Branden Barnes

Professor Shobha Vatsa CYSE 450

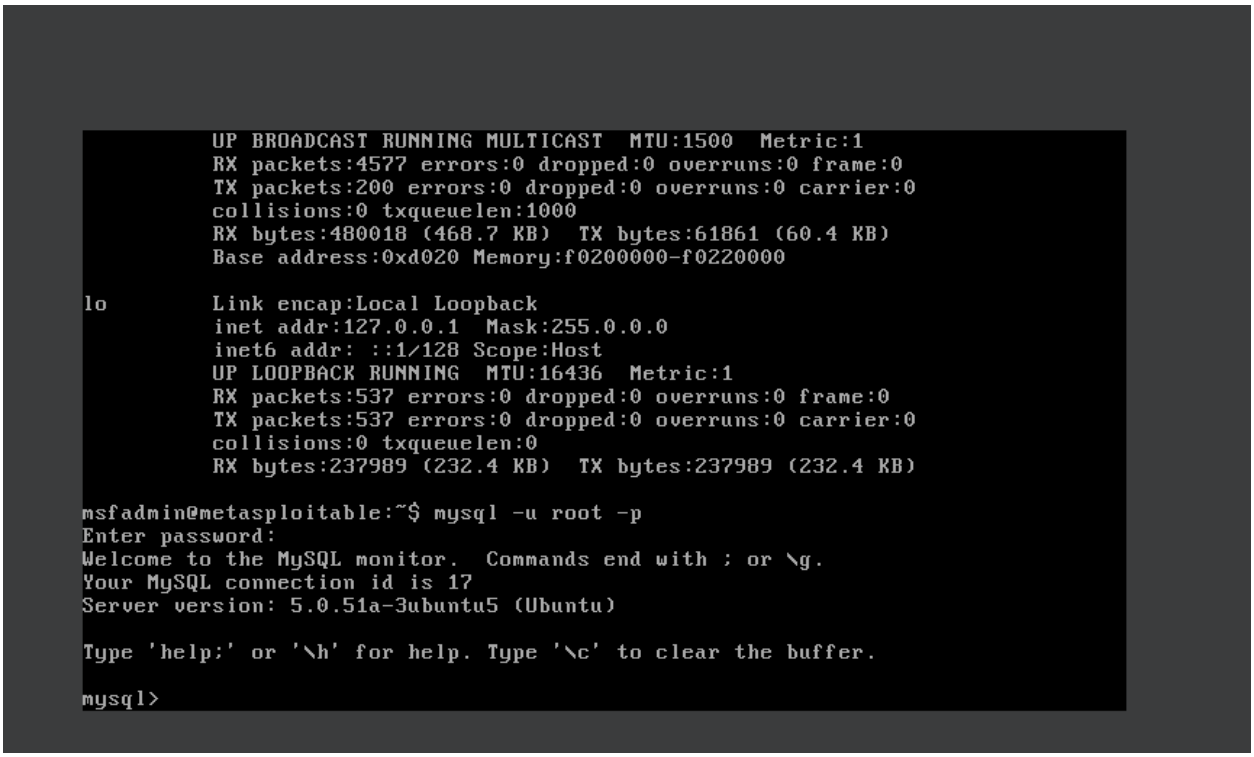
Assignment 9

In this lab, you will understand how to test a web application for SQL injection. You will learn how to execute error-based and UNION-based SQL injection using Burp Suite.

SQL injection is one of the most common web-based attack which is used to execute malicious SQL statements.
This exercise requires Metasploitabl2 VM.

Task A: Get Familiar with SQL statements.

1. Login to metasploitable2 VM.
2. Login to MySQL as root.



3. Execute SQL query to retrieve the database available in Metasploitable2 VM.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

mysql> _
```

4. Execute SQL query, use dvwa; (to select dvwa database.)
5. Execute SQL query to retrieve the available tables in dvwa database.

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

mysql> use dvwa;
Database changed
mysql> show tables;
+-----------------+
| Tables_in_dvwa  |
+-----------------+
| guestbook       |
| users           |
+-----------------+
2 rows in set (0.00 sec)

mysql>
```

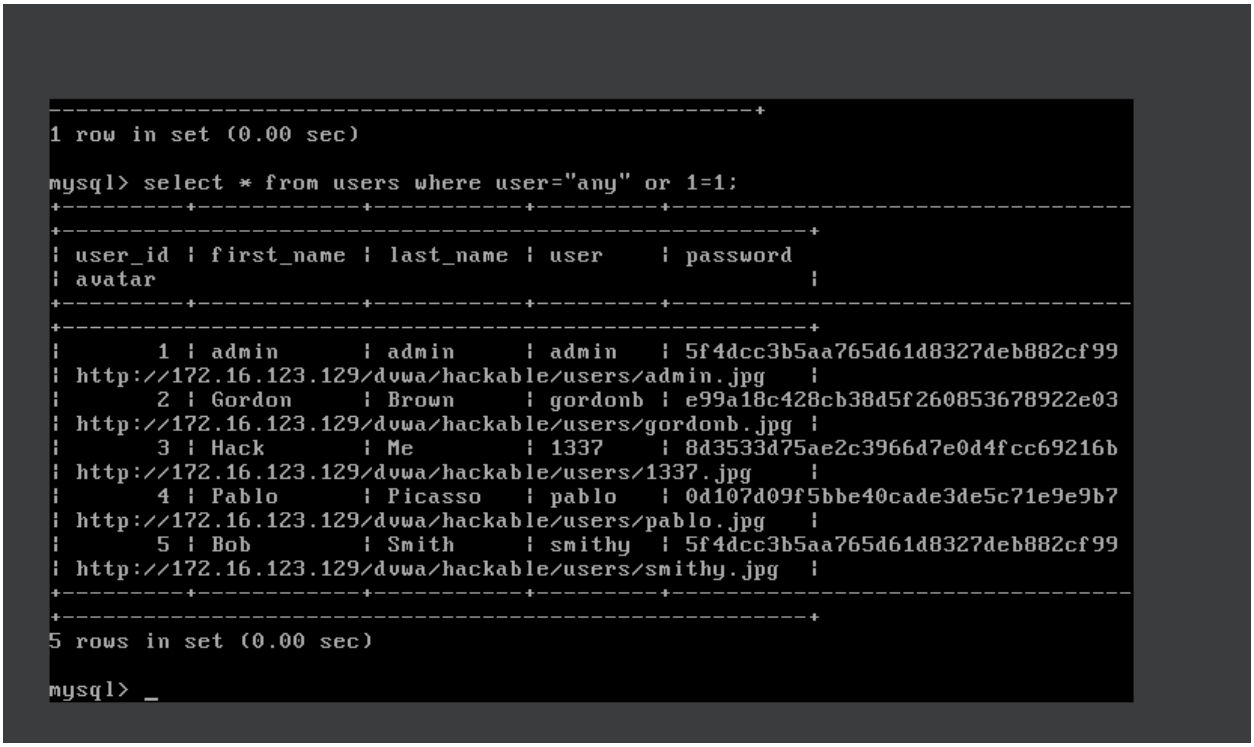
6. Execute the SQL query, SELECT * FROM user; (to retrieve all the rows and columns that are present in the user table. Here “*” is nothing but all.)

```
+----------------+
2 rows in set (0.00 sec)

mysql> select * from users;
+---------+------------+-----------+---------+----------------------------------
+--------------------------------------------------------+
| user_id | first_name | last_name | user    | password
| avatar                                                 |
+---------+------------+-----------+---------+----------------------------------
+--------------------------------------------------------+
|       1 | admin      | admin     | admin   | 5f4dcc3b5aa765d61d8327deb882cf99
| http://172.16.123.129/dvwa/hackable/users/admin.jpg    |
|       2 | Gordon     | Brown     | gordonb | e99a18c428cb38d5f260853678922e03
| http://172.16.123.129/dvwa/hackable/users/gordonb.jpg  |
|       3 | Hack       | Me        | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b
| http://172.16.123.129/dvwa/hackable/users/1337.jpg     |
|       4 | Pablo      | Picasso   | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7
| http://172.16.123.129/dvwa/hackable/users/pablo.jpg    |
|       5 | Bob        | Smith     | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99
| http://172.16.123.129/dvwa/hackable/users/smithy.jpg   |
+---------+------------+-----------+---------+----------------------------------
+--------------------------------------------------------+
5 rows in set (0.00 sec)

mysql> _
```

7. Execute query that retrieves the data where name attributes match admin'. This query retrieves all the columns associated with name 'admin'.

```
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select * from users where user="admin";
ERROR 1046 (3D000): No database selected
mysql> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from users where user="admin";
+---------+------------+-----------+-------+----------------------------------+-
--------------------------------------------------+
| user_id | first_name | last_name | user  | password                         |
avatar                                             |
+---------+------------+-----------+-------+----------------------------------+-
--------------------------------------------------+
|       1 | admin      | admin     | admin | 5f4dcc3b5aa765d61d8327deb882cf99 |
http://172.16.123.129/dvwa/hackable/users/admin.jpg |
+---------+------------+-----------+-------+----------------------------------+-
--------------------------------------------------+
1 row in set (0.00 sec)

mysql> _
```

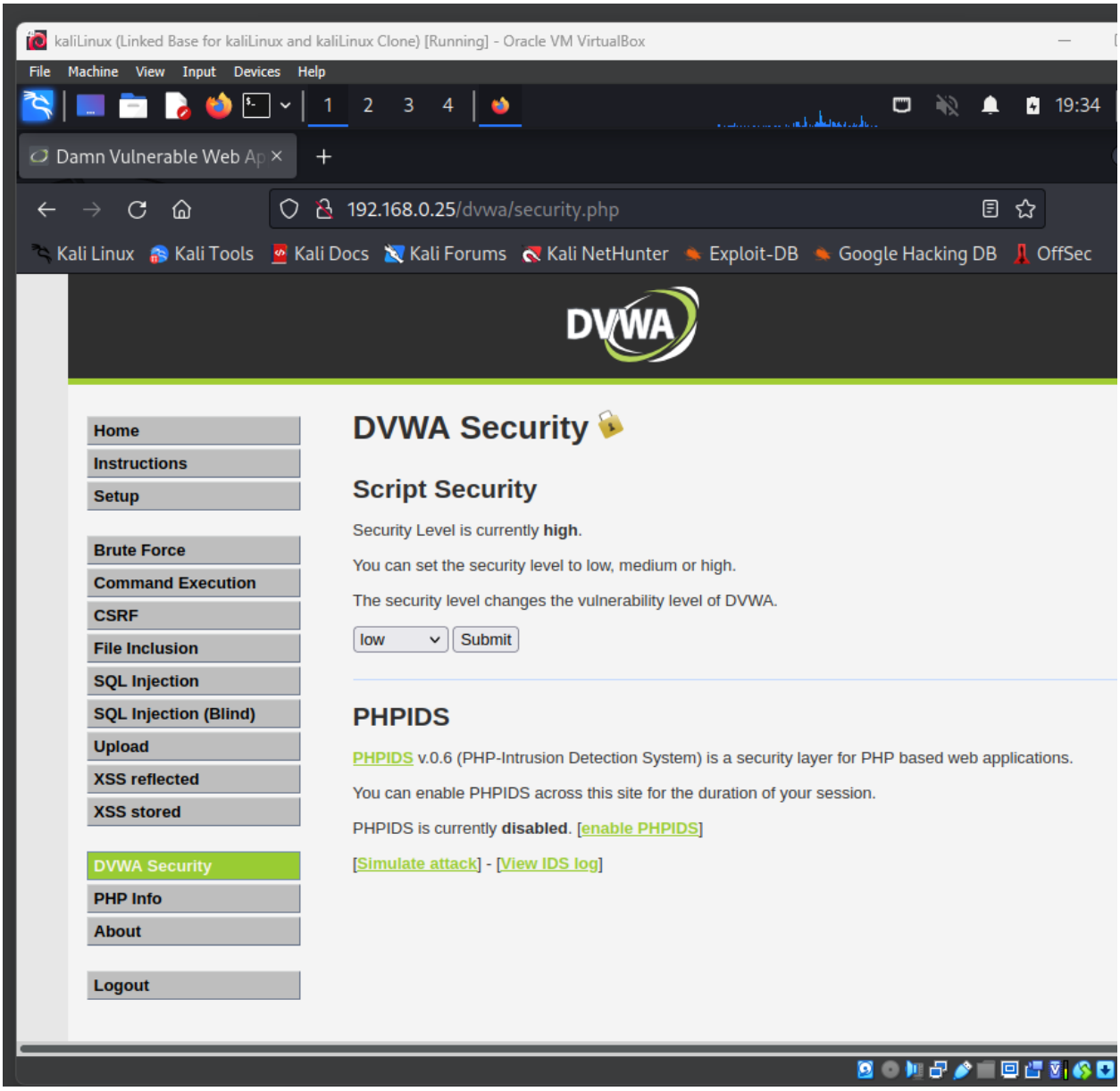
8. Execute, SELECT * FROM user where user="any" or 1=1;
Here 1=1 always returns true. So, it retrieves all the rows from the database. which is not supposed to be done.



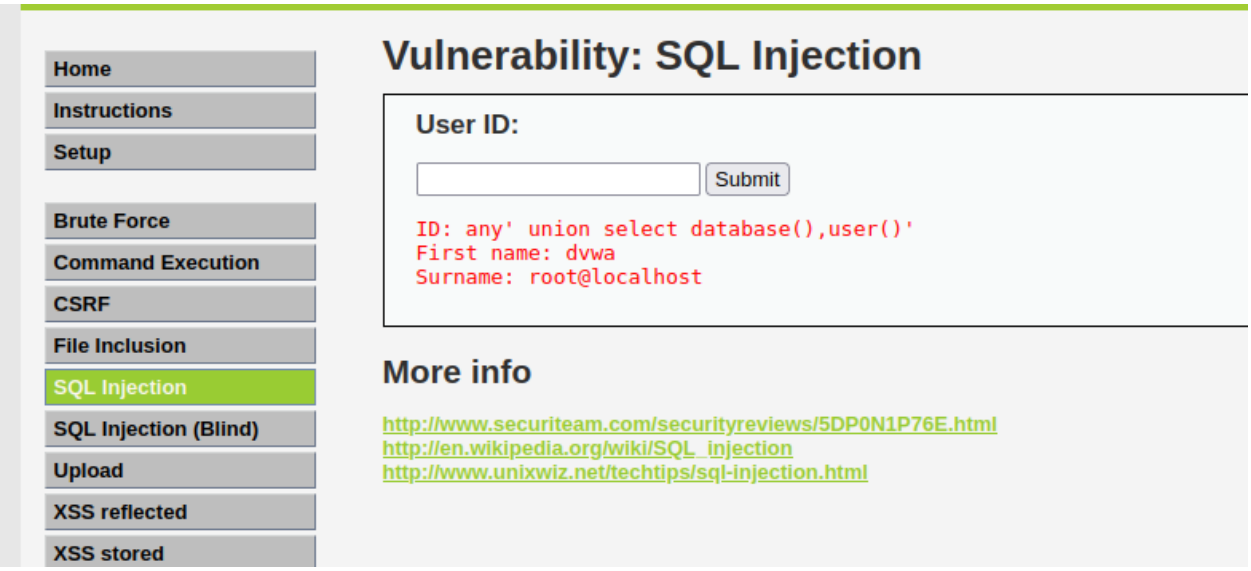
```
+-------------------------------------------------------+
1 row in set (0.00 sec)

mysql> select * from users where user="any" or 1=1;
+---------+------------+-----------+---------+----------------------------------
+-------------------------------------------------------+
| user_id | first_name | last_name | user    | password
| avatar                                                |
+---------+------------+-----------+---------+----------------------------------
+-------------------------------------------------------+
|       1 | admin      | admin     | admin   | 5f4dcc3b5aa765d61d8327deb882cf99
| http://172.16.123.129/dvwa/hackable/users/admin.jpg   |
|       2 | Gordon     | Brown     | gordonb | e99a18c428cb38d5f260853678922e03
| http://172.16.123.129/dvwa/hackable/users/gordonb.jpg |
|       3 | Hack       | Me        | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b
| http://172.16.123.129/dvwa/hackable/users/1337.jpg    |
|       4 | Pablo      | Picasso   | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7
| http://172.16.123.129/dvwa/hackable/users/pablo.jpg   |
|       5 | Bob        | Smith     | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99
| http://172.16.123.129/dvwa/hackable/users/smithy.jpg  |
+---------+------------+-----------+---------+----------------------------------
+-------------------------------------------------------+
5 rows in set (0.00 sec)

mysql> _
```

Task B: SQL Injection Attack from Webpage (as a front-end user)

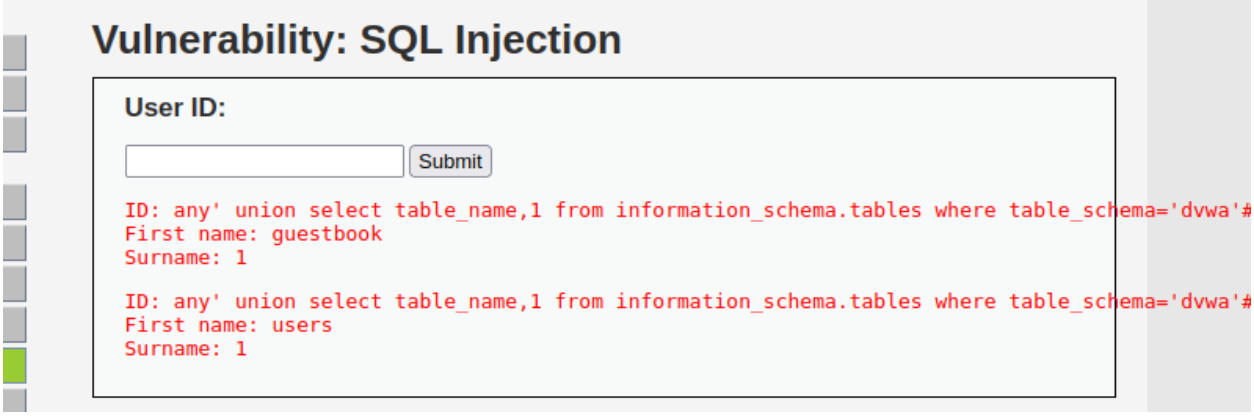
1. In a browser (in Kali Linux), type the ip address of Metasploitable 2 VM. [DO not Power off metasploitable2 VM).
2. Login to DVWA.
3. Select DVWA Security tab and change the security level to “Low.”



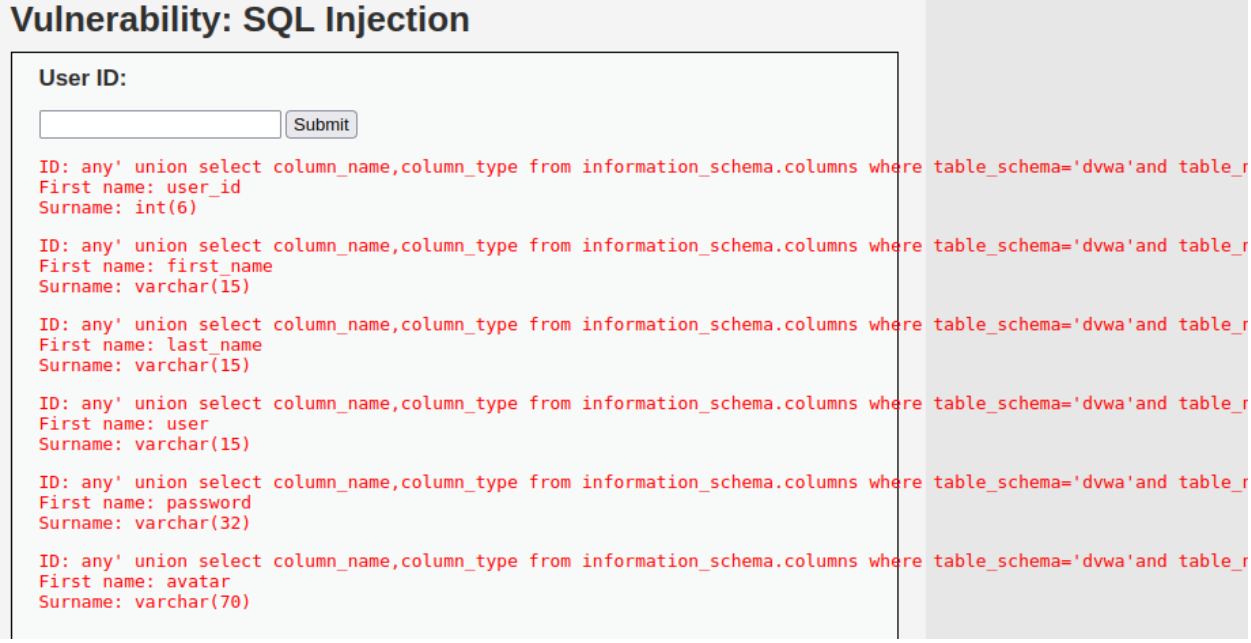
4. Select on the “SQL Injection” tab.
5. In the “User ID” box, type the query using “union” to combine multiple select statements, to fetch the database name and the username logged in to metasploitable 2 VM.



6. Once you know the name of the database, execute the query to retrieve the tables available in this database:



7. After retrieving the table names in dvwa database, retrieve the column names in user table.



8. Using the information retrieved for column names, retrieve/display the username and password for all the users in the users table.