

# Labo Chapter 4: Pentesting



## **TEAM 1TINH2**

Aleyna Arslan  
Rasmus Leseberg  
Tomas Soors  
Stef Swinnen

# INHOUDSOPGAVE

## Inhoudsopgave

<b>1 THM .....</b>	<b>4</b>
<b>1.1 Nmap .....</b>	<b>4</b>
<b>1.2 Pentesting .....</b>	<b>6</b>
<b>1.3 Pentesting Fundamentals .....</b>	<b>7</b>
<b>2 Enumeration @PXL-VM .....</b>	<b>10</b>
2.1 Flags .....	10
<b>2.2 Nmap / Zenmap .....</b>	<b>11</b>
<b>2.3 Dirb(uster) Challenge .....</b>	<b>13</b>
<b>2.4 PXL Intranet Challenge .....</b>	<b>15</b>
<b>2.5 Modern Web App Challenge .....</b>	<b>19</b>
<b>2.6 Samba Challenge .....</b>	<b>21</b>
<b>2.7 MySQL Challenge .....</b>	<b>22</b>
<b>3 Juice shop .....</b>	<b>24</b>
<b>3.1 Juice Shop - Walk The Happy Path .....</b>	<b>24</b>
<b>3.2 Juice Shop - Trivial Challenges .....</b>	<b>25</b>
<b>3.3 Juice Shop - Easy Challenges .....</b>	<b>28</b>
<b>3.4 Juice Shop - Medium Challenges .....</b>	<b>30</b>
<b>Bijlage Opdrachten .....</b>	<b>32</b>
Opdracht 1.1 Nmap .....	32
Opdracht 1.2 CC: Pen Testing .....	34
Opdracht 1.3 Pentesting Fundamentals .....	38
Opdracht 2.3 Dirbuster Challenge .....	39
Opdracht 2.5 Modern WebApp Challenge .....	41
Opdracht 2.7 MySQL Challenge .....	43
Opdracht 3.1 Juice Shop - Walk The Happy Path .....	45
Opdracht 3.2 Juice Shop - Trivial Challenges .....	50
Opdracht 3.3 Juice Shop - Easy Challenges .....	54
Opdracht 3.4 Juice Shop - Medium Challenges .....	55
<b>Bibliografie .....</b>	<b>56</b>
<b>Extra Oefeningen - Juice Shop Extra Challenges .....</b>	<b>57</b>

# TIJDSBESTEDING

✓ = taak van teamgenoot ook voltooid

	Aleyna	Rasmus	Stef	Tomas
<b>1.1 Nmap</b>	1 uur	✓	✓	✓
<b>1.2 Pentesting</b>	✓	✓	✓	50 min
<b>1.3 Pentesting Fundamentals</b>	✓	2.5 uur	✓	✓
<b>2.2 Nmap/Zenmap</b>	✓	✓	1.5 uur	✓
<b>2.3 Dirbuster Challenge</b>	40 min	✓	✓	✓
<b>2.4 PXL Intranet Challenge</b>	✓	✓	✓	2 uur
<b>2.5 Modern Web App Challenge</b>	✓	2 uur	✓	✓
<b>2.6 Samba Challenge</b>	✓	✓	2.5 uur	✓
<b>2.7 MySQL Challenge</b>	1 uur	✓	✓	✓

<b>3.1 Walk The Happy Path</b>	✓	✓	✓	30 min
<b>3.2 Juice Shop Trivial Challenges</b>	✓	2 uur	✓	✓
<b>Juice Shop Easy Challenges</b>	✓	✓	4 uur	✓
<b>Juice Shop Medium Challenges</b>	1 uur 30 min	✓	✓	✓
<b>Layout/Afwerking</b>	2 uur	1 uur	/	/
<b>TOTAAL</b>	6 uur 10 min	7 uur 30 min	8 uur	3 uur 20 min

#### Uren die niet opgenomen zijn in het overzicht:

- Totale tijd van werkduur voor opdrachten met ✓ symbool
- Extra Challenges Juice Shop

#### Aantal gehouden meetings: 4

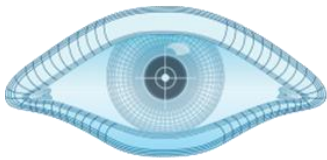
- Zondag 01.05
- Donderdag 04.05
- Zondag 08.05
- Maandag 09.05

# 1 THM

## 1.1 Nmap

Opdracht gemaakt door: [Aleyna](#)

### Task 2:



# NMAP

Nmap (Network Mapper) is een krachtige tool voor het scannen en ontdekken van netwerkkwetsbaarheden. In deze THM hebben we nmap en poorten geïntroduceerd.

De eerste stap bij het maken van deze horizontale netwerkmap is een poortscan. Wanneer een computer een netwerkservice uitvoert, opent deze een netwerkstructuur die een "poort" wordt genoemd om verbindingen te ontvangen. Er zijn poorten nodig om meerdere netwerkverzoeken te doen of om meerdere services te leveren. Als je bijvoorbeeld meerdere webpagina's tegelijk in een webbrowser laadt, moet het programma een manier hebben om te bepalen welk tabblad welke webpagina laadt. Dit wordt gedaan door een verbinding met de externe webserver tot stand te brengen via een andere poort op de lokale computer.

Er wordt een netwerkverbinding tot stand gebracht tussen twee poorten - een open poort die luistert op de server en een willekeurig gekozen poort op uw eigen computer.

Er zijn in totaal 65535 poorten beschikbaar per computer; veel hiervan zijn echter geregistreerd als standaardpoorten. HTTP-services zijn bijvoorbeeld bijna altijd te vinden op poort 80 van de server. Een HTTPS-service is te vinden op poort 443.

Met deze informatie kunnen we de volgende vragen beantwoorden:

### Answer the questions below

What networking constructs are used to direct traffic to the right application on a server?

Correct Answer

How many of these are available on any network-enabled computer?

Correct Answer

**[Research]** How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

Correct Answer

💡 Hint

### Task 3:

In de tweede task wordt uitgelegd hoe we nmap in de command prompt kunnen gebruiken, er is hier zowel een Windows als Linux versie van. Deze tool is toegankelijk door het commando nmap vervolgt met command argumenten die een programma vertellen om verschillende dingen te doen.

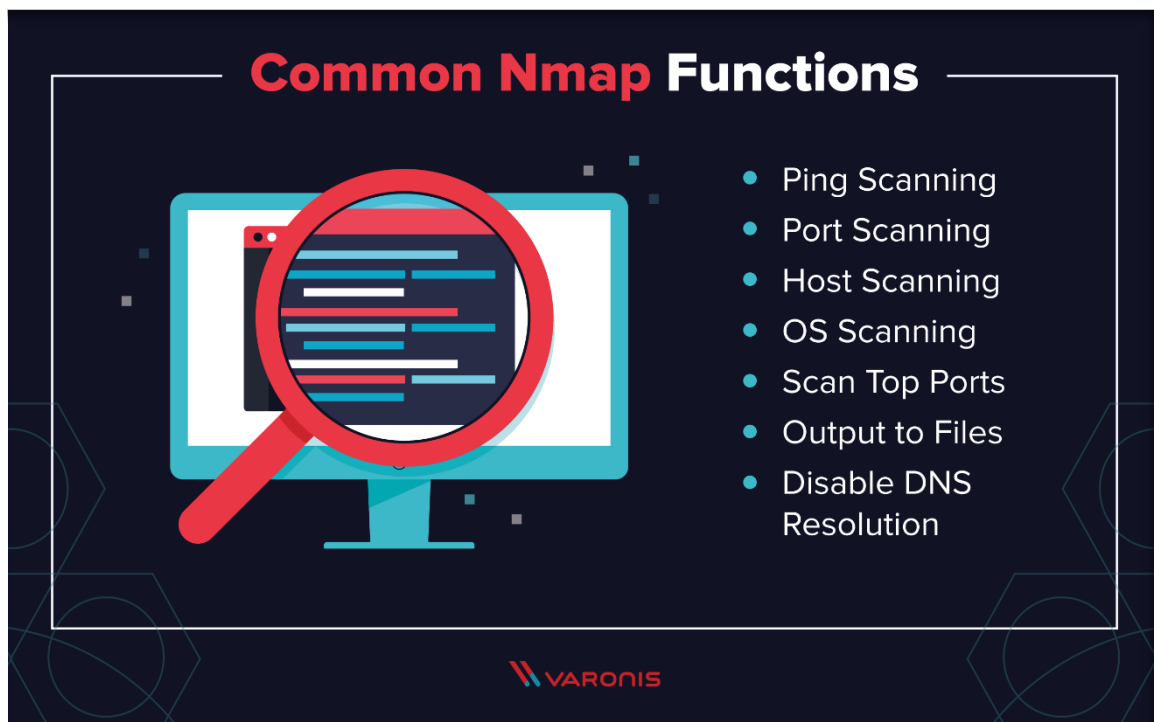
We kunnen de manpage van nmap opvragen of **nmap -help**, om te bestuderen welke prefixen er mogelijk te combineren zijn met het commando. Ook is het mogelijk om via het curl-commando een cheatsheet op te vragen dat vertelt hoe je het commando kunt gebruiken, bijvoorbeeld **curl cheat.sh/nmap**.

De help-pagina is een goede optie om de vragen van task 3 te beantwoorden (zie bijlage [foto 1](#)).

### Conclusie

Nmap is duidelijk het "Swiss Army Knife" van netwerken, dankzij de inventaris van veelzijdige opdrachten. Hiermee kan je snel essentiële informatie over je netwerk, hosts, poorten, firewalls en besturingssystemen scannen en ontdekken. Nmap heeft talloze instellingen, vlaggen en voorkeuren die systeembeheerders helpen een netwerk in detail te analyseren.

Leuk weetje: Nmap is enorm populair geworden en is terug te zien in de film 'The Matrix' en televisieprogramma 'Mr. Robot'.



## 1.2 Pentesting

Opdracht gemaakt door: [Tomas](#)

### Werking:

De eerste paar tasks gingen over Nmap. Deze waren niet al te moeilijk te vinden aan de hand van de **man page** van nmap, en de oefeningen op de server waren redelijk snel gevonden. [Foto 1 en 2.](#)

Bij netcat waren het de flags aanduiden voor verschillende toepassingen, die we ook konden vinden via de **man page** van **netcat**. [Foto 3](#)

En dan de 3<sup>de</sup> task ging over gobuster, gobuster wordt gebruikt om te achterhalen waar verschillende directories kunnen zitten op een server, en welke files waar kunnen zitten, dit is een ingebakken tool op onze attack machines. En de vragen gingen over de flags die we konden gebruiken bij deze tool. [Foto 4](#)

En dan via de attackbox konden we **gobuster** uittesten. [Foto 5](#)

Dan de volgende vragen gingen over **sqlmap**, een van de populairste sql injectie tools die der op de markt is vandaag de dag. De task vroeg naar de verschillende flags die gebruikt werden bij deze tool. [Foto 6](#)

Bij de volgende task konden we sqlmap eens uitproberen op een bepaalde server. En daar kregen we deze antwoorden uit. [Foto 7](#)

En dan ten slotte gingen we aan de slag met samba, smbmap is een beetje hetzelfde als nmap, alleen voor samba. Deze tool is heel handig voor het enumereren van samba. En bij deze task gingen we terug op zoek naar de verschillende flags voor deze tool, die behulpzaam kunnen zijn. [Foto 8](#)

En dan ten slotte gingen we kijken naar smbclient, dit kan technisch gezien hetzelfde als smbmap, alleen krijgen we hier een interactive prompt bij. En bij de laatste task gingen we terugkijken naar de verschillende flags die er bij deze tool kunnen gebruikt worden. [Foto 9](#)

### Conclusie:

Deze tools zijn allemaal heel bruikbaar en zeer user friendly om te gebruiken in onze toepassingen. En wat ons ook is opgevallen, is dat heel veel flags van verschillende tools wel overeenkomen, dus het is vrij gemakkelijk om deze tools onder de knie te krijgen zonder al te veel kennis.

## 1.3 Pentesting Fundamentals

Opdracht gemaakt door: [Rasmus](#) (foto's van de room zijn te zien in de [bijlage](#) (← click))

### Samenvatting THM Pentesting Fundamentals

**Doel:** om de verantwoordelijkheden en processen van ethical hacking te leren kennen.

### Penetration Testing Ethics

Een pen-test is een geautoriseerde audit van het securitysysteem van een computer of digitale infrastructuur. Elke soort pen-test die buiten een bepaald akkoord valt, is illegaal.

**Scope:** voor dat de pen-test plaats vindt, wordt er vastgelegd op welke specifieke vlaktes de pen-test plaats zal vinden. Bedrijven die pen-testing services aanbieden hebben een legaal framework waarbinnen zij kunnen opereren, bijvoorbeeld: de NCSC (National Cyber Security Center) heeft de CHECK accreditatie, wat betekent dat alleen goedgekeurde bedrijven geautoriseerde pen-testen mogen doen op de publieke sector en CNI systemen/netwerken.

Hackers worden in drie verschillende categorieën opgedeeld, afhankelijk van hun ethische houding:

Categorie	Omschrijving	Voorbeeld
White Hat	Blijven binnen het legale framework opereren	Iemand die een geautoriseerde pentest doet voor een toestemmend bedrijf
Grey Hat	Opereren meestal binnen het legale framework, maar vaak ook niet	Iemand die een scamming website platlegt
Black Hat	Criminelen die schade toevoegen aan andere mensen/bedrijven	Iemand die ransomware maakt om bedrijven voor losgeld af te persen

### Rules of Engagement (ROE)

Een document wat de scope vastlegt voor een pen-test tussen de pen-tester en het bedrijf. Het document bevat 3 onderdelen: permissie, scope, en de regels:

<b>Permissie</b>	Deze sectie geeft expliciet toestemming aan de pen-testers om hun taken uit te voeren. Dit onderdeel beschermt beide partijen.
<b>Test Scope</b>	Omschrijft de specifieke targets die getest moeten worden, en verduidelijkt voor de pen-tester wat hun taak is
<b>Regels</b>	Specificeert de bepaalde technieken die toegestaan zullen zijn tijdens de test, voorbeeld: Geen Phishing, maar MITM is wel toegestaan.



## Penetration Testing Methodologieën

De werkwijze van een pen-tester hun methodologie, waar de werkwijze afgeleid wordt van de targets.

Stap	Omschrijving
Information Gathering	Zo veel mogelijk toegankelijke informatie verzamelen over de target, door OSINT (Open Source Intelligence) & Research.
Enumeration/Scanning	Het ontdekken van applicaties/servers die op dat systeem runnen. Vulnerabilities zoeken!
Exploitation	De gevonden vulnerabilities testen en exploiten.
Privilege Escalation	Hier kunnen pogingen plaatsvinden om toegang tot een systeem uit te breiden. Privilege Escalation kan verticaal en horizontaal plaatsvinden.
Post-exploitation	Reporting, covering your tracks, is andere informatie ook vulnerable?

**OSSTMM** = Open-Source Security Testing Methodology Manual

**OWASP** = Open Web Application Security Project

**NIST Cybersecurity Framework 1.1** = National Institute of Standard and Technology

	Voordelen	Nadelen
OSSTMM	Framework is flexibel	Framework is moeilijk te begrijpen en bevat moeilijke definities
	Test strategieën zijn geïncorporeerd	/
OWASP	Makkelijk te begrijpen	Bevat geen accreditatie zoals CHECK
	Gespecialiseerd op webapplicaties	Geen suggesties voor software development cycles
NIST	Gebruikt door 50% van US-bedrijven	Meerdere iteraties van dezelfde frameworks
	Heeft accreditatie	Cloud computing niet inbegrepen
NCSC CAF	Wordt ondersteunt door cybersecuritybeleid van de overheid	De overheid heeft een vinger in het spel
	Heeft accreditatie	Nieuwe framework

## Black-Box/Grey-Box/White-Box Testing

**Black-Box Testing** = De tester heeft geen informatie over de werking van de applicatie en ageert als een reguliere user

**Grey-Box Testing** = De meest voorkomende vorm van testing, waar de tester beperkte informatie heeft van de interne werking.

**White-Box Testing** = low-level process wat een developer doet om de interne componenten van een applicatie te testen. Bijvoorbeeld of de functies juist werken.



## Conclusie

In deze room leert de gebruiker de basis over pen-test ethiek, methodologie, en basisprincipes van informatie toegankelijkheid bij pen-testen. Er bestaan 3 categorieën aan 'hackers', namelijk Black-Hat, Grey-Hat, en White-Hat hackers, die allemaal verschillende opvattingen van hun ethische en morele houding uitoefenen op de markt. Er bestaan meerdere frameworks die hun eigen methodologie omschrijven, waaronder OWASP en OSSTMM de meest bekende zijn. Ook al zijn er meerdere manuals met unieke frameworks, baseren de meeste methodologieën zich op dezelfde basis-stappen van pen-testen, namelijk:

Information-Gathering, Enumeration, Exploitation, Privilege Escalation en Post-exploitation

Wanneer een bepaalde pen-tester, of een bedrijf, ingehuurd wordt om security analyse te voorzien wordt er vooraf altijd een ROE ondertekend, die de bepaalde scope en methodologie vastlegt. Dit is echter van belang omdat alles wat buiten de scope valt, tegen de ROE zou zijn.

Bij het pen-testen zelf is het altijd verschillend hoe veel informatie verstrekt wordt over de scope, dus afhankelijk daarvan heeft de pen-tester 'full-knowledge', 'partial-knowledge', of 'no-knowledge' (Black/Grey/White-Box).

## 2 Enumeration @PXL-VM

### 2.1 Flags

**Valideer de gevonden flags via** <https://pxl-security-flag-validate.herokuapp.com/>

Noteer de gevonden flags en welke student(en) de flags hebben gevonden.

FLAGS VOOR TEAM: 1TINH2	Opdracht	Val (Y/N)	Student*			
			1	2	3	4
PXL{67f80f475e9491f9a5fe2da659dfffd63}	2.3	Y	X	X	X	X
PXL{b5448d6e1904b02b53ad600669ec7d04}	2.3	Y	X	X	X	X
PXL{eda0f433b3f226295d1459797ac75726}	2.4	Y	X	X	X	X
PXL{62038d9f4f69225c51d5c0b6778cfc9e}	2.4	Y	X	X	X	X
PXL{d3210c8e31c3fcf60b5860c26b1211df}	2.4	Y	X	X	X	X
PXL{025d7a4455dfb179a4155aa4dbec2977}	2.5	Y	X	X	X	X
PXL{4b34fdde81deafa1b91bd509f9bb46e7}	2.6	Y	X	X	X	X
PXL{f753062bdc05e1c97d10c4087e41c382}	2.6	Y	X	X	X	X
PXL{66e3276117041ab5ac2bdbd44e62be7f}	2.7	Y	X	X	X	X

\*Student 1 = Aleyna

\*Student 2 = Tomas

\*Student 3 = Stef

\*Student 4 = Rasmus

## 2.2 Nmap / Zenmap

Opdracht gemaakt door: Stef

### Vragen:

1. Scan de 100 meest gebruikte poorten. Zijn er services die teruggegeven worden door je nmap scan? Welk commando (en optie(s)) heb je hiervoor gebruikt?

Om de 100 meest gebruikte poorten te zien moest ik eerst root privileges hebben, dit ging via het commando **sudo su**. Hierna kon ik het commando **nmap -top-ports 100 192.168.191.135** ingeven om de poorten te zien.

```
(root@kali)-[/home/kali]
# nmap --top-ports 100 192.168.191.135
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-02 21:07 CEST
Nmap scan report for 192.168.191.135
Host is up (0.00018s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:04:F3:02 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

2. Scan de poorten 0-10000. Welke poorten staan open? Welk commando (en optie(s)) heb je hiervoor gebruikt?

```
(root@kali)-[/home/kali]
# nmap -p 0-10000 192.168.191.135
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-28 15:53 CEST
Nmap scan report for 192.168.191.135
Host is up (0.0044s latency).
Not shown: 9992 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
4208/tcp  open  vrml-multi-use
4894/tcp  open  lyskom
5355/tcp  open  llmnr
5413/tcp  open  wwiotalk
9008/tcp  open  ogs-server
9557/tcp  open  unknown
MAC Address: 00:0C:29:04:F3:02 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.28 seconds
```

Met het volgend commando kunnen we zien welke poorten open staan: **nmap -p 0-10000 192.168.191.135**. De openstaande poorten zijn te zien in de volgende foto.

3. Doe een service version detection scan van bovenstaande poorten. Welke services draaien er op deze poorten en wat is het doel van die services? We willen een beschrijving per poort!

**nmap -sV 0-10000 192.168.191.135**

De flags, **-sV** en **-p 0-10000**, die ik heb meegegeven zorgen ervoor dat de versie wordt meegegeven van de poort en dat poorten tussen 0 en 10000 worden gescand, 0 - 65526. Met het uitgevoerde commando krijg ik het volgende:

```
(kali㉿kali)-[~]
$ nmap -sV -p 0-10000 192.168.191.135
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-02 21:17 CEST
Nmap scan report for 192.168.191.135
Host is up (0.0067s latency).
Not shown: 9992 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
80/tcp    open  http             nginx 1.21.6
139/tcp   open  netbios-ssn      Samba smbd 4.6.2
445/tcp   open  netbios-ssn      Samba smbd 4.6.2
4208/tcp  open  vrml-multi-use?
4894/tcp  open  http             nginx 1.21.6
5355/tcp  open  llmnr?
5413/tcp  open  http             Node.js Express framework
9008/tcp  open  mysql            MySQL 8.0.28
9557/tcp  open  http             Apache httpd 2.4.52 ((Debian))
```

4. Wat is de versie van de nginx service en op welke poort draait deze?

De versie van nginx is 1.21.6 en draait op poorten 80 en 4894.

5. Geef een conclusie over Nmap. Bestaan er alternatieven voor Nmap? Waar zou je het kunnen toepassen?

Nmap is een praktische open source-tool die wordt gebruikt om poorten, services en nog andere informatie in een machine op te volgen. Het heeft een groot aantal aan functies die je kan gebruiken waarbij je verschillende parameters kan meegeven om je functies aan te passen aan het doel dat je moet bereiken. Nmap is dus een handige tool voor het opvolgen van informatie op je machine. Een alternatief zou Masscan zijn. Dit is een TCP-portscanner die SYN-pakketten asynchroon uitzendt en de resultaten weergeeft die lijken op Nmap.

## 2.3 Dirb(uster) Challenge

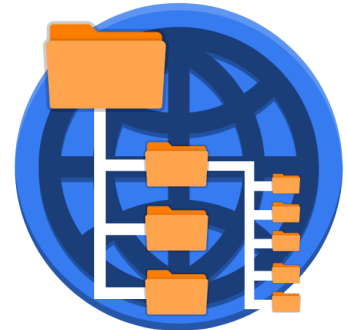
Opdracht gemaakt door: [Aleyna](#)

### Werkwijze:

Om te beginnen voeren we een nmap scan uit op het volgend IP-adres. De **-sV** zorgt ervoor dat alle services en op welke versie deze services draaien getoond worden. De **-p-** prefix scant alle poorten.

```
nmap -sV -p- 192.168.58.138
```

Hierin staat alle informatie die we nodig hebben om de vragen te beantwoorden. We zien dat de nginx server die we nodig hebben op poort **6621** draait. (Zie bijlage [foto 1](#))



Vervolgens surfte ik naar **http://192.168.58.138:6621**.

Op deze webpagina stond tekst met *"There are no flags here. Maybe you must bust something."*

Nu we weten welke poort we nodig hebben, kunnen we een brute force attack op de hidden directories en files van deze webserver uitvoeren.

Dit is mogelijk met het commando **dirb** [http://192.168.58.138:6621](http://192.168.58.138:6621/usr/share/wordlists/dirb/common.txt) **/usr/share/wordlists/dirb/common.txt**.

De brute force attack heeft succesvol plaatsgevonden. Als respons kregen we 2 hidden directories. (Zie bijlage [foto 2](#)). Op **index.html** kregen we dezelfde tekst als op poort 6621. Maar in de robots.txt file vind je een hidden directory genaamd **admin.html** en een flag terug. Op de **admin.html** pagina vind je de tweede flag.

### Vragen:

#### 1. Welke extensie heeft de index pagina op de webserver?

De index pagina van de webserver heeft een **.html** extensie.

#### 2. Hoe kan je met dirb zoeken op specifieke extensies?

```
dirb <url_base> [<wordlist_file(s)>] -X [<extension(s)>]
```

#### 3. Welke (verborgen) bestanden heb je gevonden?

- robots.txt
- index.html
- admin.html

**4.** Welke flags heb je teruggevonden in welke files?

- robots.txt → PXL{b5448d6e1904b02b53ad600669ec7d04}
- admin.html → PXL{67f80f475e9491f9a5fe2da659dff63}

**5.** Valideer de twee flags met de validator tool die terug te vinden is in de inleiding van deze opdracht! Gebruik steeds dezelfde teamnaam.

De twee flags die we gevonden hebben werden goedgekeurd in de validator tool. (Zie bijlage [foto 3 en 4](#)).

### Conclusie

Deze opgave is een goede inleiding om een basis op te bouwen voor het scannen van webcontent. Dirb zoekt naar bestaande of verborgen directories/files. Het werkt door een wordlist gebaseerde aanval op een webserver te lanceren en de reacties te analyseren. We leren tijdens de opgave niet alleen het gebruiken van dirb commando's maar ook nmap, gezien we een nmap scan moeten uitvoeren vooraleer er een brute force attack kan plaatsvinden.

## 2.4 PXL Intranet Challenge

Opdracht gemaakt door: [Tomas](#)

### 1. Waarvoor wordt Apache gebruikt?

Apache is een opensourcewebsserver die kan gebruikt worden voor verschillende operating systemen. 60% van alle webserveren zouden kunnen draaien met Apache. Het is zeer betrouwbaar, zeer snel en ook nog eens veilig om te gebruiken.

### 2. Op deze service draait een applicatie. Wat is de programmeeromgeving die gebruikt is om deze applicatie te maken?

Deze applicatie zou gemaakt zijn met JavaScript en HTML.

### 3. Bij het enumereren van de applicatie zie je dat je op een login pagina uitkomt. Verken deze. Wat zijn de foutboodschappen die je krijgt als je probeert in te loggen?

Als we een beetje kijken naar deze pagina, kunnen we zien dat het een inlogpagina is van intranet. Hier gingen we dan kijken welke foutmeldingen deze pagina zou geven moesten we een willekeurig wachtwoord en username ingeven. De foutmelding bij een foute username was "wrong username" en de foutmelding bij de juiste username, maar het foute wachtwoord, was "invalid password".

Invalid password

Wrong username

Dit wil ons dus zeggen, dat "admin" een gebruiker is waarbij we kunnen brute forcen om op zijn pagina te geraken, aangezien deze de foutmelding "Invalid Password" teruggaf.

### 4. Zoek een tool waarmee je een login formulier van een webapplicatie kan bruteforcen. Welke tool(s) heb je gevonden?

We hebben allemaal gebruik gemaakt van verschillende tools met verschillende voor- en nadelen. Zo heeft iemand gebruik gemaakt van de "burpsuite community edition" GUI om deze pagina te brute forcen. Deze was bijvoorbeeld zeer gemakkelijk in gebruik, maar was dan weer veel trager dan de andere tools die we gebruikt hebben.



Daarnaast heeft iemand anders gebruik gemaakt van Hydra, de geparalleliseerde login cracker die ingebakken zit op de Kali machine.

Deze tool is dan bijvoorbeeld veel sneller. Maar is dan weer moeilijker met de verschillende flags en argumenten die moeten gebruikt worden.

En dan ten slotte hebben we ook gebruik gemaakt van Postman.



5. Gebruik een tool om het wachtwoord van deze user te achterhalen. Beschrijf je werkwijze & uitgevoerd commando + opbouw commando.

Dus, omdat wij nu onze tools ter beschikking hebben, en onze username ook al gevonden hebben, kunnen we te werk gaan met onze tools. Na overleg leek ons de Hydra tool het gemakkelijkste en eenduidigste manier om dit op te lossen, maar hoe gaat dit in zijn werk?



Het commando dat ik gebruikt heb op mijn machine was deze:

```
sudo hydra -l admin -P /home/kali/Desktop/common_pass -s 2917 192.168.140.128 http-post-form "/index.php:username=admin&password=^PASS^:Invalid Password"
```

Maar wat houdt dit allemaal in? Eerst hebben we de **-l** flag, deze duidt aan welke username of wordlist je wilt gebruiken voor je username, en **-p** doet hetzelfde, alleen voor het wachtwoord. Voor ons password hebben we een lijst van de 1000 meest gebruikte wachtwoorden gebruikt van GitHub. De **-s** flag geeft de poort aan waar deze cracker op moet werken.

Hierna komt overduidelijk het IP-adres waar we op moeten zoeken, dit heeft geen flag nodig. Daarna gaan we kijken hoe deze login pagina werkt, en welke methode we moeten gebruiken. Aangezien de **http-post** komt van het feit dat deze pagina werkt op http, en deze werkt met **POST** in plaats van **GET**.

Status	Method	Domain	File
200	POST	192.168.188.129:2012	index.php
200	GET	192.168.188.129:2012	bootstrap.min.js
404	GET	192.168.188.129:2012	favicon.ico

Alles wat er tussen de haakjes staat wordt gezien als 1 groot argument, met het eerste argument voor de dubbele puntjes, de locatie is van deze pagina in de directory van de server.

Met erna de locatie van de username en paswoord forms in de login pagina, deze kunnen we vinden via onze inspect element. Maar, aangezien we de username al weten gaan we deze laten staan, en bij password gaan we het argument **^PASS^** zetten zodat hij weet dat hij hier alle opties van de wordlist die we hierboven hebben meegegeven, moet proberen

Request Body

```
username=mooi&password=din&login=
```

En hierna gaan we meegeven wanneer hij de login info gevonden heeft, maar omdat we niet weten hoe deze pagina er uit ziet als hij succesvol is binnengedrongen, gaan we meegeven wanneer hij gefaald is, dus we geven mee "invalid password"

Als we dit commando uitvoeren in onze terminal, krijgen we dit als resultaat:

```
(kali@kali)-[~]
└─$ sudo hydra -l admin -P /home/kali/Desktop/common_pass -s 2012 192.168.188.129 http-post-form "/index.php:username=admin&password='PASS':Invalid Password"

Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-05 03:46:05
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (l:1/p:1000), ~63 tries per task
[DATA] attacking http-post-form://192.168.188.129:2012/index.php:username=admin&password='PASS':Invalid
Password
[2012][http-post-form] host: 192.168.188.129 login: admin password: pokemon
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-05 03:46:10
```

Zoals je kunt zien, heeft hij een paswoord gevonden voor onze username. Hoera!

**Username: admin**  
**Password: pokemon**

Hiermee kunnen we inloggen op onze inlog pagina, en dan krijgen we deze pagina te zien:

## Welcome admin

PXL{eda0f433b3f226295d1459797ac75726}

- real name: John Doe
- address: Elfde-liniestraat 124 Hasselt
- email: admin@pxl.be

Hier staat dan ook onze eerste flag die we konden vinden, maar we moesten nog een 2<sup>de</sup> flag vinden op deze pagina, en dit is waar onze parameter tampering in het verhaal komt.

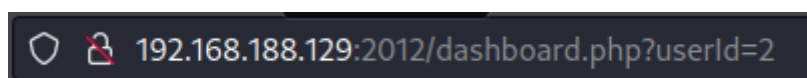
### 6. Onder welk topic uit de OWASP-top 10 kan je deze aanval plaatsen? Motiveer!

Deze aanval zouden we bij de OWASP-top 10 kunnen plaatsen onder "Security logging and monitoring failures". Deze hoort hieronder, aangezien hier eigenlijk niks wordt gelogd van de inlogpogingen die we doen, we kunnen zoveel proberen in te loggen als we willen en hier wordt niks tegen gedaan. De eigenaars krijgen geen meldingen bij deze attacks en kan dus volledig worden misbruikt.

### 7. Zoek uit wat het concept "parameter tampering" wil zeggen en beschrijf dit kort in eigen woorden.

Parameter tampering, wat is dit nu eigenlijk? Hier wordt er gebruik gemaakt van de manipulatie van de parameters die worden uitgewisseld tussen de client en de server. Deze kunnen gedaan worden in de URL of via de cookies van een pagina. En op onze website is dit vrij duidelijk zichtbaar.

### 8. Pas parameter tampering toe op de lab omgeving en beschrijf je werkwijze.



Als we eens gaan kijken naar de URL van de pagina na dat we hebben ingelogd, zien we deze URL.

In het laatste gedeelte van de URL staat "userId=2" dat wilt ons dus zeggen dat er al zeker een 1<sup>ste</sup> user is, waar we niks van af weten. Dus hier gaan we proberen of de parameter tampering kan werken door "userId=2" te veranderen naar "userId=1". En met een beetje geluk, brengt dit ons naar de 1<sup>ste</sup> gebruikerspagina.

Waar we dit te zien krijgen:

# Welcome ventieldopje24

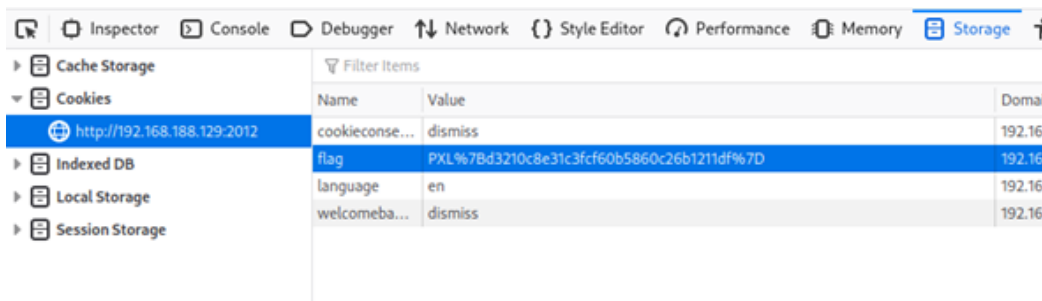
PXL{eda0f433b3f226295d1459797ac75726}

- real name: Dries Swinnen
- address: PXL{62038d9f4f69225c51d5c0b6778cfc9e}
- email: ventieldopje24@h4x0rr.net

En hier zien we dan onze 2<sup>de</sup> flag staan bij het adres van de gebruiker, weer een flag!

## 9. Ga op zoek naar de laatste flag in deze lab.

De laatste flag van deze opdracht konden we gaan zoeken aan de hand van de tip die ons gegeven werd. En na een beetje opzoek werk konden we achterhalen dat we deze in de cookies moesten gaan zoeken, de cookies kan je vinden via Inspect element > storage > cookies en daar staat de flag groot en duidelijk.



### Conclusie:

Het cracken van deze website was redelijk rechtuit en duidelijk. Na het vinden van de username moesten we het wachtwoord cracken, en dit ging nog

gemakkelijker dan gedacht, wat ons wel een beetje schrik aanjaagt voor de vulnerability van verschillende websites die wij dagelijks gebruiken. En hoe gemakkelijk het zou zijn om deze eigenlijk te cracken.

## 2.5 Modern Web App Challenge

Opdracht gemaakt door: [Rasmus](#)

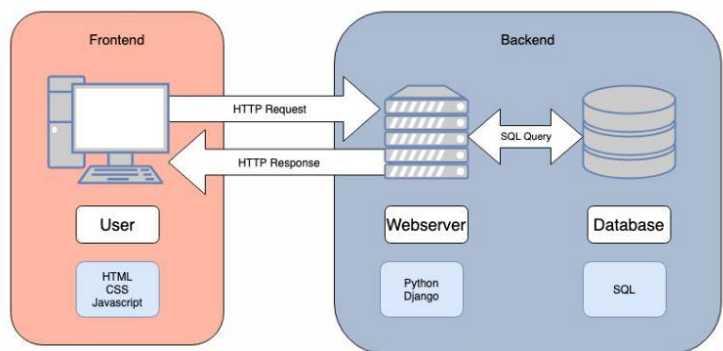
### 1. Wat zijn NodeJS en ExpressJS? Waarvoor worden ze gebruikt?

Node.js is een open source en platformonafhankelijke runtime-omgeving voor het uitvoeren van JavaScript-code buiten een browser. Het belangrijkste is dat NodeJS geen framework en ook geen programmeertaal is, maar een tool om back-end services zoals API's te bouwen.

Express.js: Express is een kleiner framework dat boven op de webserverfunctionaliteit van Node.js zit om de API's te vereenvoudigen en handige nieuwe functies toe te voegen. Het maakt het eenvoudiger om de functionaliteit van de applicatie te organiseren met middleware en routing. (*GeeksforGeeks*)

### 2. Hoe werkt de opsplitsing tussen front en backend bij een applicatie?

Het front-end is de technologie waarmee de gebruiker interactie heeft wanneer hij op de computer op het internet zit te surfen, en de back-end is de server die deze requests accepteert en de informatie terugstuurt die de gebruiker ziet. Het figuur op de rechterkant is een basisvoorbeeld, waar bij de eindgebruiker door middel van een webpagina die voorzien is van html, css, en javascript interacties uitvoert, waaruit requests gestuurd worden naar de back-end, die in dit geval uit een web-server en een database bestaat. De infrastructuur en opmaak van de back-end kan per context verschillen.



### 4. Welke andere user is aanwezig in de applicatie?

- 4.1 Door **nmap -p- -sV 192.168.221.137** blijkt poort 5501 de service node.js en Express framework te gebruiken. Poortnummers zullen per gebruiker variëren (zie [foto 1](#)).
- 4.2 Login op 192.168.221.137:5501 met de credentials. Behalve om weer uit te loggen is er een functie om het wachtwoord te veranderen. Als op die functie geklikt wordt, verandert de URL ook (zie [foto 2](#)). De andere gebruiker die aanwezig is, is 'admin', (zie [foto 1](#)).

### 5. Zoek een manier om in te loggen als deze gebruiker.

- 5.1 Ik heb hiervoor Burp Suite Community Edition gebruikt, een tool wat voor pen-testen van web-apps gebruikt wordt. Bij het opstarten van een temporary project navigeer je naar tabblad 'Proxy', dan sub-tabblad 'Intercept'.

- 5.2 Open de Burp browser en navigeer naar de login pagina bij 192.168.221.137:5501
- 5.3 Login als 'john' en verander het wachtwoord van deze persoon
- 5.4 Binnen de Burp Suite is het mogelijk om de http history te zien onder het tabblad 'HTTP History'. Bekijk hier de POST request naar /api/changepassword van john (zie [foto3](#)). Ook te zien is nog een cookie (flag) uit de oefening 2.4.
- 5.5 Stuur deze request naar de Repeater functie binnen Burp. Dit doe je door middel van RM → 'Send to Repeater'. De repeater functie binnen Burp is een tool wat een bepaald geselecteerd request gewijzigd kan doorsturen naar dezelfde back-end locatie. (Zie [foto 4](#)).
- 5.6 Navigeer naar het 'Repeater' tabblad, en wijzig de username en passwordsectie binnen het request naar 'admin', 'admin'. Hier wordt de request gewijzigd voordat de repeater een nieuwe request verstuurd. Op deze manier kan het wachtwoord van admin gewijzigd worden zonder in te loggen. (Zie [foto 5](#))
- 5.7 Door 'Send' te drukken wordt het wachtwoord voor admin gewijzigd en is het mogelijk om in te loggen. De Response van de Repeater was 200 (OK), en die response bevestigt de gelukte poging vanuit de backend.
- 5.8 De flag was duidelijk te zien op de admin login page (zie [foto 6](#)) en werd gevalideerd door de validator tool.

## 6. Onder welk topic uit OWASP-top 10 wordt deze aanval geplaatst?

**Broken Access Control** (BAC, OWASP No. 5) is waar aanvallers toegang kunnen krijgen en bepaalde dingen kunnen wijzigen of verwijderen, zonder dat ze daartoe machtiging zouden moeten hebben.

**Security Misconfiguration** (OWASP No. 6) is waar algemene securityinstellingen fout zijn geconfigureerd, wat zou kunnen leiden tot privilege escalation of dergelijke.

Deze opdracht zou binnen het kader van de twee bovengenoemde OWASP vulnerabilities geplaatst kunnen worden. De WebApp heeft een BAC vulnerability omdat de backend toelaat om gewijzigde POST requests door te sturen. Verder is de security configuratie van de WebApp ook heel slecht, omdat de wachtwoorden in plaintext op de server worden opgeslagen, en omdat er geen maatregel tegen privilege escalation bestaat om een normale gebruiker zoals 'john' tegen te houden om het wachtwoord van de admin te wijzigen.

**Conclusie:** Deze opdracht bevat een basale introductie tot Broken Access Control, en laat de gebruiker door middel van een gewijzigde POST-request het wachtwoord van de admin wijzigen, zonder een brute-force attack. Ook zou deze korte handleiding een goede introductie tot Burp Suite kunnen geven, een bekend en veelgebruikt pen-test tool.

## 2.6 Samba Challenge

Opdracht gemaakt door: [Stef](#)



### 1. Wat is SAMBA? Waarvoor wordt dit gebruikt?

Samba is een implementatie van het SMB/CIFS-protocol voor Unix-systemen. Het biedt ondersteuning voor cross-platform delen van bestanden, en printers voor verschillende machines. Samba kan ook functioneren als een NT4-stijl domeincontroller, en kan integreren met zowel NT4-domeinen als Active Directory domeinen als een member server.

### 2. Enumereer deze service aan de hand van de tool "SMBclient". Welke shares zijn er terug te vinden op deze service?

Na het ingeven van het commando **smbclient -L 192.168.191.135** zijn er 2 shares gevonden: **PublicShare** en **IPC\$**. De flag **-L** zorgt ervoor dat je ziet welke diensten er beschikbaar zijn op een server.

### 3. Welke bestanden heb je teruggevonden op de share? Verken deze files! Beschrijf je werkwijze.

Om de PublicShare te openen voerde ik het commando **smbclient //192.168.191.135/PublicShare** in. Hierna zou ik een wachtwoord moeten ingeven maar door gewoon op enter te drukken kunnen we dit omzeilen. Nu zien we 2 bestanden, **flag** en **secretstuff.zip**. Nu kunnen we in de prompt de commando's **get flag** en **get secretstuff.zip** ingeven. Na het commando **cat flag** zien we de eerste flag verschijnen.

**Flag: PXL{4b34fdde81deafa1b91bd509f9bb46e7}**

### 4. Hoe heb je de password protected file gekraakt?

Voor de file secretstuff.zip kunnen we openen na een paar stappen. Het eerste dat ik deed was de file kopiëren naar de file hash.txt: **zip2john secretstuff.zip > hash.txt**. Het commando **john hash.txt** zorgt ervoor dat we het password en de credentials kunnen zien. Dan unzippen we de file secretstuff.zip via **unzip secretstuff.zip**. Hierin zit een directory **share/creds.txt**. Door in die directory share te gaan en het commando **cat creds.txt** in te geven kunnen we de credentials terugvinden.

### 5. Welke credentials heb je hierin teruggevonden?

- **root**
- **secret007**

**Flag: PXL{f753062bdc05e1c97d10c4087e41c382}**

## 2.7 MySQL Challenge

Opdracht gemaakt door: [Aleyna](#)

### Vragen:

#### 1. Wat is MySQL? Waarvoor wordt dit gebruikt?

MySQL is een databasebeheersysteem, een database is een gestructureerde verzameling van gegevens die zo is georganiseerd dat ze gemakkelijk te gebruiken en op te halen zijn. MySQL is een van de systemen die deze voor u kan beheren en opslaan.

#### 2. Zoek een manier om te verbinden met de database. Hoe ben je te werk gegaan? Welke tool heb je gebruikt? Welke credentials heb je gebruikt?

Door een nmap scan te doen, krijg je een overzicht op welke poort de MySQL server draait. Dit heb ik gedaan met het commando: **nmap -sV -p- 192.168.205.131**. Hieruit bleek de MySQL server op poort 1874 te draaien.

Om verbinding te maken met de database heb ik gebruik gemaakt van het commando **mysql --host 192.168.205.131 --port 1874 --user root --password** daarna werd er geprompt voor een wachtwoord, hier heb ik het wachtwoord **secret007** ingetoetst.

De inlog credentials heb ik achterhaald door toegang te krijgen tot de containers van de docker. Dit heb ik gedaan met een tool genaamd Portainer. Door het commando **docker volume create portainer\_data** te runnen, heb ik een volume gecreëerd die de Portainer Server zal gebruiken om zijn database op te slaan. Vervolgens heb ik het commando **docker run -d -p 8000:8000 -p 9443:9443 --name portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v portainer\_data:/data portainer/portainer-ce:latest** uitgevoerd om de Portainer Server container te installeren.

Wanneer je naar de website **https://192.168.205.131:9443** surft, kom je in de Portainer-omgeving. Daarna navigeer je naar Containers en zie je alle containers die dit labo omvat (zie [foto 1](#)). In geval van deze opdracht, navigeerde ik verder naar de container **sec-mysql-challenge-1**. In het environment van deze container stonden de gegevens om in de MySQL-database te geraken (zie bijlage [foto 2](#)).

Ook staat de flag van deze challenge in de container, uiteraard is die ook te achterhalen in de docker door het commando **docker exec sec-mysql-challenge-1 env | grep FLAG** in te geven.

```
[root@sec-lab ~]# docker exec sec-mysql-challenge-1 env | grep FLAG
FLAG1=PxL{66e3276117041ab5ac2bdbd44e62be7f}
```

```
MySQL [(none)]> show databases
→ ;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| pxl |
| sys |
+-----+
5 rows in set (0.108 sec)
```

Om het toch uitdagend te maken, ga ik in de database zoeken naar de flag. Door **show databases;** in te geven, krijg ik een lijst van alle databases. Het leek me verstandig om eerst in de pxl database te kijken, het commando **use pxl** gaf mij toegang tot de database. Vervolgens heb ik het commando **show tables;** uitgevoerd om te zien welke tabellen er in deze database zitten. Ik heb een **SELECT \*** toegepast op alle tabellen tot dat ik bij tabel users bij gebruiker Erik de flag **PxL{66e3276117041ab5ac2bdbd44e62be7f}** terugvond.



### 3. Welke databases zijn er aanwezig? Welke tabellen zijn er terug te vinden in welke database?

De databases die aanwezig zijn: **information\_schema**, **mysql**, **pxl**, **sys**, **performance\_schema**.

Door **use <databasename>** te runnen, krijg je toegang tot de database, en vervolgens **show tables;** geeft toegang tot welke tabellen er zich in die database bevinden.

- information\_schema → 79 tabellen
- mysql → 37 tabellen
- pxl → 3 tabellen: metadata, posts, users
- sys → 101 tabellen
- performance\_schema → 110 tabellen

### 4. Welke users zijn aanwezig op de mysql database?

```
SELECT User  
FROM mysql.user;
```

Er zijn 2 gebruikers op de mysql database, genaamd **root** en **joske**.

### 5. Welk hashing algoritme is er gebruikt voor de wachtwoorden van de gebruikers? Kraak deze wachtwoorden!

Het algoritme dat is toegepast op de wachtwoorden van de gebruikers in de pxl database is MD5. Dit algoritme is snel te herkennen, maar bij twijfel is het mogelijk te dubbelchecken met Hash Analyzer. Ik heb de wachtwoorden kunnen kraken door een online decryption tool te gebruiken.

**admin:** thisissecret

**Lode:** p4ssw0rd123

**Dries:** hunter4

**Erik:** secretpassword4

### 6. Valideer de flag met de validator tool die terug te vinden is in de inleiding van deze opdracht!

De gevonden flag **PXL{66e3276117041ab5ac2bdbd44e62be7f}** werd gevalideerd door de validator tool (zie bijlage [foto 7](#)).



# 3 Juice shop

## 3.1 Juice Shop - Walk The Happy Path

Opdracht gemaakt door: [Tomas](#)

### Werkwijze:



1. Eerst gingen we gewoon op zoek naar een simpel product in de zoekbalk. [Foto 1](#)
2. Dan gingen we hier een review op schrijven. [Foto 2](#)
3. Hierna gingen we een paar dingen toevoegen aan ons winkelmandje. [Foto 3](#)
4. En uiteindelijk ons winkelmandje aanpassen. [Foto 4](#)
5. Hierna gaan we naar de checkout. [Foto 5](#), [Foto 6](#), [Foto 7](#)
6. Het vinden van de pagina om onze username te veranderen was niet echt moeilijk, gewoon op je account klikken en je bent er. [Foto 8](#)
7. De volgende vraag was om een recycling box te kopen, deze vonden we niet direct onder de aangeboden producten dus hebben we het product dat het beste overeenstemt besteld, de "fruit press". [Foto 9](#)
8. Onze eerder gemaakte bestelling was volgens de tracking al onderweg en verwacht bezorgd te worden binnen dit en 1 dag. [Foto 10](#)
9. Het wachtwoord veranderen was ook redelijk straight forward. [Foto 11](#)
10. De customer feedback geven is ook redelijk gemakkelijk. [Foto 12](#)
11. En de 'About U's pagina staat veel info over de webshop, inclusief de customer feedback. [Foto 13](#)

## 3.2 Juice Shop - Trivial Challenges

Opdracht gemaakt door: [Rasmus](#)

### 2.1 ACCESS A CONFIDENTIAL DOCUMENT

#### Methodologie

1. Enumeratie met **dirb 192.168.221.137:9534** om hidden directories te vinden. Uitslag te zien in [foto 1](#).
2. Naar **192.168.221.137:9534/ftp** surfen om hidden files te vinden, zie [foto 2](#).
3. **acquisitions.md** openen om een confidential document te lezen, zie [foto 3](#).

#### Link naar OWASP

Sensitive Data Exposure: Door een dirbuster enumeratie te doen was het mogelijk om hidden directories te vinden en ook te accessen. Het is Sensitive Data Exposure omdat de directories en files niet beveiligd zijn met privileges of andere security measures.

#### Bescherming?

Bepaalde directories zouden password protected kunnen zijn, of access privileges alleen aan de admin geven.

### 2.2 ERROR HANDLING

#### Methodologie

Op de login pagina van de Juice Shop een singel quote ' ingeven, met een random password. Dit zou een standard query zijn om te kijken of de login pagina voor SQL-injection vulnerable zou zijn. De error message is 'neither graceful nor consistent', zie [foto 4](#).

#### Link naar OWASP

Security Misconfiguration: Een applicatie is vulnerable to attack wanneer de data niet gevalideerd of gefiltered wordt door de back end. Omdat dit een server error heeft geprovoceerd, is het duidelijk dat de WebApp vulnerable is voor dit soort attacks.

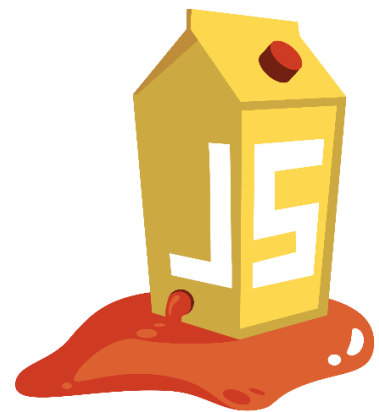
#### Bescherming?

De back-end op een manier programmeren zodat special characters in het inlog-scherm worden opgevat, en een logische fout-melding tonen.

### 2.3 SCORE BOARD

#### Methodologie

Vanuit het menu linksboven is het mogelijk om naar de score-board pagina te browsen, zie [foto 5](#).



Ook door middel van gokken was het mogelijk de URL op te sporen onder `/#/score-board`.

[Link naar OWASP:](#)

Dit is geen vulnerability, de score-board is bedoeld om toegankelijk te zijn, dus dit zou onder Miscellaneous geplaatst kunnen worden.

[Bescherming?](#)

Niet van toepassing

## 2.4 DOM XSS

[Methodologie](#)

In de zoekbalk is het mogelijk om een XSS-attack te plegen. Door het meegegeven script in de zoekbalk in te geven, wordt een alert getoond, zie [foto 6](#).

[Link naar OWASP](#)

XSS is waar door een script-injectie (bijvoorbeeld) bepaalde informatie tevoorschijn zou kunnen halen vanuit de web-page. Op deze manier kunnen cookies, session tokens of andere informatie met behulp van een script uit de web-page gehaald worden.

[Bescherming?](#)

OWASP heeft een [cheat sheet](#) om XSS-injecties te voorkomen. Zoals zij zelf schrijven op de web-page, is er geen enkele techniek die XSS compleet kan overwinnen. Wel zou een combinatie van Framework Security technieken effectief zijn om XSS tegen te gaan.

## 2.5 ZERO STARS

[Methodologie](#)

Het is mogelijk om feedback achter te laten bij de 'Customer Feedback' tab. De Submit button zal niet klik-baar zijn, als geen stars geselecteerd worden. Door middel van html tampering is het mogelijk om dat attribuut te veranderen binnen de html.

1. Selecteer de Submit knop binnen de inspectie pagina
2. Verwijder het 'disabled = true' attribuut.
3. Submit de review zonder sterren, en kijk of het is gelukt, zie [foto 7](#) en [foto 8](#).

[Link naar OWASP](#)

Improper Input Validation: Door middel van het veranderen van bepaalde html attributen is het mogelijk om voor de gebruiker bepaalde functies te achterhalen, in dit geval: een zero-start feedback te geven aan de juice shop.

[Bescherming?](#)

OWASP heeft een [cheat sheet](#) wat HTML5 Security aanpakt. Door middel van die cheat sheet is het mogelijk om uitgebreide informatie te vinden en bepaalde HTML5 Security maatregelen te nemen.

## 2.6 BONUS PAYLOAD

### Methodologie

Dezelfde methode werd hier gebruikt als in 2.4. Het meegegeven script werd in de zoekbalk geïnjecteerd, en het resultaat daarvan was een SoundCloud file met een leuk deuntje, zie [foto 9](#).

### Link naar OWASP

XSS is waar door een script-injectie (bijvoorbeeld) bepaalde informatie tevoorschijn zou kunnen halen vanuit de web-page. Op deze manier kunnen cookies, session tokens of andere informatie met behulp van een script uit de web-page gehaald worden.

### Bescherming?

OWASP heeft een [cheat sheet](#) om XSS-injecties te voorkomen. Zoals zij zelf schrijven op de web-page, is er geen enkele techniek die XSS compleet kan overwinnen. Wel zou een combinatie van Framework Security technieken effectief zijn om XSS tegen te gaan.

## 2.7 BULLY CHATBOT

### Methodologie

Omdat de moeilijkheidsgraad van deze Challenge 1 ster is, was het zeer waarschijnlijk dat het door middel van normale instructies aan de chatbot wel mogelijk zou zijn om de coupon codes te achterhalen. Was deze Challenge moeilijker, had ik misschien andere technieken moeten gebruiken.

In dit geval was het heel simpel om gewoon naar de coupon codes te vragen: 'give me coupon codes', en de bot geeft ze door, zie [foto 10](#). De chatbot is alleen toegankelijk voor mensen met een account, dus het is belangrijk om die aan te maken.

### Link naar OWASP

Omdat er verder geen injectie of speciale achterhaling van informatie gebeurt door middel van OWASP-technieken, zou dit ook onder Miscellaneous geplaatst kunnen worden. Het is gewoon een chatbot die coupon codes weggeeft aan gebruikers die de juiste instructie geven.

### Bescherming?

In de back-end zou het mogelijk zijn om ervoor te zorgen dat de chatbot geen geheime informatie doorgeeft. Het feit dat die chatbot informatie over de coupon codes heeft is al apart, normaalgesproken zou een hulp-assistent-bot alleen over informatie moeten beschikken wat te maken heeft met bepaalde technische problemen.

**Conclusie:** bij de Juice Shop Trivial Challenges was het mogelijk om een klein aantal makkelijke oefeningen te doorlopen aan de hand van bepaalde technieken. XSS kwam voornamelijk aan bod in 2.4, en 2.6, terwijl de andere opdrachten te maken waren door middel van zoekwerk op de Juice shop pagina zelf, en het inspecteren van bepaalde elementen. Door de links te leggen naar bepaalde OWASP-categorieën wordt het ook snel duidelijk welke techniek bij welke categorie hoort, en door middel van extra research leert de gebruiker ook veel over bepaalde preventieve methoden die OWASP voorziet voor deze attacks.

## 3.3 Juice Shop - Easy Challenges

Opdracht gemaakt door: [Stef](#) (zie [bijlage](#) voor screenshots)

### 3.1 VIEW BASKET



#### Methodologie

Eerst log je in als een gebruiker op de Juice Shop, hierna voeg je wat artikelen toe aan je winkelmand. Als dit gebeurd is ga je naar inspecteren via rechtermuisklik en klik je op storage en daarna session storage aan de linker kant. Er verschijnen wat gegevens en je klikt op bid. Dit kan je aanpassen en zo is de challenge compleet na het vernieuwen van de pagina.

#### Link naar OWASP

Broken Access Control, de attacker zou geen toegang mogen hebben tot de gegevens van een andere gebruiker, in dit geval de shopping basket. De attacker zou in deze context als administrator ingelogd zijn op het systeem.

#### Bescherming?

Bij het aanmaken van een account zou er een melding moeten komen voor de sterkte van het wachtwoord. Dat geeft aan hoe sterk/zwak een wachtwoord is, als het niet sterk genoeg is zou je het moeten aanpassen.

### 3.2 FIVE-STAR FEEDBACK

#### Methodologie

Door eerst in de admin section te komen kunnen we in dit scherm de feedback zien en verwijderen met het vuilbakje dat erlangs staat.

#### Link naar OWASP

Dit is wederom een voorbeeld van Broken Access Control, je zou alleen als administrator de feedback kunnen verwijderen. Dit zou voor een gewone gebruiker onmogelijk zijn want die kan niet zomaar inloggen met de gegevens van de administrator.

#### Bescherming?

Het account van de administrator zou beter beveiligd moeten worden om dit te voorkomen.

### 3.3 ADMIN SECTION

#### Methodologie

Eerst moest ik aanmelden met het admin account. Via inspecteren kon ik hierna in de debugger het script main.js vinden. Door als keyword op admin te zoeken kon ik het path vinden met administration erin. Dit geef je in bij de URL boven aan en zo was de challenge compleet.

[Link naar OWASP](#)

Broken Access Control, een gewone gebruiker zou normaal niet zomaar kunnen inloggen met de gegevens van de administrator.

[Bescherming?](#)

In dit geval zou de URL beter beveiligd moeten worden tegen XSS om te voorkomen dat dit gebeurt.

### 3.4 LOGIN ADMIN

[Methodologie](#)

Voor deze challenge moeten we een SQL-injectie doen, we loggen in met als gebruikersnaam ' or 1=1 -- en eender welk paswoord, ik nam **Password**. Hierna weten we ook wat de e-mail van de administrator is: **admin@juice-sh.op'** -- .

[Link naar OWASP](#)

Dit is een voorbeeld van SQL-Injectie, we gebruiken een query om de login van de admin te omzeilen.

[Bescherming?](#)

Er zijn tools zoals Seeker die je kunnen helpen om je website veiliger te maken tegen injecties.

### 3.5 PASSWORD STRENGTH

[Methodologie](#)

Door in te loggen met de e-mail van de admin en het password admin123, gevonden door een brute force attack met de rainbow table, was de challenge al compleet.

[Link naar OWASP](#)

Broken Authentication

[Bescherming?](#)

Het account van de administrator moet beter beveiligd worden, dat gaat met een sterker wachtwoord.

## 3.4 Juice Shop - Medium Challenges

Opdracht gemaakt door: [Aleyna](#)



### 4.1 ADMIN REGISTRATION

#### Methodologie

Allereerst ben ik opzoek gegaan naar tools om een gebruiker admin privileges te geven. Wanneer je inlogt als admin en de webpagina inspecteert zie je dat de role "admin" is toegekend aan gebruiker Admin. Via Burp Proxy is het mogelijk de code te intercepten door gewoonweg "role" toe te voegen en hier "admin" aan toe te kennen. Zie bijlage [foto 1](#).

[Link naar OWASP](#)

Improper Input Validation: als software input niet goed valideert, kan dit ervoor zorgen dat bepaalde delen van het system onbedoelde input ontvangen, wat zal resulteren in een gewijzigde controlestroom.



#### Bescherming

OWASP biedt een [cheat-sheet](#) aan die gedetailleerde uitleg geeft over hoe je Improper Input Validation kunt voorkomen.

### 4.2 FORGED FEEDBACK

#### Methodologie

Sinds dat Juice Shop bekend staat voor het niet valideren van ontvangen gegevens, is het mogelijk via Burp de back-end te intercepten zoals we bij Admin Registration gedaan hebben. Nadat we een feedback gepost hebben via een ingelogd account kunnen we de POST-request in element inspecteren bekijken. Deze vervolgens in Burp plakken en wijzigen naar een ander userID, ik heb ID 1 van gebruiker Admin genomen en zijn e-mailadres die we in de vorige challenges achterhaald hebben meegegeven in het POST-request. Zie bijlage [foto 2](#).

[Link naar OWASP](#)

Broken Access Control: privilege escalation betekent dat gebruikers bevoegdheden kunnen krijgen die niet voor hen bedoeld zijn. Wanneer deze rechten worden toegekend kunnen de gebruikers bestanden verwijderen, privégegevens bekijken of ongewenste programma's installeren.

#### Bescherming

Het matchen van de cookiegegevens van een gebruiker met een JSON-veld zou een grote bijdrage leveren aan het oplossen van zulke problemen. Als de cookie van gebruiker A inhoud verzendt die is gemarkeerd voor gebruiker B, behandel deze dan als ongeautoriseerd.

## 4.3 FORGED REVIEW

### Methodologie

Om een review te plaatsen in iemand anders naam heb ik gebruik gemaakt van het programma Postman. Door zelf een review te plaatsen op mijn account heb ik het PUT-request in developer tools geïnspecteerd om vervolgens de request body te plakken in Postman en de auteur te veranderen naar **admin@juice-sh.op**. Zie bijlage [foto 3](#).

### Link naar OWASP

Omdat de server de ingelogde gebruiker niet vergelijkt met de naam die via JSON wordt meegegeven is hier sprake van Broken Access Control.

### Bescherming

Toegang tot functionaliteit standaard weigeren. Gebruik toegangscontrolelijsten en op rollen gebaseerde authenticatiemechanismen.

## 4.4 RESET JIM'S PASSWORD

### Methodologie

Om het wachtwoord van Jim te resetten moeten we eerst weten te antwoorden op zijn security question. Wanneer we op "Forgot Password" klikken, en vervolgens op het vraagteken naast de security question veld, krijgen we te zien dat zijn security question: *"What's your eldest siblings middle name?"* is. Om deze vraag te kunnen beantwoorden moeten we informatie hebben over Jim, dit kunnen we verzamelen door de Juice Shop verder te verkennen en te zien op welke producten hij mogelijk reacties heeft geplaatst waarin hij dit soort informatie toevallig vrijgeeft. Na heel wat opzoekwerk gedaan te hebben kwam ik een reactie tegen waarin hij: *"Looks so much better on **my** uniform than the boring Starfleet symbol."* Naderhand ben ik op Google "Jim Starfleet" gaan googelen en kwam ik James T. Kirk tegen. Op zijn Wikipedia-pagina onder categorie "Family" stond dat George Samuel Kirk zijn broer is. Aangezien Samuel de middle name van George is, heb ik mijn poging gewaagd en dit bleek ook het antwoord te zijn op de security question. [Foto 4](#)

### Link naar OWASP

Broken Authentication: dit is geen technische kwetsbaarheid. In werkelijkheid zijn er geen goede beveiligingsvragen omdat mensen te veel persoonlijke informatie over zichzelf delen op sociaal media platformen.

### Bescherming

Implementeer waar mogelijk MFA om geautomatiseerde, inloggegevens, gestolen aanvallen op het gebied van hergebruik van inloggegevens te voorkomen.



# Bijlage Opdrachten

## Opdracht 1.1 Nmap

### Foto 1

*Answer the questions below*

---

What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS

Correct Answer

Which switch would you use for a "UDP scan"?

-sU

Correct Answer

If you wanted to detect which operating system the target is running on, which switch would you use?

-O

Correct Answer

Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV

Correct Answer

The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v

Correct Answer

Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?

(Note: it's highly advisable to always use *at least* this option)

-vv

Correct Answer

We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.

What switch would you use to save the nmap results in three major formats?

-oA

Correct Answer

What switch would you use to save the nmap results in a "normal" format?

-oN

Correct Answer

A very useful output format: how would you save results in a "grepable" format?

Correct Answer

Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

How would you activate this setting?

Correct Answer

Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier, and can incur errors!

How would you set the timing template to level 5?

Correct Answer

We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?

Correct Answer

How would you tell nmap to scan ports 1000-1500?

Correct Answer

A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?

Correct Answer

How would you activate a script from the nmap scripting library (lots more on this later!)?

Correct Answer

How would you activate all of the scripts in the "vuln" category?

Correct Answer

 Hint

# Opdracht 1.2 CC: Pen Testing

## Foto 1

Answer the questions below

What does nmap stand for?

Network Mapper

Correct Answer

How do you specify which port(s) to scan?

-p

Correct Answer

How do you do a "ping scan"(just tests if the host(s) is up)?

-sn

Correct Answer

What is the flag for a UDP scan?

-sU

Correct Answer

How do you run default scripts?

-sC

Correct Answer

How do you enable "aggressive mode"(Enables OS detection, version detection, script scanning, and traceroute)

-A

Correct Answer

What flag enables OS detection

-O

Correct Answer

How do you get the versions of services running on the target machine

-sV

Correct Answer

## Foto 2

Deploy the machine

No answer needed

Question Done

How many ports are open on the machine?

1

Correct Answer

What service is running on the machine?

Apache

Correct Answer

What is the version of the service?

2.4.18

Correct Answer

What is the output of the http-title script(included in default scripts)

Apache2 Ubuntu Default Page: It Works

Correct Answer

## Foto 3

Answer the questions below

How do you listen for connections?

-l

Correct Answer

How do you enable verbose mode(allows you to see who connected to you)?

-v

Correct Answer

How do you specify a port to listen on

-p

Correct Answer

How do you specify which program to execute after you connect to a host(One of the most infamous)?

-e

Correct Answer

How do you connect to udp ports

-iU

Correct Answer

## Foto 4

Answer the questions below

How do you specify directory/file brute forcing mode?	<input type="text" value="dir"/>	Correct Answer
How do you specify dns bruteforcing mode?	<input type="text" value="dns"/>	Correct Answer
What flag sets extensions to be used? Example: If the php extension is set, and the word is "admin" then gobuster will test admin.php against the webserver	<input type="text" value="-x"/>	Correct Answer
What flag sets a wordlist to be used?	<input type="text" value="-w"/>	Correct Answer
How do you set the Username for basic authentication(if the directory requires a username/password)?	<input type="text" value="-U"/>	Correct Answer
How do you set the password for basic authentication?	<input type="text" value="-P"/>	Correct Answer
How do you set which status codes gobuster will interpret as valid? Example: 200,400,404,204	<input type="text" value="-s"/>	Correct Answer
How do you skip ssl certificate verification?	<input type="text" value="-k"/>	Correct Answer
How do you specify a User-Agent?	<input type="text" value="-a"/>	Correct Answer
How do you specify a HTTP header?	<input type="text" value="-H"/>	Correct Answer
What flag sets the URL to bruteforce?	<input type="text" value="-u"/>	Correct Answer

## Foto 5

Deploy the machine	<input type="text" value="No answer needed"/>	Question Done
What is the name of the hidden directory	<input type="text" value="secret"/>	Correct Answer
What is the name of the hidden file with the extension xxa	<input type="text" value="password"/>	Correct Answer

## Foto 6

Answer the questions below

How do you specify which url to check?

-u

Correct Answer

What about which google dork to use?

-g

Correct Answer

How do you select(lol) which parameter to use?(Example: in the url <http://ex.com?test=1> the parameter would be test.)

-p

Correct Answer

What flag sets which database is in the target host's backend?(Example: if the flag is set to mysql then sqlmap will only test mysql injections).

--dbms

Correct Answer

How do you select the level of depth sqlmap should use(Higher = more accurate and more tests in general).

--level

Correct Answer

How do you dump the table entries of the database?

--dump

Correct Answer

Which flag sets which db to enumerate?

(Case sensitive)

-D

Correct Answer

Which flag sets which table to enumerate?

(Case sensitive)

-T

Correct Answer

Which flag sets which column to enumerate?

(Case sensitive)

-C

Correct Answer

How do you ask sqlmap to try to get an interactive os-shell?

--os-shell

Correct Answer

What flag dumps all data from every table

--dump-all

Correct Answer

## Foto 7

Answer the questions below

Set the url to the machine ip, and run the command

No answer needed

Question Done

How many types of sqli is the site vulnerable to?

3

Correct Answer

Dump the database.

No answer needed

Question Done

What is the name of the database?

tests

Correct Answer

How many tables are in the database?

2

Correct Answer

What is the value of the flag?

found\_me

Correct Answer

## Foto 8

*Answer the questions below*

How do you set the username to authenticate with?	<input type="text" value="-u"/>	Correct Answer
What about the password?	<input type="text" value="-p"/>	Correct Answer
How do you set the host?	<input type="text" value="-H"/>	Correct Answer
What flag runs a command on the server(assuming you have permissions that is)?	<input type="text" value="-x"/>	Correct Answer
How do you specify the share to enumerate?	<input type="text" value="-s"/>	Correct Answer
How do you set which domain to enumerate?	<input type="text" value="-d"/>	Correct Answer
What flag downloads a file?	<input type="text" value="-download"/>	Correct Answer
What about uploading one?	<input type="text" value="-upload"/>	Correct Answer
Given the username "admin", the password "password", and the ip "10.10.10.10", how would you run ipconfig on that machine	<input type="text" value="smbmap -u 'admin' -p 'password' -H 10.10.10.10 -x 'ipconfig'"/>	Correct Answer

## Foto 9

*Answer the questions below*

How do you specify which domain(workgroup) to use when connecting to the host?	<input type="text" value="-w"/>	Correct Answer
How do you specify the ip address of the host?	<input type="text" value="-i"/>	Correct Answer
How do you run the command "ipconfig" on the target machine?	<input type="text" value="-c 'ipconfig'"/>	Correct Answer
How do you specify the username to authenticate with?	<input type="text" value="-U"/>	Correct Answer
How do you specify the password to authenticate with?	<input type="text" value="-P"/>	Correct Answer
What flag is set to tell smbclient to not use a password?	<input type="text" value="-N"/>	Correct Answer
While in the interactive prompt, how would you download the file test, assuming it was in the current directory?	<input type="text" value="get test"/>	Correct Answer
In the interactive prompt, how would you upload your /etc/hosts file	<input type="text" value="put /etc/hosts"/>	Correct Answer

# Opdracht 1.3 Pentesting Fundamentals

## Foto 1

Answer the questions below

You are given permission to perform a security audit on an organisation; what type of hacker would you be?

White Hat

Correct Answer

Hint

You attack an organisation and steal their data, what type of hacker would you be?

Black Hat

Correct Answer

What document defines how a penetration testing engagement should be carried out?

Rules of Engagement

Correct Answer

## Foto 2

Answer the questions below

What stage of penetration testing involves using publicly available information?

Information Gathering

Correct Answer

If you wanted to use a framework for pentesting telecommunications, what framework would you use? Note: We're looking for the acronym here and not the full name.

OSSTMM

Correct Answer

What framework focuses on the testing of web applications?

OWASP

Correct Answer

## Foto 3

Answer the questions below

You are asked to test an application but are not given access to its source code - what testing process is this?

Black Box

Correct Answer

You are asked to test a website, and you are given access to the source code - what testing process is this?

White Box

Correct Answer

## Foto 4

ACME has approached you for an assignment. They want you to carry out the stages of a penetration test on their infrastructure. View the site (by clicking the green button on this task) and follow the guided instructions to complete this exercise.

[View Site](#)

Answer the questions below

Complete the penetration test engagement against ACME's infrastructure.

THM{PENTEST\_COMPLETE}

Correct Answer

## Opdracht 2.3 Dirbuster Challenge

Foto 1

```
(kali㉿kali)-[~]
$ nmap -sV -p- 192.168.58.138
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-27 02:40 EDT
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.89% done; ETC: 02:40 (0:00:05 remaining)
Stats: 0:01:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.89% done; ETC: 02:41 (0:00:11 remaining)
Nmap scan report for 192.168.58.138
Host is up (0.00093s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         nginx 1.21.6
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
1589/tcp  open  http         Apache httpd 2.4.52 ((Debian))
5355/tcp  open  llmnr?
5480/tcp  open  mysql        MySQL 8.0.28
6621/tcp  open  http         nginx 1.21.6
7591/tcp  open  unknown
7987/tcp  open  http         Node.js Express framework
```

Foto 2

```
(kali㉿kali)-[~]
$ dirb http://192.168.58.138:6621 /usr/share/wordlists/dirb/common.txt

____
DIRB v2.22
By The Dark Raver
____

START_TIME: Wed Apr 27 02:44:08 2022
URL_BASE: http://192.168.58.138:6621/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

____

GENERATED WORDS: 4612

— Scanning URL: http://192.168.58.138:6621/ —
+ http://192.168.58.138:6621/index.html (CODE:200|SIZE:75)
+ http://192.168.58.138:6621/robots.txt (CODE:200|SIZE:61)

____

END_TIME: Wed Apr 27 02:44:13 2022
DOWNLOADED: 4612 - FOUND: 2
```



Foto 3 en 4

## Valideer flags

1TINH2

PXL{67f80f475e9491f9a5fe2da659dff63}

VALIDEER

## Valideer flags

1TINH2

PXL{b5448d6e1904b02b53ad600669ec7d}

VALIDEER

## Proficiat!

Deze flag is goedgekeurd door het systeem en werd geregistreerd als gevonden! Succes met de volgende challenge.

EEN ANDERE FLAG  
PROBEREN

# Opdracht 2.5 Modern WebApp Challenge

Foto 1

**Welkom john**

Nieuwe leden:

- admin
- john

Verander wachtwoord

Log uit

Foto 2

Not secure | 192.168.221.137:5501/change-password

## Verander wachtwoord

Geef hier je nieuwe wachtwoord in:

Login

Foto 3

Burp Suite Community Edition v2022.2.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
1	http://192.168.221.137:5501	GET	/			304	237						192.168.221.137
3	http://192.168.221.137:5501	GET	/polyfills.6c2fef277189580b.js			304	238	script	js				192.168.221.137
4	http://192.168.221.137:5501	GET	/runtime.68f249e270e34de1.js			304	237	script	js				192.168.221.137
5	http://192.168.221.137:5501	GET	/main.239268c923d2624b.js			304	239	script	js				192.168.221.137
6	http://192.168.221.137:5501	POST	/api/login/		✓	200	347	JSON					192.168.221.137
7	http://192.168.221.137:5501	POST	/api/changepassword/		✓	200	268	JSON					192.168.221.137

Request Response

Pretty Raw Hex

```
4 Accept: application/json, text/plain, */*
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
6 Content-Type: application/json
7 Origin: http://192.168.221.137:5501
8 Referer: http://192.168.221.137:5501/change-password
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
11 Cookie: flag=FXL17Bd3210c8e31c3f60b5860c26b1211df17D; language=en; welcomebanner_status=dismiss
12 Connection: close
13
14 {
  "username": "john",
  "password": "secret1"
}
```

Inspector

Request Attributes 2

Request Cookies 3

Request Headers 11

Response Headers 7

0 matches

## Foto 4

The screenshot shows the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main toolbar has tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The Proxy tab is active, showing a list of intercepted HTTP requests. The filter is set to 'Hiding CSS, image and general binary content'. The list shows several requests, with the last one (ID 7) highlighted. This request is a POST to /api/changepassword/ with a status of 200 and a JSON response. The right pane shows the 'Request' tab with the raw request data. The 'Inspector' pane on the right shows a dropdown menu with options like 'Send to Intruder', 'Send to Repeater', 'Send to Sequencer', 'Send to Comparer', 'Send to Decoder', 'Show response in browser', 'Request in browser', 'Engagement tools [Pro version only]', 'Copy URL', 'Copy as curl command', and 'Copy to file'.

#	^	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
1		http://192.168.221.137:5501	GET	/			304	237						192.168.221
3		http://192.168.221.137:5501	GET	/polyfills.6c2fef277189580b.js			304	238	script	js				192.168.221
4		http://192.168.221.137:5501	GET	/runtime.68f249e270e34de1.js			304	237	script	js				192.168.221
5		http://192.168.221.137:5501	GET	/main.239268c923d2624b.js			304	239	script	js				192.168.221
6		http://192.168.221.137:5501	POST	/api/login/		✓	200	347	JSON					192.168.221
7		http://192.168.221.137:5501	POST	/api/changepassword/		✓	200	268	JSON					192.168.221

```
4 Accept: application/json, text/plain, */*
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
6 Chrome/100.0.4896.127 Safari/537.36
7 Content-Type: application/json
8 Origin: http://192.168.221.137:5501
9 Referer: http://192.168.221.137:5501/change-password
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
12 Cookie: flag=FXL47Bd3210c8e31c3fcf60b5860c26b1211df47D; language=en; welcomebanner_status=dismiss
13 Connection: close
14 {
  "username": "john",
  "password": "secret1"
}
```

## Foto 5

The screenshot shows the Burp Suite interface with a request and response view. The 'Request' tab is active, showing a POST request to /api/changepassword/. The 'Response' tab is also active, showing the server's response. The response is a 200 OK status with a JSON body indicating that the password was changed.

```
1 POST /api/changepassword/ HTTP/1.1
2 Host: 192.168.221.137:5501
3 Content-Length: 39
4 Accept: application/json, text/plain, */*
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
6 Content-Type: application/json
7 Origin: http://192.168.221.137:5501
8 Referer: http://192.168.221.137:5501/change-password
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
11 Cookie: flag=FXL47Bd3210c8e31c3fcf60b5860c26b1211df47D; language=en; welcomebanner_status=dismiss
12 Connection: close
13
14 {
  "username": "admin",
  "password": "admin"
}
```

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Access-Control-Allow-Origin: *
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 29
6 ETag: W/"1d-fgA+2QI6tQXiSyJdNS6fDkh1bVs"
7 Date: Fri, 22 Apr 2022 13:18:31 GMT
8 Connection: close
9
10 {
  "status": "password changed"
}
```

## Foto 6

Welkom admin

Nieuwe leden:

- admin
- john

PXL{025d7a4455dfb179a4155aa4dbec2977}

Verander wachtwoord

Log uit

## Opdracht 2.7 MySQL Challenge

Foto 1

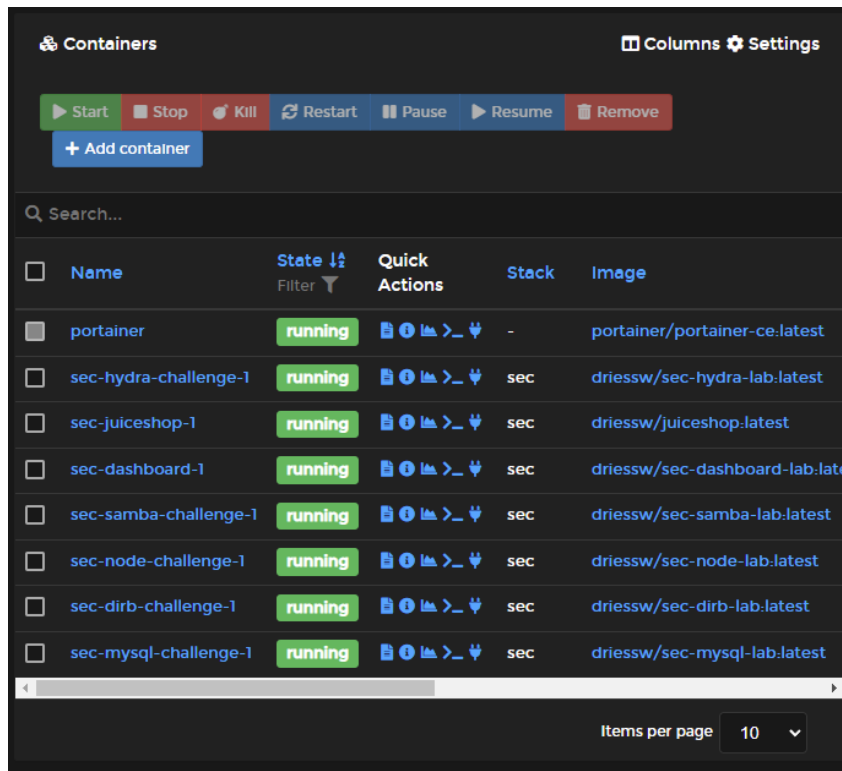


Foto 2

ENV	FLAG1	PXL{66e3276117041ab5ac2bdbd44e62be7f}
	GOSU_VERSION	1.14
	MYSQL_MAJOR	8.0
	MYSQL_PASSWORD	password
	MYSQL_ROOT_PASSWORD	secret007
	MYSQL_USER	joske
	MYSQL_VERSION	8.0.28-1debian10
	PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

## Proficiat!

Deze flag is goedgekeurd door het systeem en werd geregistreerd als gevonden! Succes met de volgende challenge.

EEN ANDERE FLAG  
PROBEREN

## Hogeschool PXL flag validator

Gebruik deze tool op je flags te valideren. Geef je teamnaam en flag in in het formulier aan de linkerkant.

Een flag heeft een vaste structuur, namelijk PXL{...}. De inhoud van de flag is uniek per challenge en per team. Je kan dus niet samenwerken met andere teams

*Vragen? Neem contact op met je vaklector!*

# Opdracht 3.1 Juice Shop - Walk The Happy Path

Foto 1

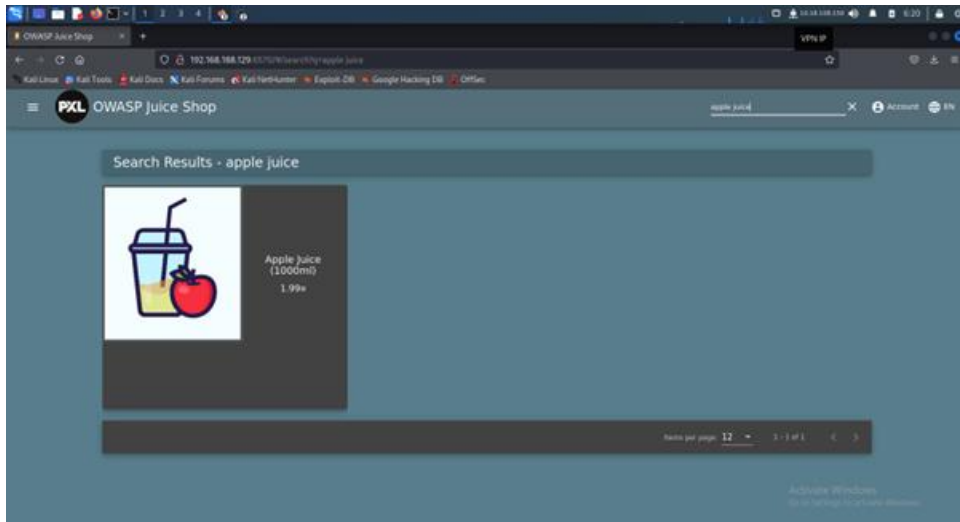


Foto 2

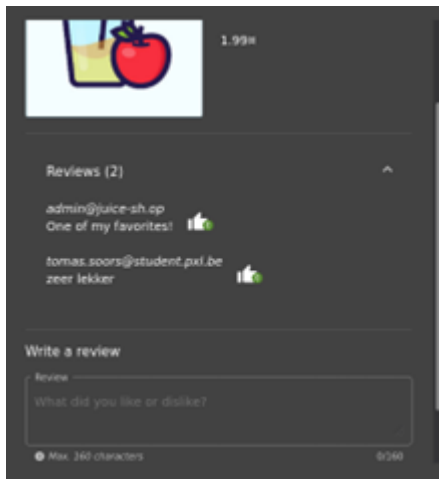


Foto 3

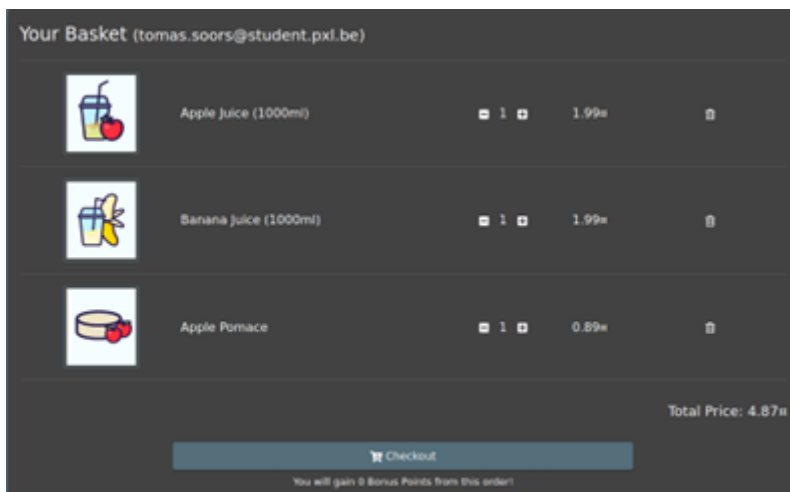


Foto 4

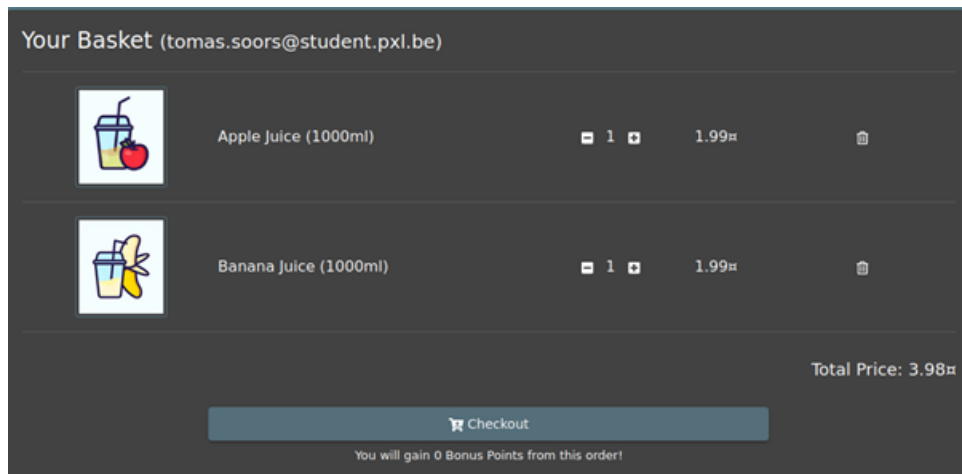


Foto 5

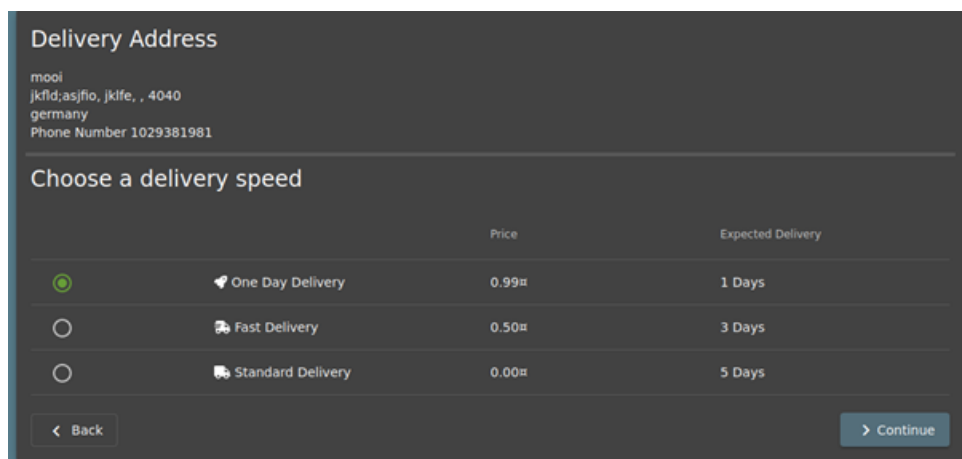


Foto 6

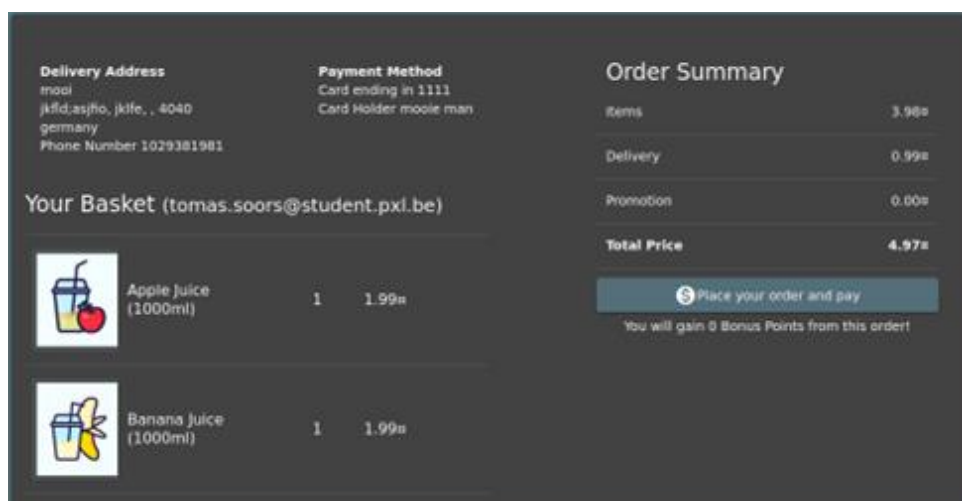


Foto 7



### Thank you for your purchase!

Your order has been placed and is being processed. You can check for status updates on our [Track Orders](#) page.

Your order will be delivered in 2 days.

**Delivery Address**  
mool  
jkfd;asjfo, jkffe, , 4040  
germany  
Phone Number 1029381981

#### Order Summary




Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99€	1	1.99€
Banana Juice (1000ml)	1.99€	1	1.99€
Items			3.98€
Delivery			0.99€
Promotion			0.00€
<b>Total Price</b>			<b>4.97€</b>

You have gained 0 Bonus Points from this order!

Foto 8

## User Profile



Email:  
tomas.soors@student.pxl.be

Username:  
customer service

[Set Username](#)

File Upload:

[Browse...](#) No file selected.

[Upload Picture](#)

or

Image URL:  
e.g. <https://www.gravatar.com/avatar/740d2c82418cad913a7386181a69f>

[Link Image](#)



Foto 9

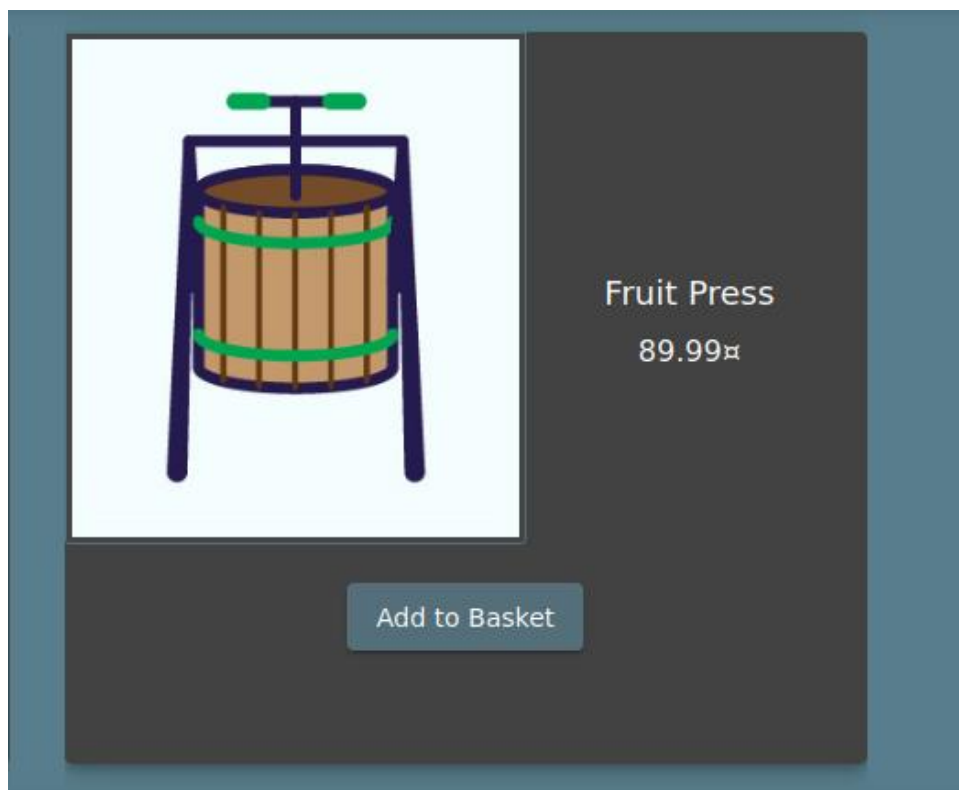


Foto 10

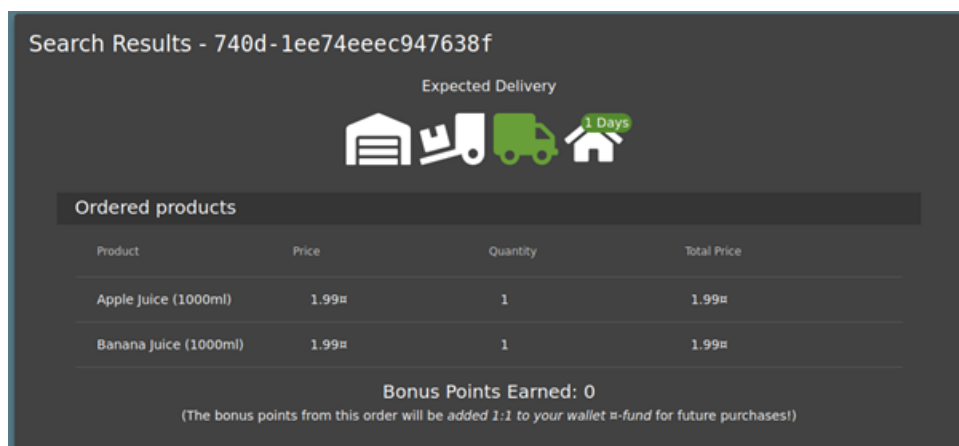


Foto 11

## Change Password

Current Password \*

New Password \*

Repeat New Password \*

*Password must be 5-40 characters long.* 14/40

14/20


 Change

Foto 12

## Customer Feedback


Author

\*\*\*as.soors@student.pxl.be

Comment \*

dit is een geweldige webshop


*Max. 160 characters* 29/160

Rating 

CAPTCHA: What is  $6+5+5$  ?

Result \*

16

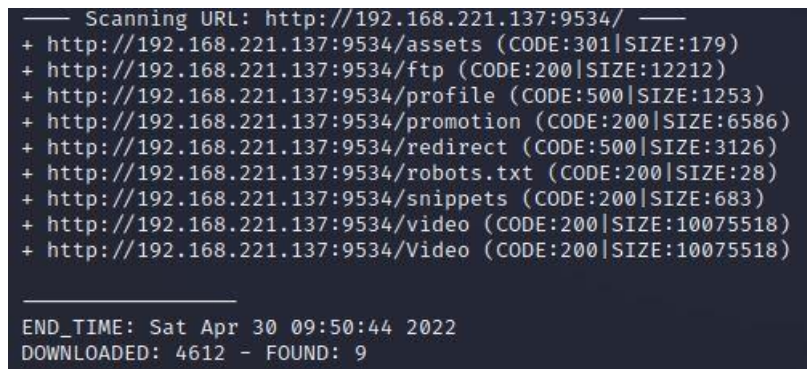
 Submit

## Foto 13



## Opdracht 3.2 Juice Shop - Trivial Challenges

### Foto 1



### Foto 2



## Foto 3

### # Planned Acquisitions

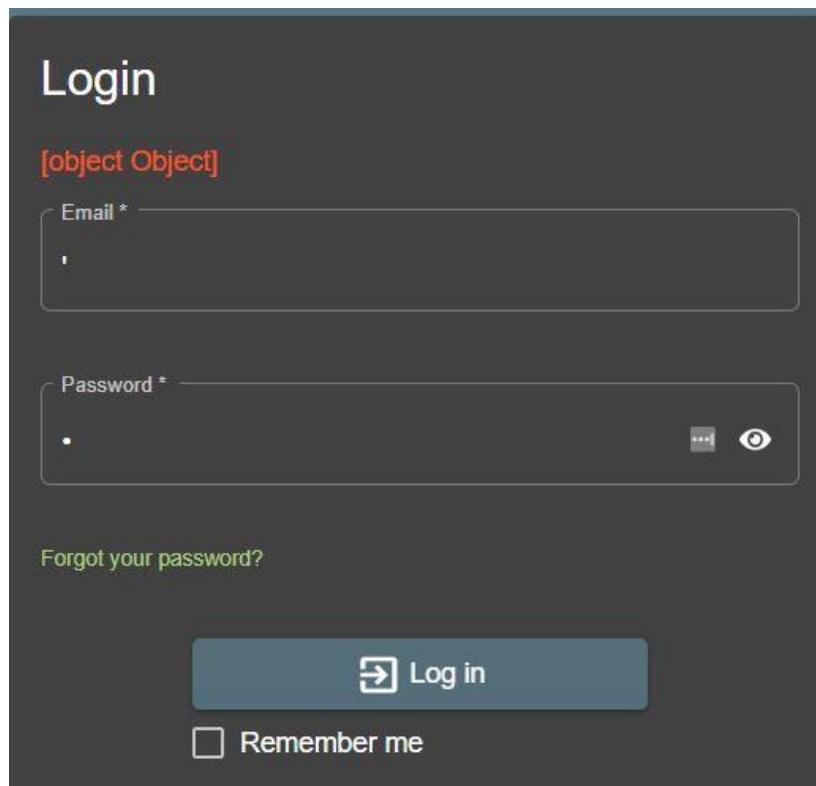
> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year. This will have a significant stock market impact as we will elaborate in detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.

## Foto 4




**Login**

[object Object]

Email \*

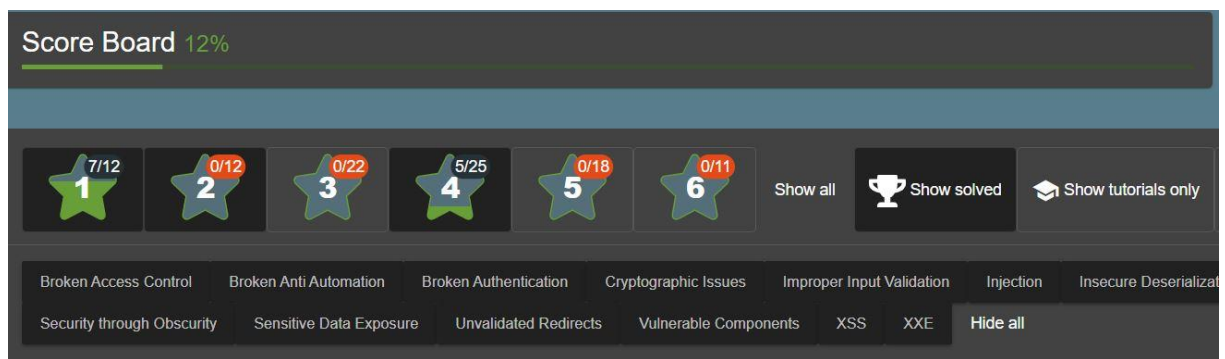
Password \*

Forgot your password?

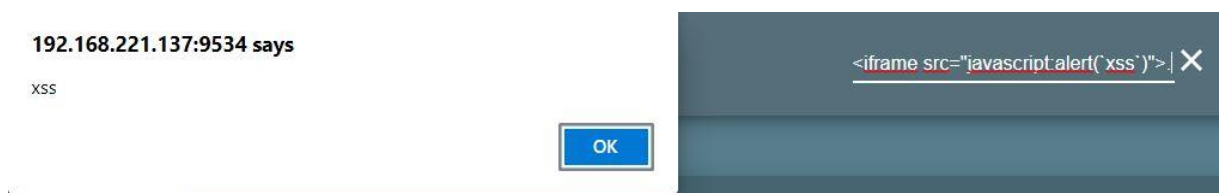
 Log in

☐ Remember me

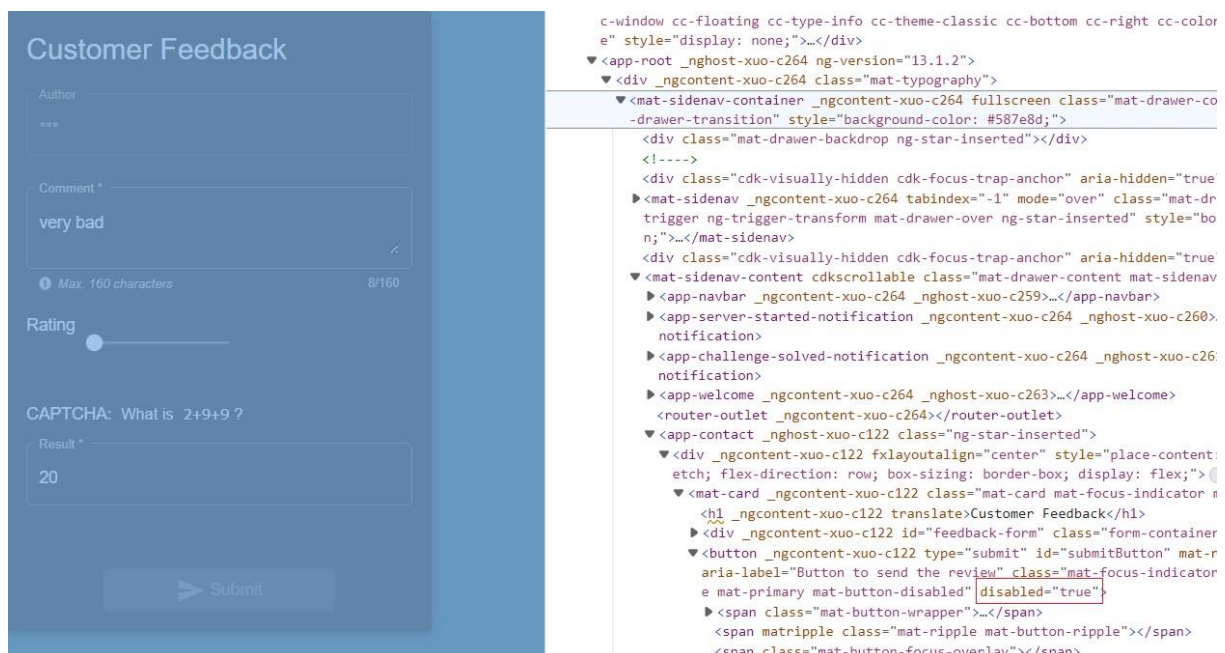
## Foto 5



## Foto 6



## Foto 7



## Foto 8



Foto 9

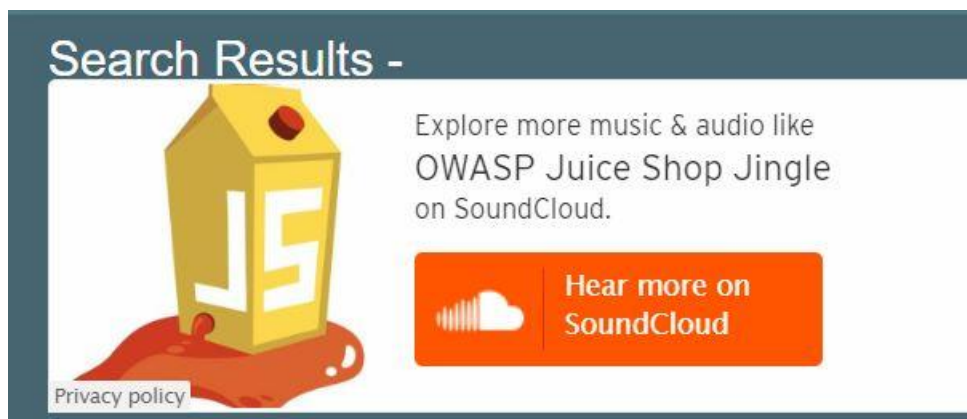


Foto 10



## Opdracht 3.3 Juice Shop - Easy Challenges

Foto 1

You successfully solved a challenge: View Basket (View another user's shopping basket.)

Foto 2

You successfully solved a challenge: Five-Star Feedback (Get rid of all 5-star customer feedback.)

Foto 3

You successfully solved a challenge: Admin Section (Access the administration section of the store.)

Foto 4

You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

Foto 5

You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)

## Opdracht 3.4 Juice Shop - Medium Challenges

Foto 1

Admin Registration	★ ★ ★	Register as a user with administrator privileges.	<input checked="" type="checkbox"/>
--------------------	-------	---	-------------------------------------

Foto 2

Forged Feedback	★ ★ ★	Post some feedback in another user's name.	<input checked="" type="checkbox"/>
-----------------	-------	--	-------------------------------------

Foto 3

Forged Review	★ ★ ★	Post a product review as another user or edit any user's existing review.	Broken Access Control	<input checked="" type="checkbox"/> Solved	
---------------	-------	---	-----------------------	--	--

Foto 4

Reset Jim's Password	★ ★ ★	Reset Jim's password via the <b>Forgot Password</b> mechanism with <i>the original answer</i> to his security question.	<input checked="" type="checkbox"/>
----------------------	-------	---	-------------------------------------



# Bibliografie

GeeksforGeeks. (2020, 9 december). *Node.js vs Express.js*. Geraadpleegd op 30 april

2022, van <https://www.geeksforgeeks.org/node-js-vs-express->

[js/#:~:text=js%3A-,Node.,approaches%20and%20principles%20of%20Node.](https://www.geeksforgeeks.org/node-js-vs-express-js/#:~:text=js%3A-,Node.,approaches%20and%20principles%20of%20Node.)

# Extra Oefeningen – Juice Shop Extra Challenges

Totaal aantal extra challenges gedaan: 20

Totaal aantal juice shop challenges Labo: 16   Extra: 20   Totaal: 36

## 1. Easter egg

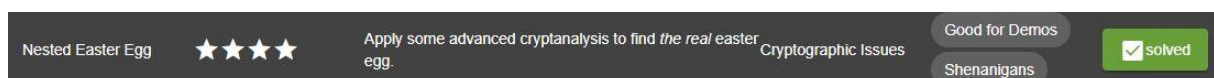
Gemaakt door: [Rasmus](#)



1. Dirbuster op het ipadres, om /ftp te vinden.
2. Haal de versleutelde string van eastere.gg:  
L2d1ci9xcmlmL25lci9mYi9zaGFhbc9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXlvcn5mZ3JlL3J0dA==
3. Base64-decodeer dit tot:  
/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt
4. ROT13-decodeer dit tot:  
/the/devs/are/so/funny/they/hid/an/easter/egg/in/the/easter/egg

## 2. Nested Easter Egg

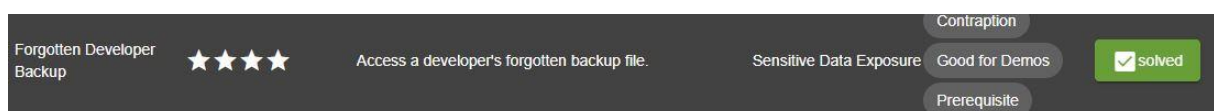
Gemaakt door: [Rasmus](#)



1. Bezoek  
<http://localhost:3000/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg> gevonden van de vorige oefening

## 3. Forgotten Developer Backup

Gemaakt door: [Rasmus](#)



1. Ga naar <http://localhost:3000/ftp>
2. Het rechtstreeks openen van <http://localhost:3000/ftp/package.json.bak> zal niet werken omdat het een illegaal bestandstype is.

3. Met behulp van een Poison Null Byte (%00) toevoegen kan het filter worden misleid
4. `http://localhost:3000/ftp/package.json.bak%2500.md` %2500.md maakt het mogelijk om de file te downloaden

## 4. Forgotten Sales Backup

Gemaakt door: [Rasmus](#)

Forgotten Sales Backup ★★★★★ Access a salesman's forgotten backup file. Sensitive Data Exposure Contraption ☒ solved

1. Zelfde methode met %2500.md om de file te downloaden
2. Om `http://localhost:3000/ftp/coupons_2013.md.bak%2500.md` te downloaden

## 5. Misplaced Signature File

Gemaakt door: [Rasmus](#)

Misplaced Signature File ★★★★★ Access a misplaced SIEM signature file. Sensitive Data Exposure Contraption ☒ solved

1. Gebruik weer de %2500.md om de de file `suspicious_errors.yml` te downloaden
2. Om `http://localhost:3000/ftp/suspicious_errors.yml%2500.md` te downloaden

## 6. Poison Null Byte

Gemaakt door: [Rasmus](#)

Poison Null Byte ★★★★★ Bypass a security control with a Poison Null Byte to access a file not meant for your eyes. Improper Input Validation Prerequisite ☒ solved

1. Doe een van de vorige challenges om deze by default te completen

## 7. Login MC SafeSearch

Gemaakt door: [Rasmus](#)

Login MC SafeSearch ★★ Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass. Sensitive Data Exposure OSINT Shenanigans ☒ solved

1. Google Mc. SafeSearch en vind de video Protect ya Passwordz (hint wijst op Google)
2. In de video wordt bekend dat MC SafeSearch de naam van zijn hond "Mr. Noodles" als wachtwoord gebruikte, maar "sommige klinkers in nullen" veranderde.
3. Ga naar `http://localhost:3000/#/login` en log in met e-mail `mc.safesearch@juice-sh.op` en wachtwoord 'Mr. N00dles' om deze challenge te completen.

## 8. Security Policy

Gemaakt door: [Rasmus](#)

Security Policy ★★ Behave like any "white-hat" should before getting into the action. Miscellaneous Good Practice ☒ solved

1. Bezoek <https://securitytxt.org/> voor meer informatie over een voorgestelde standaard waarmee websites beveiligingsbeleid kunnen definiëren. (hint)
2. Vraag het beveiligingsbeleidsbestand aan bij de server op <http://localhost:3000/security.txt> om de challenge op te lossen.

## 9. Exposed Metrics

Gemaakt door: [Rasmus](#)

Exposed Metrics ★ Find the endpoint that serves usage data to be scraped by a popular monitoring system. Sensitive Data Exposure Good Practice ☒ solved <>

1. Scroll door [https://prometheus.io/docs/introduction/first\\_steps](https://prometheus.io/docs/introduction/first_steps) (link verwijst naar github)
2. /metrics wordt vaak beschreven, e.g. "Prometheus expects metrics to be available on targets on a path of /metrics."
3. Ga naar <http://localhost:3000/metrics> om de Prometheus /metrics te bekijken

## 10. Missing encoding

Gemaakt door: [Rasmus](#)

Missing Encoding ★ Retrieve the photo of Bjørn's cat in "melee combat-mode". Improper Input Validation Shenanigans ☒ solved

1. Ga naar <http://localhost:3000/#/photo-wall>
2. Inspecteer het afwezige image bestand bij " #zatschi #wde posthoneedsfourlegs"
3. Er is een tag `<img_ngcontent-akt-c18="" class="image" src="assets/public/images/uploads/-#zatschi-#whoneedsfourlegs-1572600969477.jpg" alt=" #zatschi #whoneedsfourlegs">` in the source
4. RM à 'Open in new tab' op de src element van de image
5. In de URL zijn er twee #'s die je moet verwijderen, zodat de URL correct wordt geïnterpreteerd.
6. Ga naar de correcte URL

## 11. Outdated Allowlist

Gemaakt door: [Rasmus](#)

Outdated Allowlist ★ Let us redirect you to one of our crypto currency addresses which are not promoted any longer. Unvalidated Redirects Code Analysis ☒ solved

1. Open main.js in de DevTools van de browser
2. Als je zoekt naar /redirect?to= en door alle instances bladert, ziet u drie functies die worden aangeroepen door verborgen knoppen op de pagina
3. Ga naar de eerste redirect link:  
`http://localhost:3000/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm` om de challenge te completen

## 12. Repetitive Registration

Gemaakt door: [Rasmus](#)

Repetitive Registration ★ Follow the DRY principle while registering a user. Improper Input Validation ☒ solved

1. Ga naar `http://localhost:3000/#/register`.
2. Vul alle vereiste informatie in, behalve het veld Password en Repeat Password
3. Typ bijv. 12345 in het veld Password
4. Typ nu 12345 in het veld Repeat Password
5. Ga ten slotte terug naar het veld Password en verander het in een ander wachtwoord. Het veld Repeat Password geeft niet de verwachte fout.
6. Klik op Submit om met deze user te registreren

## 13. Use a deprecated B2B interface that was not properly shut down.

Gemaakt door: [Rasmus](#)

Deprecated Interface ★★ Use a deprecated B2B interface that was not properly shut down. Security Misconfiguration Contraption Prerequisite ☒ solved

1. Log in met een random user
2. Via het menu ga naar 'Complaint'
3. Als je probeert een file te uploaden, zijn alleen pdf en zip files toegestaan.
4. Inspecteer de main.js in de DevTools en zoek naar 'zip'
5. Bij 'allowedMimeType array' staan ook de filetypes "application/xml" en "text/xml", naast PDF en ZIP.
6. Maak een random .xml bestand aan
7. Voeg deze file toe aan de complaint en klik submit om de challenge te completen.

## 14. Meta Geo Stalking

Gemaakt door: [Rasmus](#)

Meta Geo Stalking

★★

Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to Sensitive Data Exposure reset his password via the [Forgot Password](#) mechanism.

OSINT

☒ solved

1. Ga naar de Photo Wall en zoek naar een foto wat een user namens Jonny heeft geüpload.
2. Download deze en extraheer de metadata daarvan met exiftool <file>
3. In de metadata staan coördinaten, waar deze photo wellicht werd genomen. Zoek deze op Google.
4. De 'Daniel Boone National Forest' is het bos op deze locatie
5. Ga naar de login en klik 'Forgot your Password'
6. Vul in john@juice-sh.op voor de email en 'Daniel Boone National Forest' als het antwoord op de security vraag
7. Maak een nieuw password aan en click Submit.

## 15. Determine the answer to Emma's security question

Gemaakt door: [Rasmus](#)

Visual Geo Stalking

★★

Determine the answer to Emma's security question by looking at an upload of her to the Photo Wall and use it to Sensitive Data Exposure reset her password via the [Forgot Password](#) mechanism.

OSINT

☒ solved

1. Ga naar de Photo Wall en zoek naar een gebruiker namens Emma. Die bestaat niet, maar 'E=ma2' komt wel in de buurt.
2. Open de afbeelding zodat inzoomen mogelijk is, en zoek naar de naam van het gebouw (linker venster op 1ste verdieping)
3. Geef bij de Forgot Password Security Question 'ITsec' in, en verander het wachtwoord.

## 16. Bjoern's Favorite Pet

Gemaakt door: [Aleyna](#)

Bjoern's Favorite Pet

★★★

Reset the password of Bjoern's OWASP account via the [Forgot Password](#) mechanism with the original answer to his security question.

Broken Authentication

☒

1. Zoek op Google "Bjoern OWASP"
2. Type "Björn Kimminich Pet" in op Google Afbeeldingen
3. Je vindt een foto afkomstig van Twitter met in de caption "Zaya"
4. Antwoord op Bjoern's security question is Zaya

## 17. Login Bender

Gemaakt door: [Aleyna](#)

Login Bender

☆☆☆

Log in with Bender's user account.

Injection

✓

1. SQL injectie: [bender@juice-sh.op'--](#)
2. Wachtwoord willekeurig invullen
3. Je bent ingelogd

## 18. Login Jim

Gemaakt door: [Aleyna](#)

Login Jim

☆☆☆

Log in with Jim's user account.

Injection

✓

1. SQL injectie: [jim@juice-sh.op'--](#)
2. Wachtwoord willekeurig invullen
3. Je bent ingelogd

## 19. Upload Type

Gemaakt door: [Aleyna](#)

Upload Type

☆☆☆

Upload a file that has no .pdf or .zip extension. Improper Input Validation

✓

1. Maak een POSTverzoek aan `http://<ip>:<port>/file-upload` met een parameter "file" die bvb een .txt extensie bevat met een grootte van minder dan 200 kB.

## 20. Upload Size

Gemaakt door: [Aleyna](#)

Upload Size

☆☆☆

Upload a file larger than 100 kB.

Improper Input Validation

✓

1. Maak een POST verzoek via Burp of Postman op `http://<ip>:<port>/file-upload` met een parameter file die een PDF-bestand van meer dan 100 kB maar minder dan 200 kB bevat