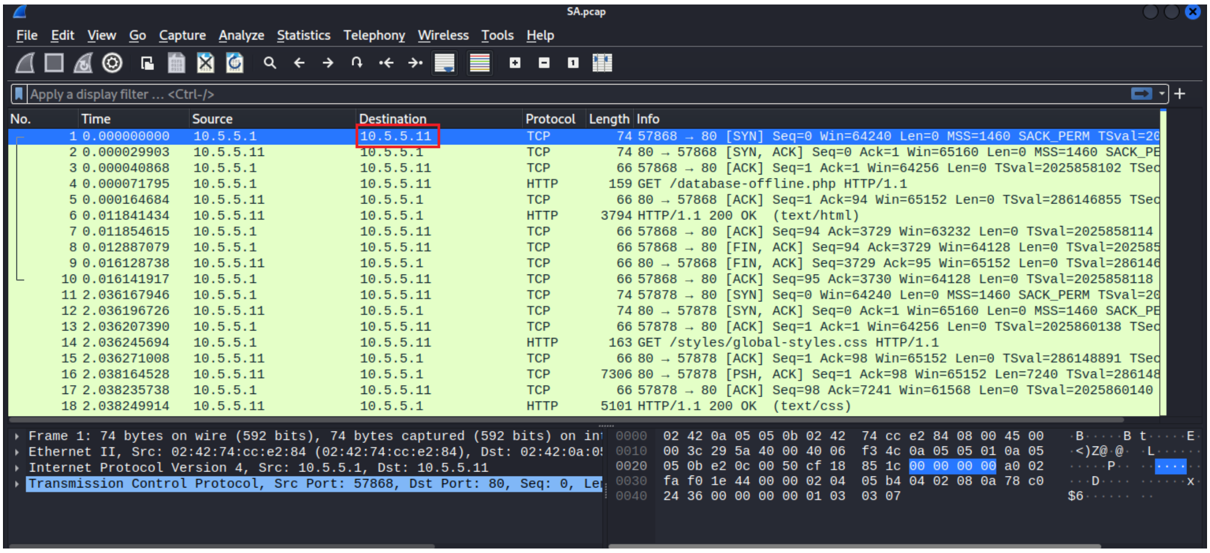
Challenge 4: Analyze a PCAP File to Find Information


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
```

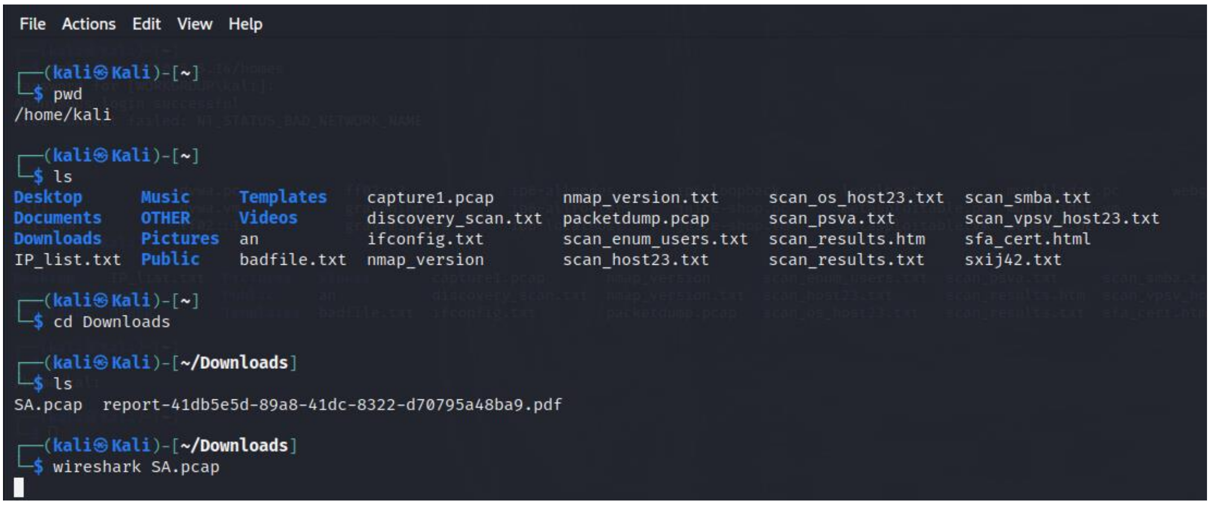
```
0000  02 42 0a 05 05 0b 02 42  74 cc e2 84 08 00 45 00   ·B·····B t·····E·
0010  00 3c 29 5a 40 00 40 06  f3 4c 0a 05 05 01 0a 05   ·<)Z@·@· ·L······
0020  05 0b e2 0c 00 50 cf 18  85 1c 00 00 00 00 a0 02   ·····P·· ········
0030  fa f0 1e 44 00 00 02 04  05 b4 04 02 08 0a 78 c0   ···D···· ······x·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

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.

Challenge 4: Analyze a Wireshark Capture File to Find The Location of A File Containing Flag Iinformation

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

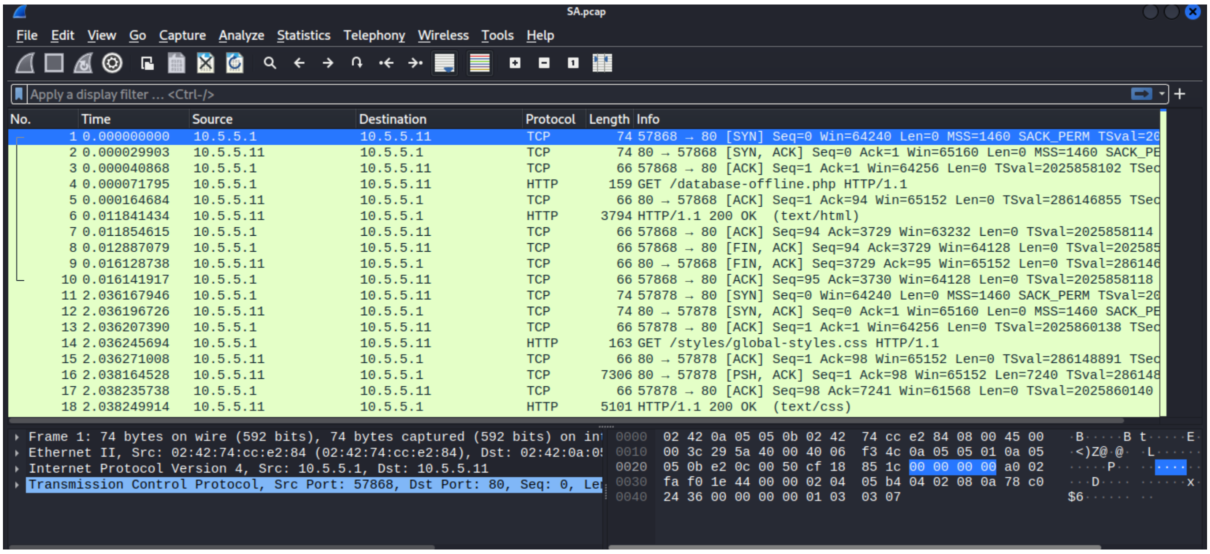
Analyze the content of the PCAP file to determine the IP address of the target computer and the URL location of the file with the Challenge 4 code.



```
┌──(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-/>

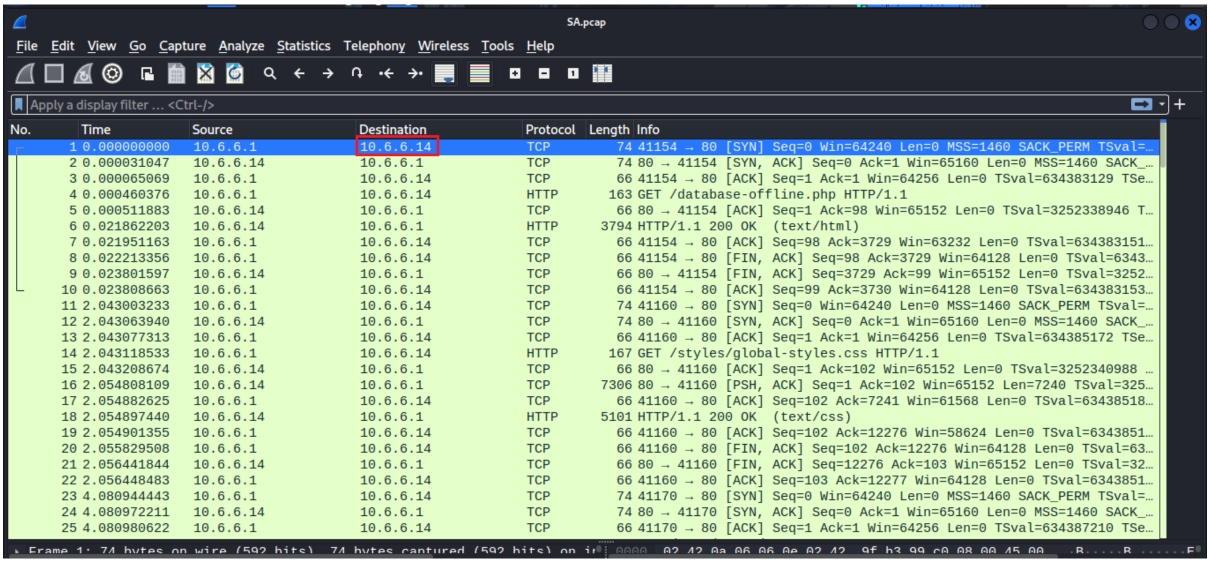
```
No.  Time        Source      Destination  Protocol Length Info
   1 0.000000000 10.5.5.1    10.5.5.11    TCP        74 57868 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=20
   2 0.000029903 10.5.5.11   10.5.5.1     TCP        74 80 → 57868 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 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

Challenge 4: Analyze a Wireshark Capture File to Find The Location of A File Containing Flag Iinformation


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 i   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?

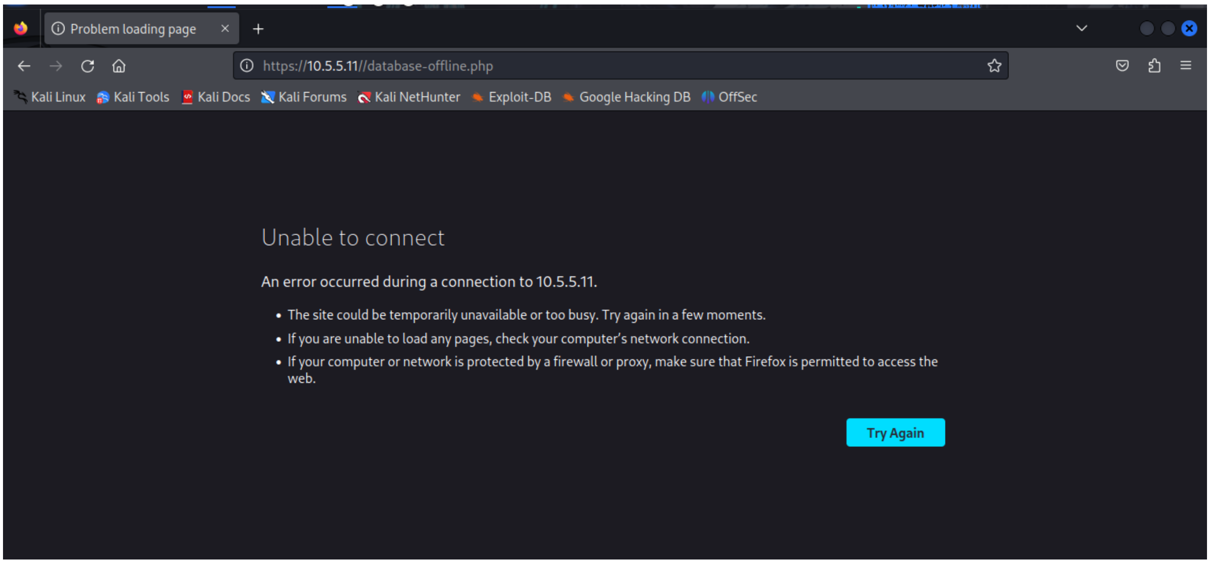
The directories on the target revealed in the PCAPs are

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

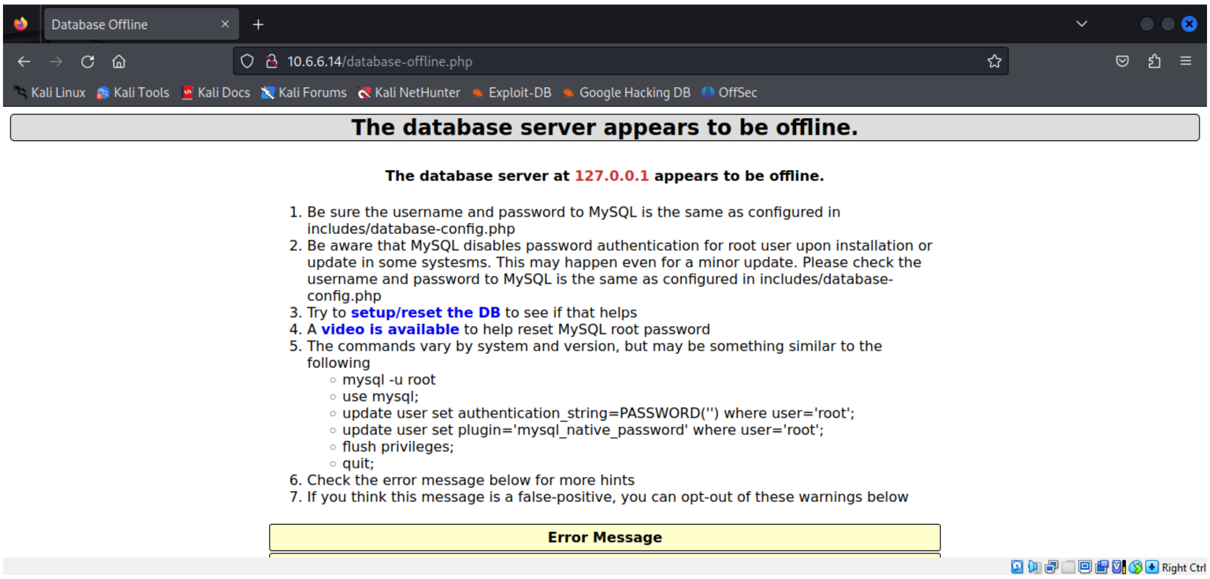


Unable to connect

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.

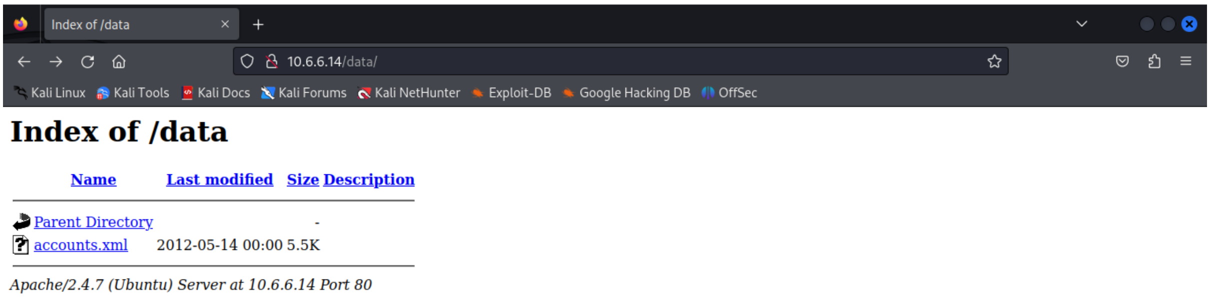
The database server at 127.0.0.1 appears to be offline.

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

Challenge 4: Analyze a Wireshark Capture File to Find The Location of A File Containing Flag Iinformation

10.6.6.14/data

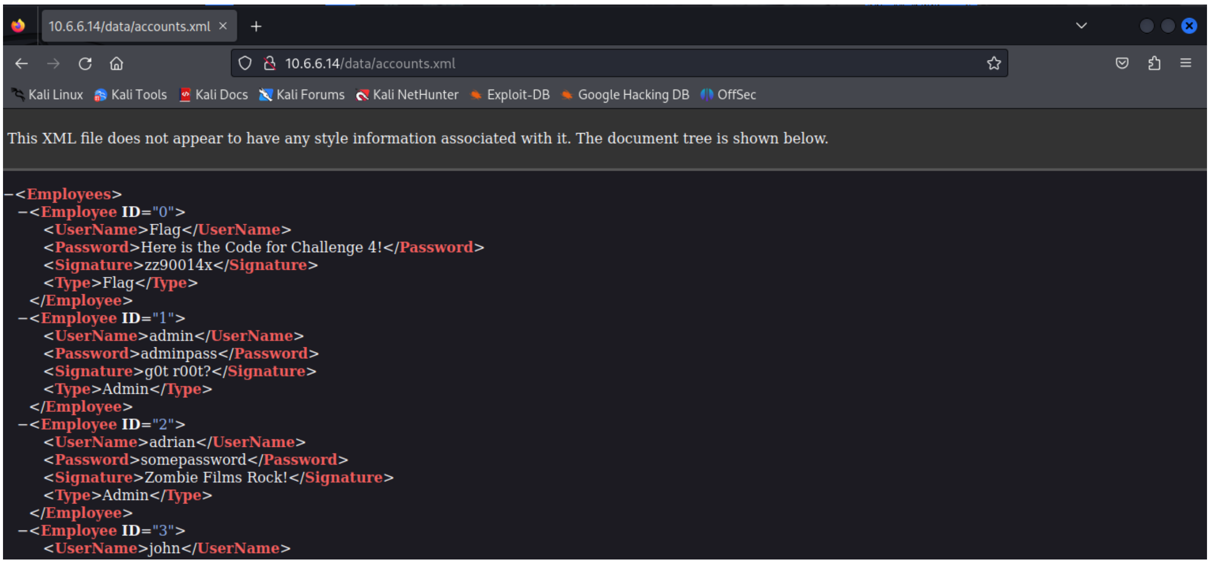


Index of /data

```
     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