

Capstone

Challenge 1:

What is the password of Bob Smith's account? Answer: "password", username "smithy"

What is the name of file with the code? My_passwords.txt

What is the message contained in the file? Enter the code that you find in the file. Congratulations!

You found the flag for Challenge 1!

The code for this challenge is **8748wf8J**.

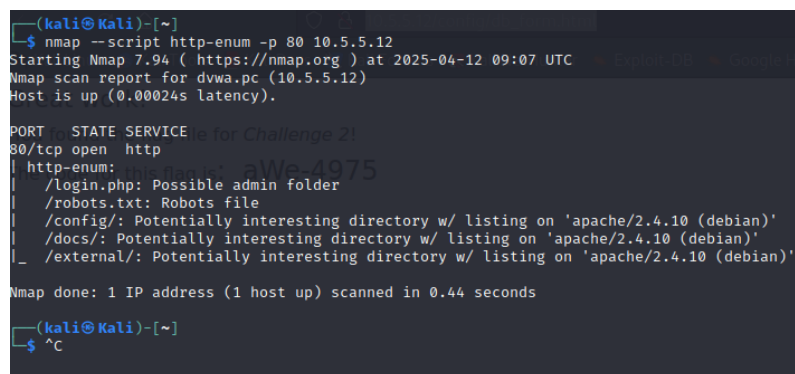
What are five remediation methods for preventing SQL injection exploits?

- Using prepared statements
- Error handling
- Input validation
- Stored procedures
- Least(or restrict) privileges for database permissions.

Challenge 2:

Which directories can be accessed through a web browser to list the files and subdirectories that they contain? /config/ , /docs/, /external/

I just add a sc here:



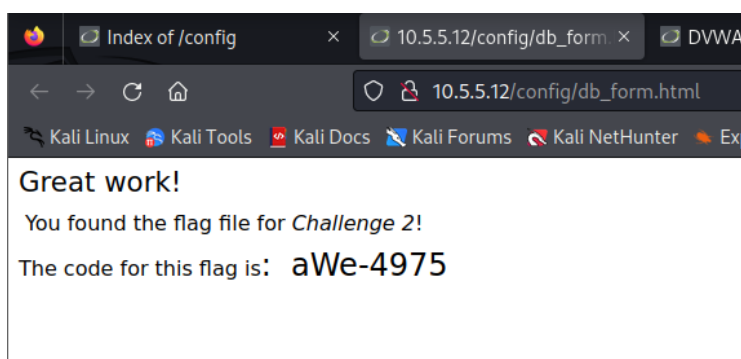
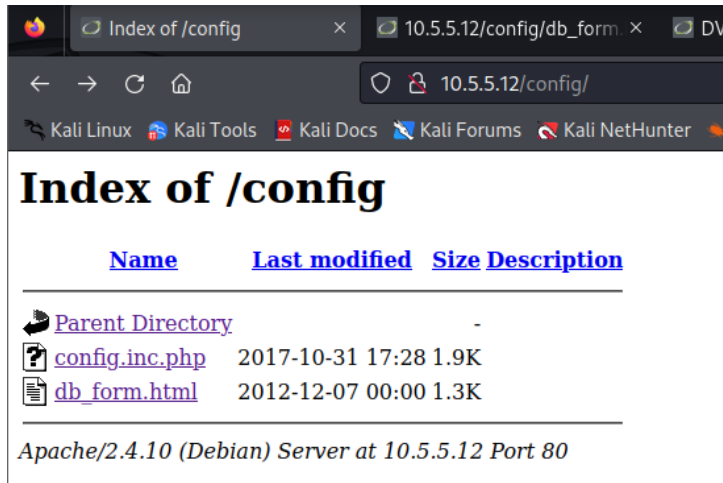
```
(kali@kali)-[~]
$ nmap --script http-enum -p 80 10.5.5.12
Starting Nmap 7.94 ( https://nmap.org ) at 2025-04-12 09:07 UTC
Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.00024s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|   /login.php: Possible admin folder
|   /robots.txt: Robots file
|   /config/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /docs/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /external/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

(kali@kali)-[~]
$ ^C
(kali@kali)-[~]
```

In which two subdirectories can you look for the file?

Answer here is /config/ and /external/. They were listed as potentially interesting directories.



Step 4: Answer: First i would disable directory listing in config and second adding a index.html to each folder.

Challenge 3:

Step 1:

```
Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.00026s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
```

Host here was 10.5.5.14. Other hosts were closed. I used basic nmap scan with port 139 and 445 as parameters.

Step 2:

What shares are listed on the SMB server? Which ones are accessible without a valid user login?

- Homes
- Workfiles
- Print@

- IPC\$

These were accessible without user login: workfiles and print\$

```
(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
```

Step 3: Investigate each shared directory to find the file.

```
(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. 6137648 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. 6137648 blocks available
smb: \OTHER\> cat sxij42.txt
cat: command not found
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (14.4 KiloBytes/sec) (average 14.4 KiloBytes/sec)
smb: \OTHER\>

File Actions Edit View Help
(kali@kali)-[~]
$ ls
Desktop Documents Downloads Music OTHER Pictures Public Templates Videos bobsmith_hash.txt sxij42.txt
(kali@kali)-[~]
$ cat sxij42.txt
Congratulations! bobsmith (a bobsmith) scanned in 9.78 seconds
You found the flag for Challenge 3!
The code for this challenge is NWS39691.
(kali@kali)-[~]
$
```

In which share is the file found? Print\$

What is the name of the file with Challenge 3 code? Sxij42.txt

Enter the code for Challenge 3 below: NWS39691

I searched for a while for this flag. I found the flag from "Printer Drivers" and there was one subdirectory(?) called "OTHER" so i had to check that out. I downloaded the .txt file to kali on used cat-command to reveal its content!

Step 4: Research and propose SMB attack remediation.

What are two remediation methods for preventing SMB servers from being accessed?

- Disable Smbv1
- Use strong authentication and access control(install security updates regularly)

Challenge 4:

Step1:

What is the IP address of the target computer? 10.5.5.11

What directories on the target are revealed in the PCAP?

- /test/
- /data/
- /includes/
- /passwords/

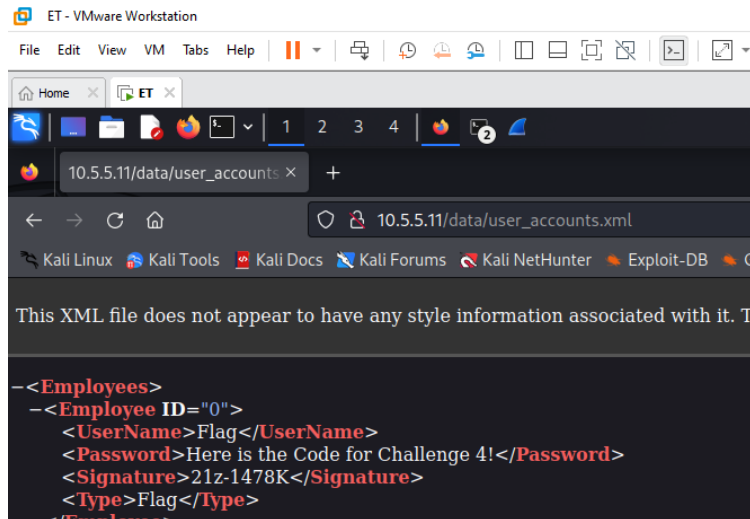
Step 2: Use a web browser to display the contents of the directories on the target computer.

Use a web browser to investigate the URLs listed in the Wireshark output. Find the file with the code for Challenge 4.

What is the URL of the file? 10.5.5.11/data/user_accounts.xml

What is the content of the file? Various usernames and passwords!

What is the code for Challenge 4? 21z-1478K



Step 3

What are two remediation methods that can prevent unauthorized persons from viewing the content of the files? Encryption protocols and maybe VPN? HTTPS insted of HTTP...