Final Capstone Activity

# 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.

# 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 and 192.168.0.0/24 networks.

# Required Resources

* Kali VM customized for the Ethical Hacker course

# Instructions

## Challenge 1: SQL Injection

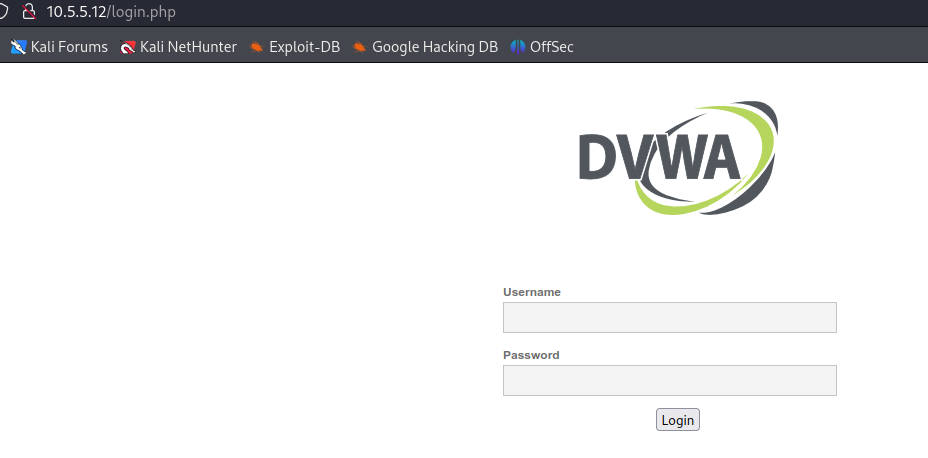
**Total points: 25**

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 with Challenge 1 code and use **Bob Smith's** account credentials to open the file at 192.168.0.10 to view its contents.

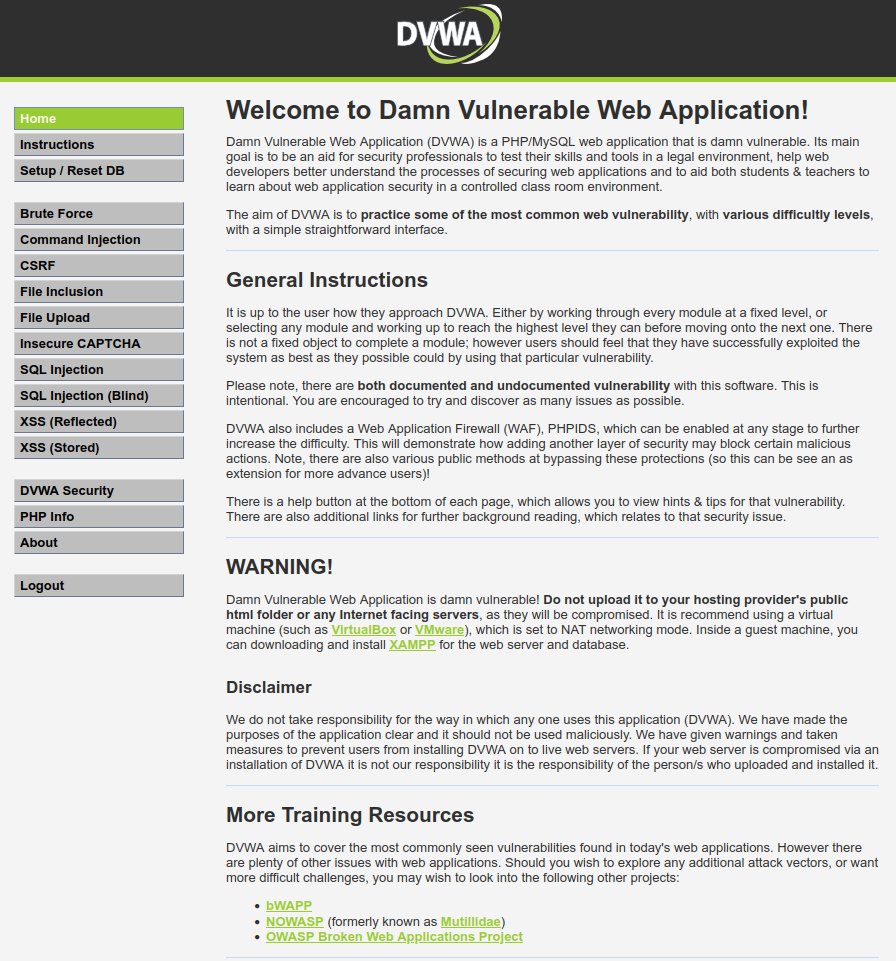
### Preliminary setup

* + - 1. Open a browser and go to the website at 10.5.5.12.

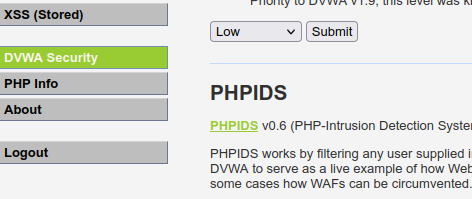
**Note:** If you have problems reaching the website, remove the https:// prefix from the IP address in the browser address field.



* + - 1. Login with the credentials **admin / password**.

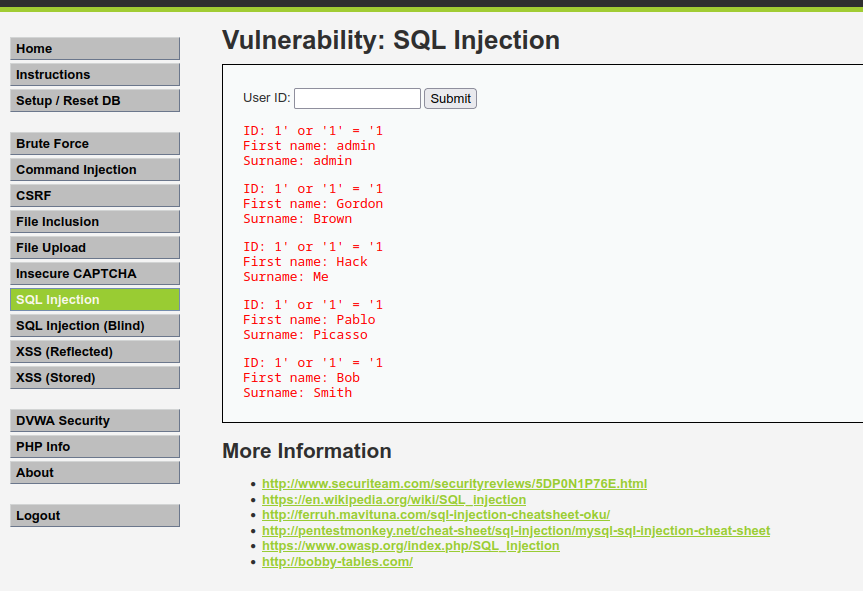


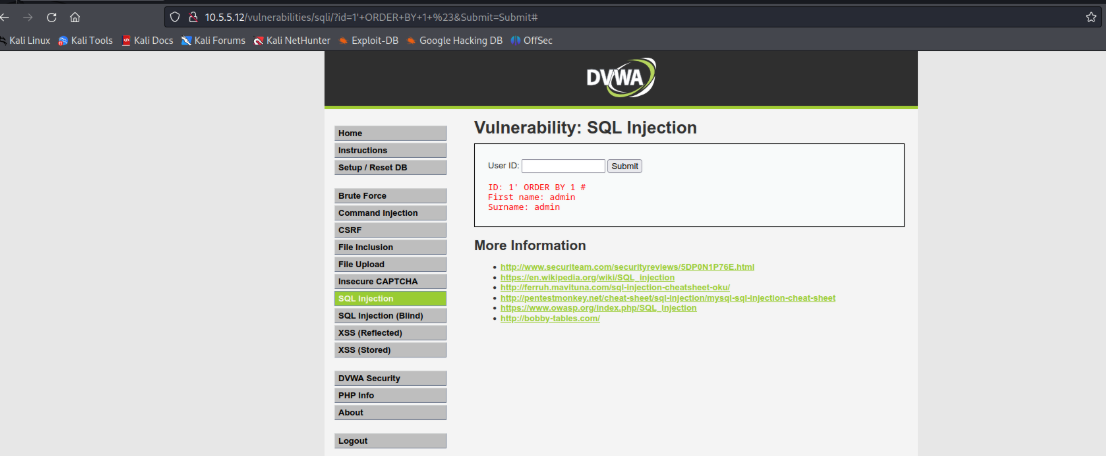
* + - 1. Set the DVWA security level to **low** and click **Submit**.



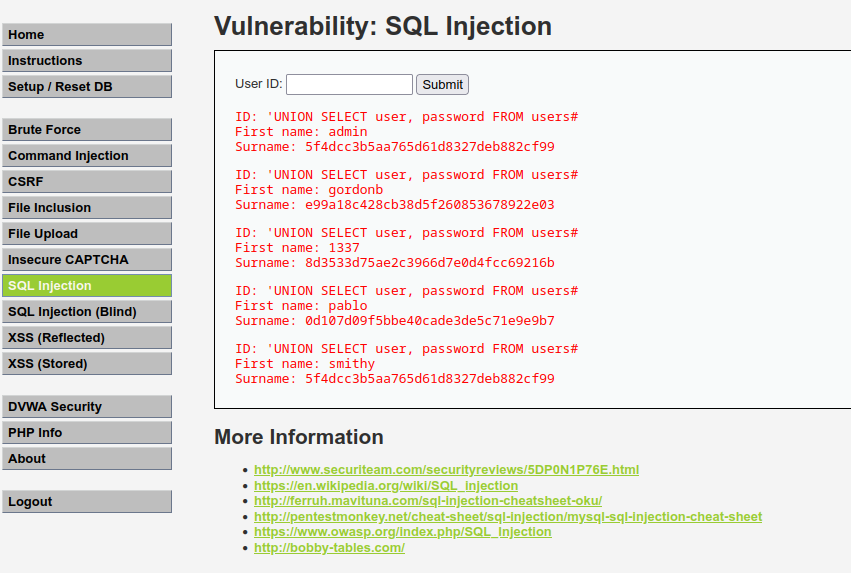
### Retrieve the user credentials for the Bob Smith’s account.

* + - 1. Identify the table that contains usernames and passwords.





* + - 1. Locate a vulnerable input form that will allow you to inject SQL commands.

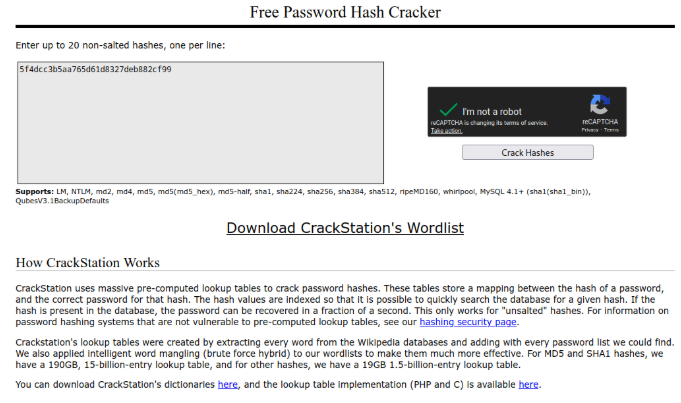


* + - 1. Retrieve the username and the password hash for **Bob Smith's** account.



### Crack Bob Smith’s account password.

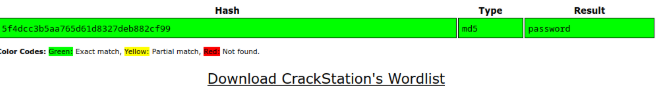
Use any password hash cracking tool desired to crack **Bob Smith**’s password.



#### Question

What is the password of **Bob Smith’s** account?

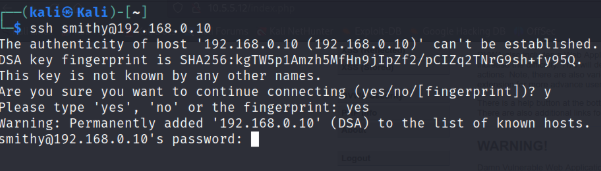
Password

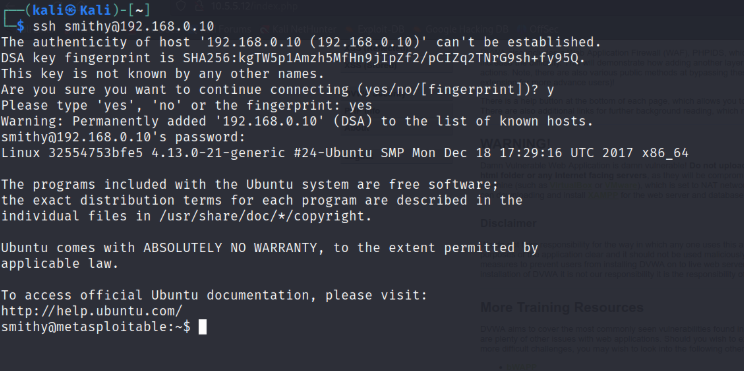


Pe your answers here.

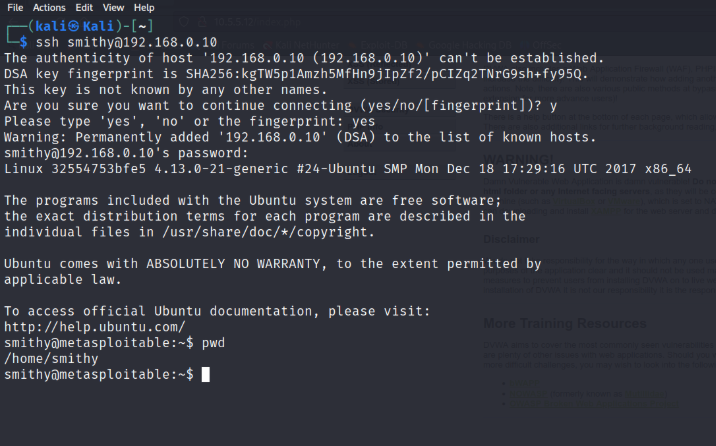
### Locate and open the file with Challenge 1 code.

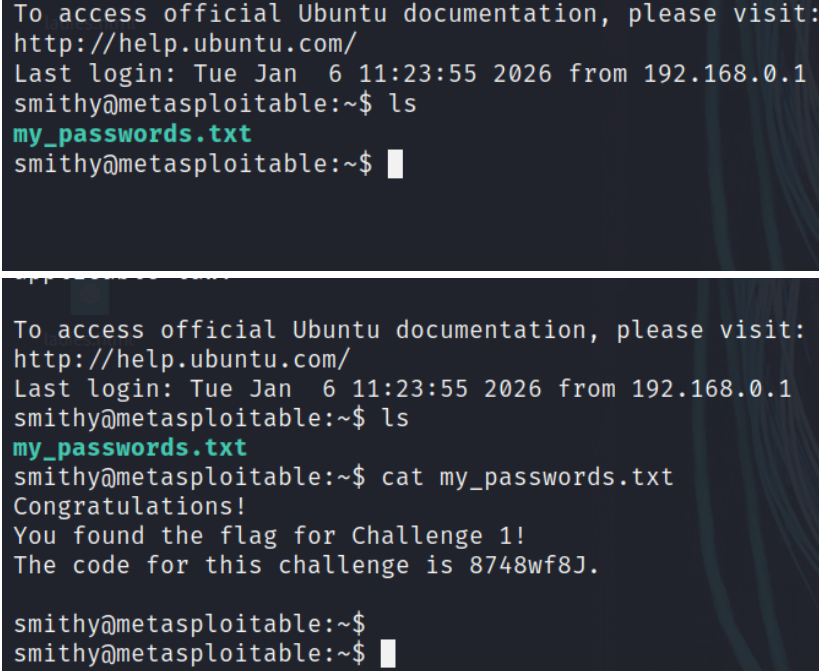
* + - 1. Log into **192.168.0.10** as **Bob Smith**.
* Use ssh
* ssh <username>@<ip address> then enter the password for the user





* + - 1. Locate and open the flag file in the user's home directory.





#### Question

What is the name of the file with the code?

my\_passwords.txt

Type your answers here.

#### Question

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.

Five remediation methods for preventing SQL injection exploits:

1. Install the latest software and security patches from vendors when available

2. Validate all input before it reaches your database

3. Give accounts that connect to the SQL database only the minimum privileges needed.

4. Use a Web Application Firewall (WAF)

5. Use parameterized queries or prepared statements

Type your answers here.

### Research and propose SQL attack remediation

#### Question

What are five remediation methods for preventing SQL injection exploits?

 **Use parameterized queries (prepared statements)**

* Separate SQL code from user input so inputs are treated strictly as data, not executable SQL.

 **Input validation and sanitization**

* Validate input using allow-lists (e.g., expected formats, lengths, types) and reject unexpected characters.

 **Use stored procedures (securely written)**

* Stored procedures that do not build dynamic SQL reduce injection risk when parameters are properly handled.

 **Apply least-privilege database access**

* Ensure application database accounts have only the minimum permissions required (e.g., no DROP or ALTER rights).

 **Escape user input and use ORM frameworks**

* Proper escaping or using Object-Relational Mapping (ORM) tools helps prevent malicious SQL from executing.

Type your answers here.

## Challenge 2: Web Server Vulnerabilities

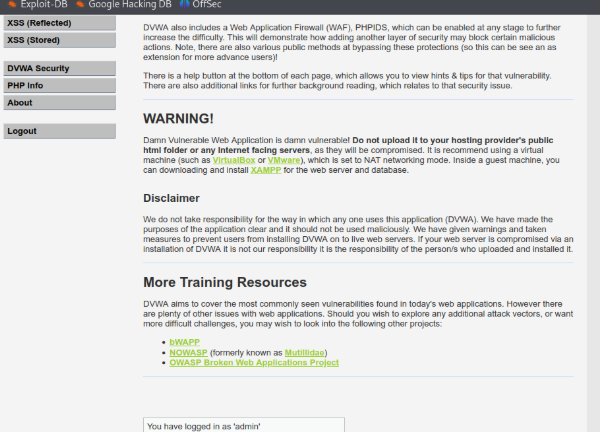
**Total points: 25**

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.

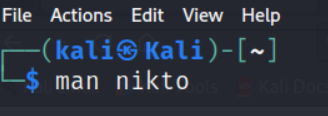
### Preliminary setup

1. If not already, log into the server at 10.5.5.12 with the **admin / password** credentials.
2. Set the application security level to low.

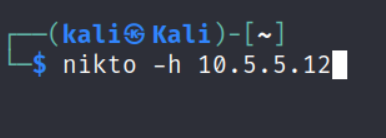


### From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation.

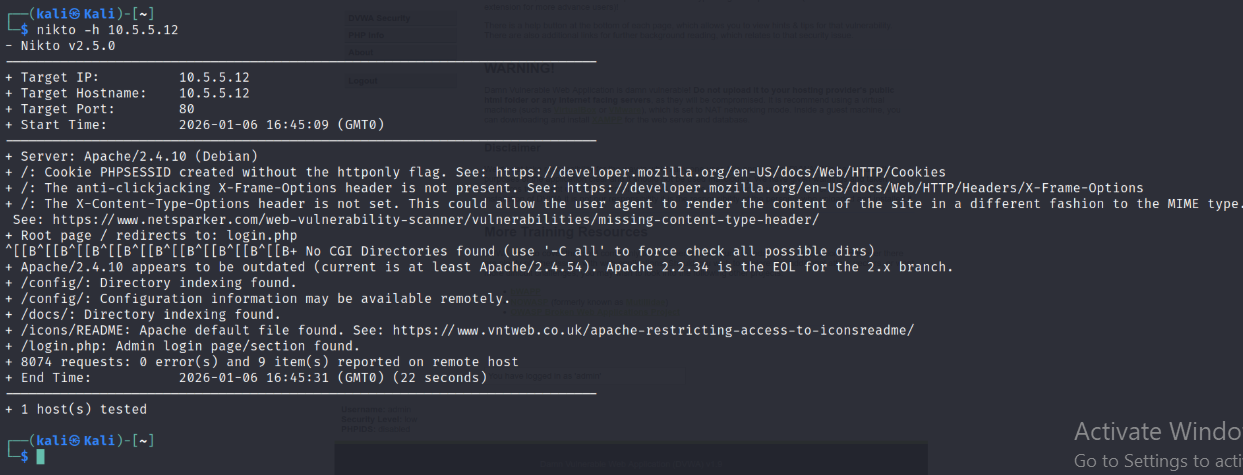
Perform reconnaissance on the server to find directories where indexing was found.







Scanning



#### Question

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

/config/: Directory indexing found.

+ /config/: Configuration information may be available remotely.

+ /docs/: Directory indexing found.

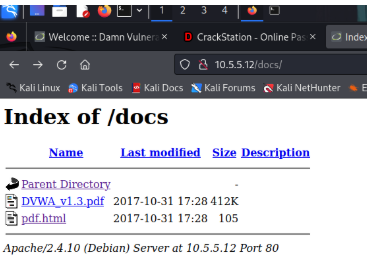
+ /icons/README: Apache default file found. See: <https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/>

+ /login.php: Admin login page/section found.

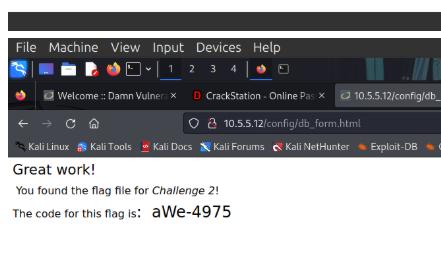
### View the files contained in each directory to find the db\_form.html file.

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.

Address path 10.5.5.12







#### Questions

In which two subdirectories can you look for the file? (‘/config’ or ‘/docs’

T’/c

A

A

A

address path 10.5.5.12ype your answers here.

What is the filename with the Challenge 2 code? - db\_form.html

Type your answers here.

Which subdirectory held the file? - /config

Type your answers here.

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

Great work

You found the flaf file for challenge 2

The code flag is: aWe-4975

Type your answers here.

### Research and propose directory listing exploit remediation.

#### Question:

What are two remediation methods for preventing directory listing exploits? (Disable directroy listing on the web server and implement proper access controls/permissions

Tykkkpe your answers here.

Answers may vary but include: Configure your web server to prevent directory listings for all paths beneath the web root. Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing.

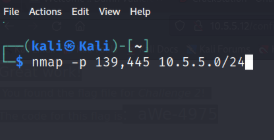
## Challenge 3: Exploit open SMB Server Shares

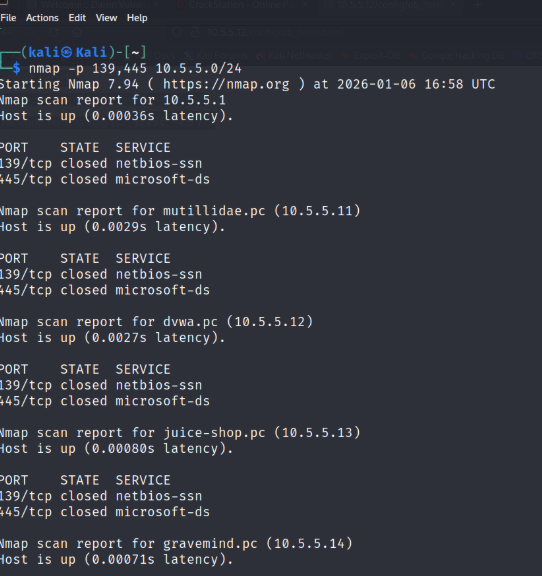
**Total points: 25**

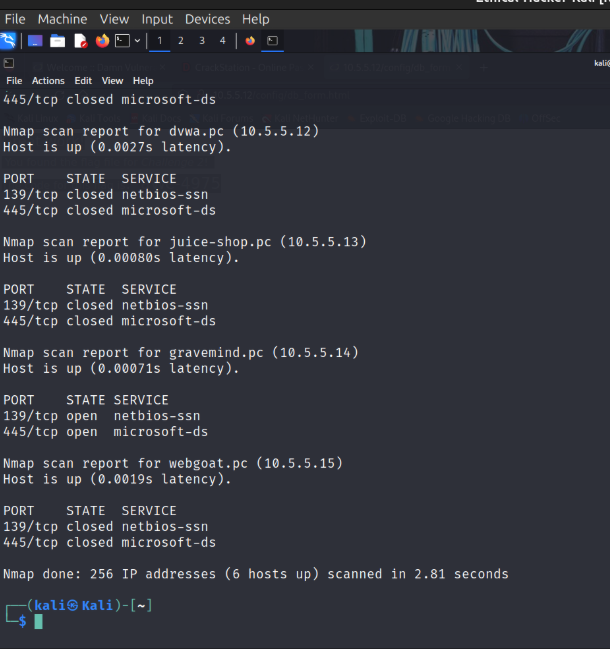
In this part, you want to discover if there are any unsecured shared directories located on an SMB server in the 10.5.5.0/24 network. You can use any of the tools you learned in earlier labs to find the drive shares available on the servers.

### Scan for potential targets running SMB.

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







#### Question

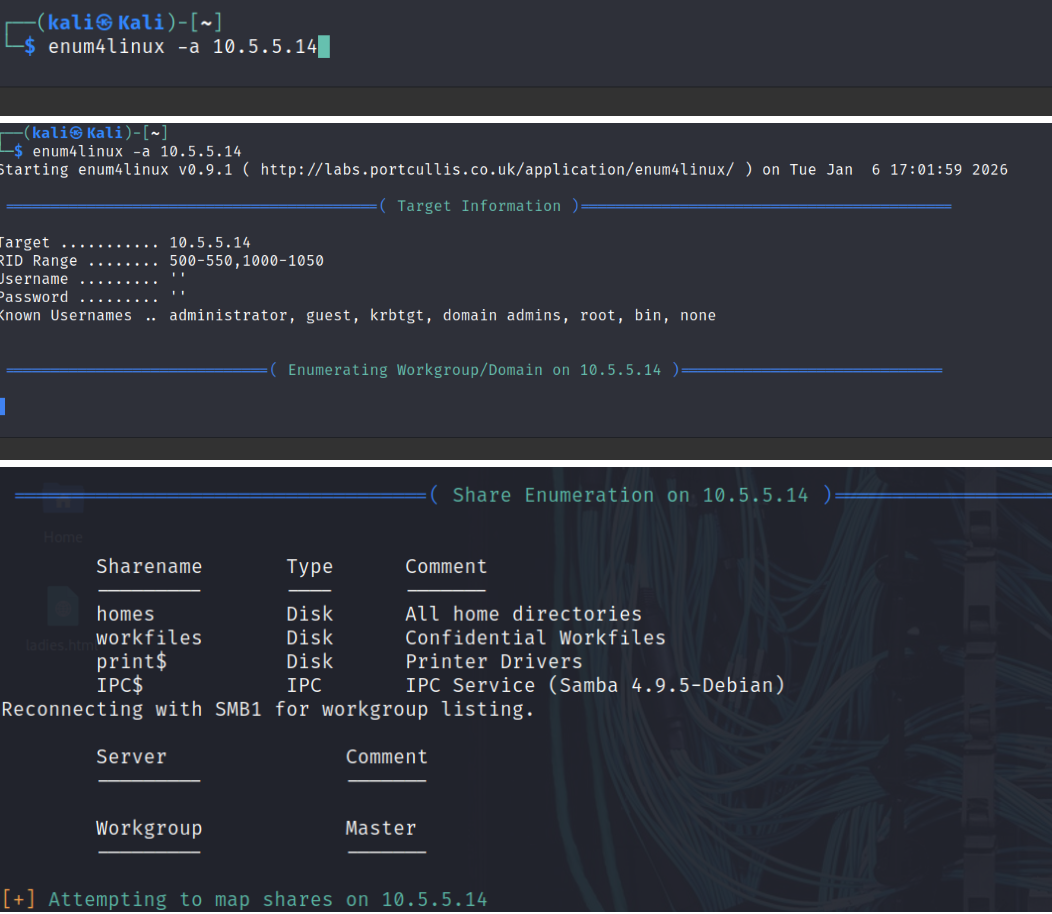
Which host on the 10.5.5.0/24 network has open ports indicating it is likely running SMB services? -10.5.5.14

Type your answers here.

### 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.

Enum4linux Tool



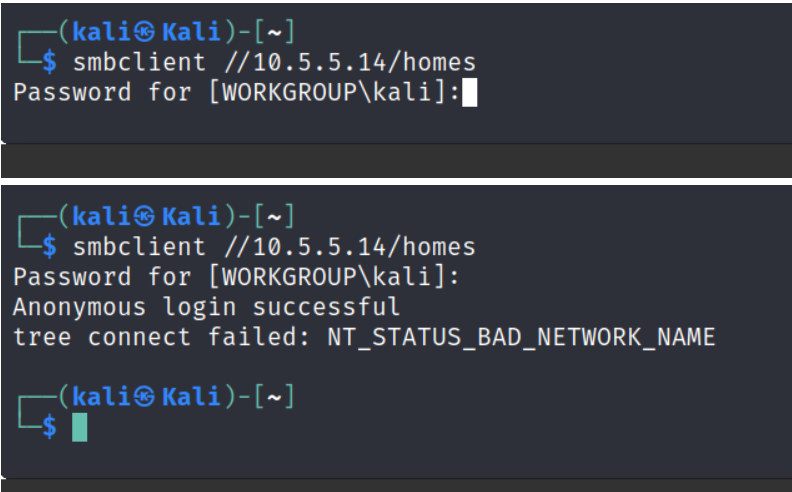
#### Question

What shares are listed on the SMB server? Which ones are accessible without a valid user login? – (home disk all directories, workfiles disk confidential workfiles, print$ disk printer drivers,IPC$ IPC IPC Service (Samba 4.9.5- Debian)

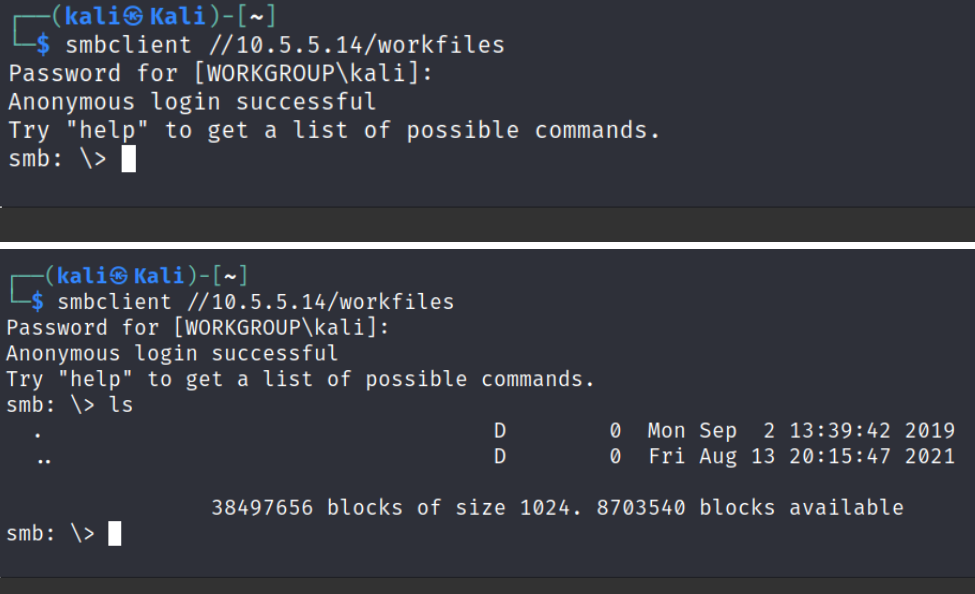
Type your answers here.

### Investigate each shared directory to find the file.

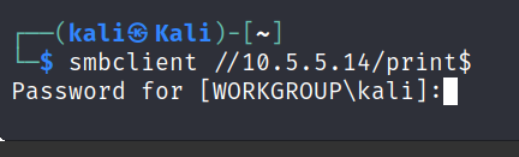
Use the SMB-native client to access the drive shares on the SMB server. Use the dir, ls, cd, and other commands to find subdirectories and files.



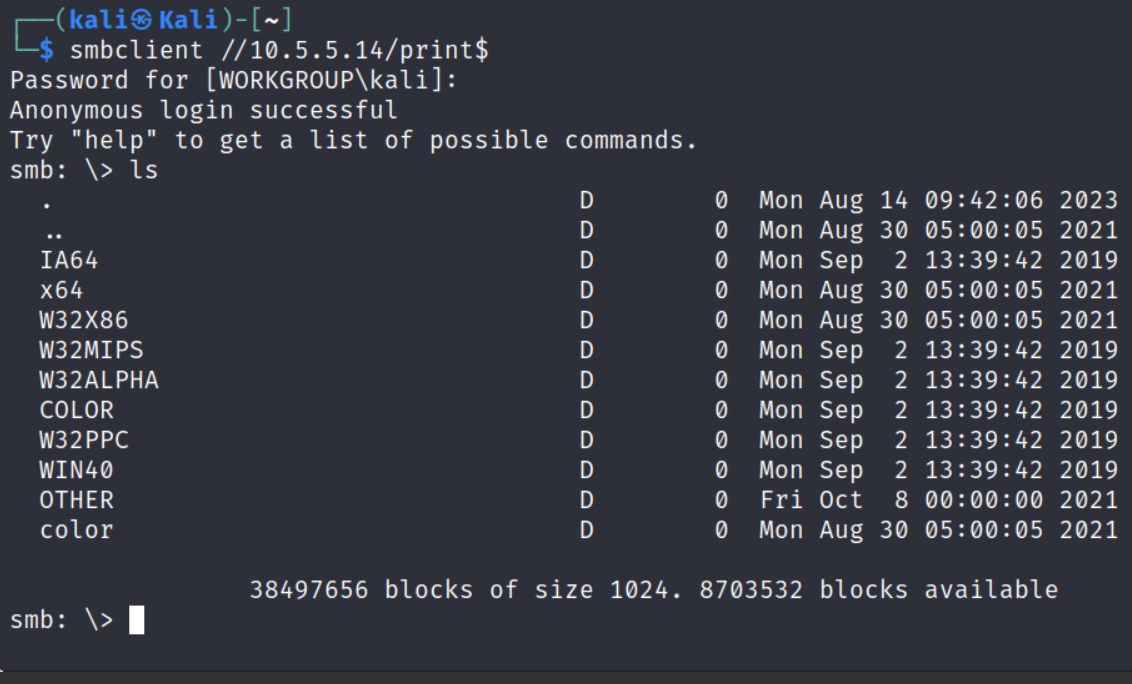
/workfiles



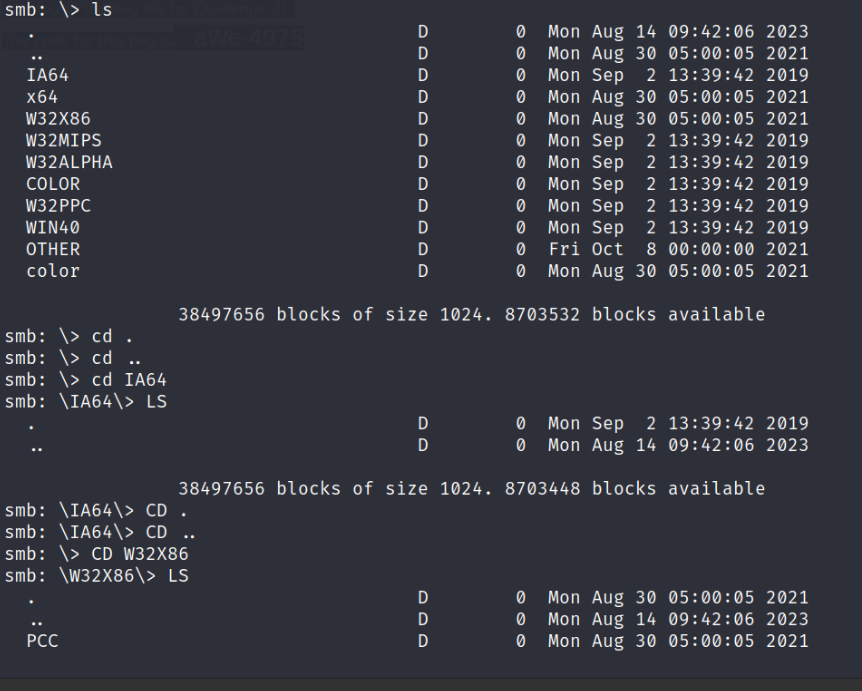
/print$

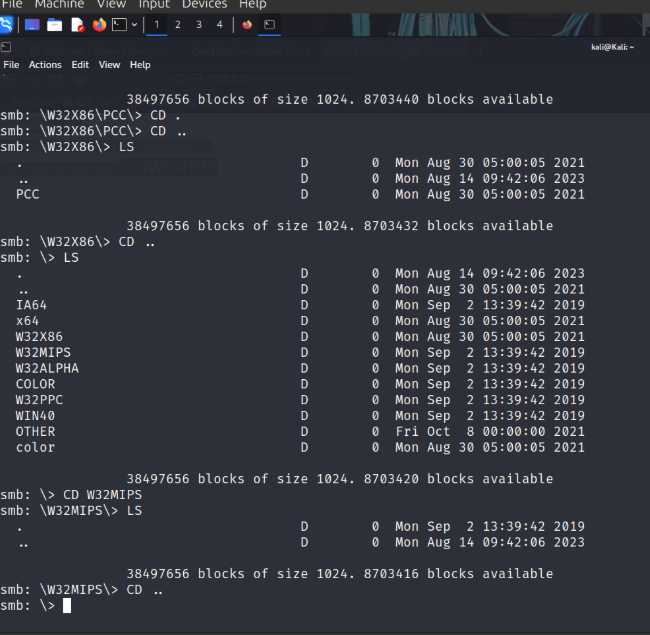


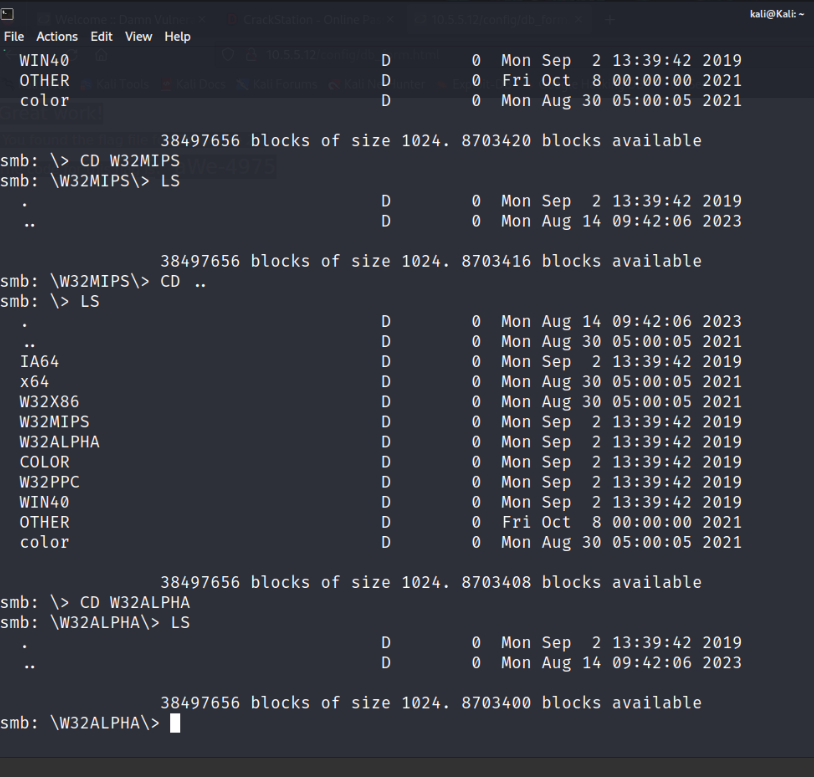
List of directories and results



Checking the directories







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

#### Questions

In which share is the file found?

Print$

Type your answers here.

What is the name of the file with Challenge 3 code?

sxij42.txt

Type your answers here.

Enter the code for Challenge 3 below.

Congratulations!

You found the flag for Challenge 3!

The code for this challenge is NWs39691.

Type your answers here.

### Research and propose SMB attack remediation.

#### Question

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

* Restrict SMB access using firewalls and network segmentation
* Enforce strong authentication and disable insecure SMB versions

Type your answers here.

## Challenge 4: Analyze a .pcap file to find information.

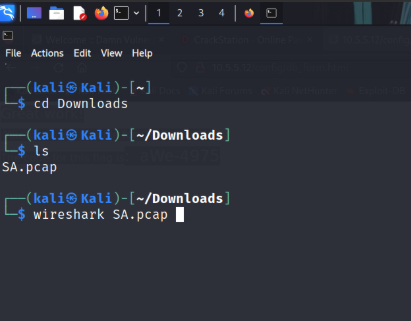
**Total Points**: **25**

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.

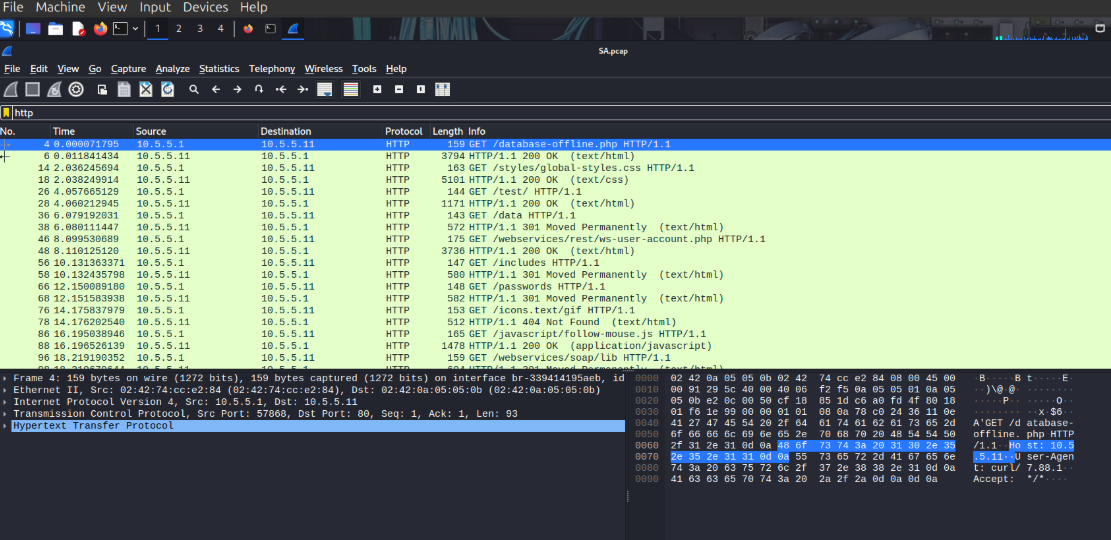
### Find and analyze the SA.pcap file.

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

* Open wireshark



Filter traffic



#### Question

What is the IP address of the target computer? -10.5.5.11

Type your answers here.

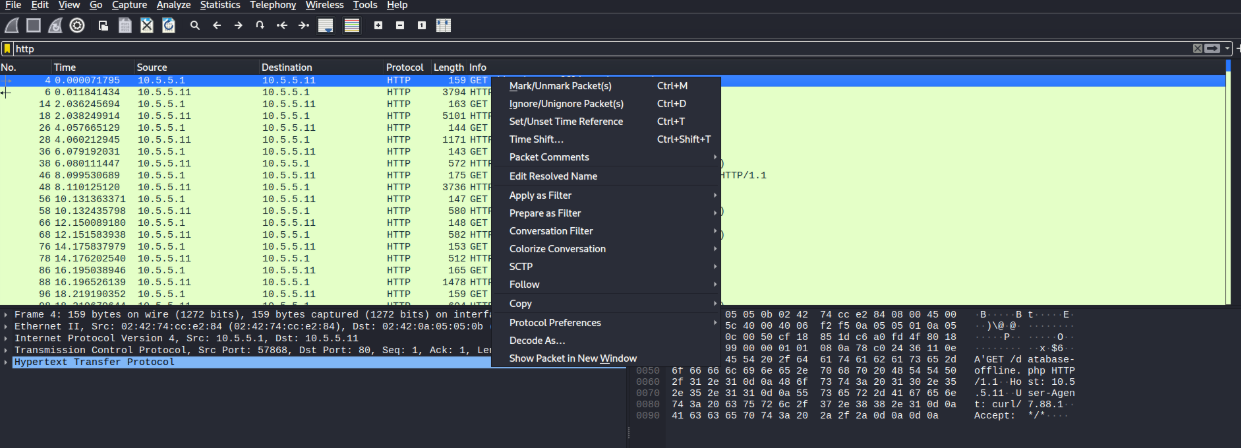
* What directories on the target are revealed in the PCAP?
* /database-offline.php
* /styles/global-styles.css
* /test/HTTP/1.1
* /webservices/rest/ws-user-account.php
* /data

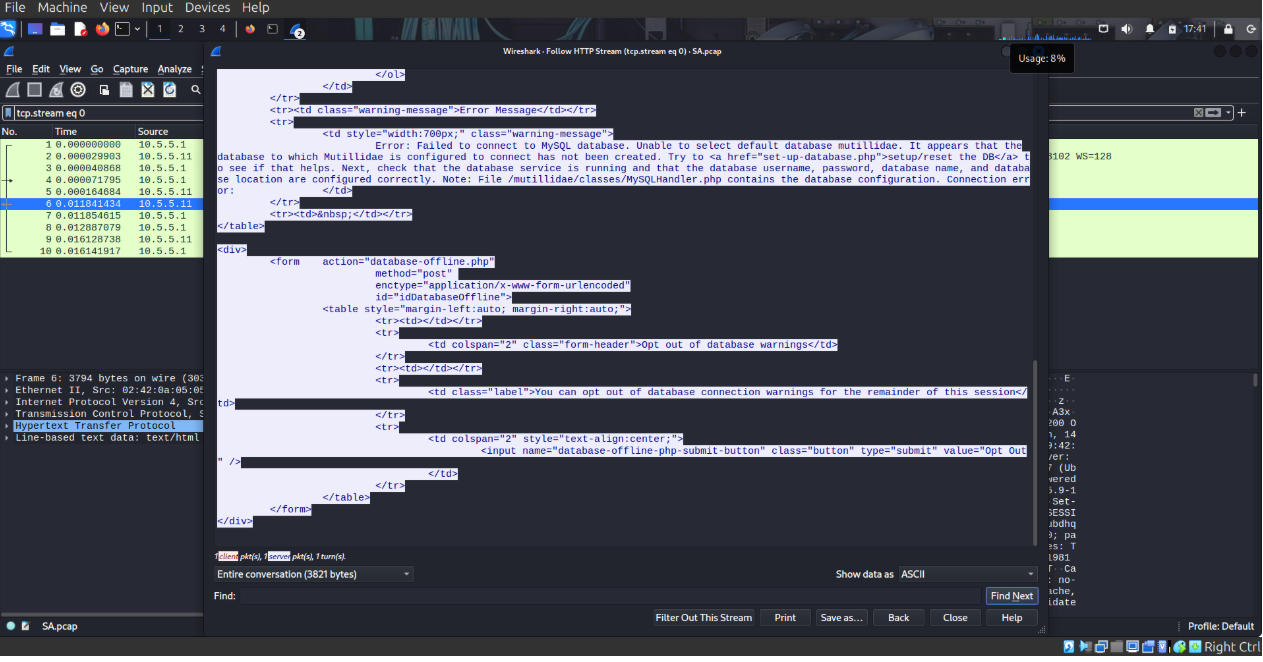
Type your answers here.

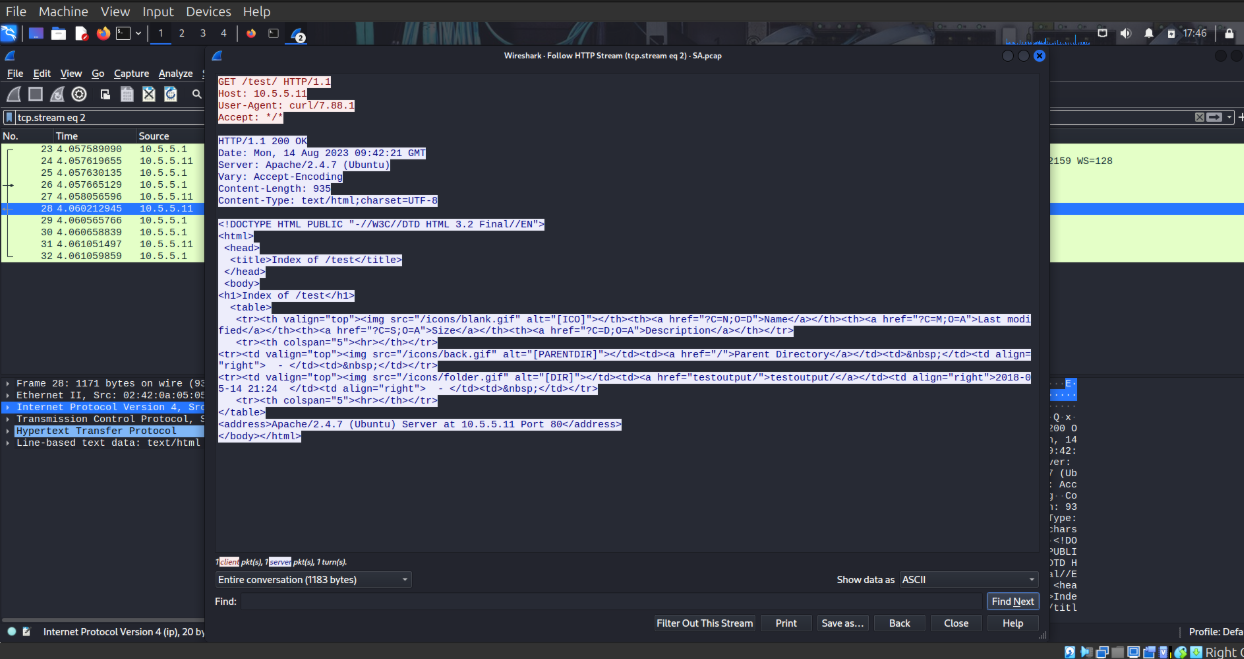
### Use a web browser to display the contents of the directories on the target computer.

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

Right click traffic and click follow > http stream







#### Questions

What is the URL of the file?

<http://10.5.5.11/data>

Type your answers here.

What is the content of the file? - <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>

<Type>Admin</Type>

</Employee>

<Employee ID="6">

<UserName>samurai</UserName>

<Password>samurai</Password>

<Signature>Carving fools</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="7">

<UserName>jim</UserName>

<Password>password</Password>

<Signature>Rome is burning</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="8">

<UserName>bobby</UserName>

<Password>password</Password>

<Signature>Hank is my dad</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="9">

<UserName>simba</UserName>

<Password>password</Password>

<Signature>I am a super-cat</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="10">

<UserName>dreveil</UserName>

<Password>password</Password>

<Signature>Preparation H</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="11">

<UserName>scotty</UserName>

<Password>password</Password>

<Signature>Scotty do</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="12">

<UserName>cal</UserName>

<Password>password</Password>

<Signature>C-A-T-S Cats Cats Cats</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="13">

<UserName>john</UserName>

<Password>password</Password>

<Signature>Do the Duggie!</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="14">

<UserName>kevin</UserName>

<Password>42</Password>

<Signature>Doug Adams rocks</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="15">

<UserName>dave</UserName>

<Password>set</Password>

<Signature>Bet on S.E.T. FTW</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="16">

<UserName>patches</UserName>

<Password>tortoise</Password>

<Signature>meow</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="17">

<UserName>rocky</UserName>

<Password>stripes</Password>

<Signature>treats?</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="18">

<UserName>tim</UserName>

<Password>lanmaster53</Password>

<Signature>Because reconnaissance is hard to spell</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="19">

<UserName>ABaker</UserName>

<Password>SoSecret</Password>

<Signature>Muffin tops only</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="20">

<UserName>PPan</UserName>

<Password>NotTelling</Password>

<Signature>Where is Tinker?</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="21">

<UserName>CHook</UserName>

<Password>JollyRoger</Password>

<Signature>Gator-hater</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="22">

<UserName>james</UserName>

<Password>i<3devs</Password>

<Signature>Occupation: Researcher</Signature>

<Type>Admin</Type>

</Employee>

<Employee ID="23">

<UserName>ed</UserName>

<Password>pentest</Password>

<Signature>Commandline KungFu anyone?</Signature>

<Type>Admin</Type>

</Employee>

</Employees>

What is the code for Challenge 4?

21z-1478K

asaTygggpe your answers here.

Tyhhhhhhhpe your answers here.

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

Further examine the capture file. The contents of the files are transmitted in clear text and can be viewed in Wireshark.

#### Question

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

Proper access control

Encryption

Type your answers here.

Congratulations! You have completed the skills assessment.