jamk.fi

Data security testing

Lab 5: Web applications

Timo Lehosvuo, M3426@student.jamk.fi

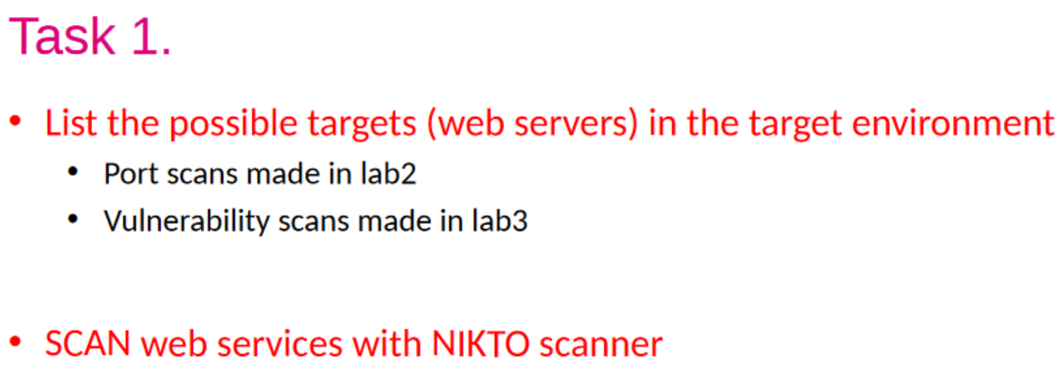
Raportti
Data Security Testing, Markku Vajaranta
Syksy 2020
Tieto- ja viestintätekniikan koulutusohjelma
Tekniikan ja liikenteen ala

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Sisällysluettelo

1 Web server scans

1.1 Tehtävä 1

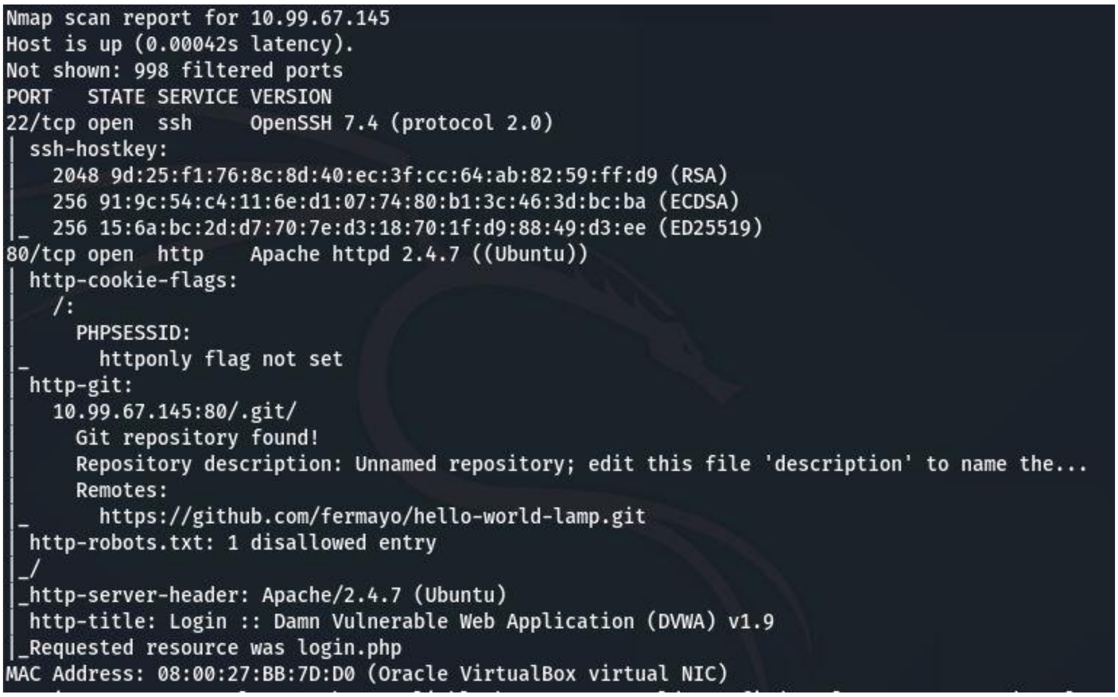


Task 1.

- List the possible targets (web servers) in the target environment
  - Port scans made in lab2
  - Vulnerability scans made in lab3
- SCAN web services with NIKTO scanner

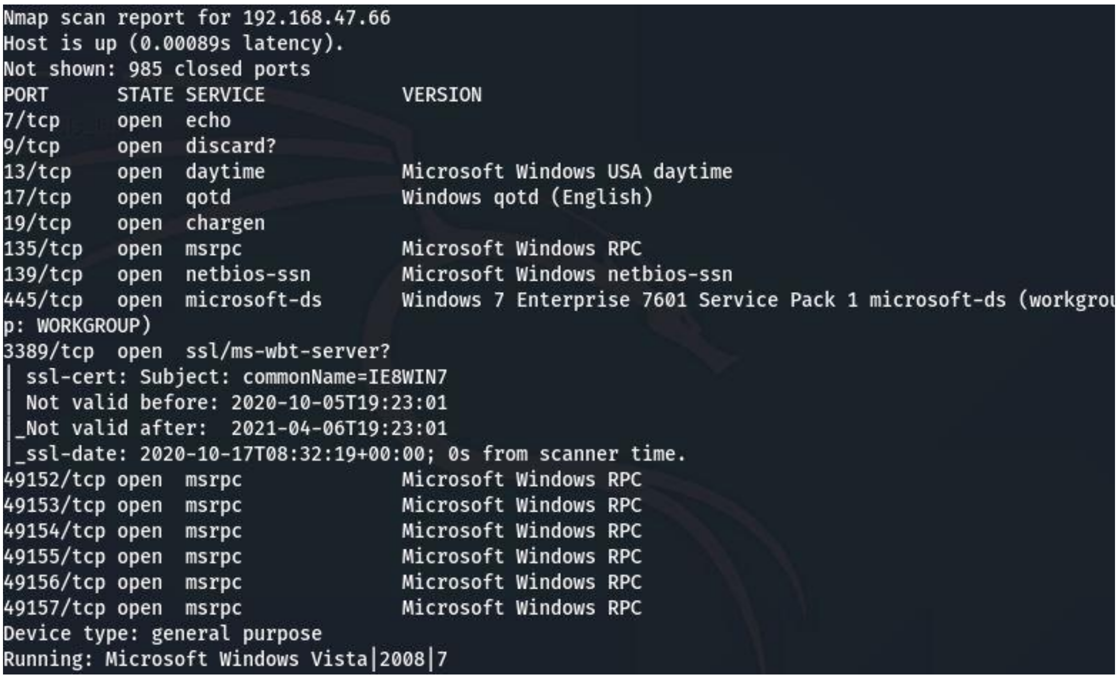
Kuva 1: Tehtävänanto 1.

Aloitin tehtävän listaamalla kaikki mahdollisista palvelut ja osan haavoittuvuuksista Linux ja Windows koneella (En listaa kaikkia haavoittuvuuksia koska niitä oli monta sataa):



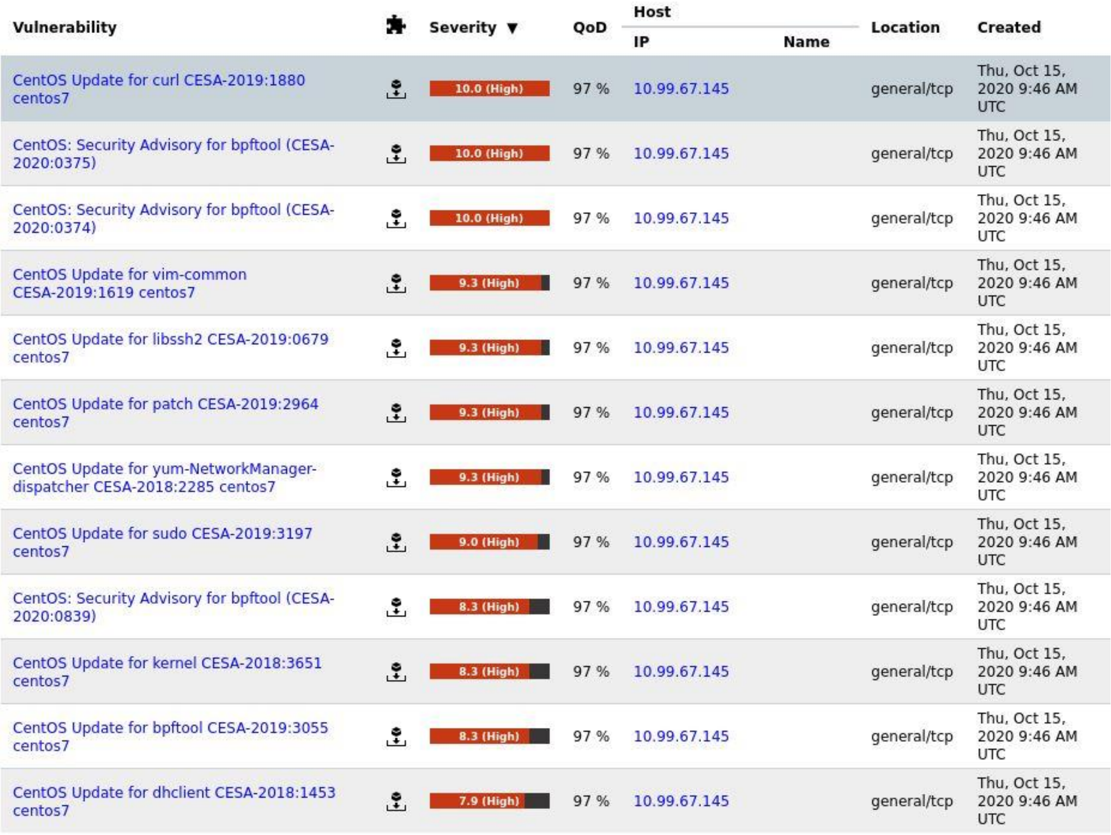
```
Nmap scan report for 10.99.67.145
Host is up (0.00042s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 9d:25:f1:76:8c:8d:40:ec:3f:cc:64:ab:82:59:ff:d9 (RSA)
|   256 91:9c:54:c4:11:6e:d1:07:74:80:b1:3c:46:3d:bc:ba (ECDSA)
|_  256 15:6a:bc:2d:d7:70:7e:d3:18:70:1f:d9:88:49:d3:ee (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-git:
|   10.99.67.145:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|     Remotes:
|_      https://github.com/fermayo/hello-world-lamp.git
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-title: Login :: Damn Vulnerable Web Application (DVWA) v1.9
|_Requested resource was login.php
MAC Address: 08:00:27:BB:7D:D0 (Oracle VirtualBox virtual NIC)
```

Kuva 2: Linuxin kohteet.



```
Nmap scan report for 192.168.47.66
Host is up (0.00089s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE            VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime            Microsoft Windows USA daytime
17/tcp    open  qotd               Windows qotd (English)
19/tcp    open  chargen
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgrou
p: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=IE8WIN7
| Not valid before: 2020-10-05T19:23:01
|_Not valid after:  2021-04-06T19:23:01
|_ssl-date: 2020-10-17T08:32:19+00:00; 0s from scanner time.
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  msrpc              Microsoft Windows RPC
49157/tcp open  msrpc              Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
```

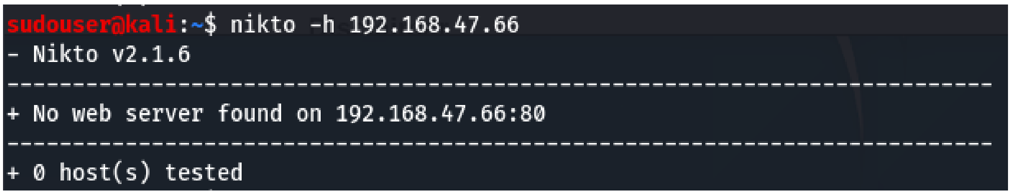
Kuva 3: Windows kohteet.



Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
CentOS Update for curl CESA-2019:1880 centos7		10.0 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS: Security Advisory for bpftool (CESA-2020:0375)		10.0 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS: Security Advisory for bpftool (CESA-2020:0374)		10.0 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for vim-common CESA-2019:1619 centos7		9.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for libssh2 CESA-2019:0679 centos7		9.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for patch CESA-2019:2964 centos7		9.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for yum-NetworkManager-dispatcher CESA-2018:2285 centos7		9.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for sudo CESA-2019:3197 centos7		9.0 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS: Security Advisory for bpftool (CESA-2020:0839)		8.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for kernel CESA-2018:3651 centos7		8.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for bpftool CESA-2019:3055 centos7		8.3 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC
CentOS Update for dhclient CESA-2018:1453 centos7		7.9 (High)	97 %	10.99.67.145		general/tcp	Thu, Oct 15, 2020 9:46 AM UTC

Kuva 4: Haavoittuvuuksia.

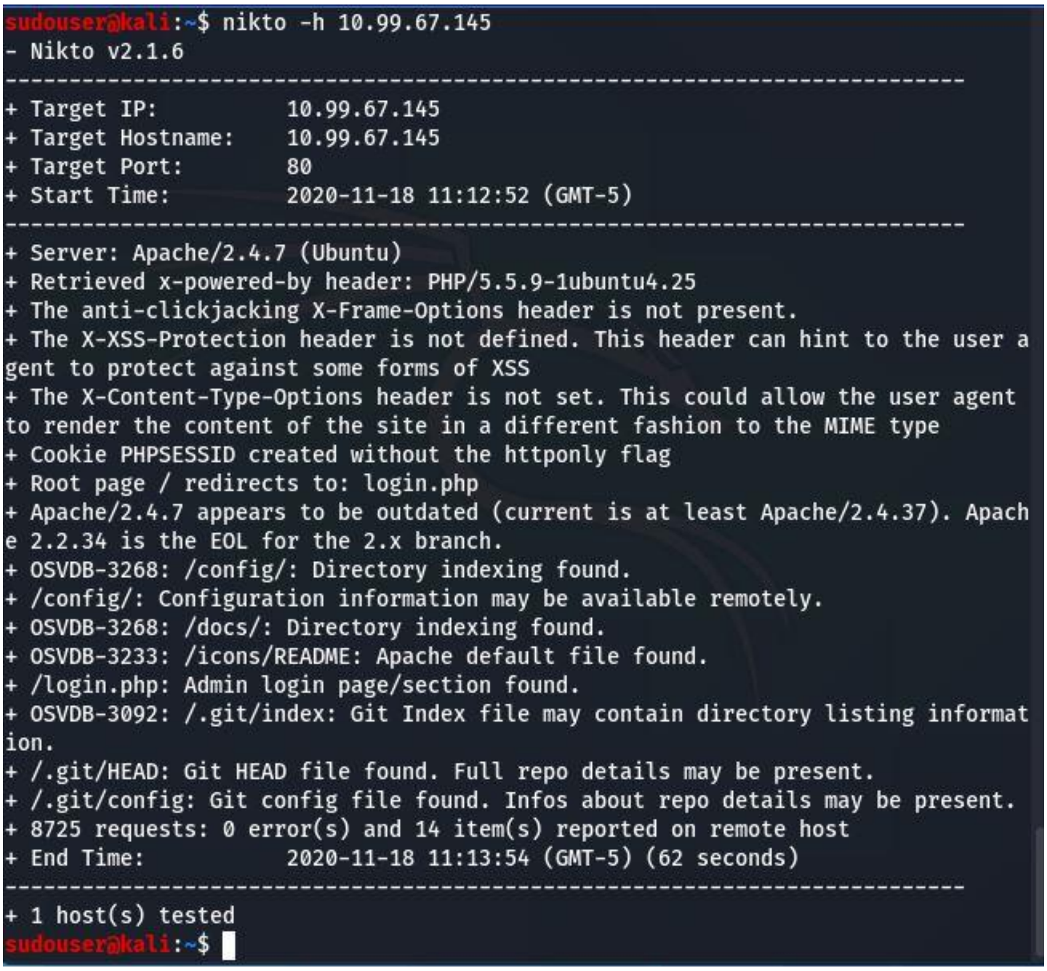
Seuraavaksi skannasin kohteet käyttäen ”nikto” webbi skanneria. Aikaisemmista tuloksista selviää, ettei Windowsilla pyöri web-palveluita mutta tarkistin sen kumminkin:



```
sudouser@kali:~$ nikto -h 192.168.47.66
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 192.168.47.66:80
---------------------------------------------------------------------------
+ 0 host(s) tested
```

Kuva 5: Windowsilla ei ole webbi palvelinta.

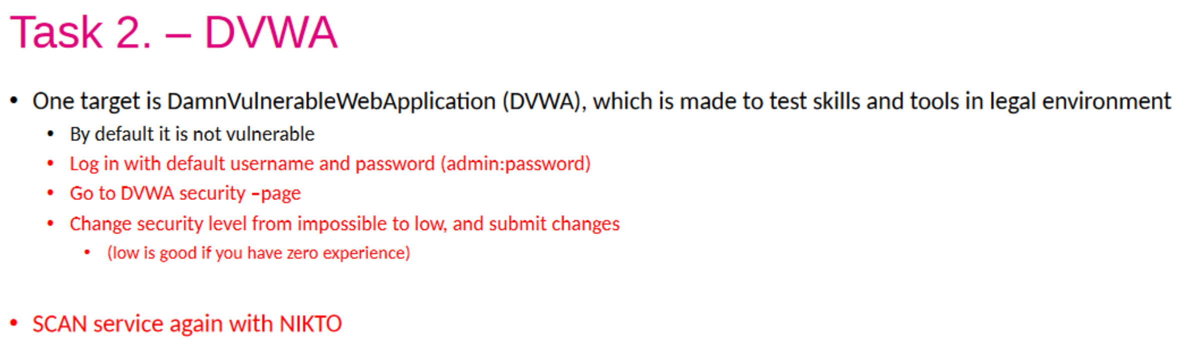
Linuxilla taas oli useampi palvelu, jotka skannasin niktolla:



```
sudouser@kali:~$ nikto -h 10.99.67.145
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.99.67.145
+ Target Hostname:    10.99.67.145
+ Target Port:        80
+ Start Time:         2020-11-18 11:12:52 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.25
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Root page / redirects to: login.php
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apach
e 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ OSVDB-3092: /.git/index: Git Index file may contain directory listing informat
ion.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /.git/config: Git config file found. Infos about repo details may be present.
+ 8725 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2020-11-18 11:13:54 (GMT-5) (62 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
sudouser@kali:~$
```

Kuva 6: Linuxin skannaus niktolla.

1.2 Tehtävä 2

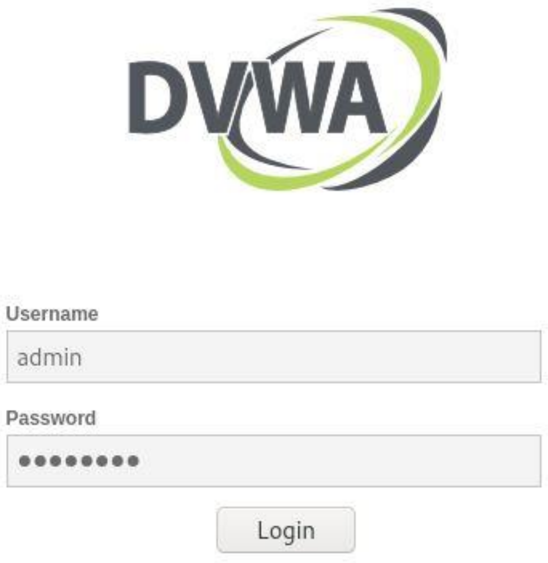


Task 2. – DVWA

- One target is DamnVulnerableWebApplication (DVWA), which is made to test skills and tools in legal environment
  - By default it is not vulnerable
  - Log in with default username and password (admin:password)
  - Go to DVWA security -page
  - Change security level from impossible to low, and submit changes
    - (low is good if you have zero experience)
- SCAN service again with NIKTO

Kuva 7: Tehtävänanto 2

Kirjauduin sisään DVWA:han tehtävänannon mukaisesti ja vaihdoin ”security” tason matalaksi. Asetuksiin pääsi valitsemalla sivupalkista ”DVWA security” ja sieltä pudotusvalikosta ”low”:



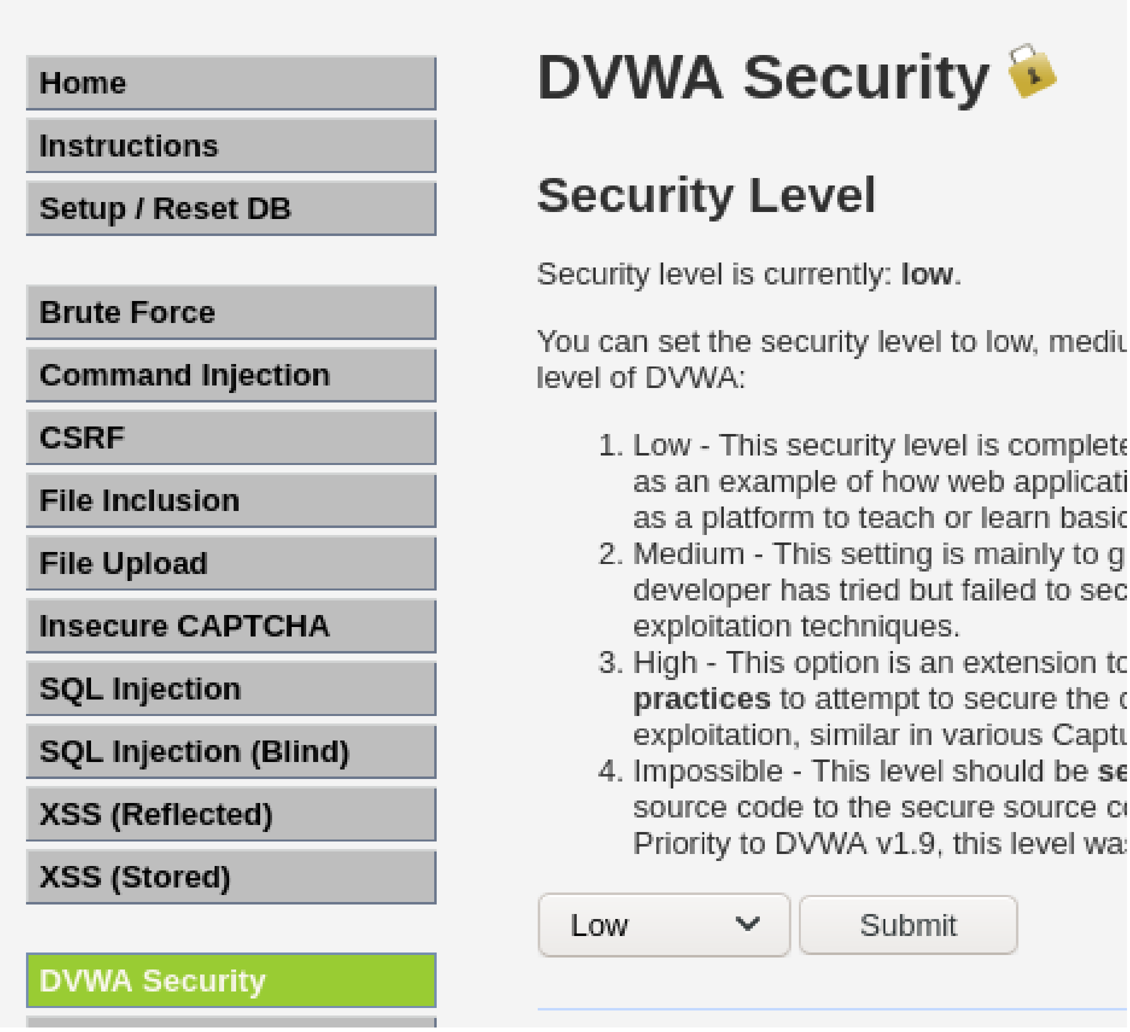
Username

admin

Password

●●●●●●●●

Kuva 8: DVWA login.



DVWA Security

Security Level

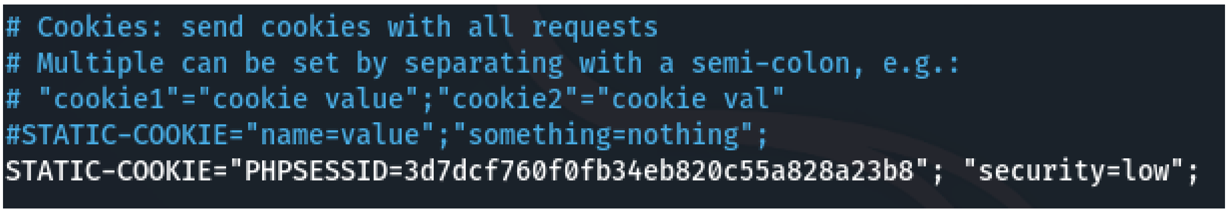
Security level is currently: **low**.

You can set the security level to low, mediu
level of DVWA:

1. Low - This security level is complete
as an example of how web applicati
as a platform to teach or learn basic
2. Medium - This setting is mainly to g
developer has tried but failed to sec
exploitation techniques.
3. High - This option is an extension to
practices to attempt to secure the c
exploitation, similar in various Captu
4. Impossible - This level should be **se**
source code to the secure source co
Priority to DVWA v1.9, this level wa

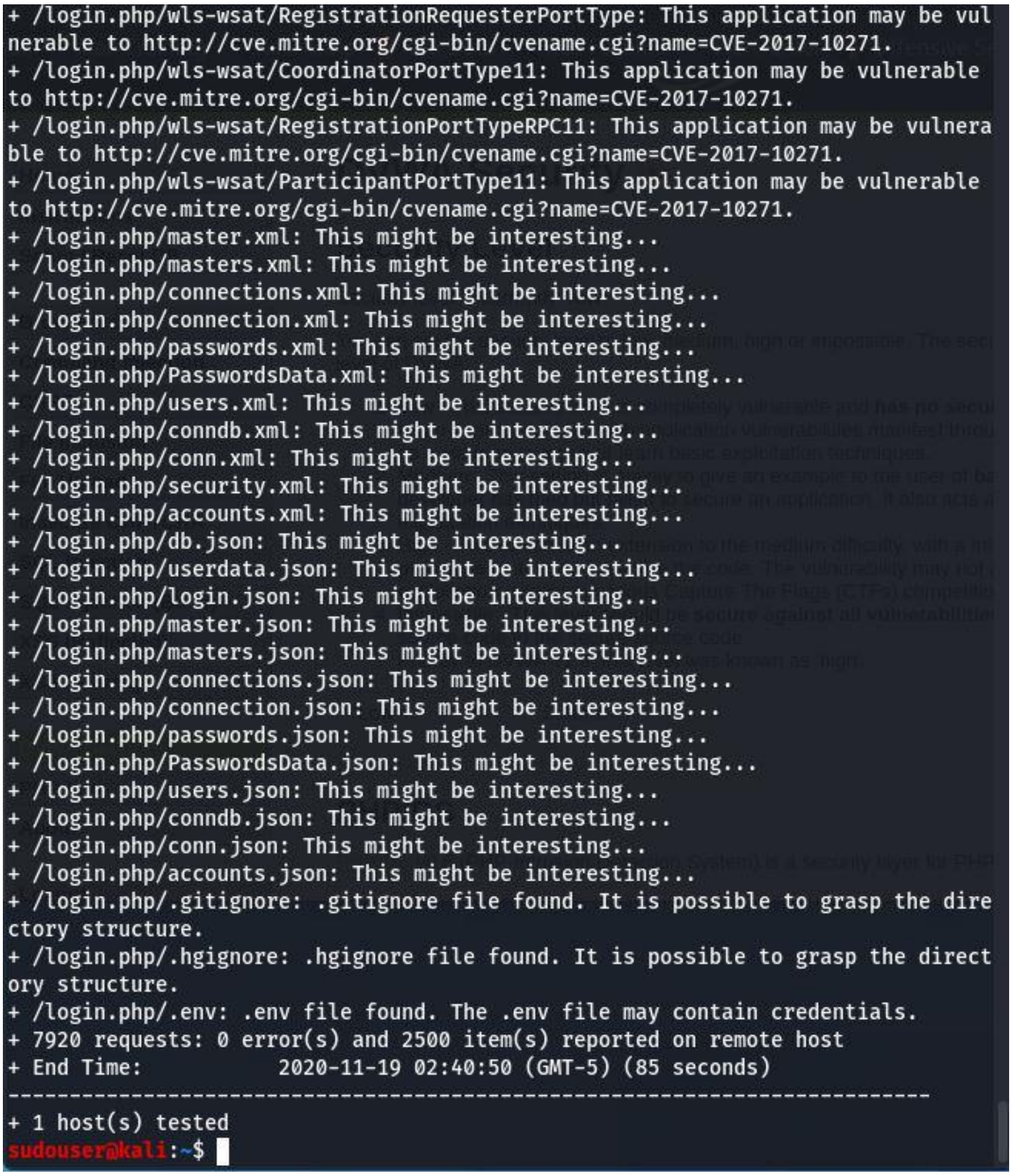
Kuva 9: DVWA security.

Jotta skannaus onnistuisi tarvitsin ”cookien”, jonka sain kuuntelemalla verkkoliikennettä Wireshark ohjelmalla. Tämän jälkeen asetin nikton konfiguraatio tiedostoon ”cookien” jonka olin saanut ja skannasin kohdetta uudestaan komennolla ”nikto -h http://10.99.67.145/login.php”:



```
# Cookies: send cookies with all requests
# Multiple can be set by separating with a semi-colon, e.g.:
# "cookie1"="cookie value";"cookie2"="cookie val"
#STATIC-COOKIE="name=value";"something=nothing";
STATIC-COOKIE="PHPSESSID=3d7dcf760f0fb34eb820c55a828a23b8"; "security=low";
```

Kuva 10: Cookie.



```
+ /login.php/wls-wsat/RegistrationRequesterPortType: This application may be vul
nerable to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.
+ /login.php/wls-wsat/CoordinatorPortType11: This application may be vulnerable
to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.
+ /login.php/wls-wsat/RegistrationPortTypeRPC11: This application may be vulnera
ble to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.
+ /login.php/wls-wsat/ParticipantPortType11: This application may be vulnerable
to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.
+ /login.php/master.xml: This might be interesting...
+ /login.php/masters.xml: This might be interesting...
+ /login.php/connections.xml: This might be interesting...
+ /login.php/connection.xml: This might be interesting...
+ /login.php/passwords.xml: This might be interesting...
+ /login.php/PasswordsData.xml: This might be interesting...
+ /login.php/users.xml: This might be interesting...
+ /login.php/conndb.xml: This might be interesting...
+ /login.php/conn.xml: This might be interesting...
+ /login.php/security.xml: This might be interesting...
+ /login.php/accounts.xml: This might be interesting...
+ /login.php/db.json: This might be interesting...
+ /login.php/userdata.json: This might be interesting...
+ /login.php/login.json: This might be interesting...
+ /login.php/master.json: This might be interesting...
+ /login.php/masters.json: This might be interesting...
+ /login.php/connections.json: This might be interesting...
+ /login.php/connection.json: This might be interesting...
+ /login.php/passwords.json: This might be interesting...
+ /login.php/PasswordsData.json: This might be interesting...
+ /login.php/users.json: This might be interesting...
+ /login.php/conndb.json: This might be interesting...
+ /login.php/conn.json: This might be interesting...
+ /login.php/accounts.json: This might be interesting...
+ /login.php/.gitignore: .gitignore file found. It is possible to grasp the dire
ctory structure.
+ /login.php/.hgignore: .hgignore file found. It is possible to grasp the direct
ory structure.
+ /login.php/.env: .env file found. The .env file may contain credentials.
+ 7920 requests: 0 error(s) and 2500 item(s) reported on remote host
+ End Time:           2020-11-19 02:40:50 (GMT-5) (85 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
sudouser@kali:~$ 
```

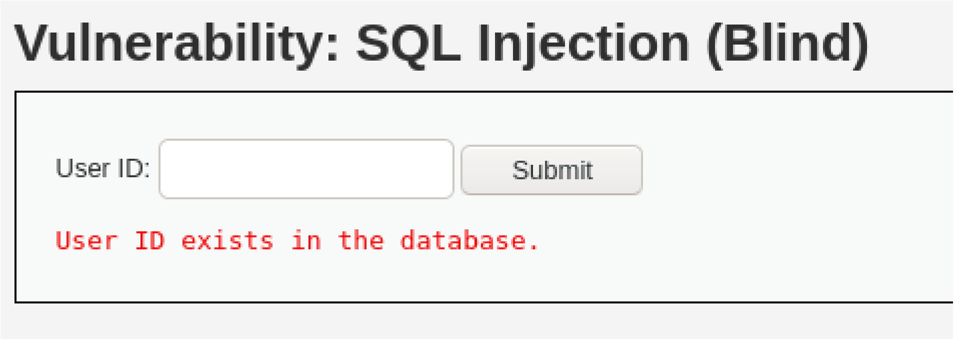
Kuva 11: Nikto skannaus keksillä.

1.3 Tehtävä 3

Task 3. – SQLMap

- SCAN DVWA SQLi –site/form with SQLMAP –software

Kuten aiemmassa tehtävässä niin skannasin sivustoa mutta käytin SQLMAP ohjelmaa. Ensiksi käynnistin kuuntelun wiresharkista, sitten menin DVWA:n kohtaan ”sql injection (blind)” ja kirjoitin hakukenttään ”1”:

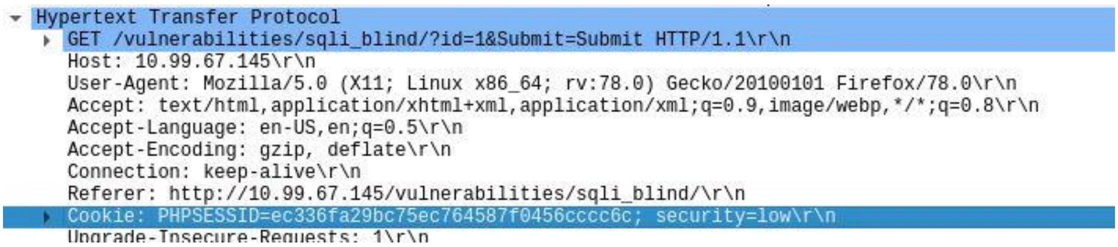


Vulnerability: SQL Injection (Blind)

User ID exists in the database.

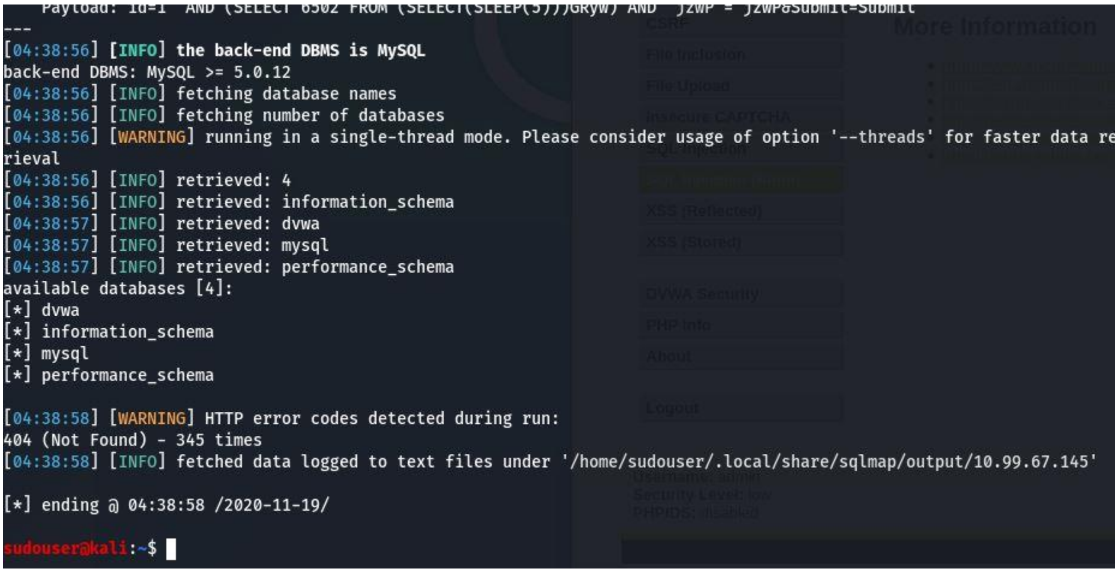
Kuva 12: SQL Injektio.

Tämän jälkeen hain keksin Wiresharkista ja skannasin kohteen komennolla ”sqlmap -u ” http://10.99.67.145/vulnerabilities/sqli_blind/?id=1&Submit=Submit#” –cookie=” PHPSESSID=ec336fa29bc75ec764587f0456cccc6c; security=low” –dbs”:



```
▾ Hypertext Transfer Protocol
  ▸ GET /vulnerabilities/sqli_blind/?id=1&Submit=Submit HTTP/1.1\r\n
    Host: 10.99.67.145\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://10.99.67.145/vulnerabilities/sqli_blind/\r\n
  ▸ Cookie: PHPSESSID=ec336fa29bc75ec764587f0456cccc6c; security=low\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

Kuva 13: Wireshark cookie.

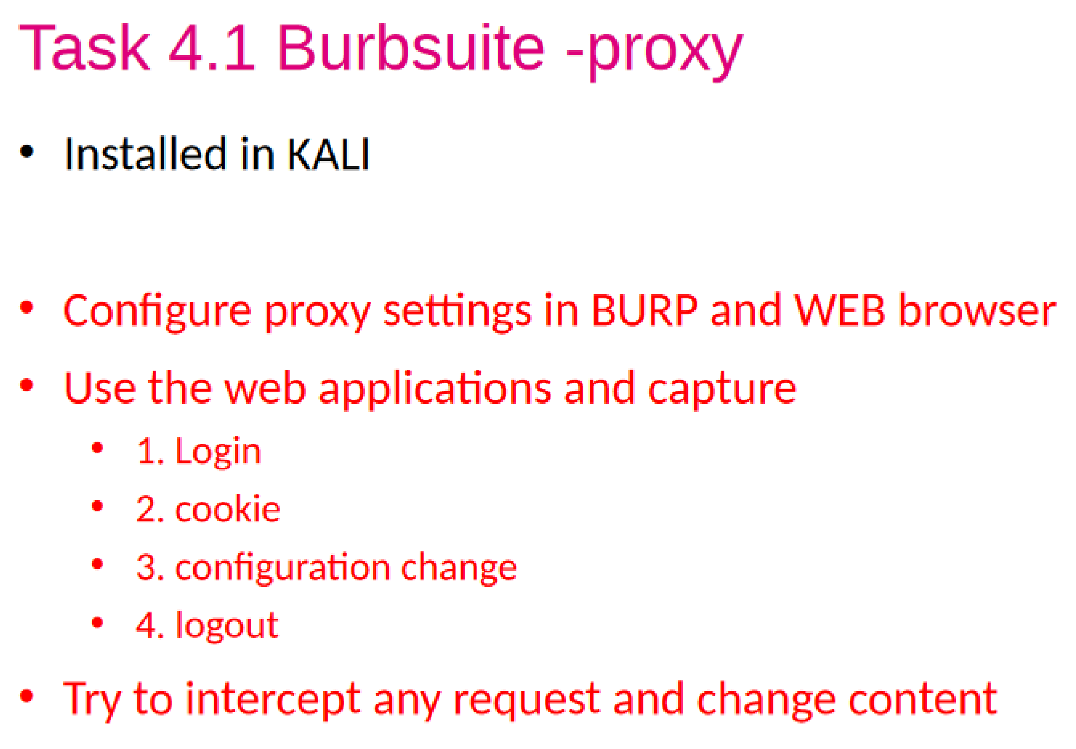


```
    Payload: id=1' AND (SELECT 6502 FROM (SELECT(SLEEP(5)))GRyw) AND 'jZwP'='jZwP&Submit=Submit
---
[04:38:56] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[04:38:56] [INFO] fetching database names
[04:38:56] [INFO] fetching number of databases
[04:38:56] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data re
rieval
[04:38:56] [INFO] retrieved: 4
[04:38:56] [INFO] retrieved: information_schema
[04:38:57] [INFO] retrieved: dvwa
[04:38:57] [INFO] retrieved: mysql
[04:38:57] [INFO] retrieved: performance_schema
available databases [4]:
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema

[04:38:58] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 345 times
[04:38:58] [INFO] fetched data logged to text files under '/home/sudouser/.local/share/sqlmap/output/10.99.67.145'

[*] ending @ 04:38:58 /2020-11-19/

sudouser@kali:~$ █
```

Kuva 14: SQLMAP tulokset.

Kuvasta nähdään, että SQLMAP löysi neljä tietokantaa.

1.4 Tehtävä 4



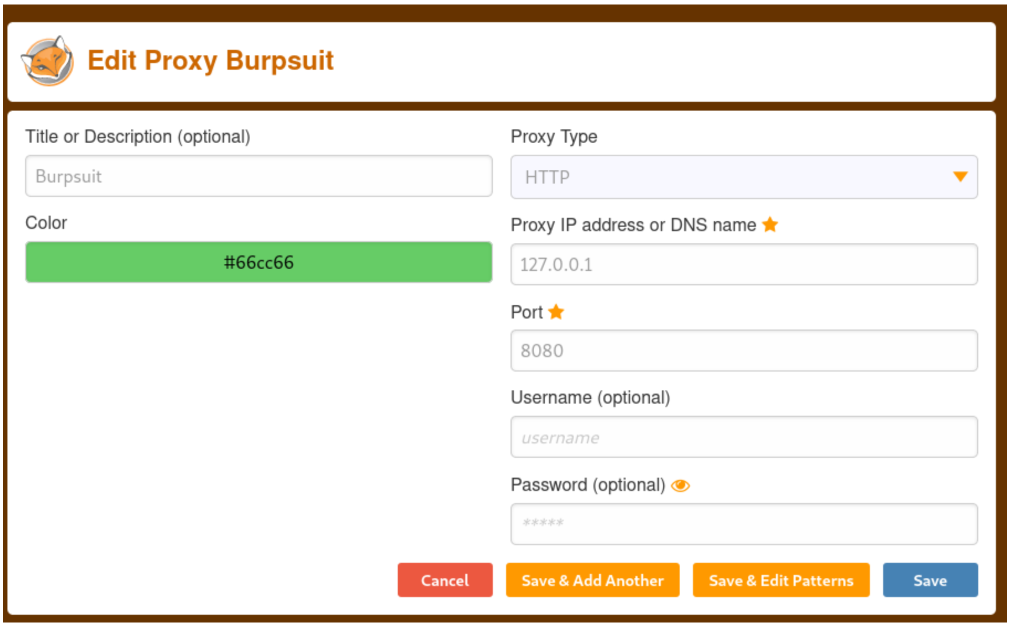
Task 4.1 Burbsuite -proxy

- Installed in KALI

- Configure proxy settings in BURP and WEB browser
- Use the web applications and capture
  - 1. Login
  - 2. cookie
  - 3. configuration change
  - 4. logout
- Try to intercept any request and change content

Kuva 15: Tehtävänanto 4.

Tehtävänä oli tehdä saman asian kuin edellisissä tehtävissä mutta vain eri työkalulla. Aloitin asentamalla Firefox -selaimeen ”foxyproxy” lisäosa mikä auttaa proxyn valitsemisessa ja laitoin sen kuuntelemaan localhostia:



Edit Proxy Burpsuit

Title or Description (optional): Burpsuit

Color: #66cc66

Proxy Type: HTTP

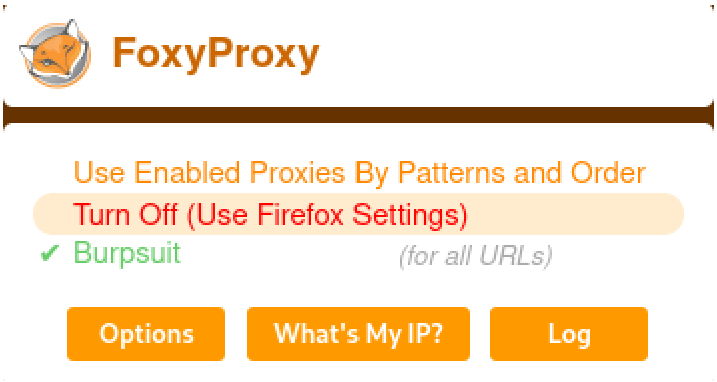
Proxy IP address or DNS name ★: 127.0.0.1

Port ★: 8080

Username (optional): username

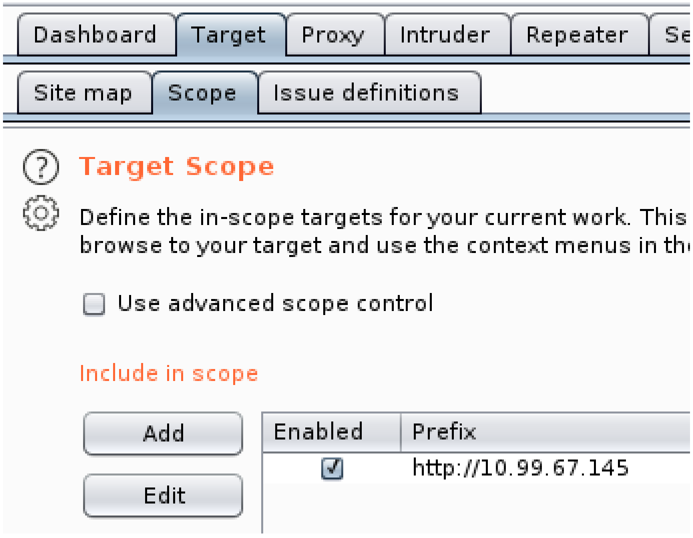
Password (optional): *****

Kuva 16: Foxyproxy.


FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
✓ Burpsuit
(for all URLs)
Options
What's My IP?
Log

Kuva 17: Foxyproxy 2.

Tämän jälkeen Käynnistin Burpsuite ja laitoin sen kuuntelemaan DVWA:ta eli IP-osoitetta 10.99.67.145:



Target Scope

Define the in-scope targets for your current work. This browse to your target and use the context menus in th

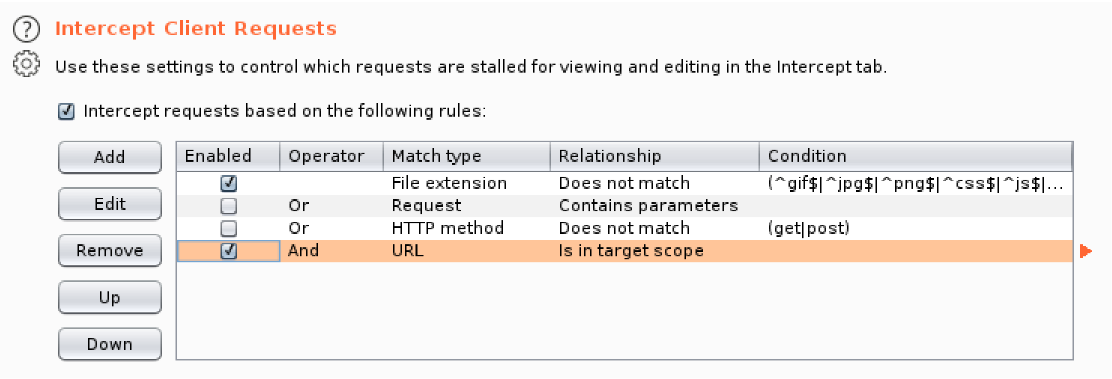
□ Use advanced scope control

Include in scope

Enabled	Prefix
☑	http://10.99.67.145

Kuva 18: Burpsuite konfiguraatio 1.

Lisäsin myös täpän kohtaan ”ULR is in the target scope”:



Intercept Client Requests

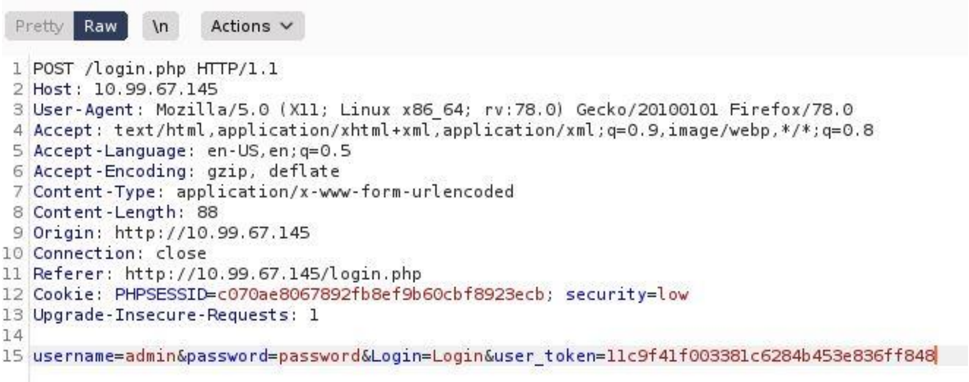
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
☑	And	URL	Is in target scope	

Kuva 19: Burpsuite konfiguraatio 2.

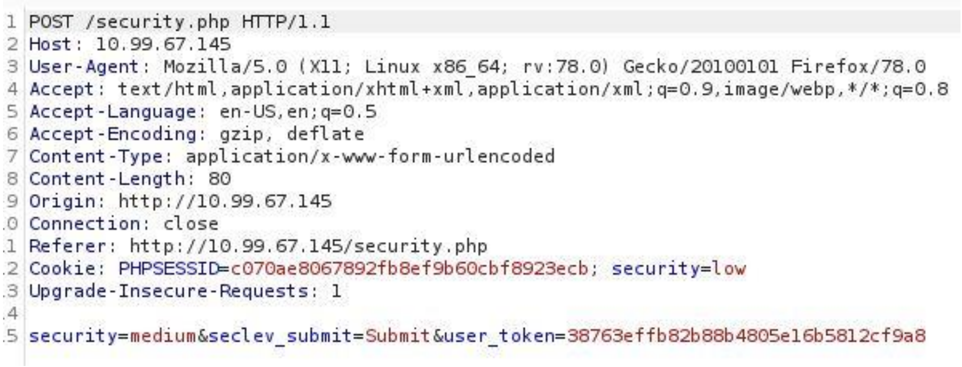
Sitten laitoin ”interceptin” päälle ja kirjauduin sisään:



```
POST /login.php HTTP/1.1
Host: 10.99.67.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Origin: http://10.99.67.145
Connection: close
Referer: http://10.99.67.145/login.php
Cookie: PHPSESSID=c070ae8067892fb8ef9b60cbf8923ecb; security=low
Upgrade-Insecure-Requests: 1

username=admin&password=password&Login=Login&user_token=11c9f41f003381c6284b453e836ff848
```

Kuva 20: Login.php.

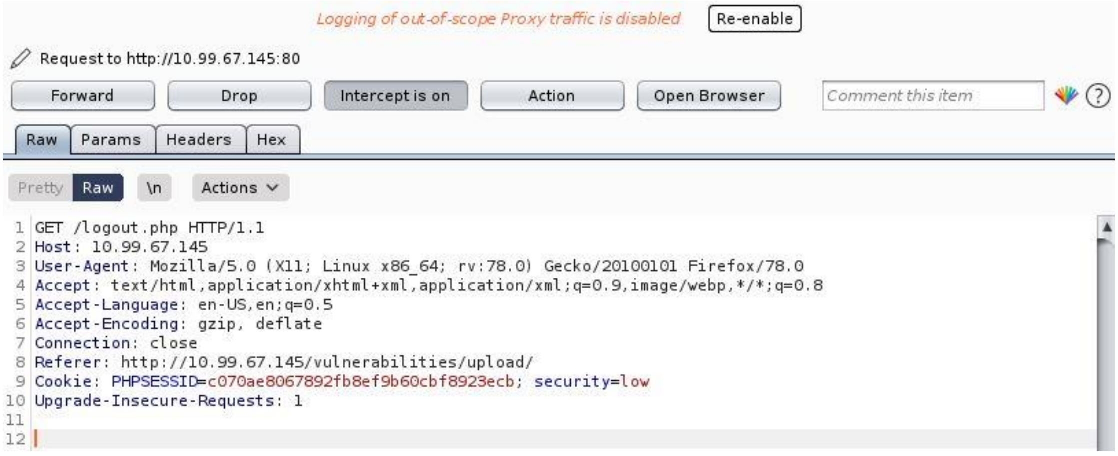
Yllä olevasta kuvasta nähdään tunnukset ja ”cookie”. Seuraavaksi nappasin konfiguraatio muutoksen:



```
POST /security.php HTTP/1.1
Host: 10.99.67.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 80
Origin: http://10.99.67.145
Connection: close
Referer: http://10.99.67.145/security.php
Cookie: PHPSESSID=c070ae8067892fb8ef9b60cbf8923ecb; security=low
Upgrade-Insecure-Requests: 1

security=medium&seclev_submit=Submit&user_token=38763effb82b88b4805e16b5812cf9a8
```

Kuva 21: Cookie ja konfiguraation muutos.

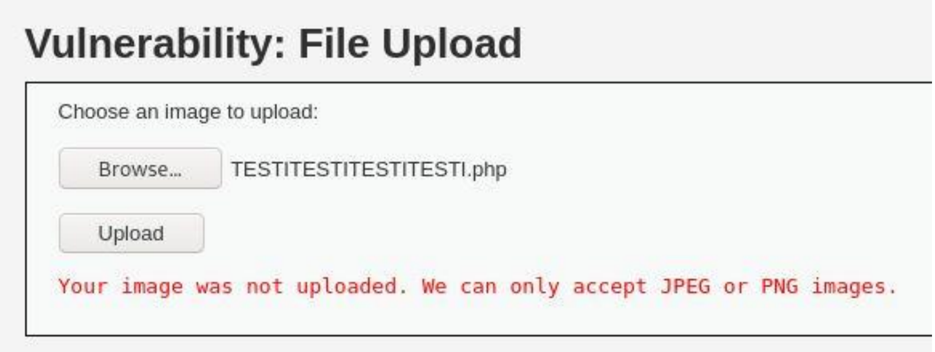
”Cookie” kohdasta nähdään, että ”security” taso on ”low” ja ”security” kohdassa se yritetään muuttaa arvoon ”medium”. Lopuksi kirjauduin ulos:



```
GET /logout.php HTTP/1.1
Host: 10.99.67.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.99.67.145/vulnerabilities/upload/
Cookie: PHPSESSID=c070ae8067892fb8ef9b60cbf8923ecb; security=low
Upgrade-Insecure-Requests: 1


```

Kuva 22. Logout.php

Viimeisessä kohdassa muutin tiedoston tyyppiä, jotta sain sen ladattua palvelimelle. Tätä varten minun piti muutta DVWA:n ”security” taso arvoon ”medium”, koska ”low” salli php päätteisten tiedostojen lataamisen palvelimelle

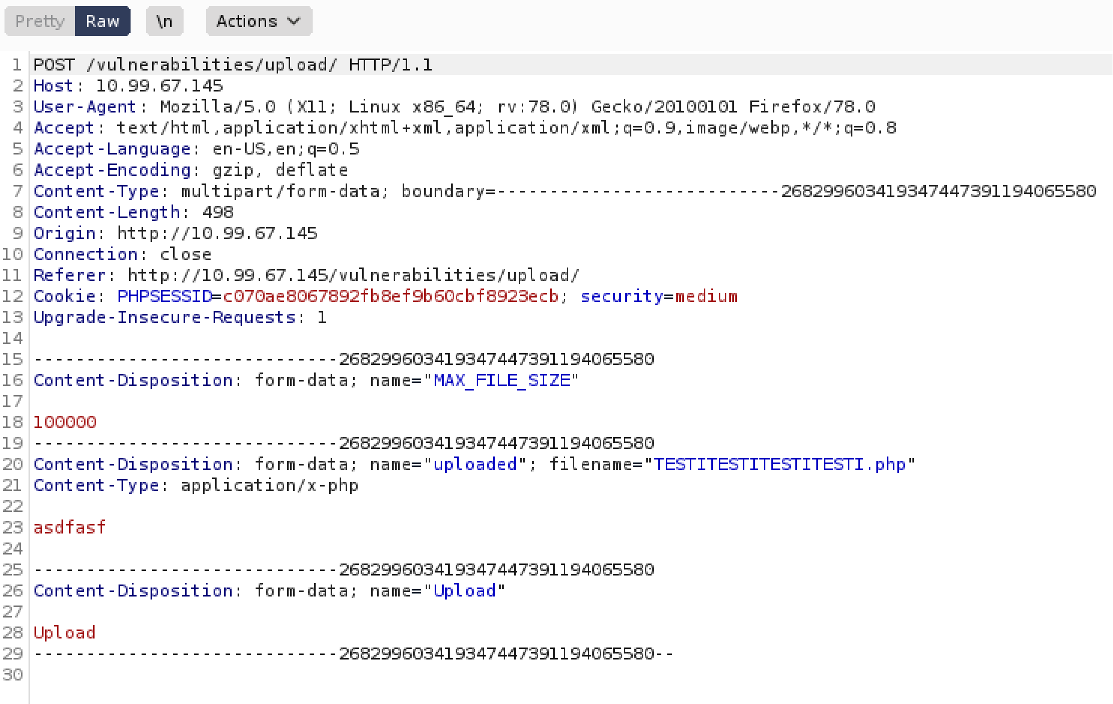


Vulnerability: File Upload

Choose an image to upload:

```
Your image was not uploaded. We can only accept JPEG or PNG images.
```

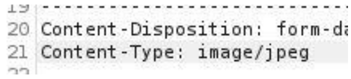
Kuva 23: DVWA ei salli php päätteisiä tiedostoja medium tasolla.



```
POST /vulnerabilities/upload/ HTTP/1.1
Host: 10.99.67.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------268299603419347447391194065580
Content-Length: 498
Origin: http://10.99.67.145
Connection: close
Referer: http://10.99.67.145/vulnerabilities/upload/
Cookie: PHPSESSID=c070ae8067892fb8ef9b60cbf8923ecb; security=medium
Upgrade-Insecure-Requests: 1

-----------------------------268299603419347447391194065580
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------268299603419347447391194065580
Content-Disposition: form-data; name="uploaded"; filename="TESTITESTITESTITESTI.php"
Content-Type: application/x-php

asdfasf

-----------------------------268299603419347447391194065580
Content-Disposition: form-data; name="Upload"

Upload
-----------------------------268299603419347447391194065580--

```

Kuva 24: File upload kaappaus.

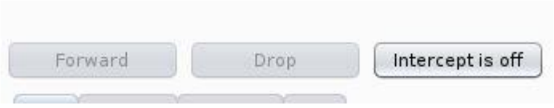
Kuvasta nähdään että ”Content-Type” on ”application/x-php”, muutin tämä arvoon ”image/jpeg”:



```
----------------------------
Content-Disposition: form-da
Content-Type: image/jpeg
```

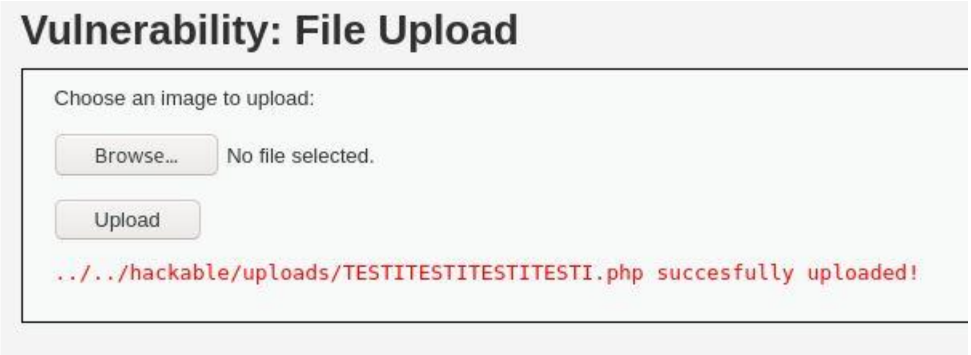
Kuva 25: Tyypin muutos.

Käskin burpsuite ”forwartoida” kaappauksen ja otin ”interceptionin” pois päällä:



Kuva 26: Forward ja intercept off.

Lopulta sain ladattua php skriptini palvelimelle:



Vulnerability: File Upload

Choose an image to upload:

No file selected.

```
../../hackable/uploads/TESTITESTITESTITESTI.php succesfully uploaded!
```

Kuva 27: TESTI.php upload.