Experiment 3: Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi

Aim:

To examine and setup DVWA website to test the vulnerability of attacks and to perform SQL injection attack

Installing DVWA:

open kali linux

open the terminal

enter the command

cd /var/www/html

open the firefox browser and type dvwa github

click the link and copy the url and paste in terminal

sudo git clone https://github.com/digininja/DVWA

give command----> ls

check the folder dvwa

mv dvwa DVWA

ls

cd DVWA

cd config

check the folder config.inc.php.dist

sudo cp config.inc.php.dist config.inc.php

ls

cat config.inc.php

sudo nano config.inc.php

change db user===user

p@ssword ==pass------->chage

cat config.inc.php

check it is change or not

sudo service mysql start

sudo mysql -u root -p

create user dvwa;

create user dvwa@localhost identified by 'p@ssw0rd';

grant all on dvwa.* to dvwa@localhost;

flush privileges;

exit---------- get bye... message

sudo service apache2 start

http://localhost/DVWA or http://127.0.0.1/DVWA/login.php

user name::admin

password::password

----if any one getting the problem or accessing the page

please follow the steps

cd --enter

cd /etc

cd php

cd 8.1

cd apache2.....or.....direct command

----------> cd /etc/php/8.1/apache2

check file

ls

there is php.ini file

next command .....

sudo nano php.ini

next---> ctrl + / then enter

it will show the line number and give 865

change

allow_url_fopen = On

allow_url_include = On

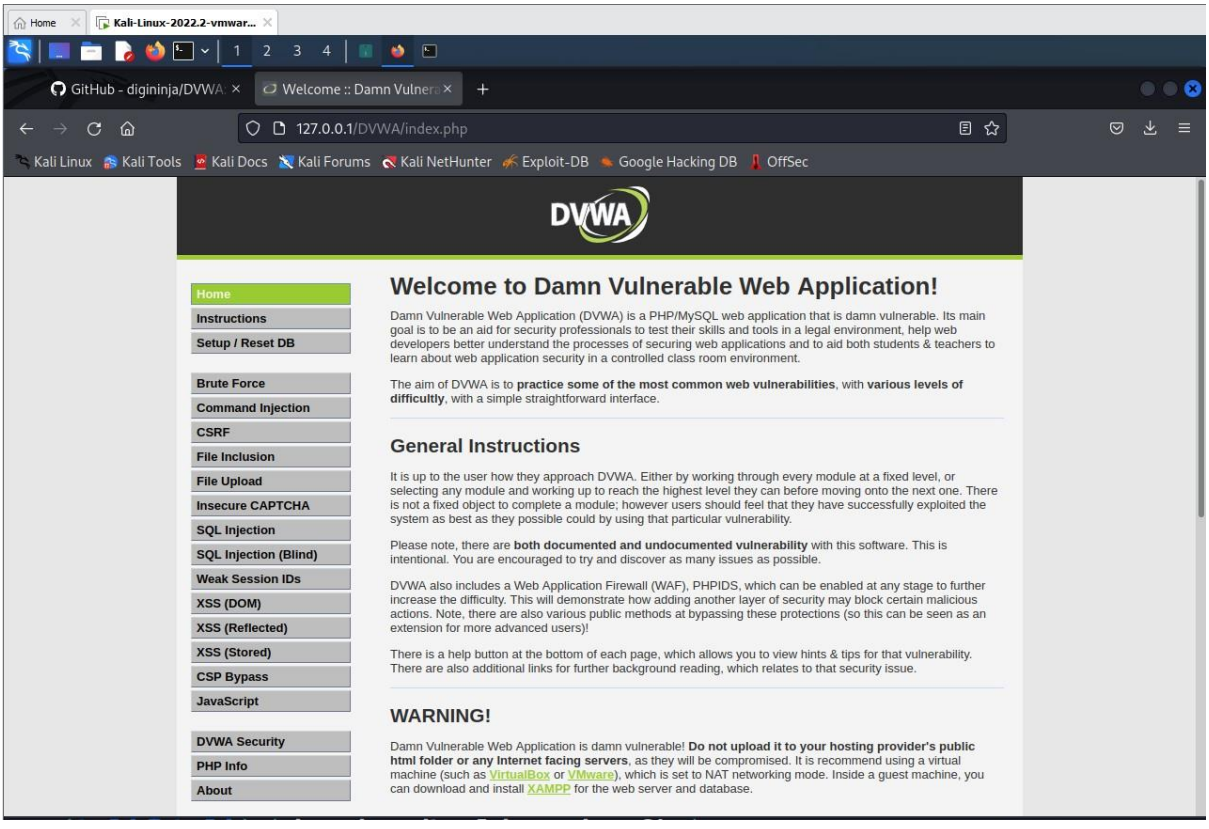
next---> ctrl + x

type y and enter

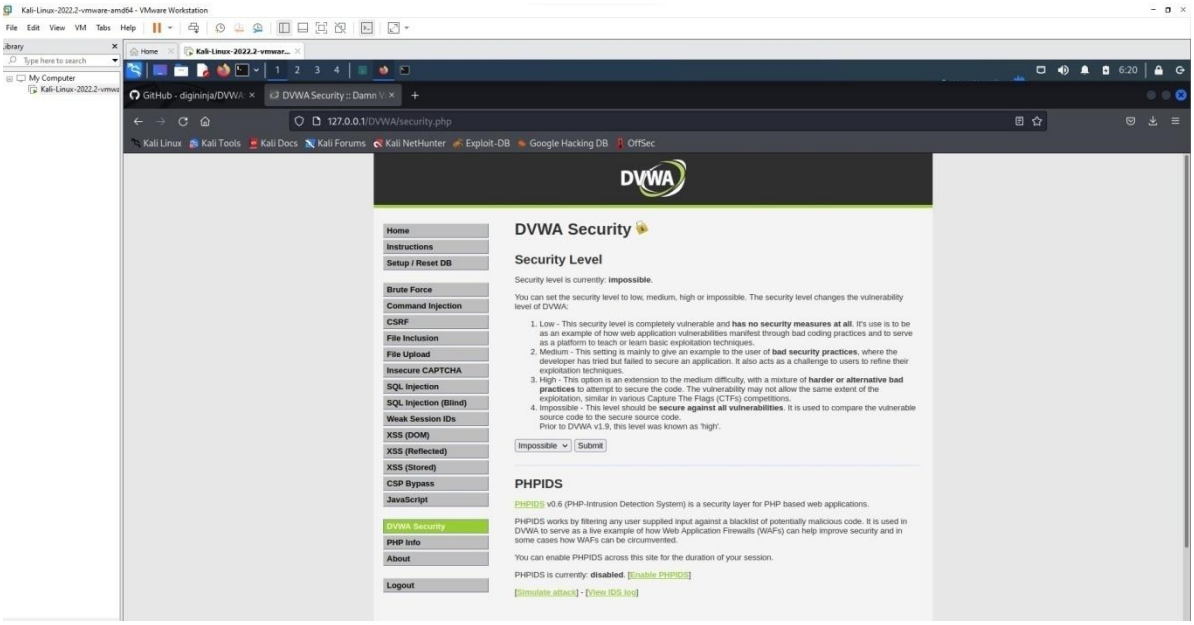
and again restart the server

sudo service apache2 restart

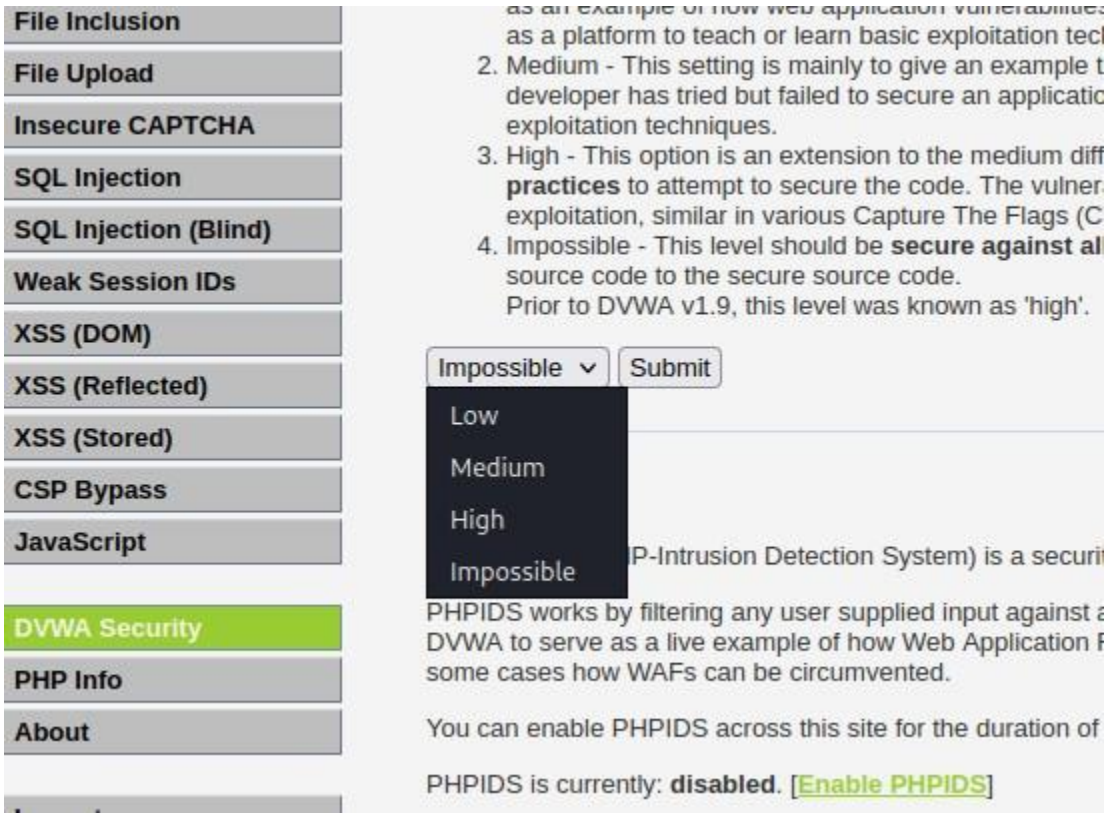
we get http://127.0.0.1/DVWA/index.php



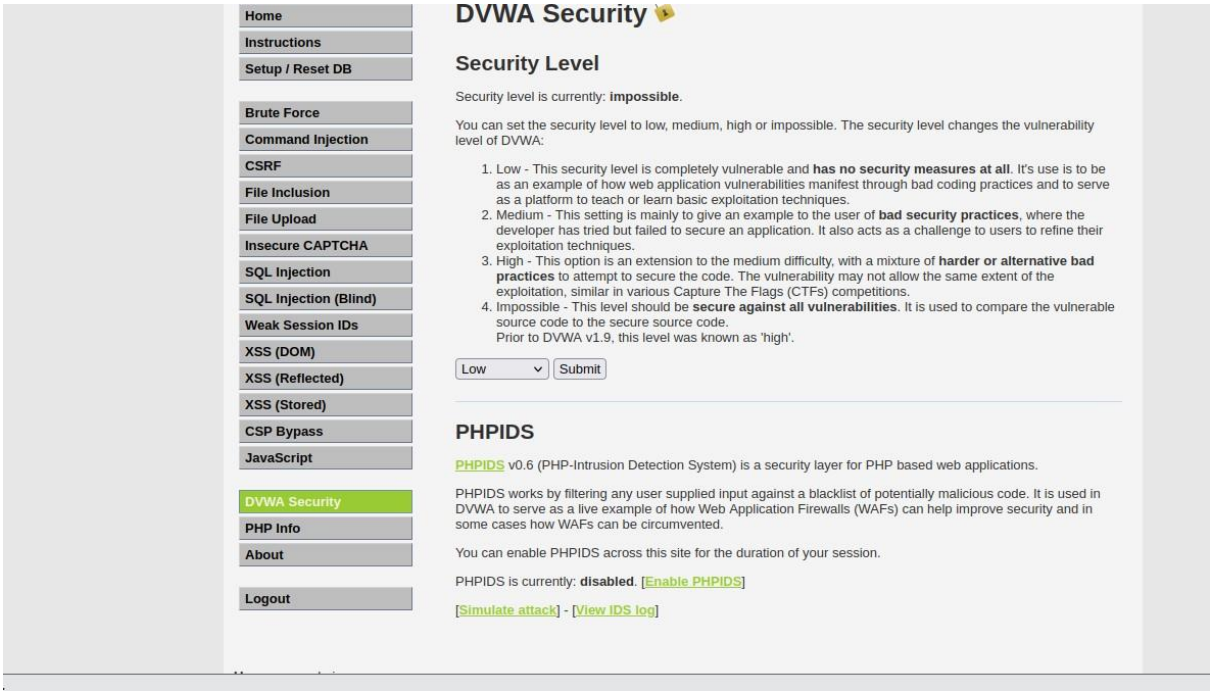
Goto DVWA security



Click on impossible



set as LOW.



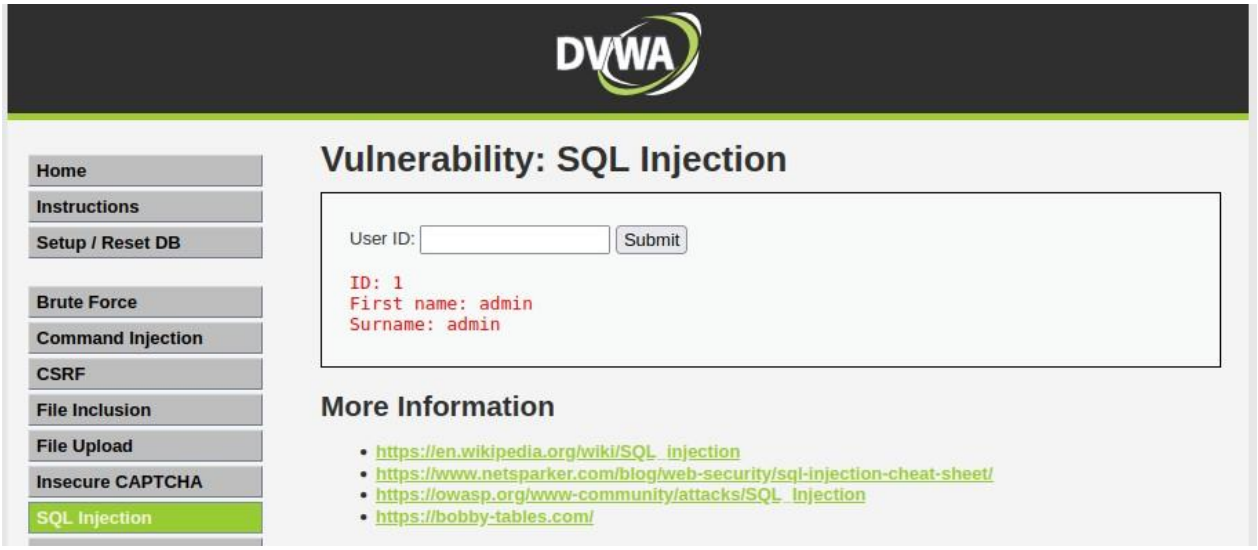
Click submit.

Attacking the

system:

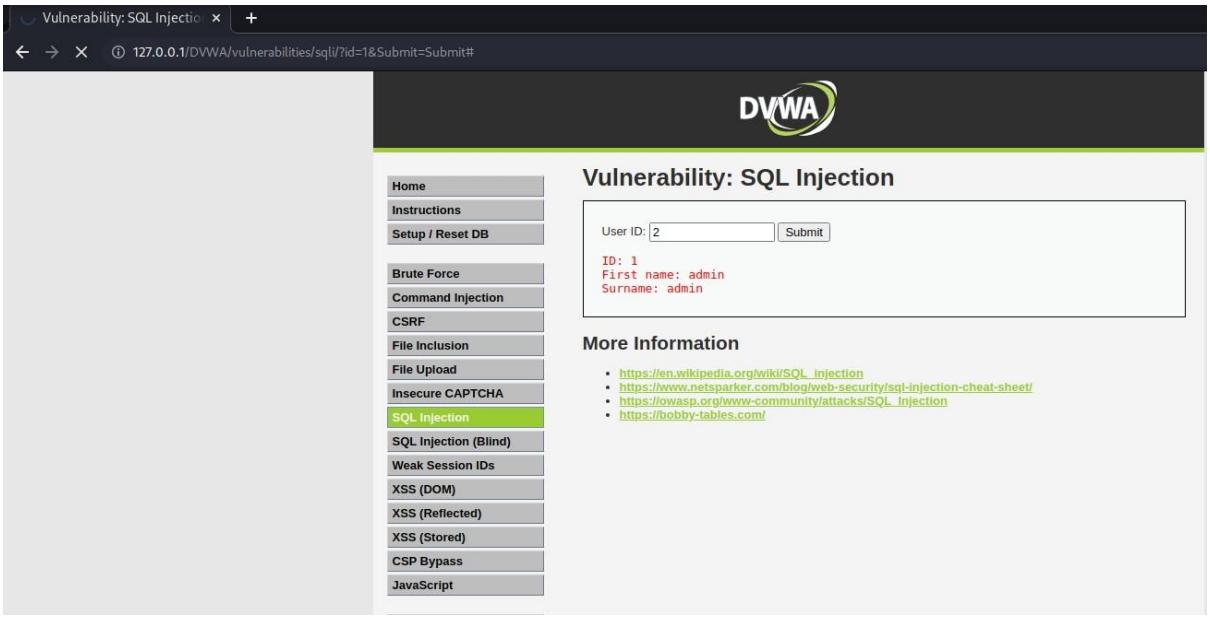
- SQLInjection:

Enter 1 and Click



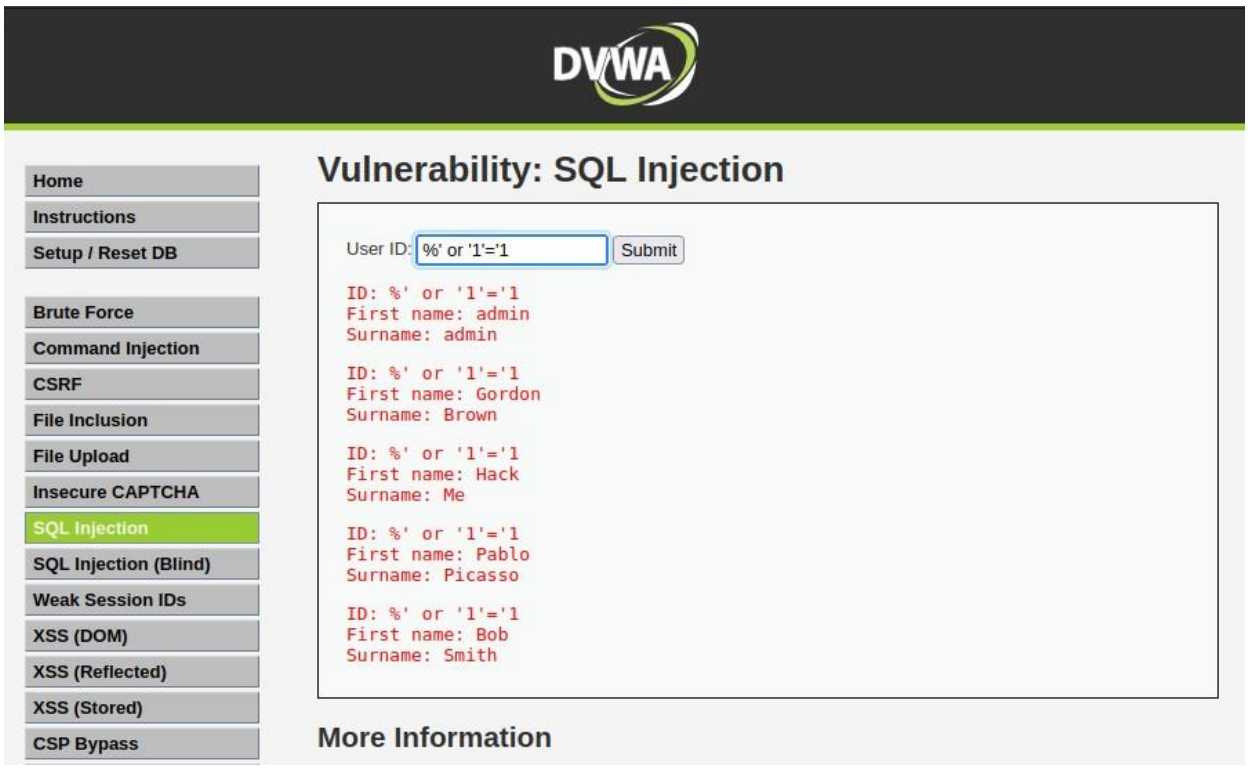
submit

Enter 2 and Click submit



Enter %’ or ‘1’=’1

It displays all the information.



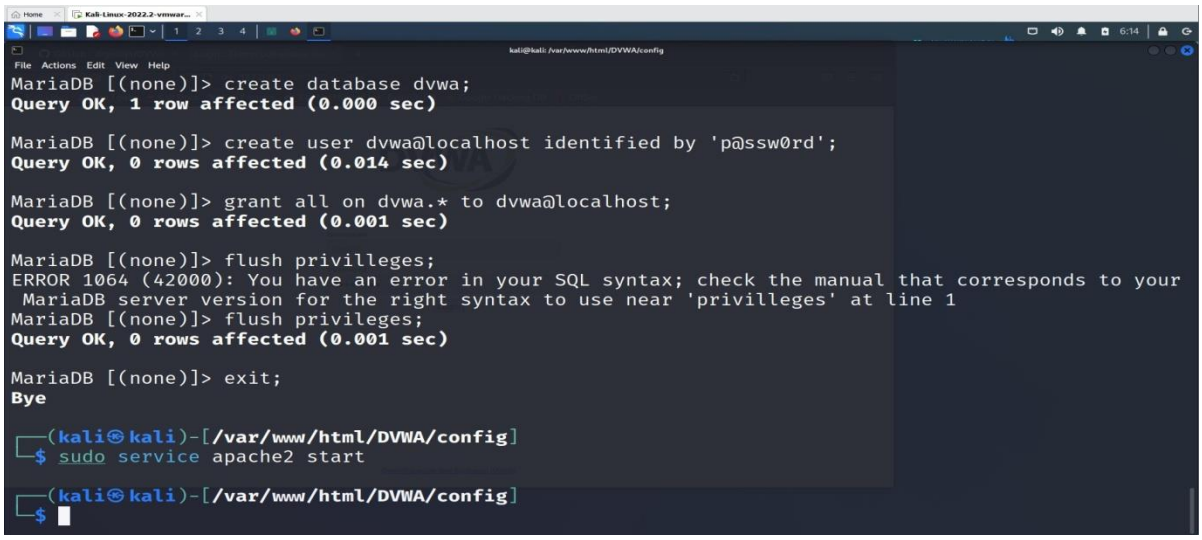
Result:

Thus the DVWA website setup and sql injection attack completed successfully

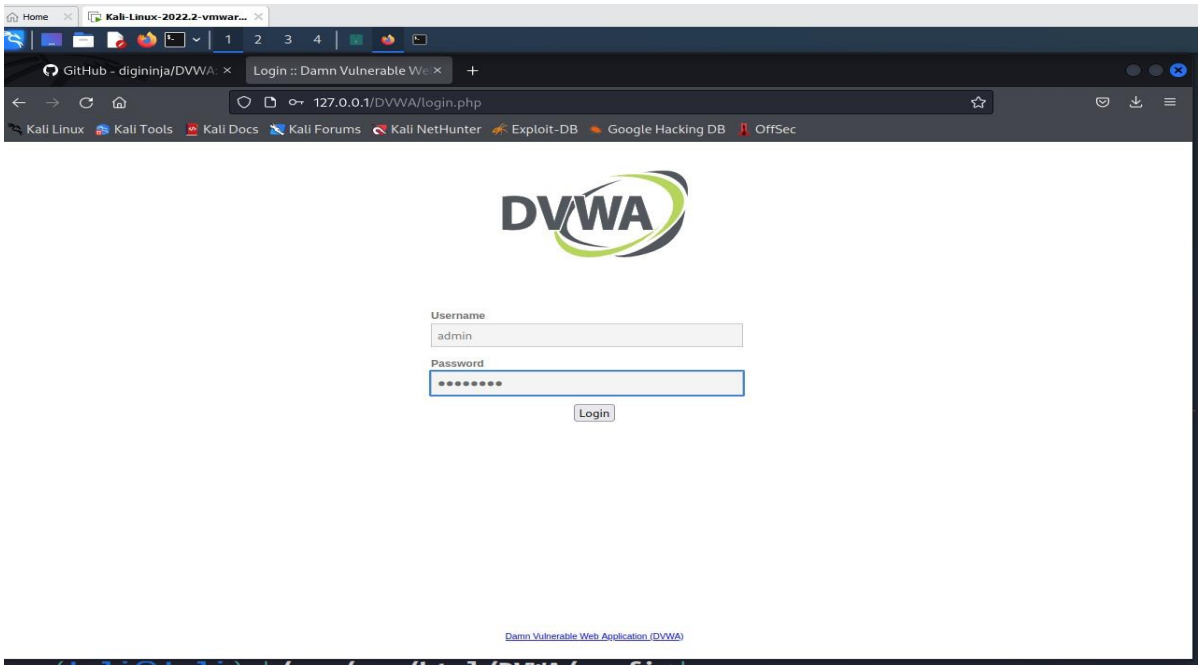
Experiment 4: Examination of a website to test the vulnerability of attacks. – XSS & CSRF & Command line injection attack.

—Command Injection Attack—

sudo service apache2 start

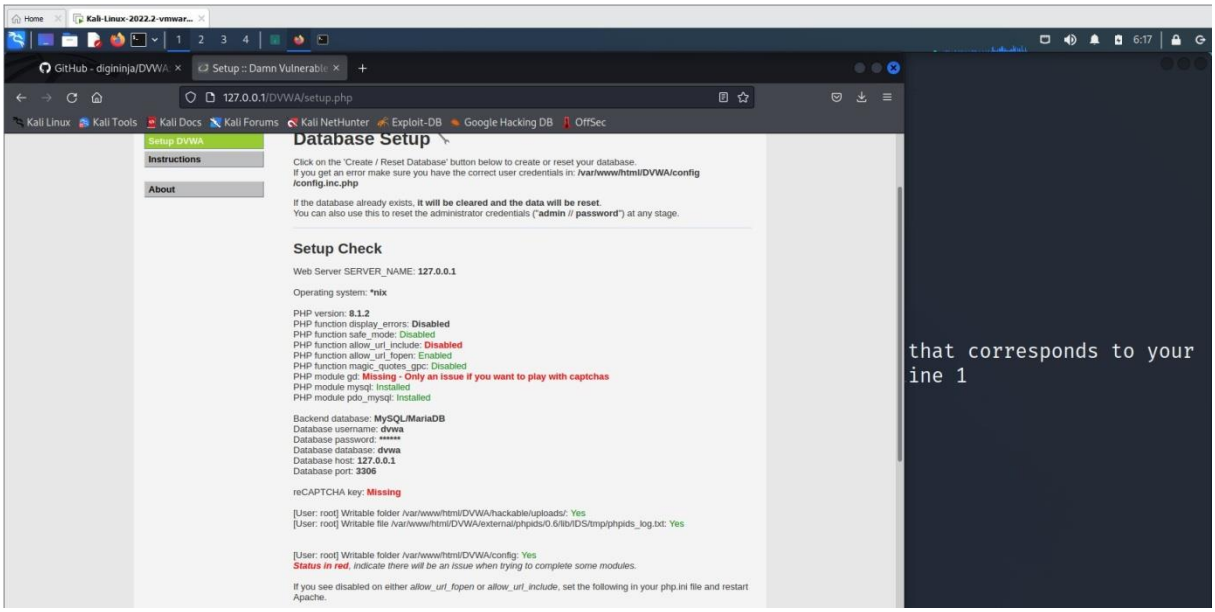


goto browser and give http://localhost/DVWA or http://127.0.0.1/DVWA/login.php



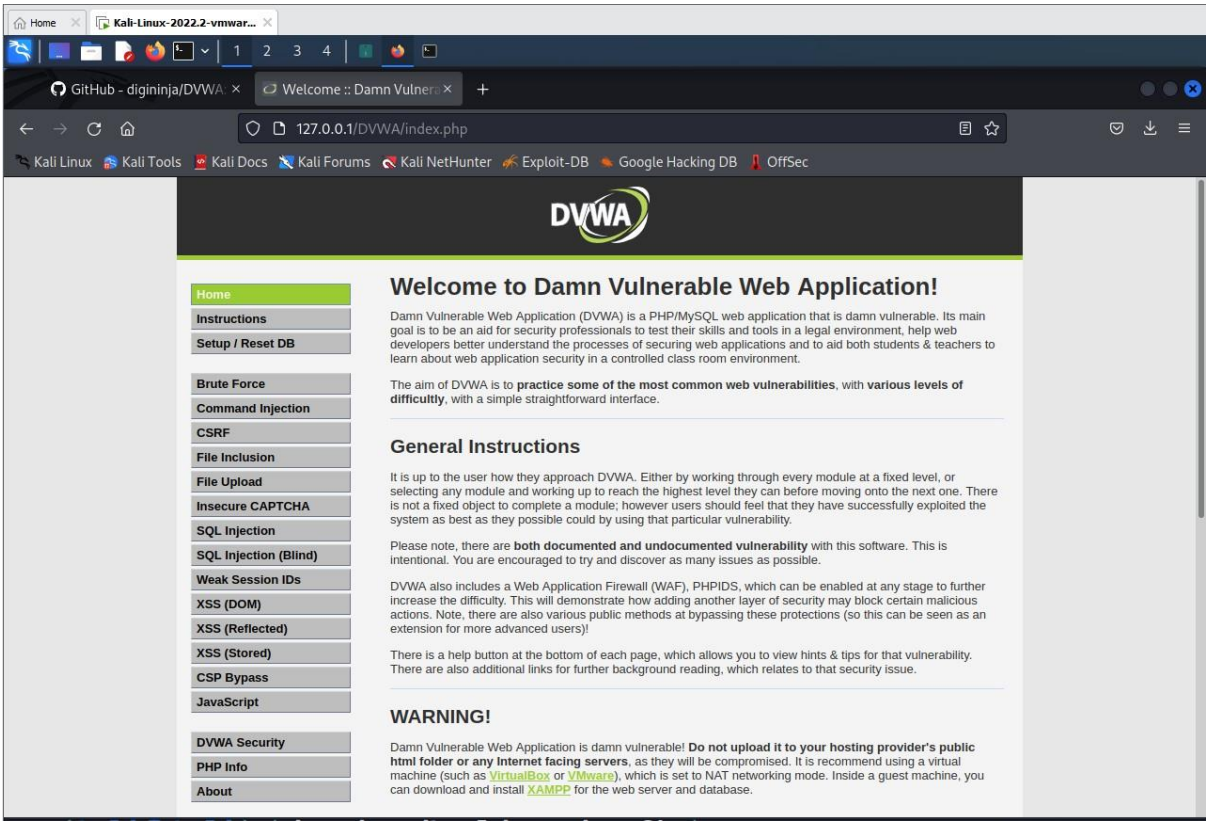
username: admin

password: password

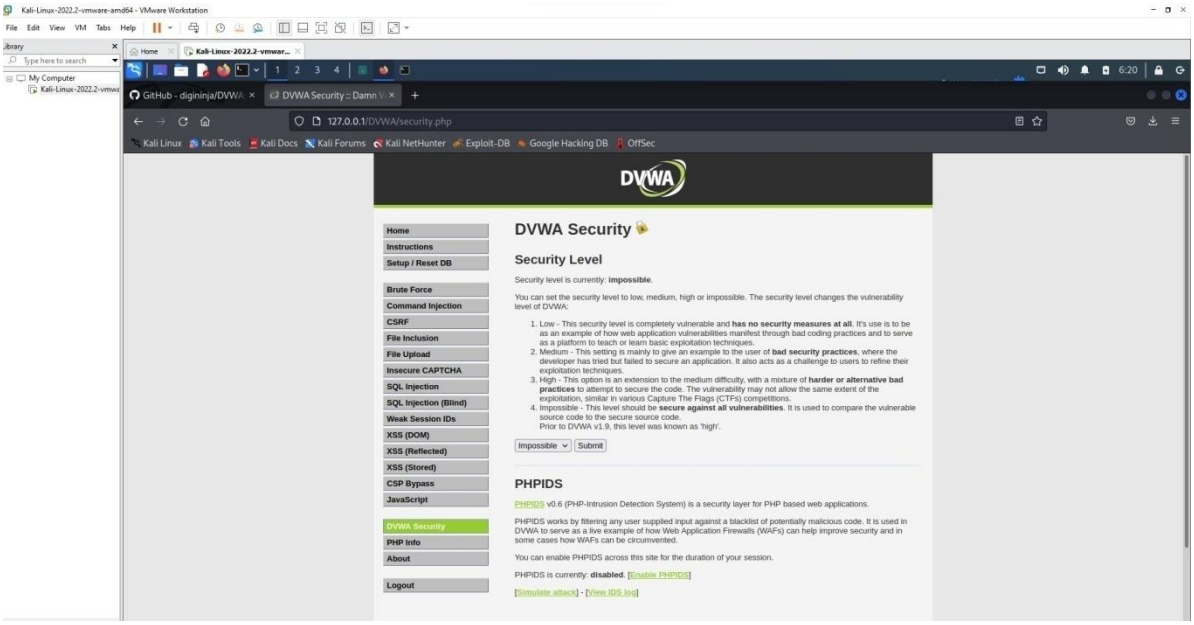


click create database

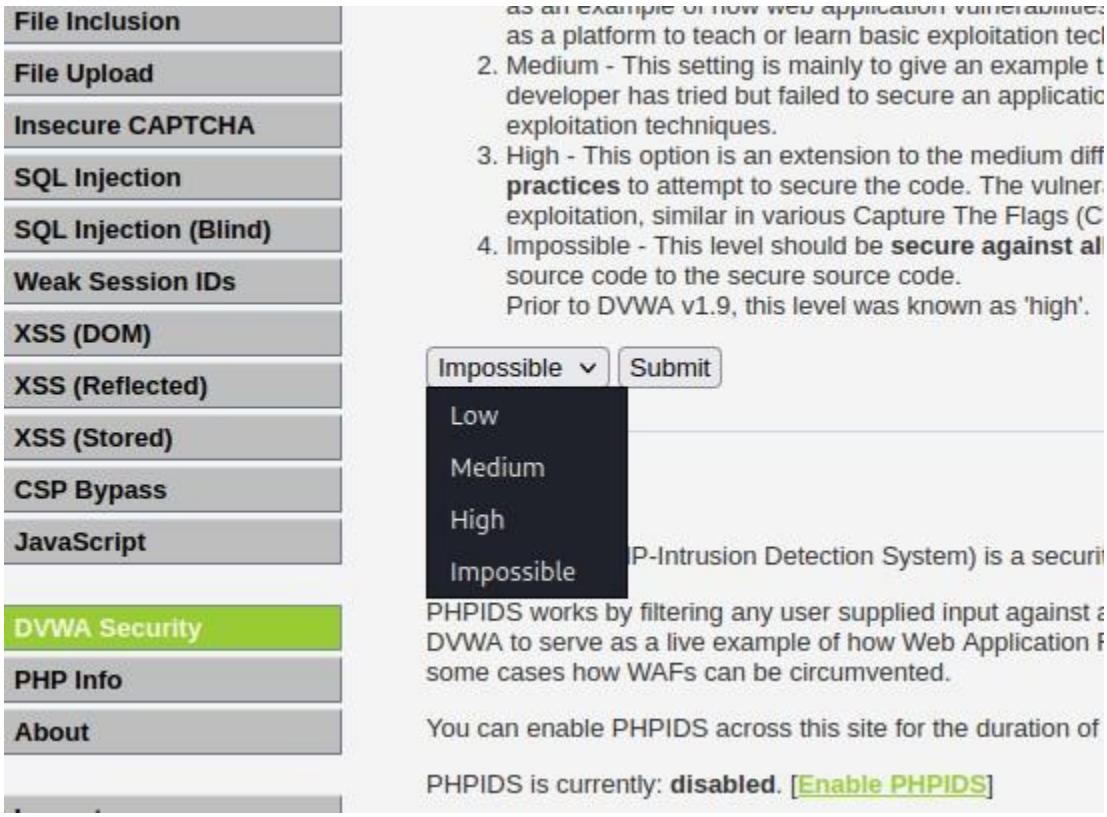
we get http://127.0.0.1/DVWA/index.php



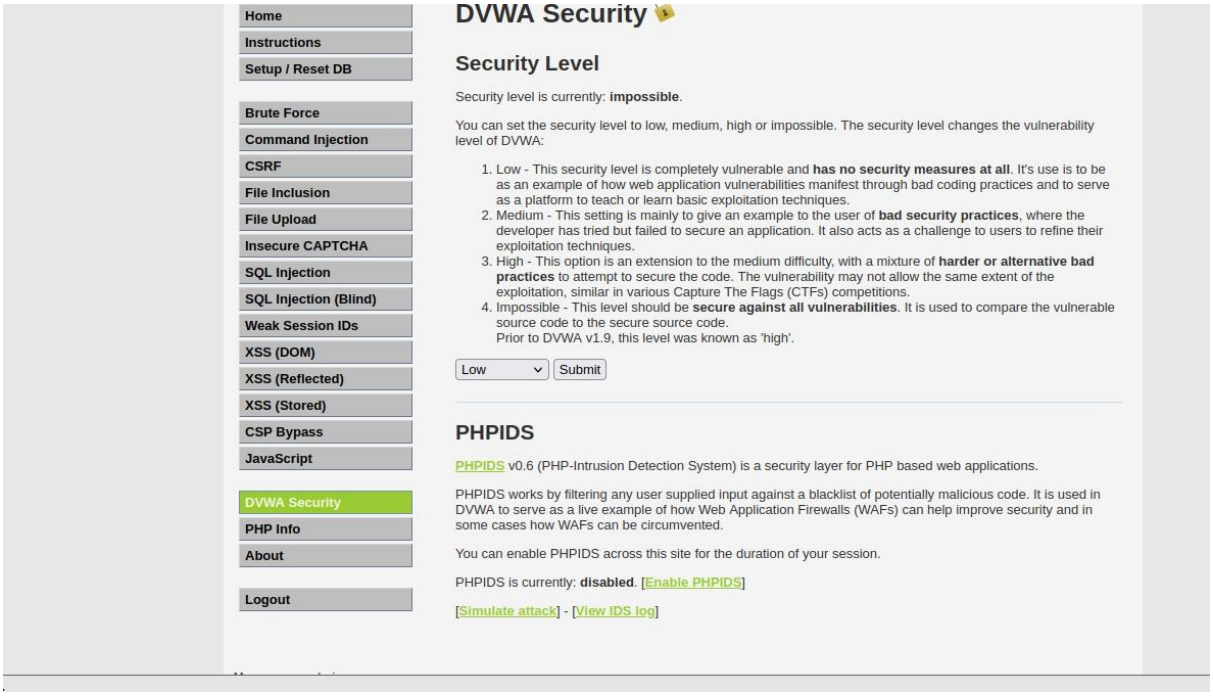
Goto DVWA security



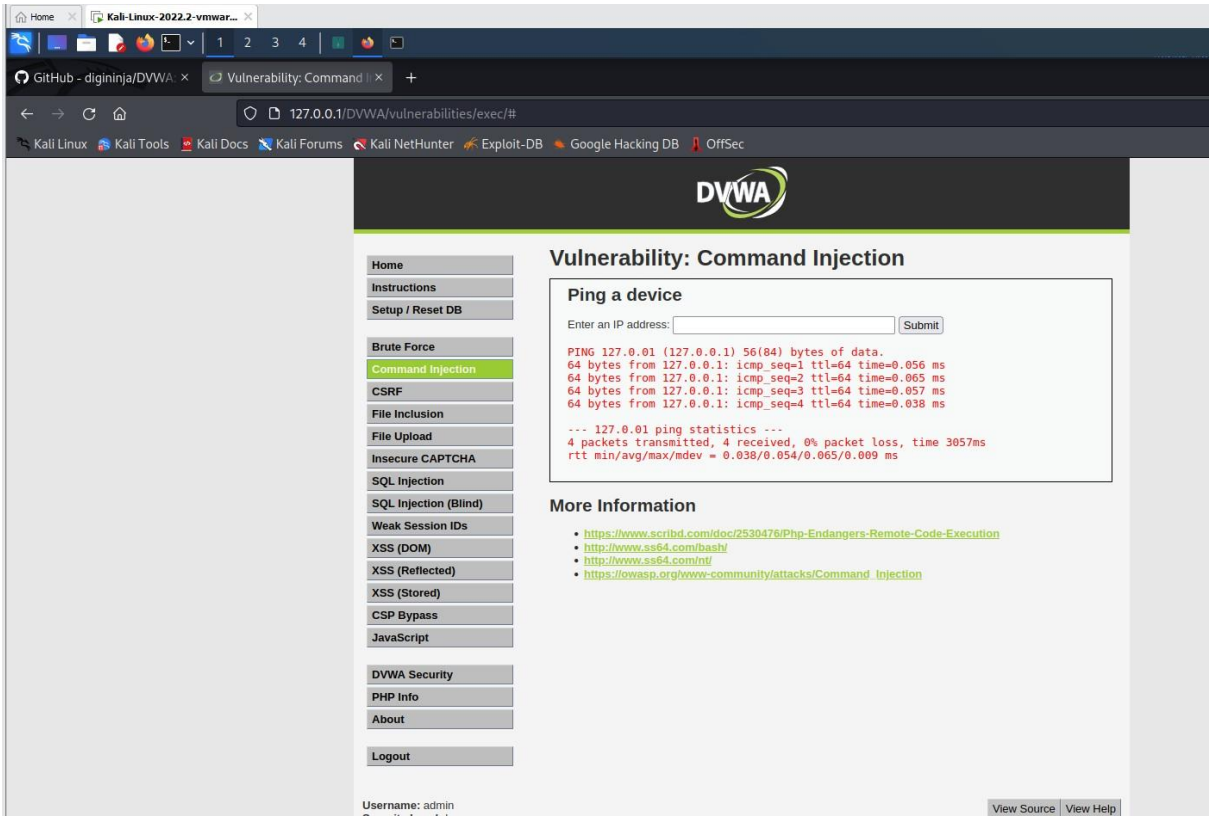
Click on impossible



Set as LOW and click Submit.

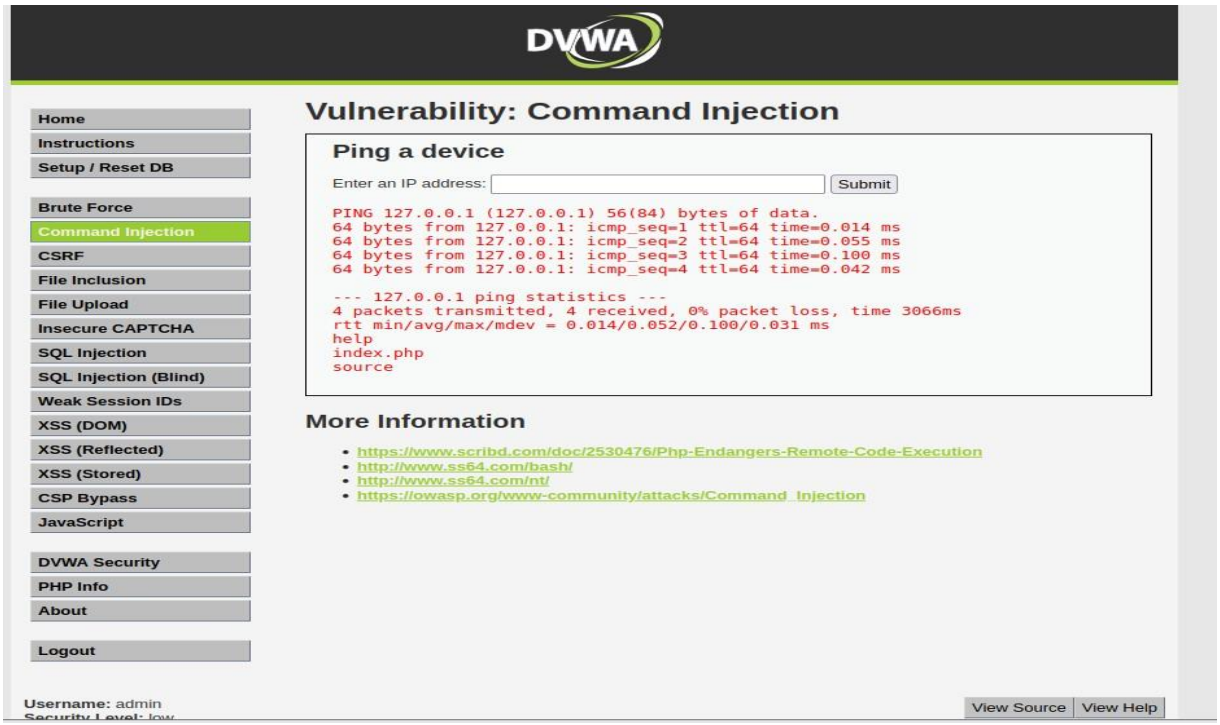


Enter IP address.

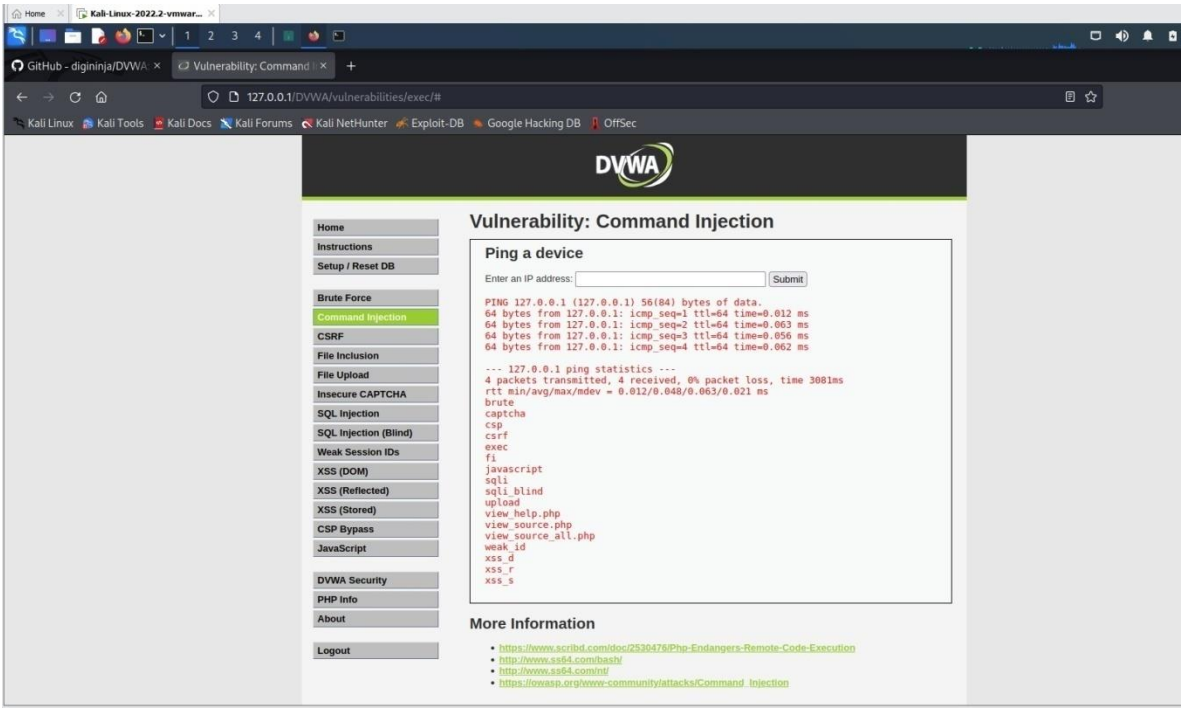


multiple commands using pipe or ;

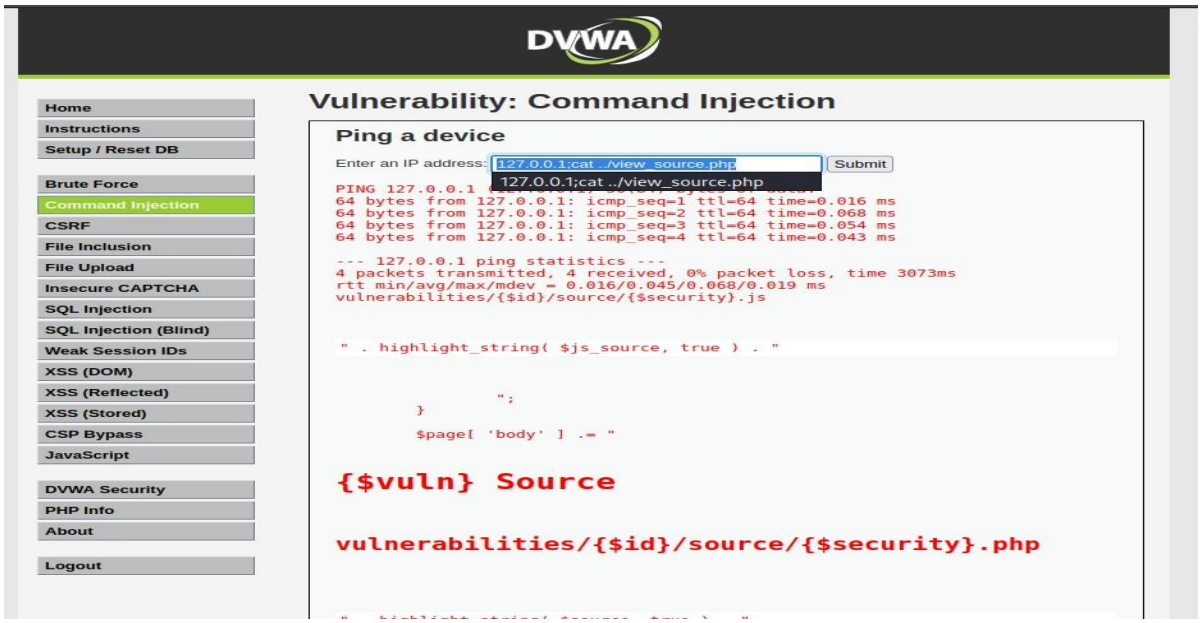
127.0.0.1;ls



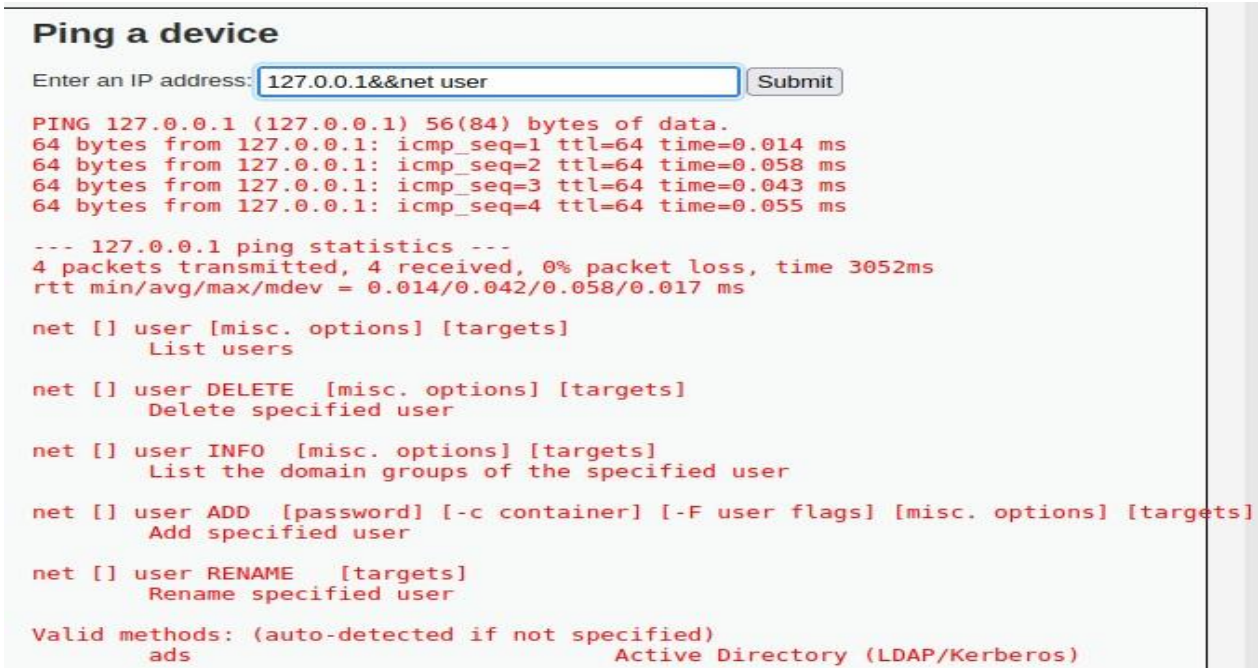
127.0.0.1;ls ../



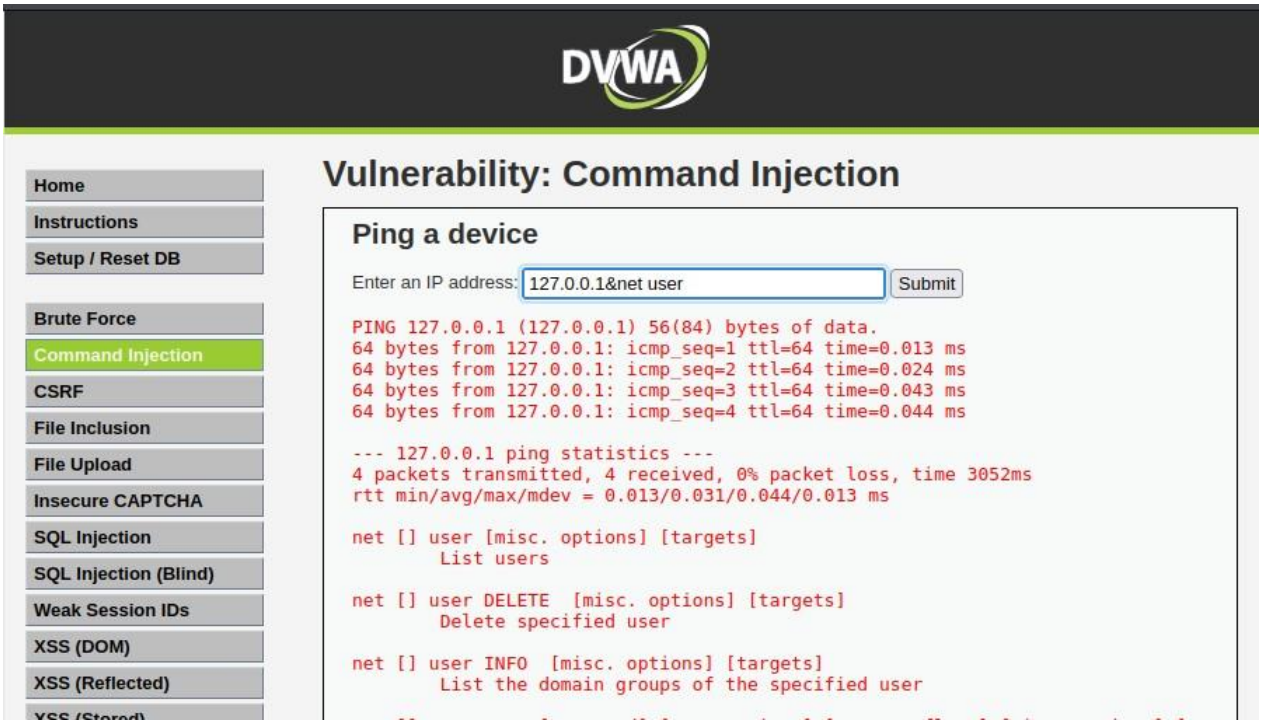
;cat ../view_source.php



Use &&net user

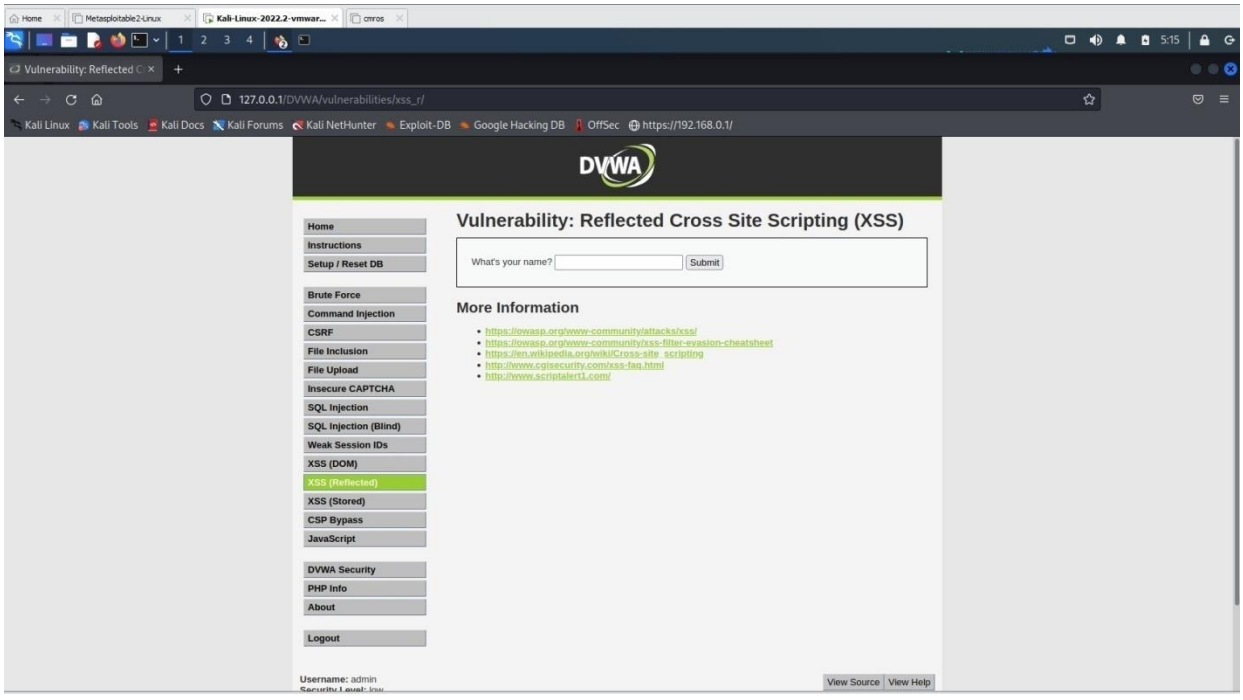


Use &net user

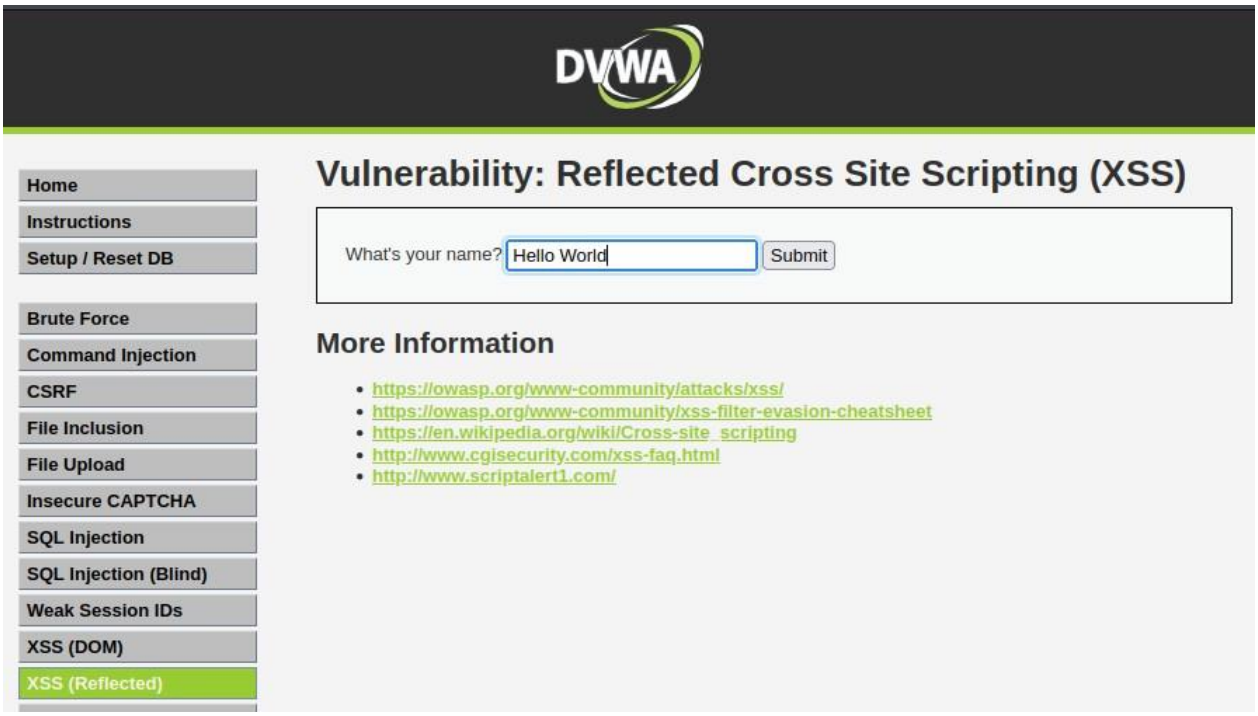


——----------XSS Attack----------

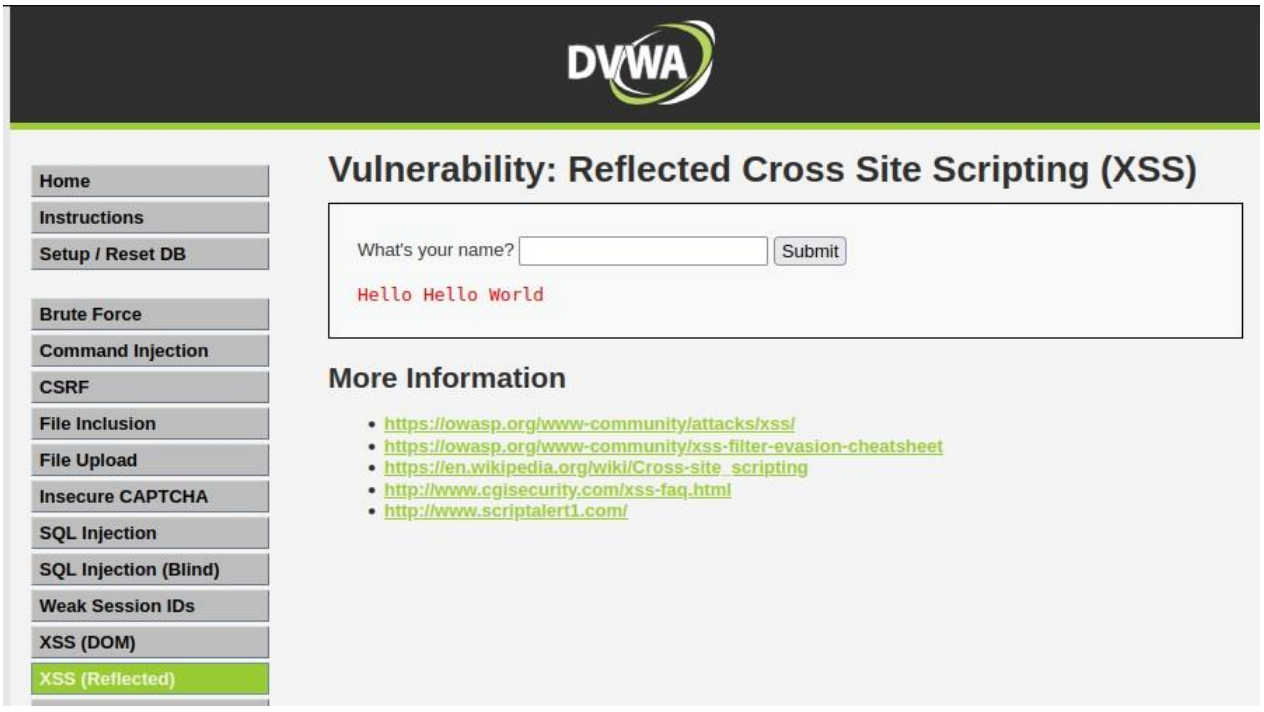
Click XSS Reflection



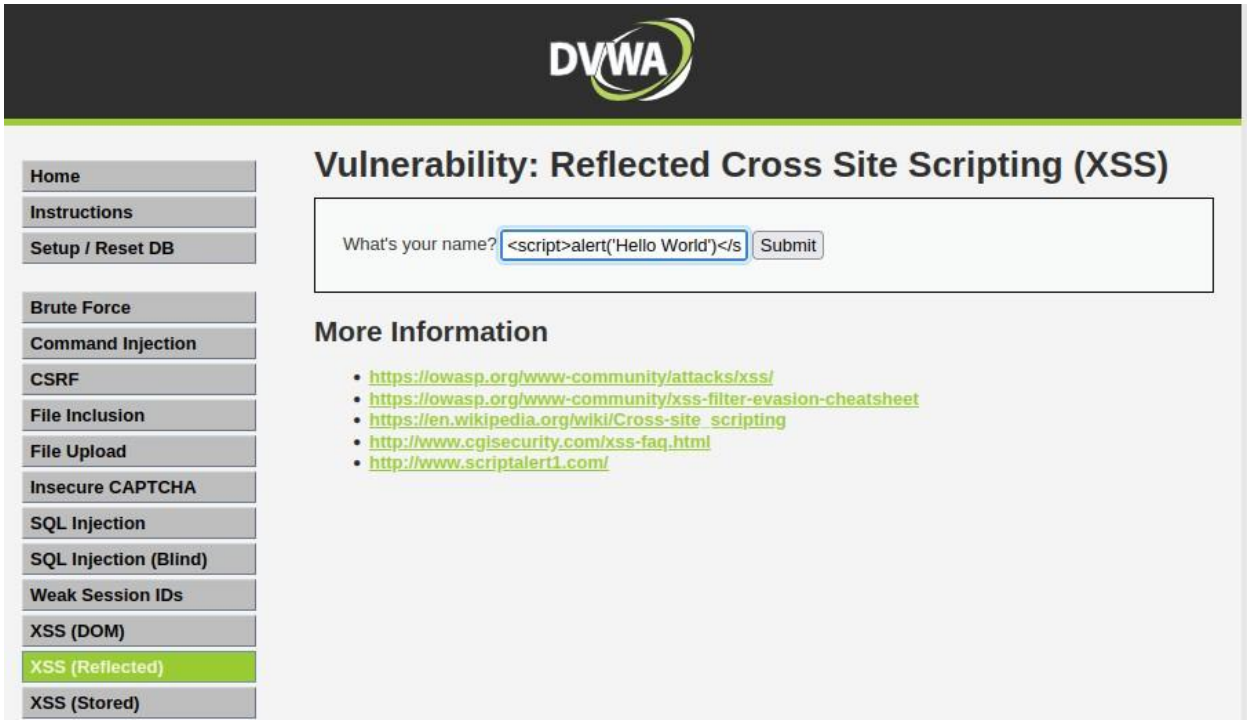
Enter any name in the text box and click submit.



It displays as

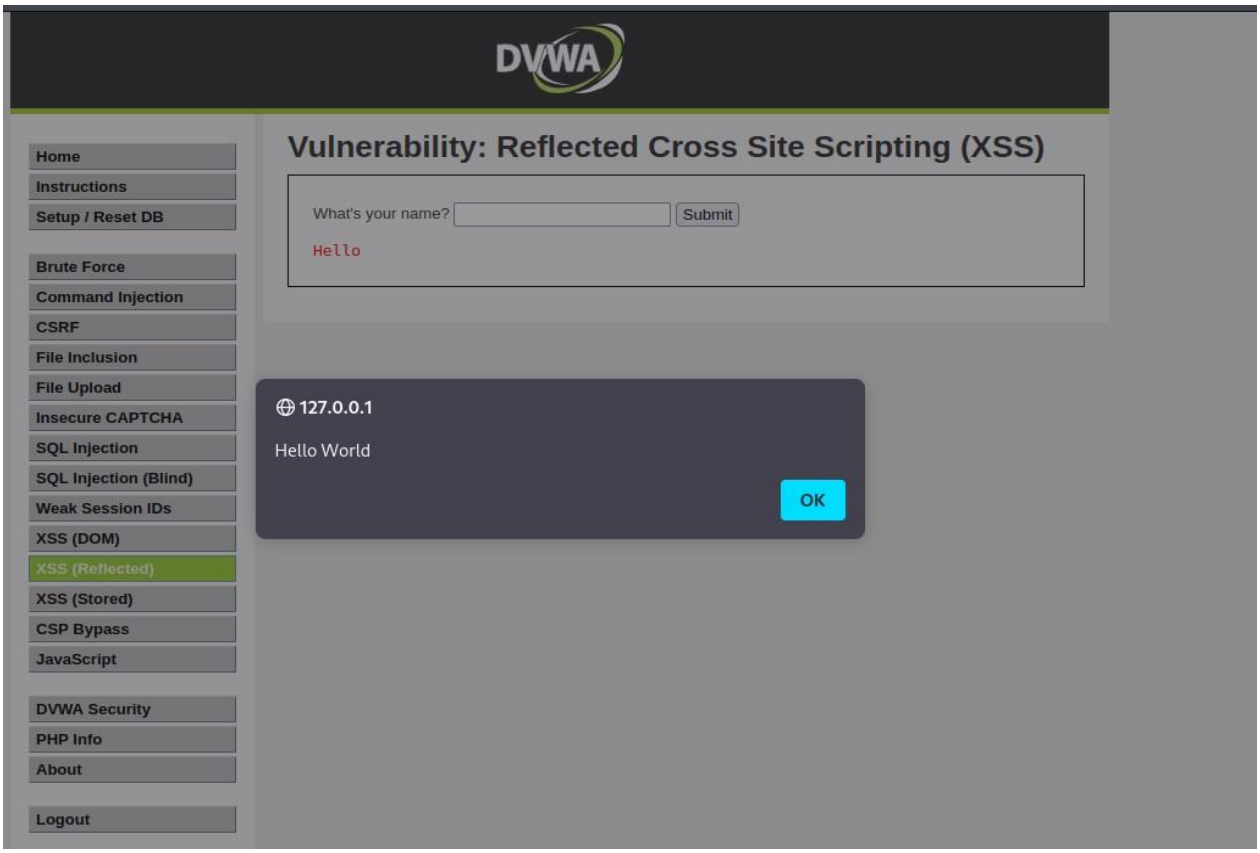


Now instead of any text let's try some script text.

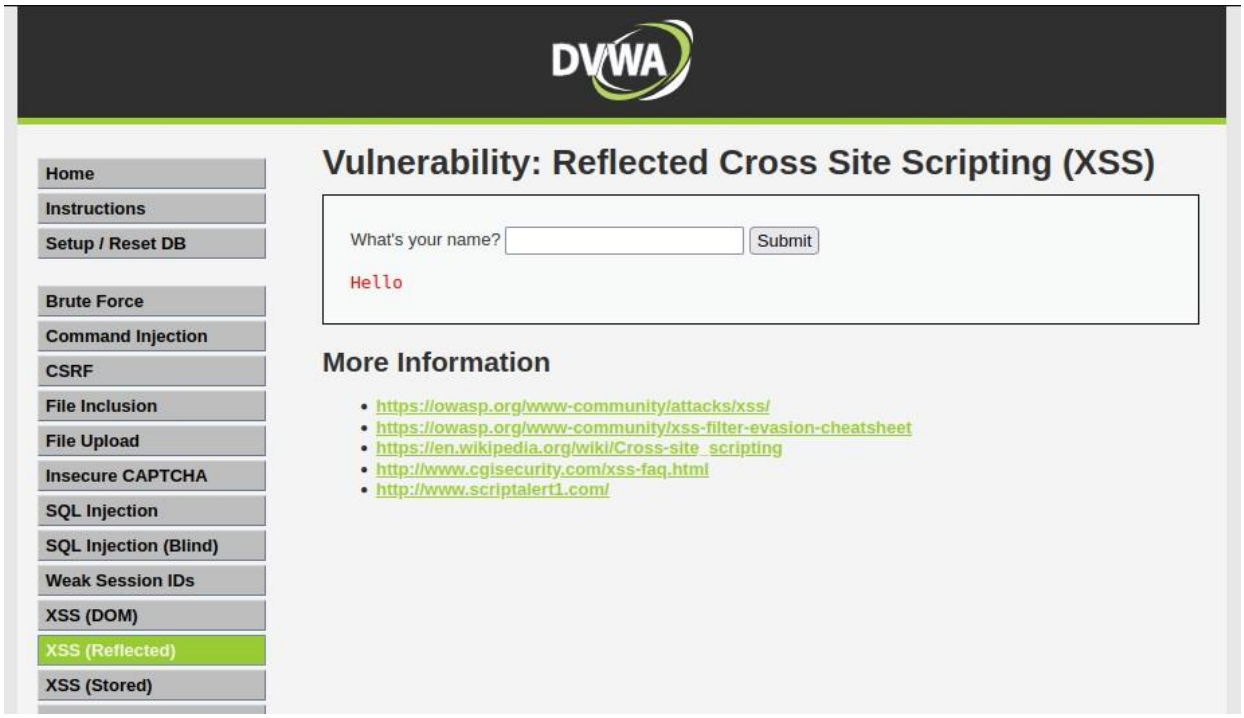


Ex: <script>alert('Hello World')</script>

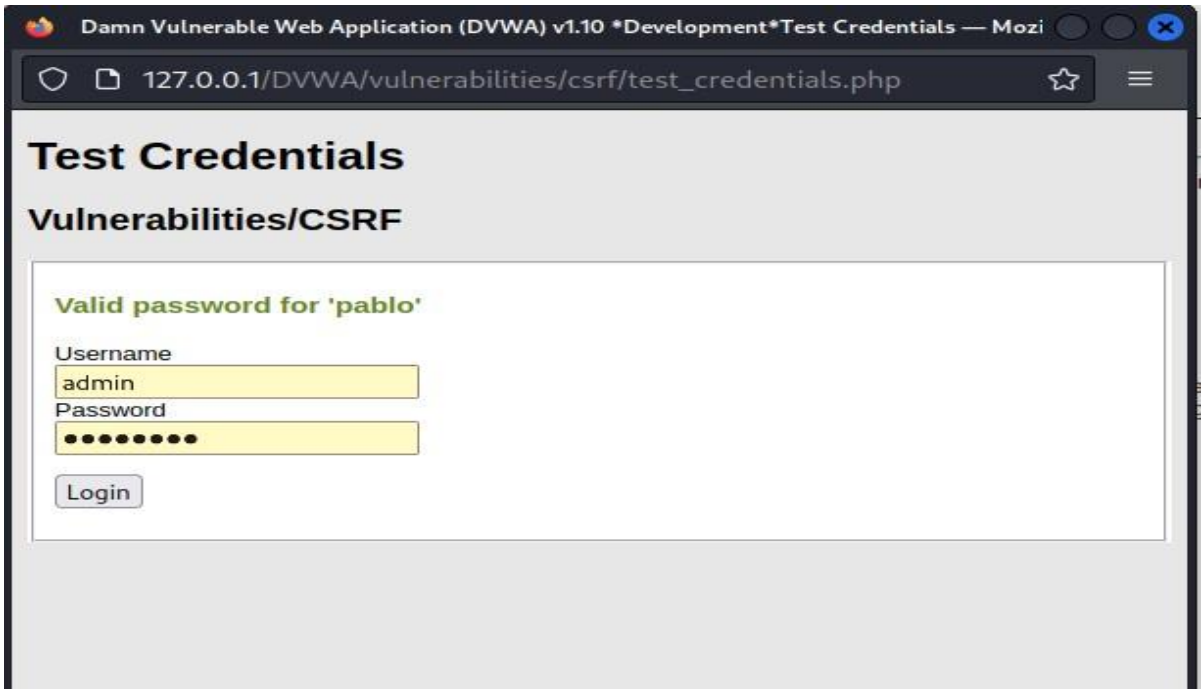
It displays an alert as shown below


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
127.0.0.1
Hello World
OK

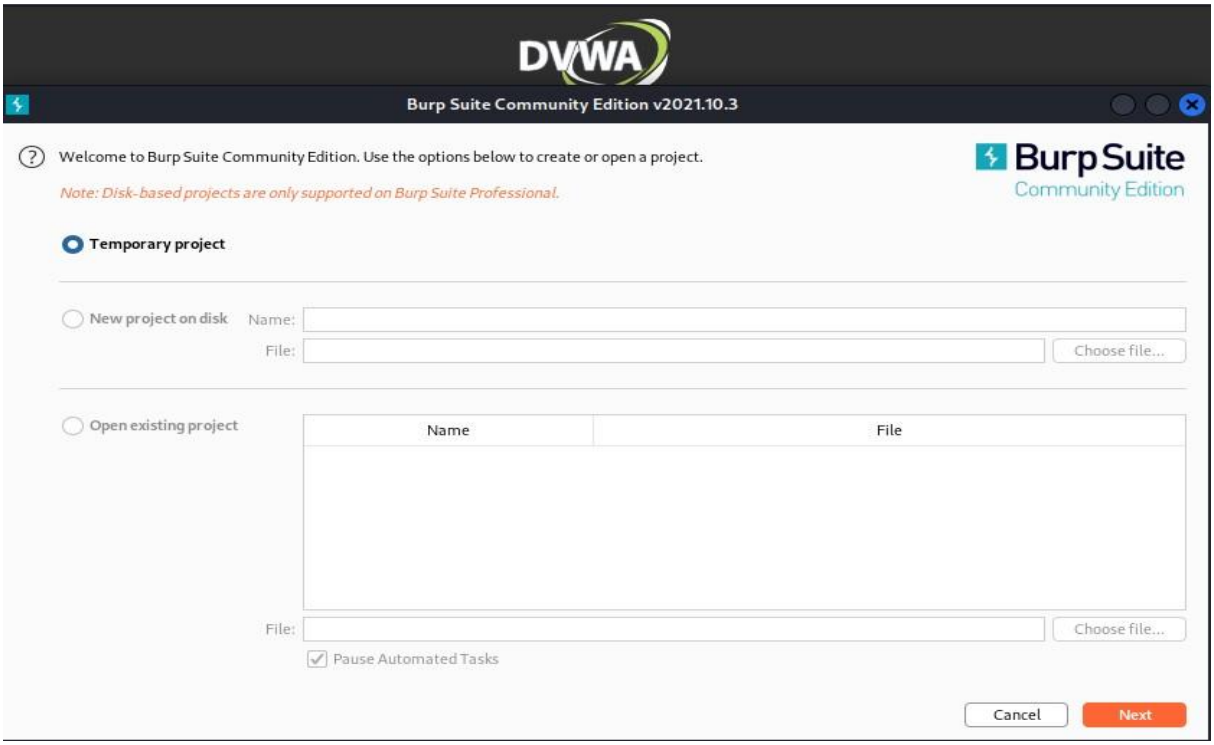
Click Ok


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/xss-filter-evasion-cheatsheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/

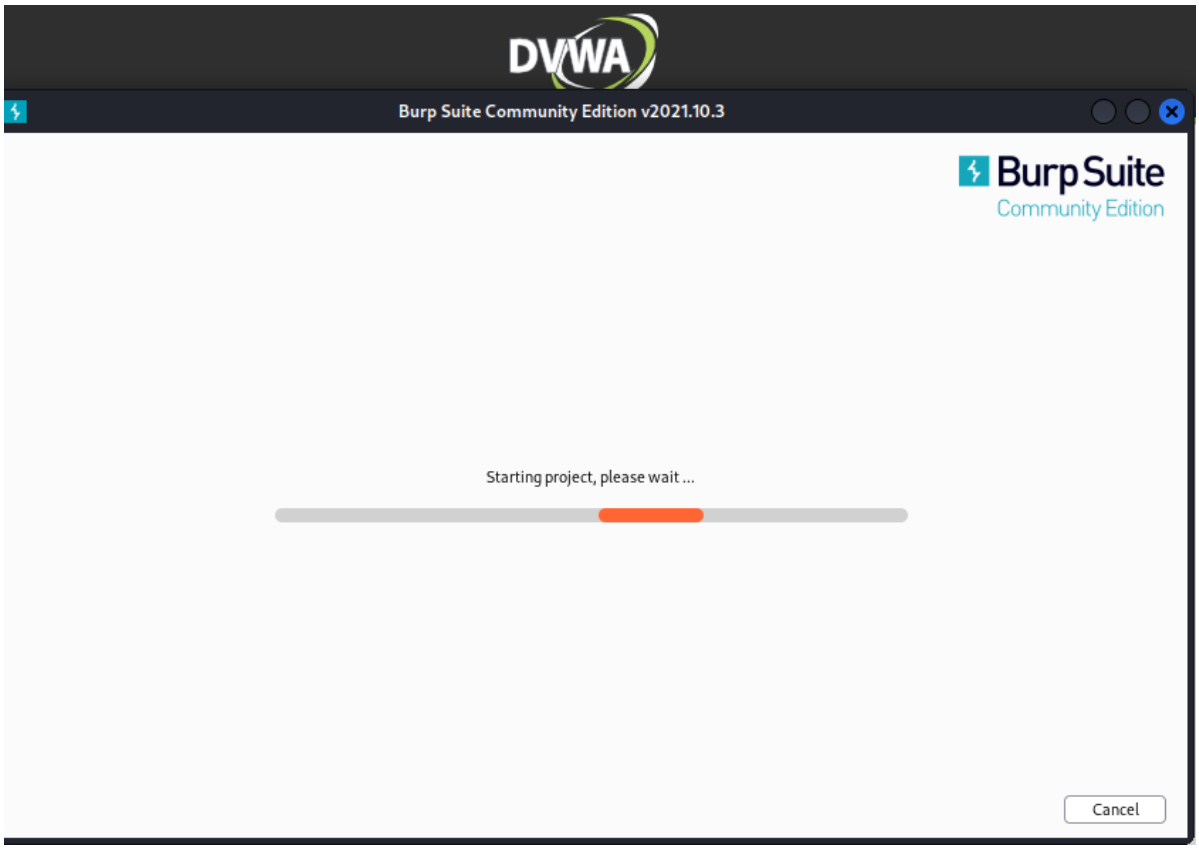
——----------CSRF ATTACK—----------

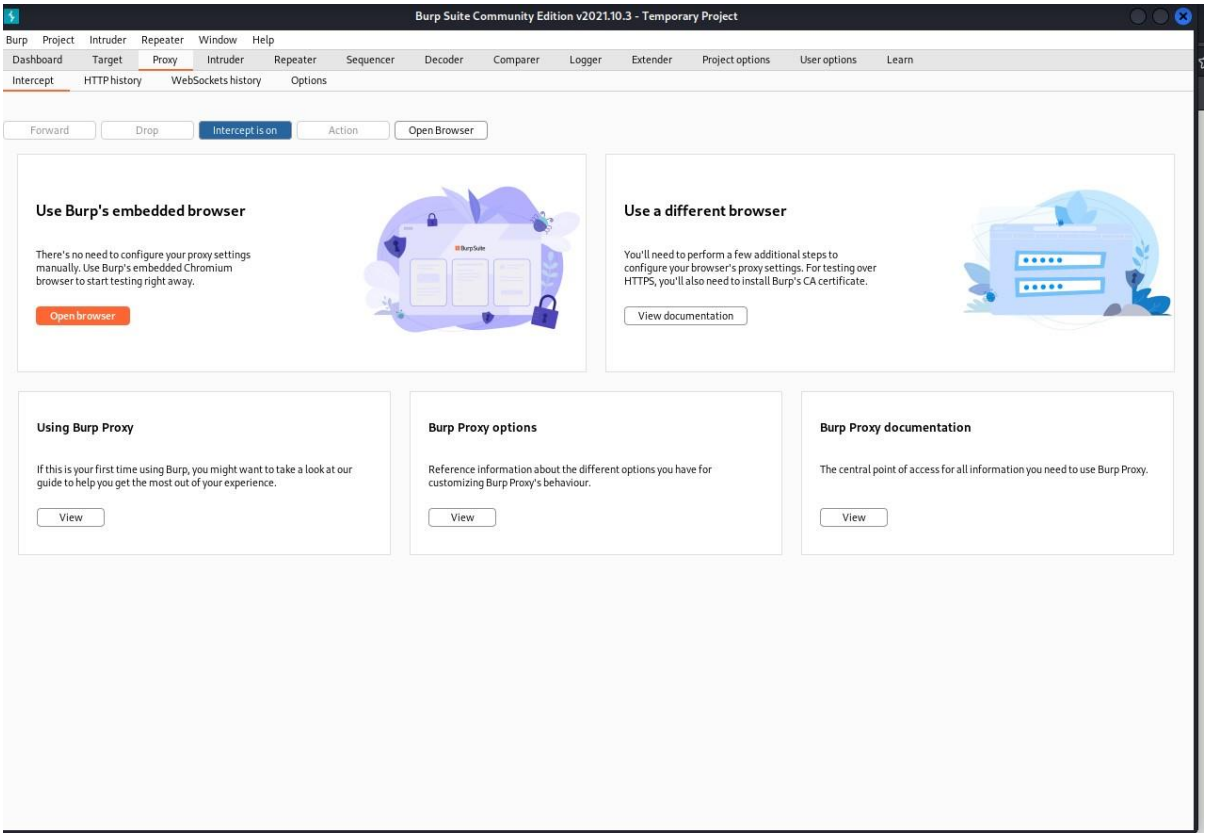


open burpsuite



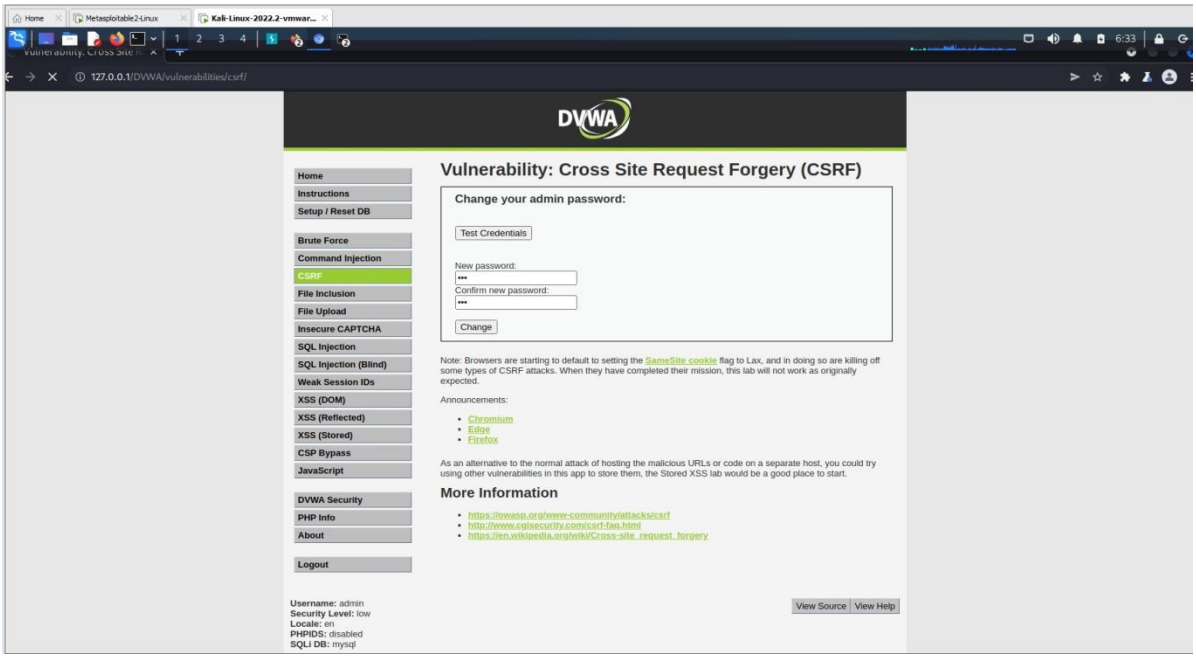
click start burp suite





open browser

search for

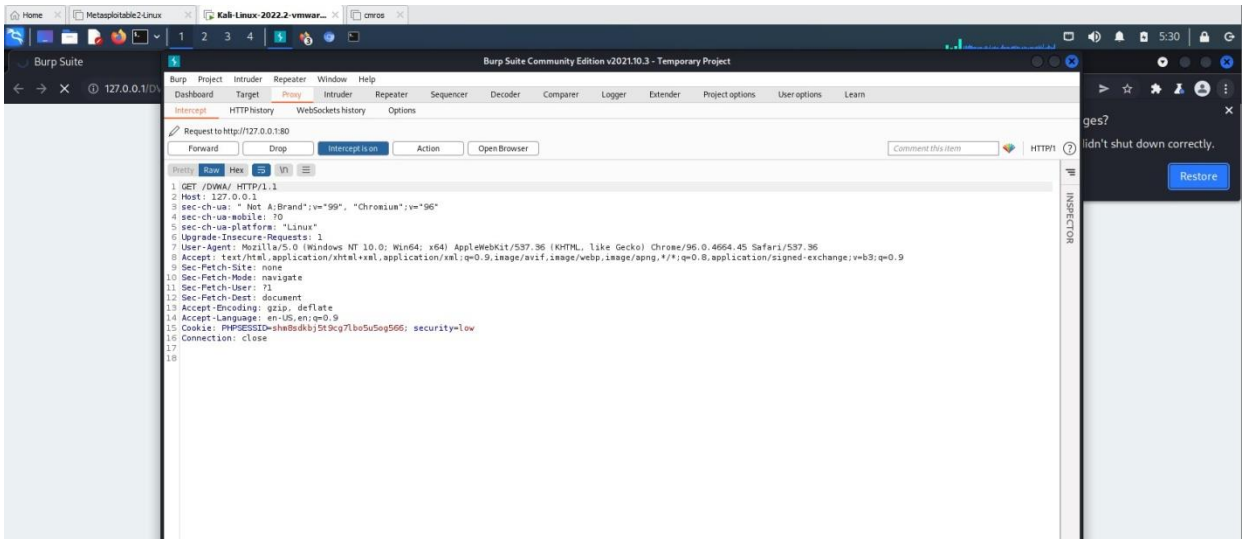


DVWA

http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_new=new&password_conf=new&Change=Change

login after inception is on

Go to browser using burp suite and



Result:

Thus the Command injection, XSS and CSRF attack completed successfully.