Capstone Project Report – Anmol Arora

Challenge 1: SQL injection

Step 1:

1. Login into DVWA with given user creds
2. Set security level to Low

A screenshot of a computer security

Description automatically generated

Step 2:

1. Identify table and check for sqli  
   A screenshot of a computer

   Description automatically generated
2. Use payloads to get info about table - <https://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>   
   ‘ UNION SELECT @@VERSION, NULL# - To get version details  
   ‘ UNION SELECT USER,PASSWORD FROM MYSQL.USER# - Gives logged in users rights to the table and shows passwords, apparently we are root  
   A screenshot of a computer

   Description automatically generated  
   But this isn’t what we want, we want bobs password, so more enumeration
3. First, we need to get database and table names and then columns!

A screen shot of a computer

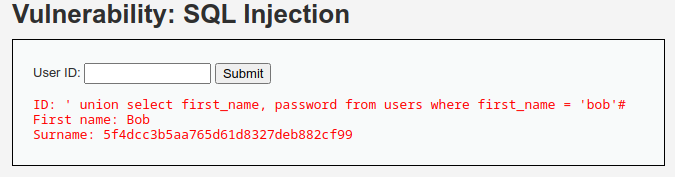
Description automatically generated  
' UNION SELECT NULL, TABLE\_NAME FROM INFORMATION\_SCHEMA.TABLES WHERE TABLE\_SCHEMA =’dvwa’#

Now we get columns from users table.

A screenshot of a computer

Description automatically generated

Finally, we get hash.

  
  
Cracking hash 5f4dcc3b5aa765d61d8327deb882cf99

A screenshot of a computer program

Description automatically generated

And username – smithy

Challenge 1 flag

A screenshot of a computer screen

Description automatically generated

Challenge 2: Web Server Vulnerability

A screenshot of a computer

Description automatically generated

The File inclusion directory has file1.php being referenced in the URL and simply changing that to /etc/passwd gives this.

But we don’t know where challenge 2 file is and I don’t like brute forcing so we upload reverse webshell.

Copy the php reverse shell, change port and ip and change url to

A screen shot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

We have shell, now to find code.

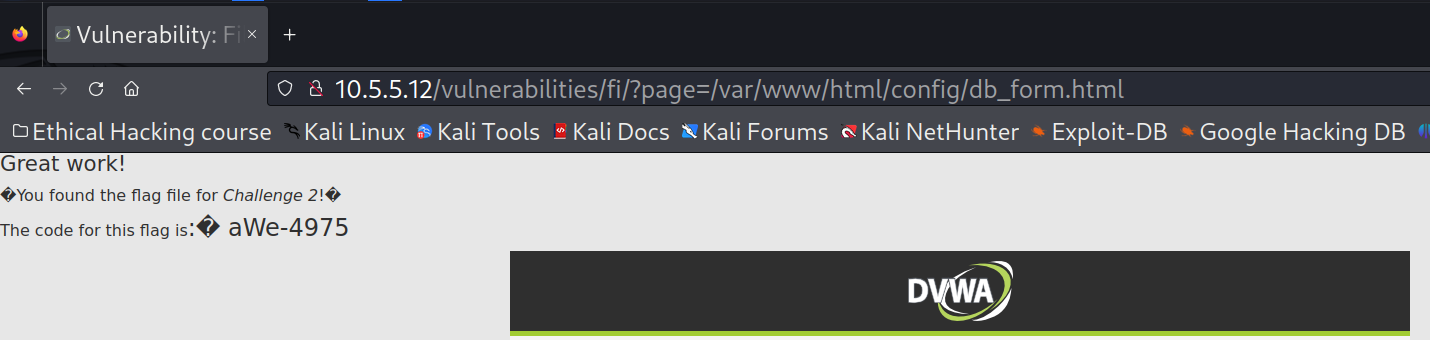
There is a flags dir and it has fi.pfp file which has some b64 code.

A screenshot of a computer

Description automatically generated  
ChatGPT to decode  
  
A screenshot of a computer

Description automatically generated  
  
Turns out there is a code after all, pop reverse shell again-> go to var/www/html and grep for Challenge  
  
A screenshot of a computer

Description automatically generated

Via WEB IS   
  


Code is aWe-4975

Challenge 3: SMB Vulnerability

Scan the range to see what hosts are up and we find one with 139 and 445 running services so that is the one with SMB.

A screenshot of a computer program

Description automatically generated

Available shares and permissions

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated  
  
The file is in OTHER is called sxij42.txt

Code is: NWs39691

Challenge 4:

From the pcap file we see target is 10.5.5.11

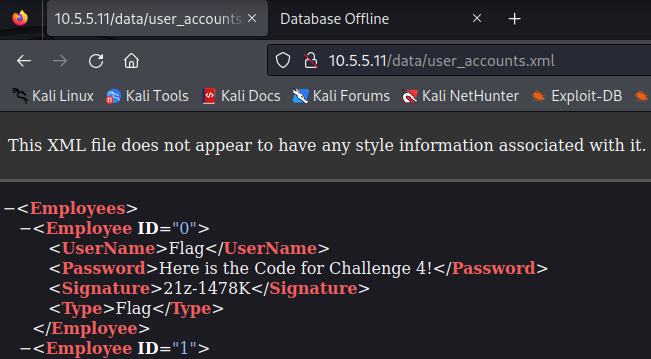
Directories that are available in capture are - testoutput

Exporting all the files from http we can see theres only 2 big files

A screenshot of a computer

Description automatically generated  
  
None of these files seem to have any Challenge codes.

Turns out my VM had some issues, imported it again and 10.5.5.11 now has a running web server.



Code: 21z-1478K