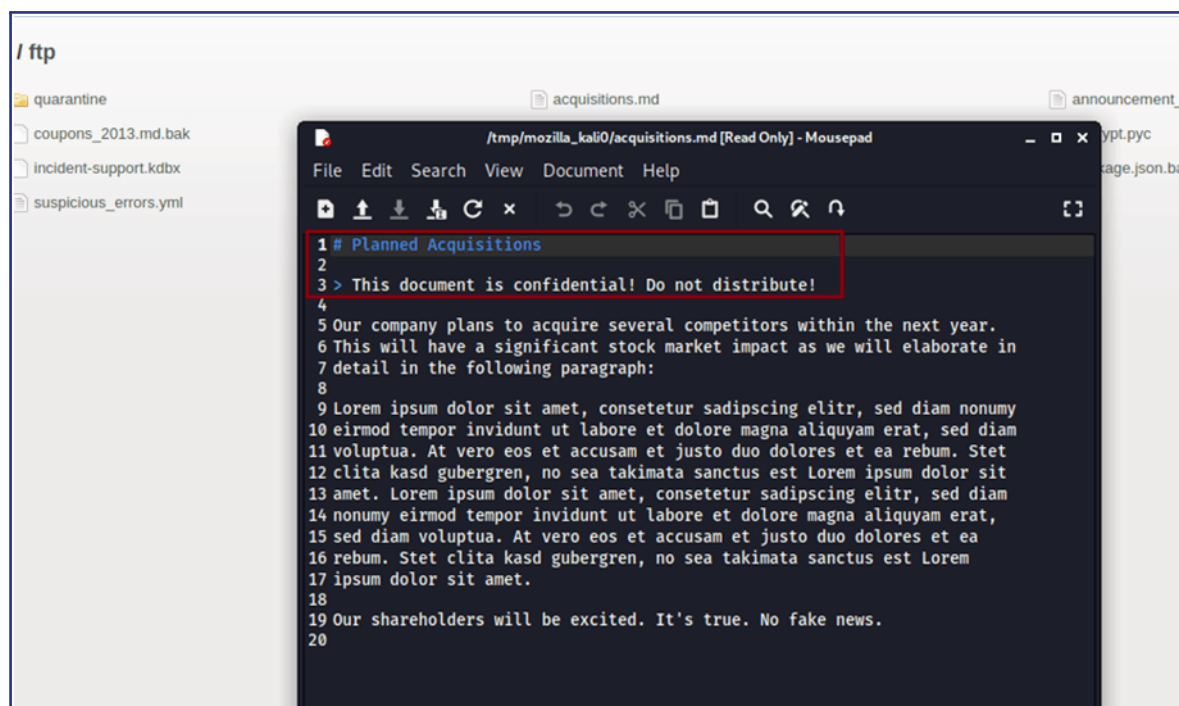
Doordat deze data vrij toegankelijk is, is het risico op een datalek groot. Daarnaast zouden deze gegevens alleen toegankelijk moeten zijn voor geauthentiseerde gebruikers.

### Aanbeveling

Geadviseerd wordt om directory listing uit te schakelen. Daarnaast wordt geadviseerd om gevoelige bestanden niet publiek beschikbaar te maken.

### Bevestiging

URL <http://127.0.0.1/ftp> is geopend. Daarbij is het bestand 'acquisitions.md' bekeken en is te zien dat deze gevoelige gegevens bevat:



Figuur 3.5: Gevoelige gegevens - open directory.

### Referenties

Checklist-ID: WSTG-CONF-01



### Classificaties

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)
- [CWE-548: Exposure of Information Through Directory Listing](#)





## Open Redirect – Parameter ‘to’

**5.3**  
**GEMIDDELD**

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

ID: 99998-NL-004

Target: localhost (127.0.0.1)

### Omschrijving

De webapplicatie valideert gebruikersinvoer onvoldoende, waardoor een aanvaller de URL zodanig kan manipuleren dat de webapplicatie verwijst naar niet-vertrouwde URL's. De webapplicatie bevat hierdoor een 'Open Redirect' kwetsbaarheid.

### Mogelijke impact

Een aanvaller kan URL's construeren die ervoor zorgen dat een gebruiker wordt doorgestuurd naar een phishing pagina waarop gevraagd wordt om vertrouwelijke gegevens, zoals inloggegevens, in te voeren. Als de gebruiker wordt misleid om op deze manier zijn inloggegevens in te voeren, kan de aanvaller inloggen als deze gebruiker.

### Aanbeveling

Het wordt aanbevolen om gebruikersinvoer strikt te valideren. De webapplicatie dient gebruikers alleen door te sturen naar URL's van vertrouwde domeinen. Deze kunnen worden bijgehouden in een whitelist.

### Bevestiging

Het volgende request is onderschept en aangepast door middel van Burp Suite:

```
GET /redirect?to=http://nfir.nl?pwmed=https://github.com/bkimminich/juice-shop HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

De webapplicatie reageert hierop met de onderstaande response:

```
HTTP/1.1 302 Found
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Location: http://nfir.nl?pwmed=https://github.com/bkimminich/juice-shop
Vary: Accept, Accept-Encoding
Content-Type: text/html; charset=utf-8
Content-Length: 166
Date: Thu, 26 Aug 2021 08:42:35 GMT
<p>Found. Redirecting to <a href="http://nfir.nl?pwmed=https://github.com/bkimminich/juice-shop">http
↪ ://nfir.nl?pwmed=https://github.com/bkimminich/juice-shop</a></p>
```

### Referenties

Checklist-ID: WSTG-CLNT-04

### Classificaties

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')





## Directory Listing is ingeschakeld

**2.3**  
**LAAG**

CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 99998-NL-005

Target: localhost (127.0.0.1)

### Omschrijving

De host heeft de directory listing module ingeschakeld.

### Mogelijke impact

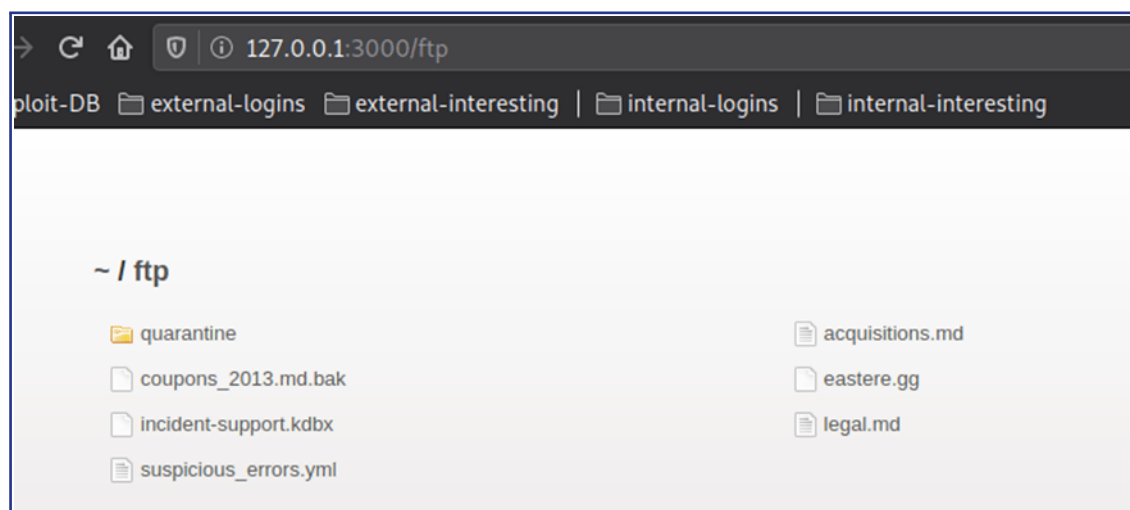
Een aanvaller kan door gebruik te maken van deze directory listing, mogelijk gevoelige gegevens bekijken en de data downloaden.

### Aanbeveling

Geadviseerd wordt om de directory listing module uit te schakelen. Hiermee wordt voorkomen dat mogelijk gevoelige bestanden kunnen worden bekeken en gedownload.

### Bevestiging

Door de URL '<http://127.0.0.1/ftp>' te bezoeken, is te zien dat directory listing is ingeschakeld:



Figuur 3.6: Directory Listing ingeschakeld.

### Referenties

Checklist-ID: WSTG-CONF-09

### Classificaties

- [CWE-548: Exposure of Information Through Directory Listing](#)



## Wachtwoordbeleid onvoldoende



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 99998-NL-006

Target: localhost (127.0.0.1)

### Omschrijving

Het gebruikte wachtwoordbeleid is niet voldoende om veilige wachtwoorden te garanderen. Hierdoor is het mogelijk om gebruik te maken van onveilige wachtwoorden.

### Mogelijke impact

Het wachtwoordbeleid maakt het mogelijk voor medewerkers om onveilige wachtwoorden te gebruiken. Deze wachtwoorden kunnen gemakkelijk worden achterhaald en vervolgens worden gebruikt om toegang te verkrijgen tot de systemen van Company BV

### Aanbeveling

Geadviseerd wordt om gebruik te maken van sterke wachtwoorden, zoals voorgeschreven volgens het NCSC:

- Voorspelbaarheid: Verbied het gebruik van een wachtwoord dat voorkomt in een actuele lijst van veelgebruikte wachtwoorden;
- Lengte: Hoe langer een wachtwoord, hoe sterker. Kies hierbij voor minimaal 10-24 karakters, en stel geen maximumlengte in;
- Levensduur: Pas geen verplichting toe op het periodiek wijzigen van het wachtwoord, dit leidt in de praktijk tot het gebruik van eenvoudiger te raden wachtwoorden;
- Variatie: Pas geen verplichting toe op het gebruik van verschillende tekens zoals hoofdletters, cijfers en leestekens, dit leidt in de praktijk tot eenvoudiger te raden wachtwoorden;

### Bevestiging

Bij het aanmaken van een nieuw account, is te zien dat een wachtwoord slechts 5 karakters hoeft te hebben:

Figuur 3.7: Account aanmaken - minimaal 5 karakters.

### Referenties

Meer informatie over deze kwetsbaarheid is te vinden op: <https://www.ncsc.nl/onderwerpen/authenticatie>

### Classificaties

- [CWE-521: Weak Password Requirements](#)



## Geen gebruik van beveiligde https-verbinding



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 99998-NL-007

Target: localhost (127.0.0.1)

### Omschrijving

De host maakt geen gebruik van een beveiligde https-verbinding.

### Mogelijke impact

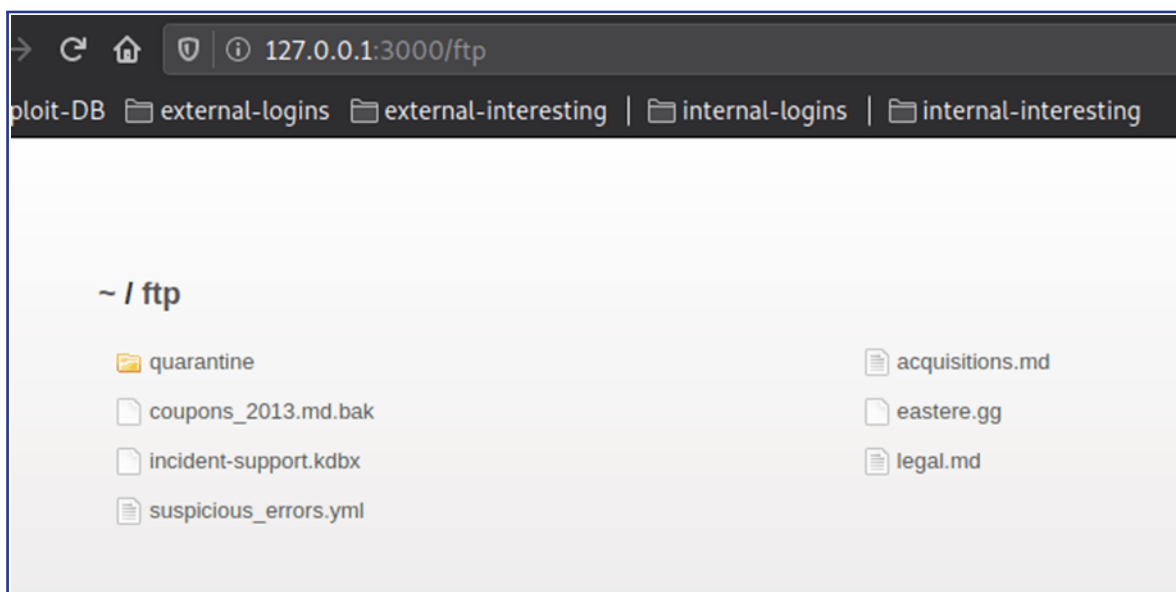
Een aanvaller kan een Man-in-the-Middle (MiTM) aanval uitvoeren. Dit betekent dat alle informatie die wordt verstuurd tussen client en server inzichtelijk zijn voor de aanvaller.

### Aanbeveling

Geadviseerd wordt om de connectie te beveiligen, bij voorkeur met TLSv1.3 als onderdeel van een toekomstvaste TLS-configuratie.

### Bevestiging

Door met Firefox naar <http://127.0.0.1> te gaan, is te zien dat er geen slotje in de URL staat. Dit betekent dat er geen beveiligde https-verbinding gebruikt wordt:



Figuur 3.8: Geen TLS.

Dit geldt voor de gehele webapplicatie.

### Referenties

Checklist-ID: WSTG-CONF-07

### Classificaties

- [CWE-319: Cleartext Transmission of Sensitive Information](#)



## Stack Trace Error – Information disclosure



CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

ID: 99998-NL-008

Target: localhost (127.0.0.1)

### Omschrijving

De API geeft een gedetailleerde foutmelding weer wanneer een foutmelding optreedt.

### Mogelijke impact

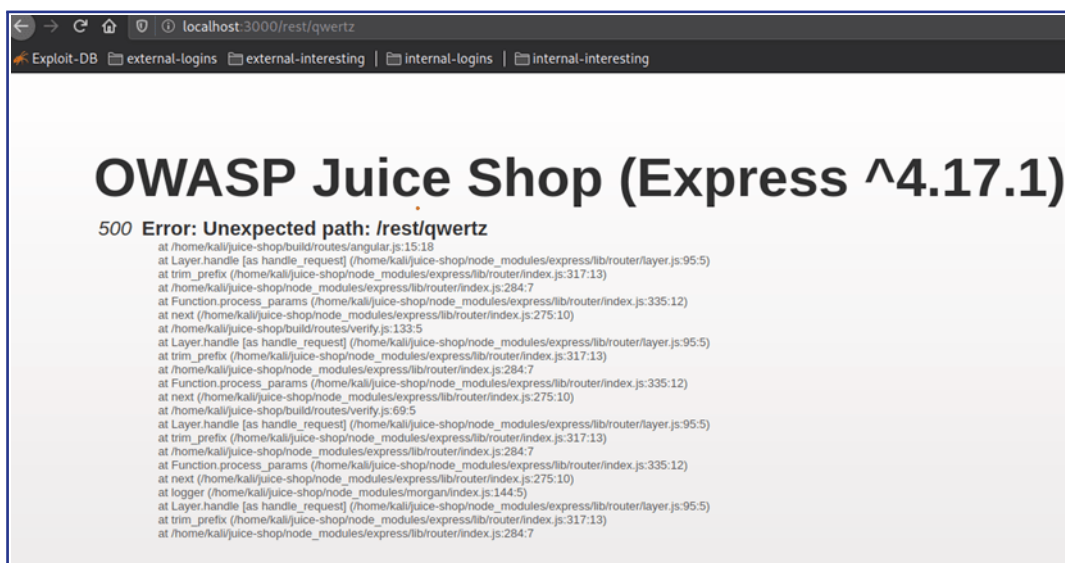
Een aanvalleur kan de foutmelding gebruiken om kennis op te doen over de gebruikte technologie en interne werking van de software.

### Aanbeveling

Geadviseerd wordt om geen gedetailleerde foutmeldingen weer te geven.

### Bevestiging

De URL '<http://127.0.0.1:3000/rest/qwertz>' wordt geopend in de browser en geeft de volgende foutmelding weer:



Figuur 3.9: Error handling in API.

### Referenties

Checklist-ID: WSTG-ERRH-01/02

### Classificaties

- CWE-209: Generation of Error Message Containing Sensitive Information



## 4. Bijlage 1: Checklist

### 4.1. OWASP WSTG / OWASP Top 10 2021

WSTG-ID	Top 10	Item	Status	Bevinding
INFO-01	NA	Conduct Search Engine Discovery Reconnaissance for Information Leakage	✓	
INFO-02	A5, A6	Fingerprint Web Server	✓	
INFO-03	A1	Review Webserver Metafiles for Information Leakage	✓	
INFO-04	NA	Enumerate Applications on Webserver	✓	
INFO-05	A1	Review Webpage Content for Information Leakage	✓	
INFO-06	NA	Identify application entry points	✓	
INFO-07	NA	Map execution paths through application	✓	
INFO-08	A5, A6	Fingerprint Web Application Framework	✓	
INFO-09	NA	Fingerprint Web Application	✓	
INFO-10	NA	Map Application Architecture	✓	
CONF-01	A1, A5, A6	Test Network Infrastructure Configuration	✓	
CONF-02	A1, A5, A9	Test Application Platform Configuration	✓	



CONF-03	A1	Test File Extensions Handling for Sensitive Information	✓	
CONF-04	A1	Review Old Backup and Unreferenced Files for Sensitive Information	✗	Directory Listing is ingeschakeld
			✗	Gevoelige bestanden beschikbaar
CONF-05	A1, A4	Enumerate Infrastructure and Application Admin Interfaces	✓	
CONF-06	A5	Test HTTP Methods	✓	
CONF-07	A5	Test HTTP Strict Transport Security	✗	Geen gebruik van beveiligde https-verbinding
CONF-08	A5	Test RIA Cross Domain Policy	N/A	
CONF-09	A1, A5	Test File Permission	✗	Directory Listing is ingeschakeld
CONF-10	NA	Test for Subdomain Takeover	✓	
CONF-11	A1	Test Cloud Storage	✓	
CONF-12	A5	Test for Content Security Policy	✓	
CONF-13	A5	Test for Path Confusion	✓	
IDNT-01	A4	Test Role Definitions	✓	
IDNT-02	A4	Test User Registration Process	✗	Wachtwoordbeleid onvoldoende
IDNT-03	A4	Test Account Provisioning Process	✓	



IDNT-04	A7	Testing for Account Enumeration and Guessable User Account	✓	
IDNT-05	A7	Testing for Weak or unenforced username policy	✓	
ATHN-01	NA	Testing for Credentials Transported over an Encrypted Channel	✓	
ATHN-02	A7	Testing for Default Credentials	✓	
ATHN-03	A7	Testing for Weak Lock Out Mechanism	✓	
ATHN-04	A1, A7	Testing for Bypassing Authentication Schema	✗	SQL Injectie – Authenticatie omzeilen
			✗	SQL Injectie – Toegang tot wachtwoordhashes
			✗	Wachtwoordbeleid onvoldoende
ATHN-05	A4, A5	Testing for Vulnerable Remember Password	✓	
ATHN-06	A4	Testing for Browser Cache Weaknesses	✓	
ATHN-07	A7	Testing for Weak Password Policy	✗	Wachtwoordbeleid onvoldoende
ATHN-08	A7	Testing for Weak Security Question Answer	✗	Wachtwoordbeleid onvoldoende
ATHN-09	A7	Testing for Weak Password Change or Reset Functionalities	✓	
ATHN-10	A7	Testing for Weaker Authentication in Alternative Channel	✓	



ATHN-11	A7	Testing Multi-Factor Authentication	✓	
ATHZ-01	A1	Testing Directory Traversal File Include	✓	
ATHZ-02	A1	Testing for Bypassing Authorization Schema	✓	
ATHZ-03	A1	Testing for Privilege Escalation	✓	
ATHZ-04	A1	Testing for Insecure Direct Object References	✓	
ATHZ-05	A1	Testing for OAuth Weaknesses	✓	
SESS-01	A2, A4	Testing for Session Management Schema	✓	
SESS-02	A5	Testing for Cookies Attributes	✓	
SESS-03	A7	Testing for Session Fixation	✓	
SESS-04	A7	Testing for Exposed Session Variables	✓	
SESS-05	A1	Testing for Cross Site Request Forgery	✓	
SESS-06	A7	Testing for Logout Functionality	✓	
SESS-07	A7	Testing Session Timeout	✓	
SESS-08	A7	Testing for Session Puzzling	✓	
SESS-09	A2	Testing for Session Hijacking	✓	
SESS-10	A2, A7	Testing JSON Web Tokens	✓	





INPV-01	A3	Testing for Reflected Cross Site Scripting	✓	
INPV-02	A3	Testing for Stored Cross Site Scripting	✓	
INPV-03	NA	Testing for HTTP Verb Tampering	✓	
INPV-04	A3	Testing for HTTP Parameter Pollution	✓	
INPV-05	A3	Testing for SQL Injection	✗	SQL Injectie – Authenticatie omzeilen
			✗	SQL Injectie – Toegang tot wachtwoordhashes
INPV-06	A3	Testing for LDAP Injection	✓	
INPV-07	A5	Testing for XML Injection	✓	
INPV-08	A3	Testing for SSI Injection	✓	
INPV-09	A3	Testing for XPath Injection	✓	
INPV-10	A3	Testing for IMAP SMTP Injection	N/A	
INPV-11	A3	Testing for Code Injection	✓	
INPV-12	A3	Testing for Command Injection	✓	
INPV-13	A3	Testing for Format String Injection	✓	
INPV-14	A3	Testing for Incubated Vulnerability	✓	
INPV-15	A3, A4	Testing for HTTP Splitting Smuggling	✓	



INPV-16	NA	Testing for HTTP Incoming Requests	✓	
INPV-17	A4	Testing for Host Header Injection	✓	
INPV-18	A4	Testing for Server-side Template Injection	✓	
INPV-19	A10	Testing for Server-Side Request Forgery	✓	
INPV-20	A1	Testing for Mass Assignment	✓	
ERRH-01	A5	Testing for Improper Error Handling	✗	Stack Trace Error – Information disclosure
ERRH-02	NA	Testing for Stack Traces	✗	Stack Trace Error – Information disclosure
CRYP-01	A2,A7	Testing for Weak Transport Layer Security	N/A	
CRYP-02	A2	Testing for Padding Oracle	✓	
CRYP-03	A2	Testing for Sensitive Information Sent via Unencrypted Channels	✗	Geen gebruik van beveiligde https-verbinding
CRYP-04	A2	Testing for Weak Encryption	N/A	
BUSL-01	A4	Test Business Logic Data Validation	✓	
BUSL-02	A4	Test Ability to Forge Requests	✓	
BUSL-03	A4	Test Integrity Checks	✓	
BUSL-04	A4	Test for Process Timing	✗	Open Redirect – Parameter 'to'



BUSL-05	A4, A7	Test Number of Times a Function Can Be Used Limits	✓	
BUSL-06	A4	Testing for the Circumvention of Work Flows	✓	
BUSL-07	A4	Test Defenses Against Application Misuse	✓	
BUSL-08	A4	Test Upload of Unexpected File Types	✓	
BUSL-09	A4	Test Upload of Malicious Files	✓	
BUSL-10	A4	Test Payment Functionality	✓	
CLNT-01	A3	Testing for DOM-Based Cross Site Scripting	✓	
CLNT-02	A3	Testing for JavaScript Execution	✓	
CLNT-03	A3	Testing for HTML Injection	✓	
CLNT-04	A4	Testing for Client-side URL Redirect	✗	Open Redirect – Parameter ‘to’
CLNT-05	A3	Testing for CSS Injection	✓	
CLNT-06	A3	Testing for Client-side Resource Manipulation	✓	
CLNT-07	A5	Testing Cross Origin Resource Sharing	✓	
CLNT-08	A3	Testing for Cross Site Flashing	✓	
CLNT-09	A5	Testing for Clickjacking	✗	



CLNT-10	A2, A3	Testing WebSockets	N/A	
CLNT-11	A5	Testing Web Messaging	N/A	
CLNT-12	A1, A4	Testing Browser Storage	✓	
CLNT-13	A3	Testing for Cross Site Script Inclusion	✓	
CLNT-14	A3	Testing for Reverse Tabnabbing	N/A	
APIT-01	A3	Testing GraphQL	N/A	

Tabel 4.1: ✓ = Geen kwetsbaarheid aangetroffen, ✗ = Kwetsbaarheid gevonden, N/A = Niet van toepassing



## 5. Bijlage 2: Scan resultaten

### 5.1. Poort scans

De volgende openstaande poorten op de beschikbare host(s) zijn aangetroffen. Host(s) zonder open poorten zijn niet opgenomen.

Host	Open poort	Service
127.0.0.1	tcp/3000	OWASP DVWA v14.5.1

Tabel 5.1: Poortscan resultaten



## 6. Bijlage 3: Overige

### 6.1. Technische hulpmiddelen

Een combinatie van technische hulpmiddelen is gebruikt om scantaken (gedeeltelijk) te automatiseren en de infrastructuur te kunnen identificeren. De uitkomsten van deze hulpmiddelen zijn te allen tijde geverifieerd. Hieronder staan de gebruikte hulpmiddelen, inclusief de bijbehorende versienummers:

Hulpmiddel	Versie	Opmerking
Burp Suite Professional	2021.8.1	Een webapplicatie audit tool.
DIRB	2.22	Een geautomatiseerd programma om map structuren van webapplicaties te identificeren.
Hashcat	6.2.3	Software om wachtwoord hashes te kraken.
Kali Linux	2021.2	Operatie Systeem voor audits.
Mozilla Firefox	78.13.0esr	Webbrowser.
Nikto	2.1.6	Een webapplicatie scanner voor bekende kwetsbaarheden.
Nmap	7.80	Een poort scanner.
OWASP ZAP zaproxy	2.12.0	Webapplicatie audit tool.
Search-That-Hash	N/A	Een script dat veel voorkomende wachtwoorden kan opzoeken in openbare bronnen.

Tabel 6.1: Technische hulpmiddelen



## 6.2. Gebruikte IP-adressen

De onderstaande IP-adressen zijn door NFIR ten tijde van de uitvoering van de penetratietest ingezet om verbinding te maken met de gespecificeerde scope.

IPv4-adres	IPv6-adres	Beschrijving
136.144.183.82	2a01:7c8:aac7:318::1	Extern IP-adres NFIR 1
95.170.71.93	2a01:7c8:bb06:10e:5054:ff:fe6d:b24e	Extern IP-adres NFIR 2
93.119.0.143	2a01:7c8:bb0a:7f:5054:ff:fe3b:73dd	Extern IP-adres NFIR 3

Tabel 6.2: Gebruikte IP-adressen

## 6.3. Ontvangen bestand

NFIR heeft de volgende bestanden ontvangen en gebruikt voor deze penetratietest:

Bestandsnaam	Beschrijving	SHA-1 hash
bestand.docx	bestand	***** ...

Tabel 6.3: Ontvangen bestanden

## 6.4. Terugdraaien wijzigingen

### 6.4.1. Whitelisting

Veel organisaties vragen zich af waarom NFIR verzoekt om zeven IP-adressen te whitelisten in de firewall als vereiste voor de start van de penetratietest. Ook wordt soms gesuggereerd dat hierdoor het testen van de technische weerbaarheid niet meer representatief zou zijn.

De reden dat dit gevraagd wordt is om te voorkomen dat onze IP-adressen geblokkeerd worden door de Intrusion Prevention / Detection System (IPS/IDS) modules van een firewall zodra de IT-infrastructuur onderzocht wordt. Dit zou zeer waarschijnlijk gebeuren doordat de (scanning) tools die gebruikt worden verzoeken afvuren op de firewall en als malafide verkeer worden herkend. Als de NFIR IP-adressen niet op de whitelist geplaatst worden, dan zou de penetratietest stil komen te liggen doordat de firewall de externe IP-adressen van NFIR blokkeert. Deze blokkade moet dan steeds vrijgegeven worden door een beheerder, en deze kostbare tijd van de penetratietest gaat dan verloren. Indien de firewall geen modules heeft die blokkades uitvoeren op basis van het ontvangen netwerkverkeer, hoeft er geen actie te worden ondernomen. Het is uiteraard niet de bedoeling om extra poorten open te zetten. Dit zou wel een vertekend beeld opleveren van de technische weerbaarheid van de extern beschikbare infrastructuur.

NFIR adviseert om te controleren of de firewall aanpassingen zijn teruggedraaid.

