Ethical Hacker : sesión 4

- Ethical Hacker : sesión 4

clase

- Modulo 14
- Modulo 15
- Modulo 16
- Modulo 17

Modulo 14: Hacking Web Applications

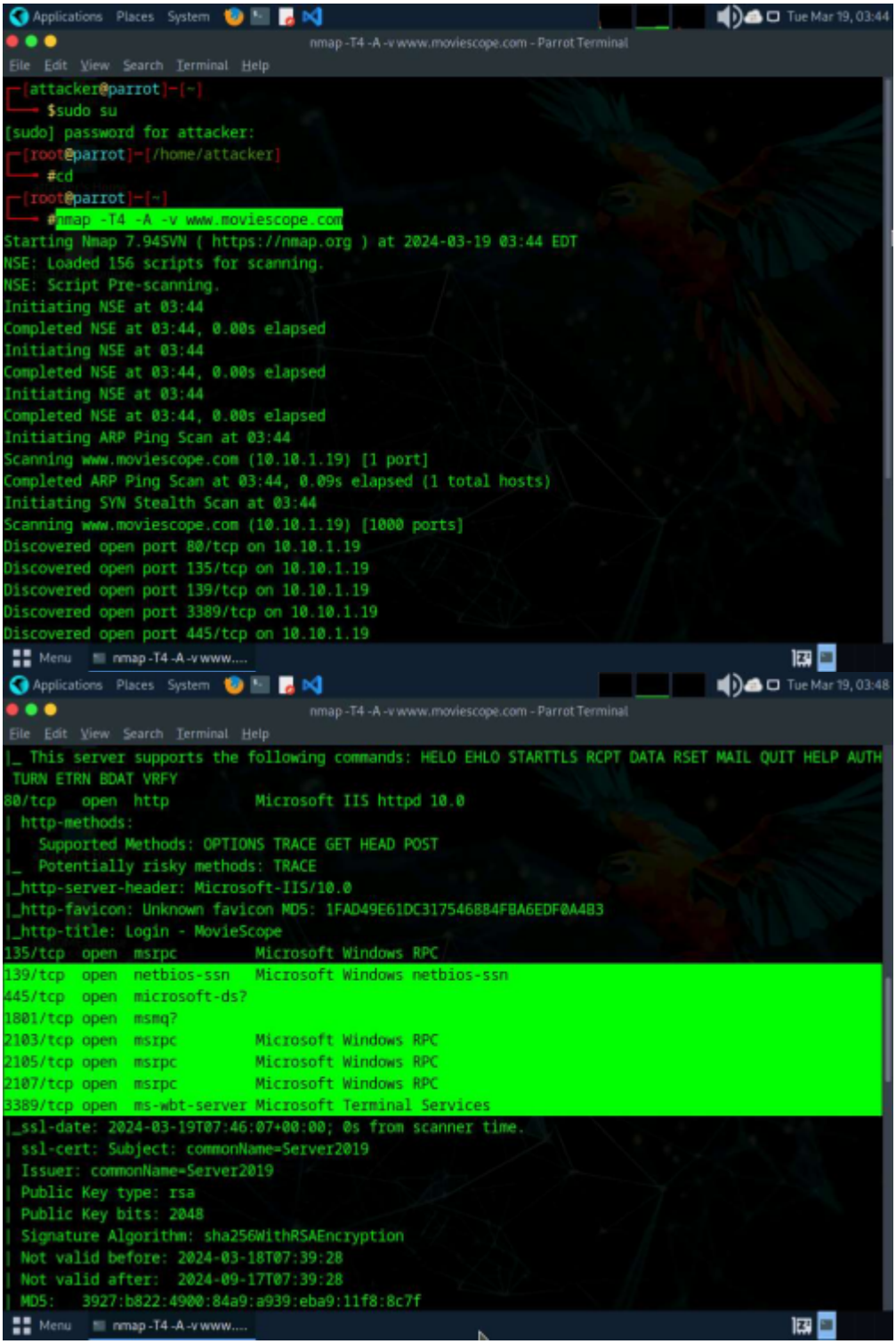
- Amenazas
- OWASP - https://owasp.org
    - asociación sin ánimo de lucro
    - proyectos relacionados con seguridad
    - Coraza - ModSecurity - set reglas programables
    - web security testint guide
- Componentes de terceros con problemas: https://blog.elhacker.net/2022/06/herramienta-YODA-encuentra-miles-plugins-maliciosos-en-wordpress.html
- Falta de monitorización
- Ataques a aplicaciones web
    - ataque transversal directorio
    - https://certifiedhacker.com/<portales/
        - se pueden escanear, permitido
        - ejemplos de vulnerabildiades
    - manipulación campos ocultos (via POST/GET)
        - amazon: `&pct-off=60-99` - Truco para añadir a la URL de amazon para ver los productos con un descuento dado.
    - pass-the-cookie
        - robar cookies para logearse en una web
    - same-site
    - command injection
        - shell
        - html
        - file
    - LDAP injection
    - XSS en comentarios (tipo 2)
    - evasión filtros XSS
    - Timing attacks
        - direct timing: deducir por la respuesta si el usuario existe o no
        - cross-site timing: paquetes de solictud manipulados usando javascript
        - browser-based timing: estimar el tiempo que tarda el server en procesar para saber si es correcto o no
    - XXE
        - invocación desde XML a una petición de fichero/recurso externo
    - redirecciones / reenvios inválidos
    - Magecart (web skimming): componentes de terceros desactualizados
    - Watering Hole (abrevadero): espera de potenciales víctimas, emboscada
    - CSRF

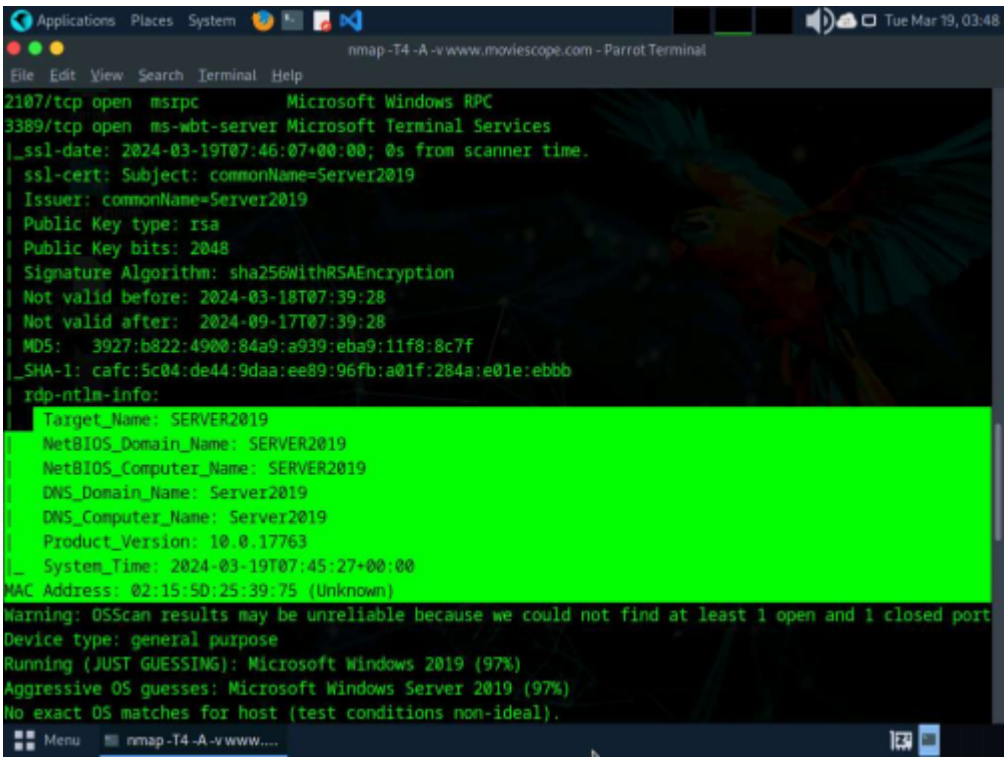
    - Manipulación / envenenamiento de cookies
    - Deserialización insegura
    - Ataques a servicios web
        - apuntes Fernando:
            - **SOAP** (Simple Object Access Protocol) es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse entre si, preguntando a UDDI por su localización, y por medio de intercambio de datos XML (documentos WSDL).
                - https://txikiboo.wordpress.com/2013/11/11/relacion-soap-wsdl-uddi/ - Artículo sobre SOAP
            - **UDDI** son las siglas del catálogo de servicios denominado Universal Description, Discovery and Integration. UDDI se comunica intercambiando archivos WSDL. Un servidor (o proveedor del servicio) debe realizar el registro de su servicio en UDDI para que sea localizable.
            - **WSDL** (Web Services Description Language), es un formato (XML) que se utiliza para describir servicios web (WS).
    - XML Poisoning
    - DNS Rebinding
        - saltarse restricciones de seguridad
        - controlar DNS secundario, bajar TTL
        - primera petición legítima, la siguiente manipulada
    - ...
- burpsuite: megaherramienta de seguridad (también vale para ZAP)
    - https://portswigger.net/burp - Descarga. Hay tres versiones:
        - Burp Suite Community Edition (gratis): https://portswigger.net/burp/communitydownload
        - Burp Suite Professional (349$ / año)
        - Burp Suite Enterprise Edition (a partir de 6000$ / año)
    - https://portswigger.net/web-security - Academy, formación gratuita, pero requiere cuenta.
    - https://portswigger.net/web-security/all-labs - Labs gratuitos, aunque requieren tener cuenta.
    - https://www.youtube.com/playlist?list=PL4TbrTdoQBY_dZQ9XI9NKwb5evvyfYQNQ - Un curso en video de Burp Suite, en español, que está bastante bien. Para novatos. Sacado de https://sniferl4bs.com/2020/06/curso-burp-suite-desde-0-presentaci%C3%B3n/
    - https://github.com/alphaSeclab/awesome-burp-suite/blob/master/Readme_en.md - Recopilación de recursos de Burp Suite

Lab 1 Module 14: Footprint the Web Infrastructure

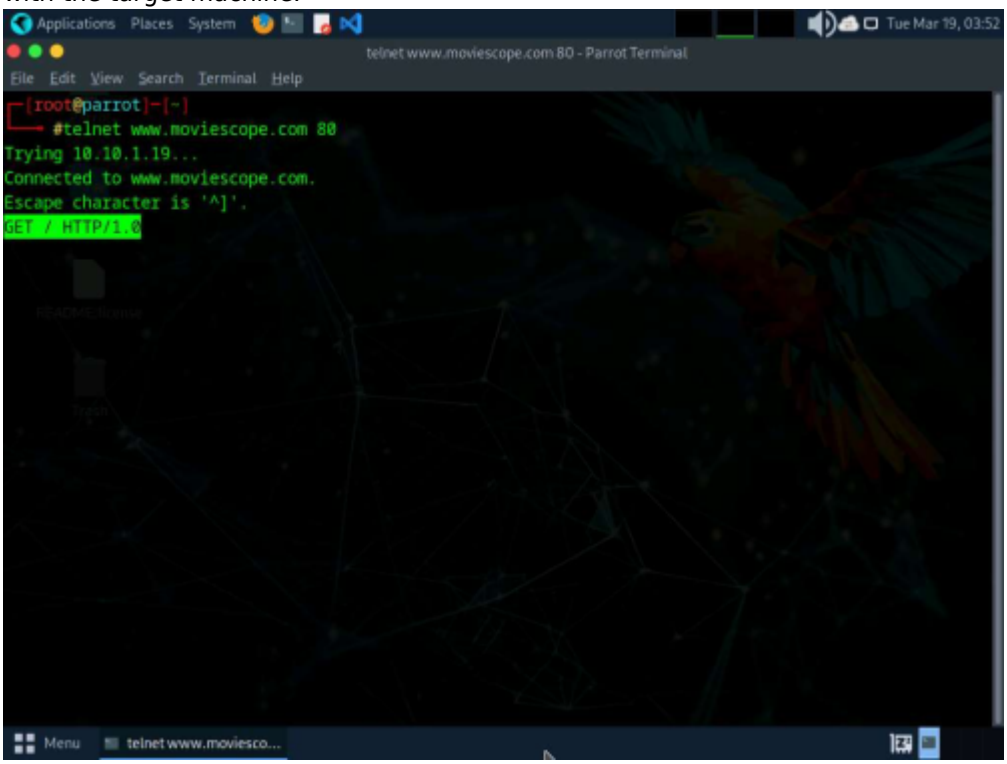
Task 1: Perform Web Application Reconnaissance using Nmap and Telnet

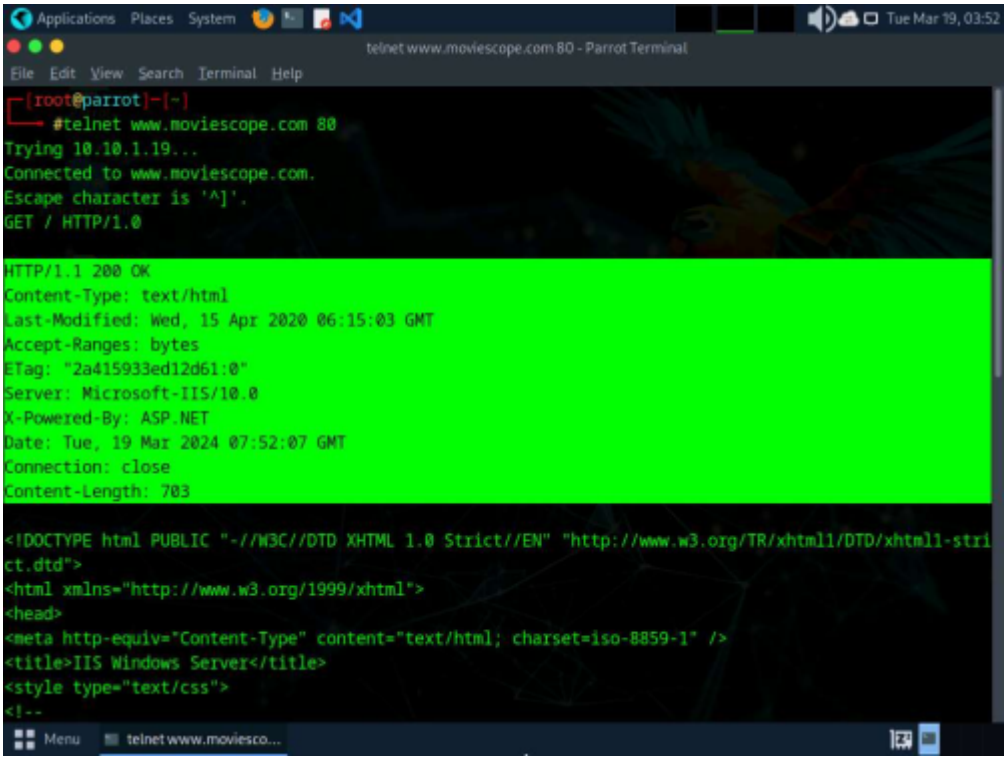
1. Perform a Whois lookup to gather information about the IP address of the web server and the complete information about the domain such as its registration details, name servers, IP address, and location.
2. Use tools such as Netcraft (https://www.netcraft.com), SmartWhois (https://www.tamos.com), WHOIS Lookup (https://whois.domaintools.com), and Batch IP Converter (http://www.sabsoft.com) to perform the Whois lookup.
3. Perform DNS Interrogation to gather information about the DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, etc.
4. Use tools such as, DNSRecon (https://github.com), and Domain Dossier (https://centralops.net) to perform DNS interrogation.
5. In the Parrot Terminal window, run nmap -T4 -A -v [Target Web Application] command (here, the target web application is www.moviescope.com) to perform a port and service discovery scan.


Applications Places System
Tue Mar 19, 03:44
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#nmap -T4 -A -v www.moviescope.com
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-19 03:44 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
Initiating NSE at 03:44
Completed NSE at 03:44, 0.00s elapsed
Initiating ARP Ping Scan at 03:44
Scanning www.moviescope.com (10.10.1.19) [1 port]
Completed ARP Ping Scan at 03:44, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 03:44
Scanning www.moviescope.com (10.10.1.19) [1000 ports]
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 445/tcp on 10.10.1.19
Menu
nmap -T4 -A -v www....
Applications Places System
Tue Mar 19, 03:48
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
TURN ETRN BDAT VRFY
80/tcp open http Microsoft IIS httpd 10.0
| http-methods:
| Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-favicon: Unknown favicon MD5: 1FAD49E61DC3175468B4FBA6EDF0A4B3
|_http-title: Login - MovieScope
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
1801/tcp open msmq?
2103/tcp open msrpc Microsoft Windows RPC
2105/tcp open msrpc Microsoft Windows RPC
2107/tcp open msrpc Microsoft Windows RPC
3389/tcp open ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-03-19T07:46:07+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Server2019
| Issuer: commonName=Server2019
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-03-18T07:39:28
| Not valid after: 2024-09-17T07:39:28
| MD5: 3927:b822:4900:84a9:a939:eba9:11f8:8c7f
Menu
nmap -T4 -A -v www....



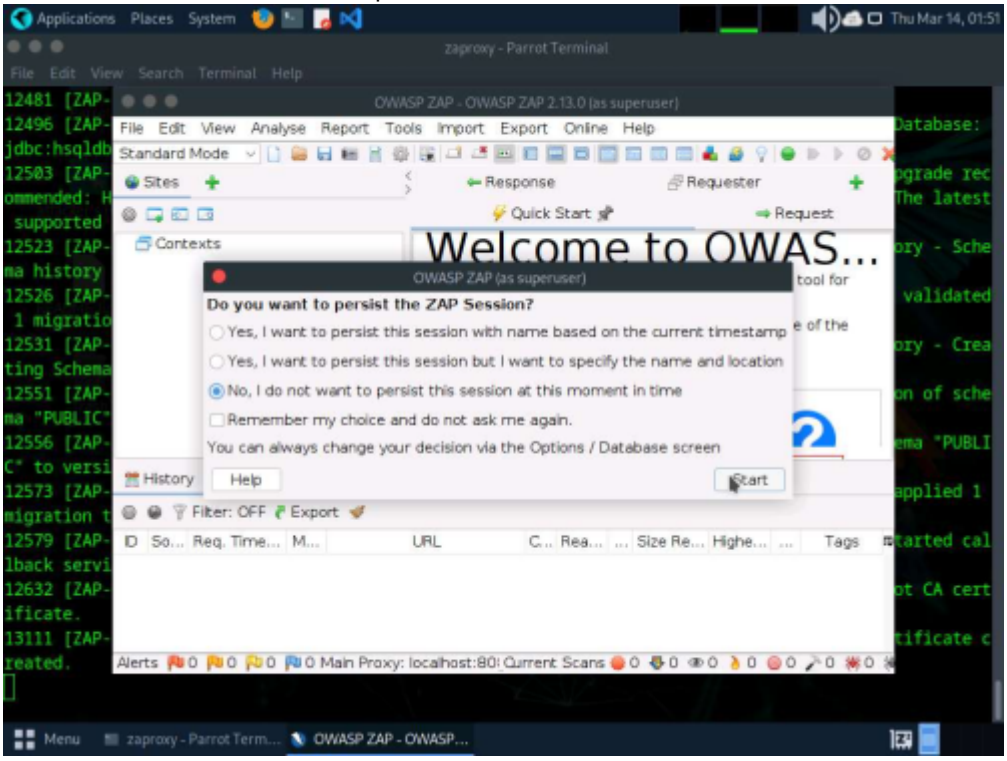
6. In the terminal window, run command telnet www.moviescope.com 80 to establish a telnet connection with the target machine.



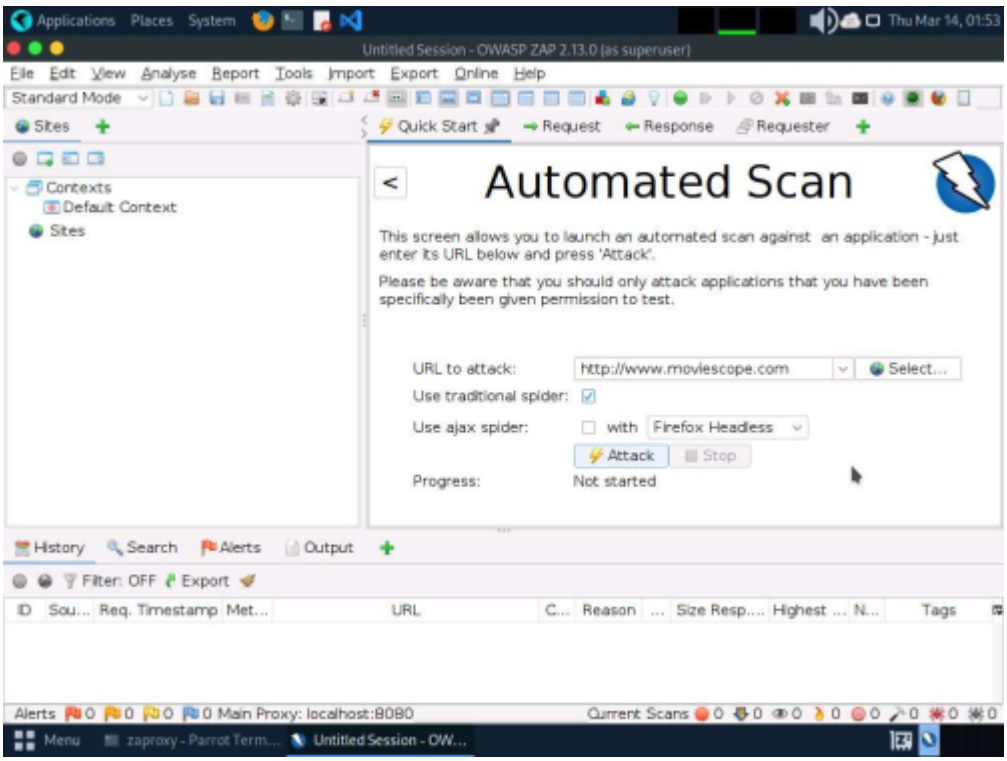


Task 2: Perform Web Spidering using OWASP ZAP

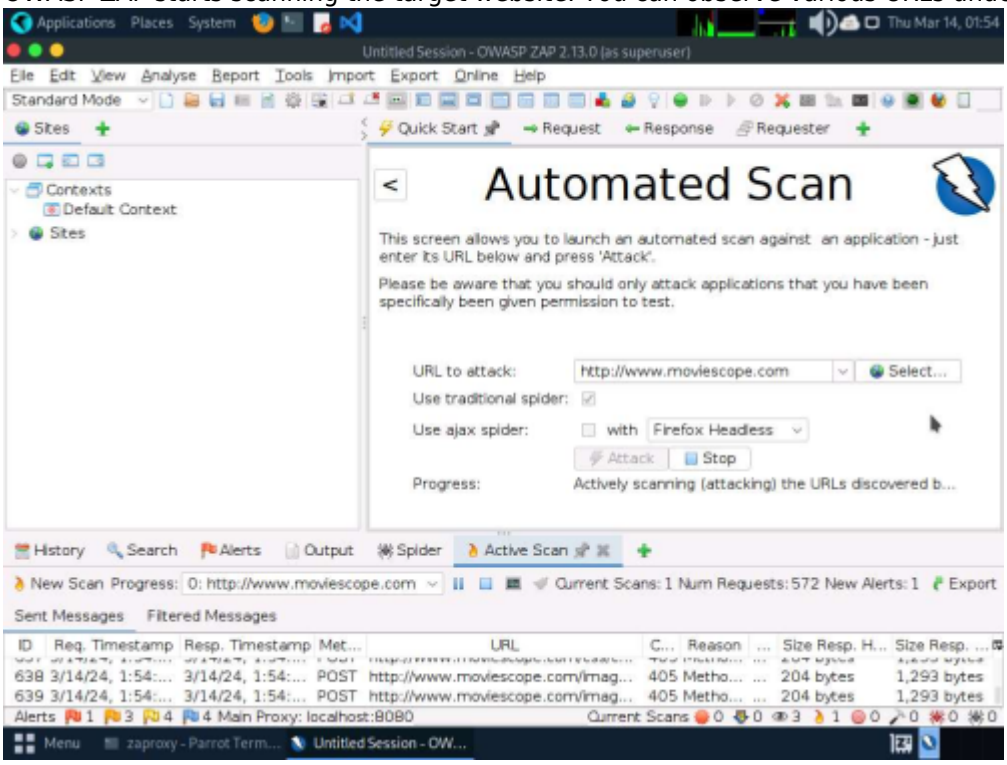
1. In the Terminal window, type zaproxy and press Enter to launch OWASP ZAP.
2. After completing initialization, a prompt that reads Do you want to persist the ZAP Session? appears; select the No, I do not want to persist this session at this moment in time radio button and click Start.



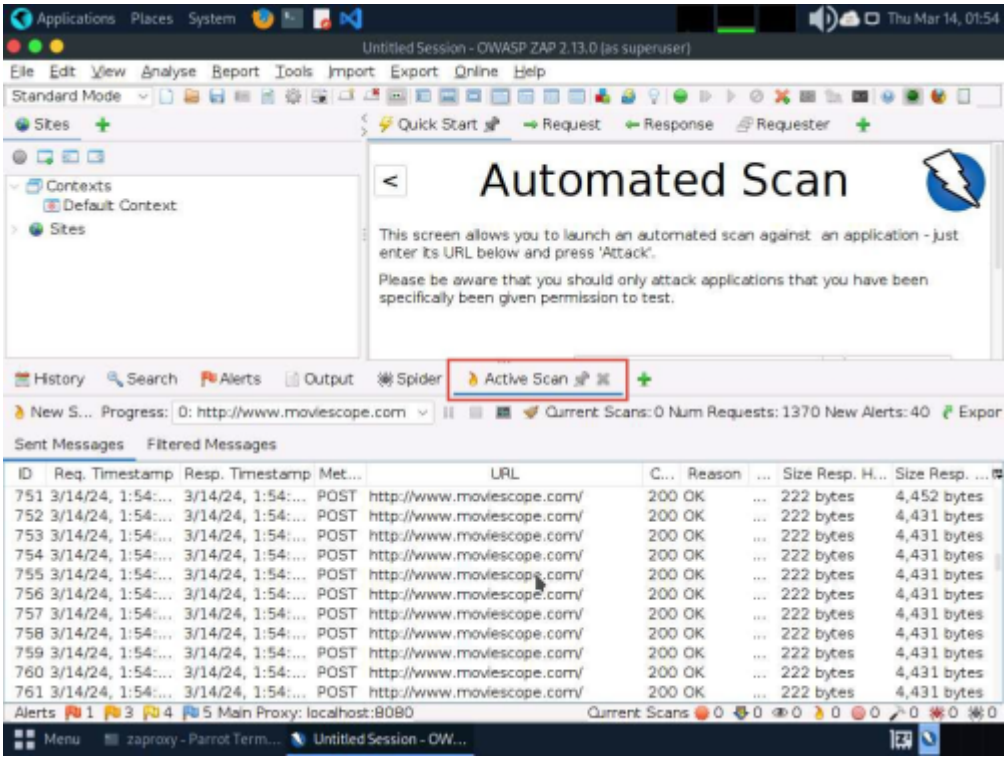
3. The Automated Scan wizard appears; enter the target website under the URL to attack field (here, www.moviescope.com). Leave the other settings to default and click the Attack button.



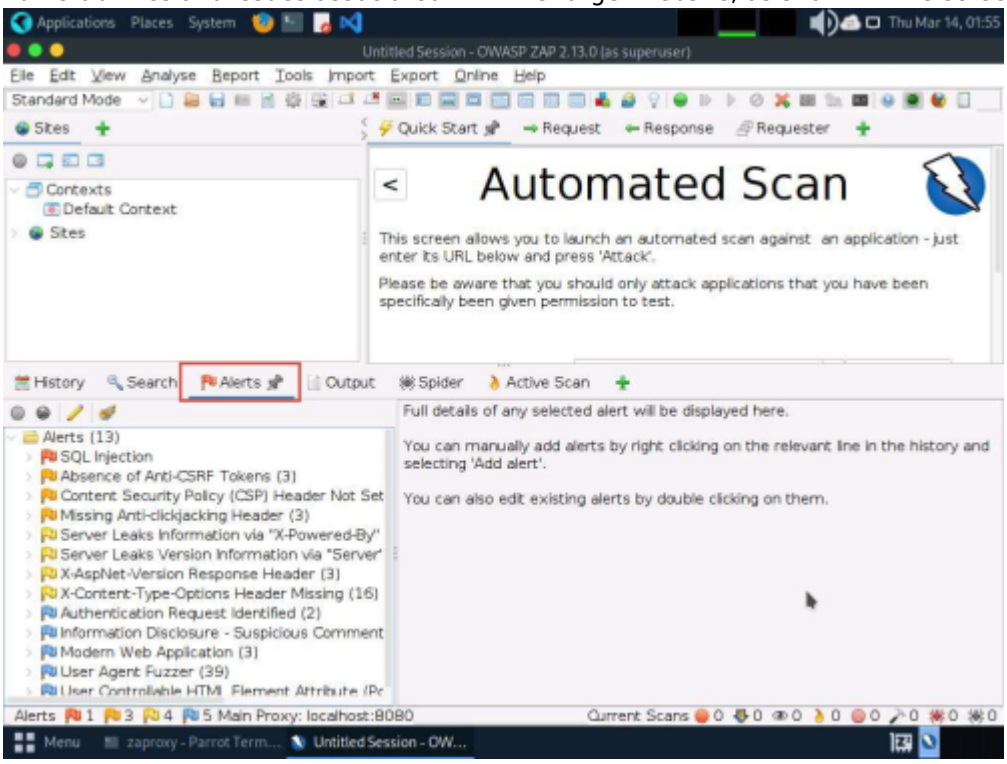
4. OWASP ZAP starts scanning the target website. You can observe various URLs under the Spider tab.



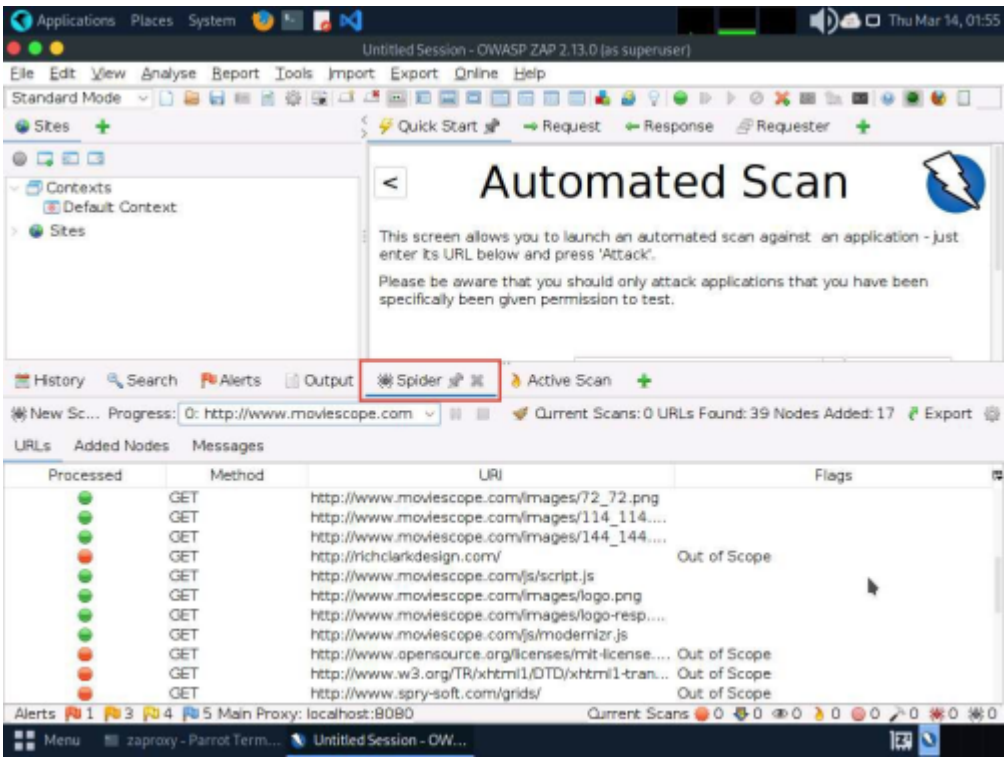
5. After performing web spidering, OWASP ZAP performs active scanning. Navigate to the Active Scan tab to observe the various scanned links.



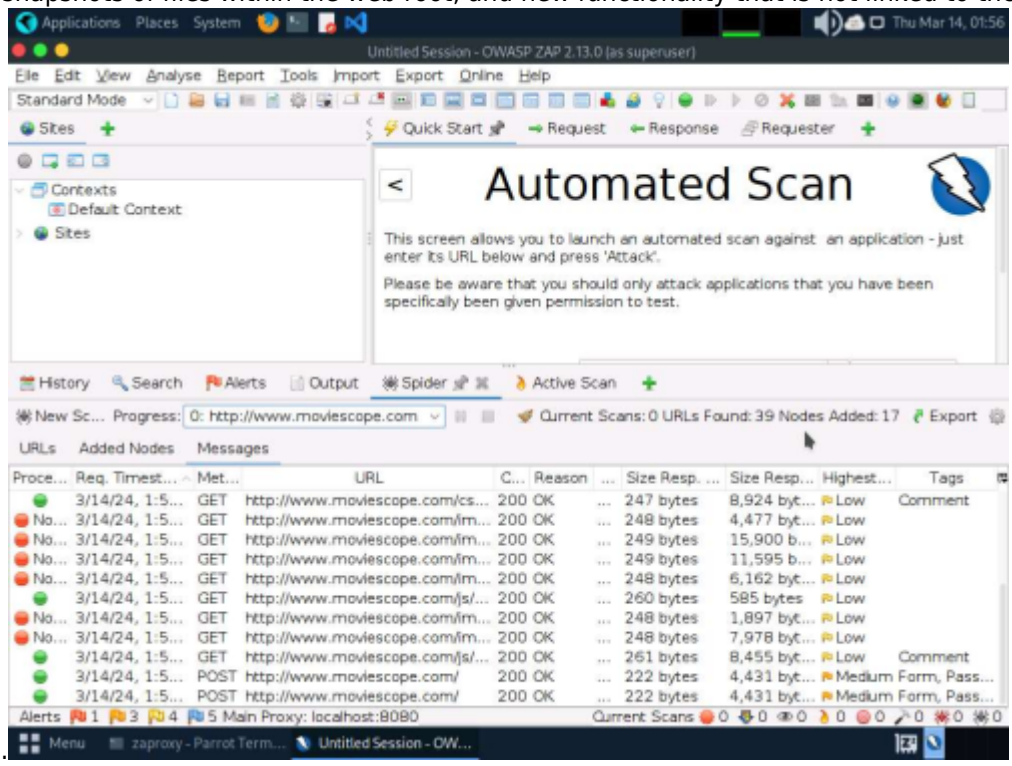
6. After completing the active scan, the results appear under the Alerts tab, displaying the various vulnerabilities and issues associated with the target website, as shown in the screenshot.



7. Now, click on the Spider tab from the lower section of the window to view the web spidering information. By default, the URLs tab appears under the Spider tab.
8. The URLs tab contains various links for hidden content and functionality associated with the target website (www.moviescope.com).

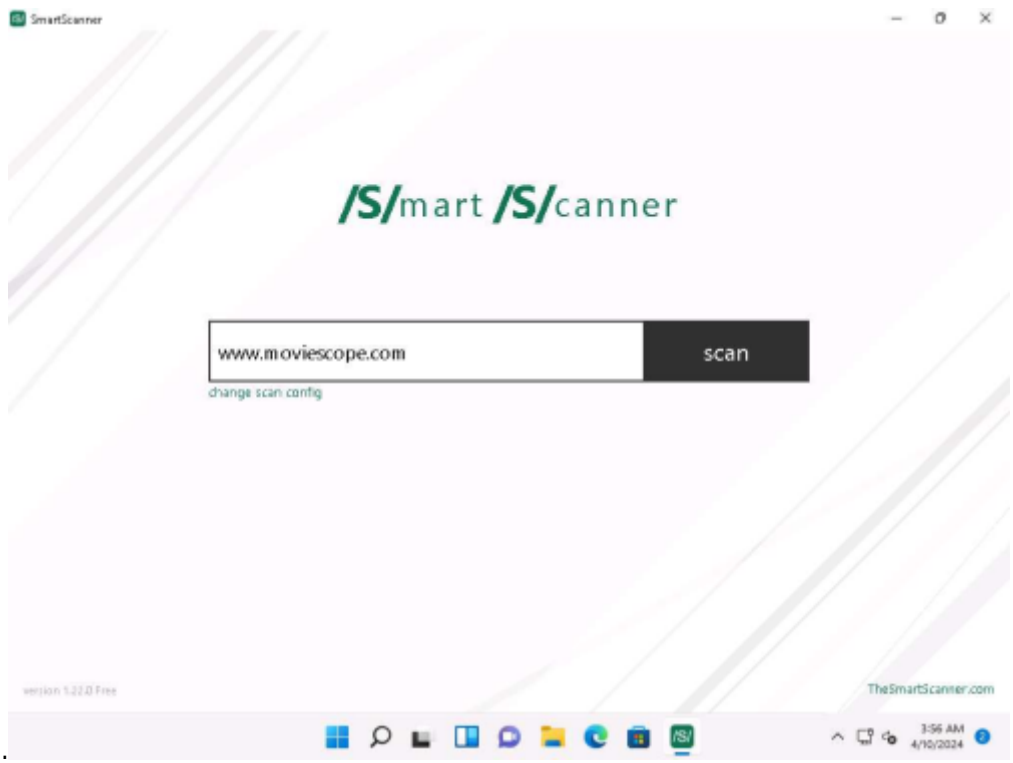


9. Now, navigate to the Messages tab under the Spider tab to view more detailed information regarding the URLs obtained while performing the web spidering, as shown in the screenshot. In real-time, attackers perform web spidering or crawling to discover hidden content and functionality, which is not reachable from the main visible content, to exploit user privileges within the application. It also allows attackers to recover backup copies of live files, configuration and log files containing sensitive data, backup archives containing snapshots of files within the web root, and new functionality that is not linked to the main application.



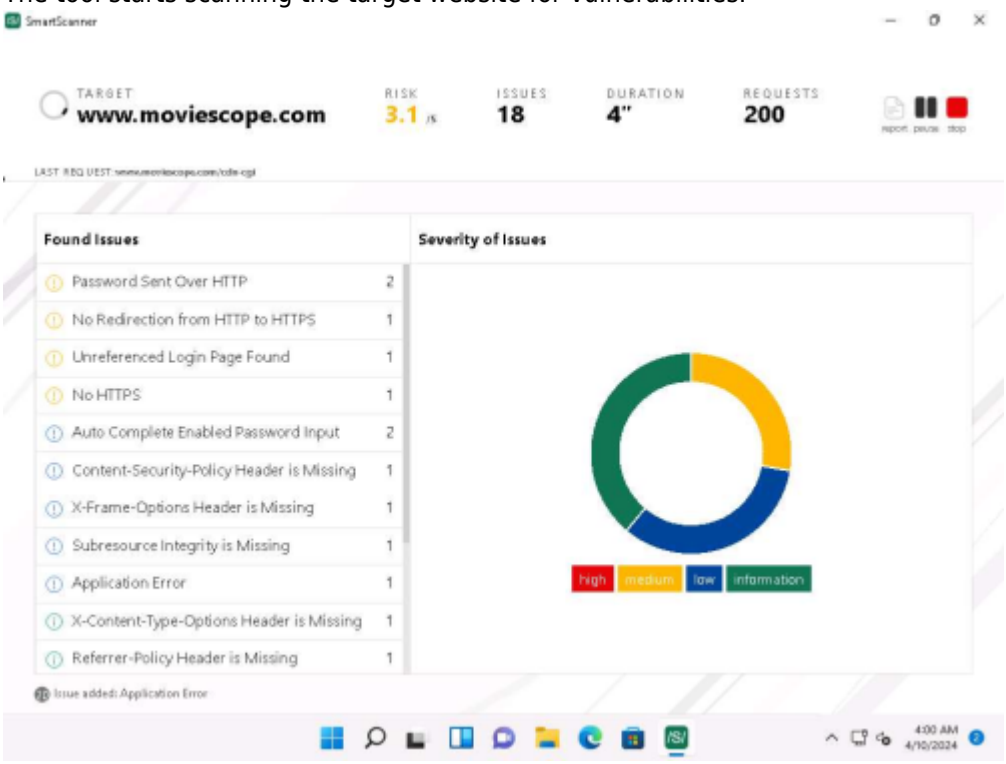
Task 3: Perform Web Application Vulnerability Scanning using SmartScanner

1. SmartScanner window appears. In the enter site address to scan field, enter www.moviescope.com and

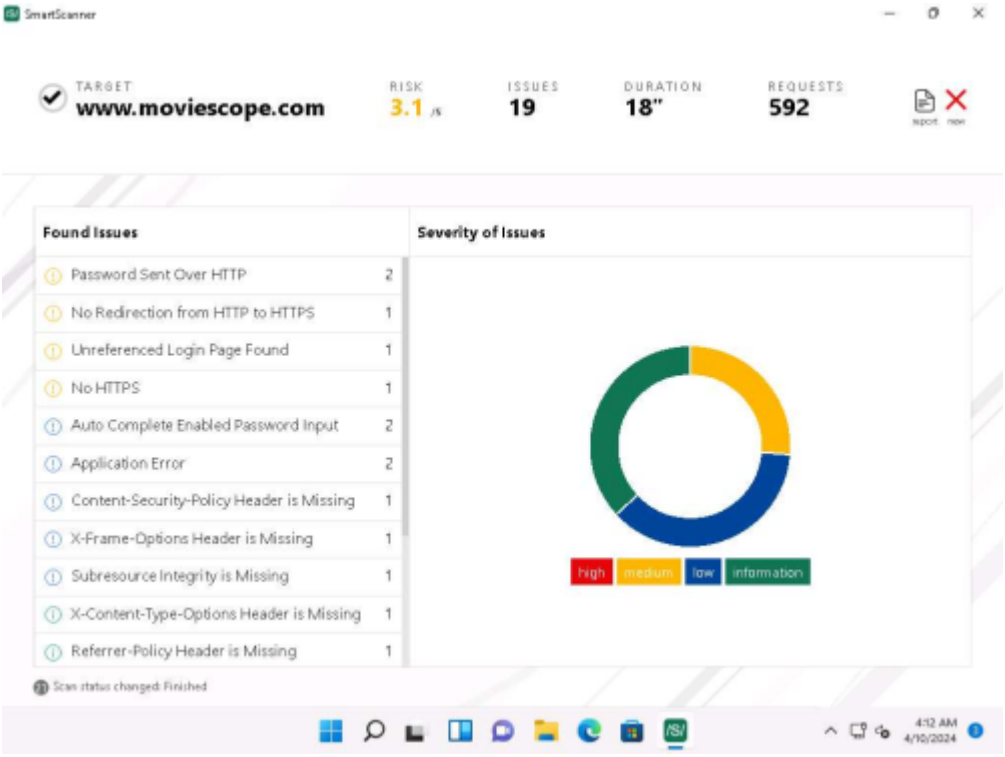


click scan button.

2. The tool starts scanning the target website for vulnerabilities.

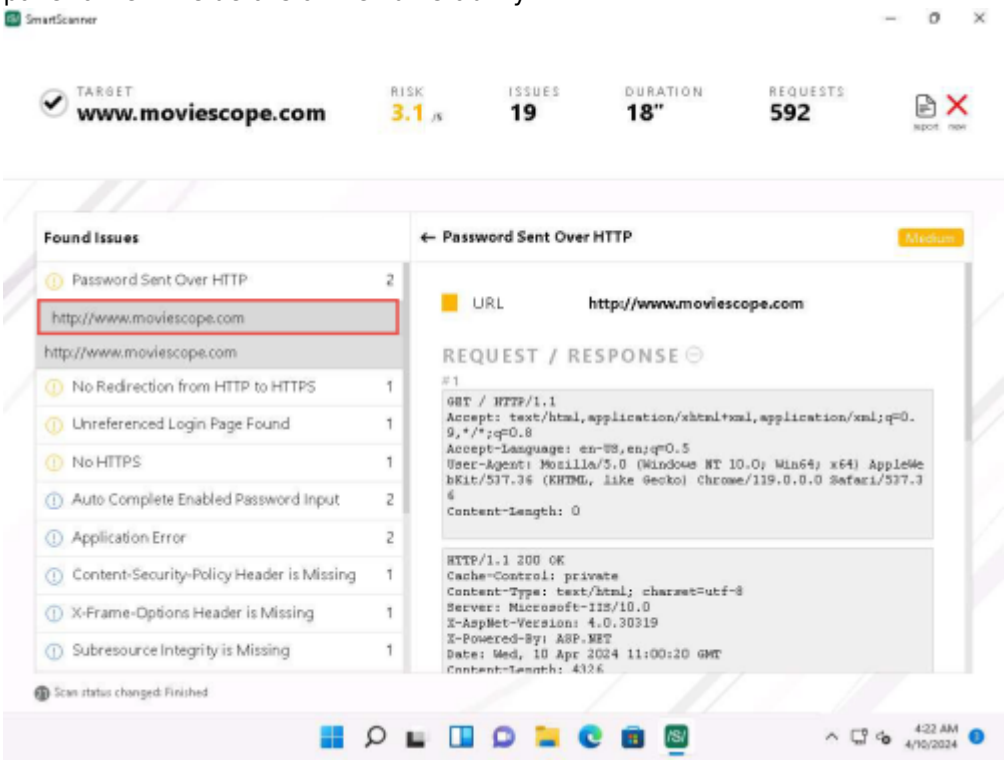


3. Once the tool completes scanning, it will display the issues that are found under Found Issues section and

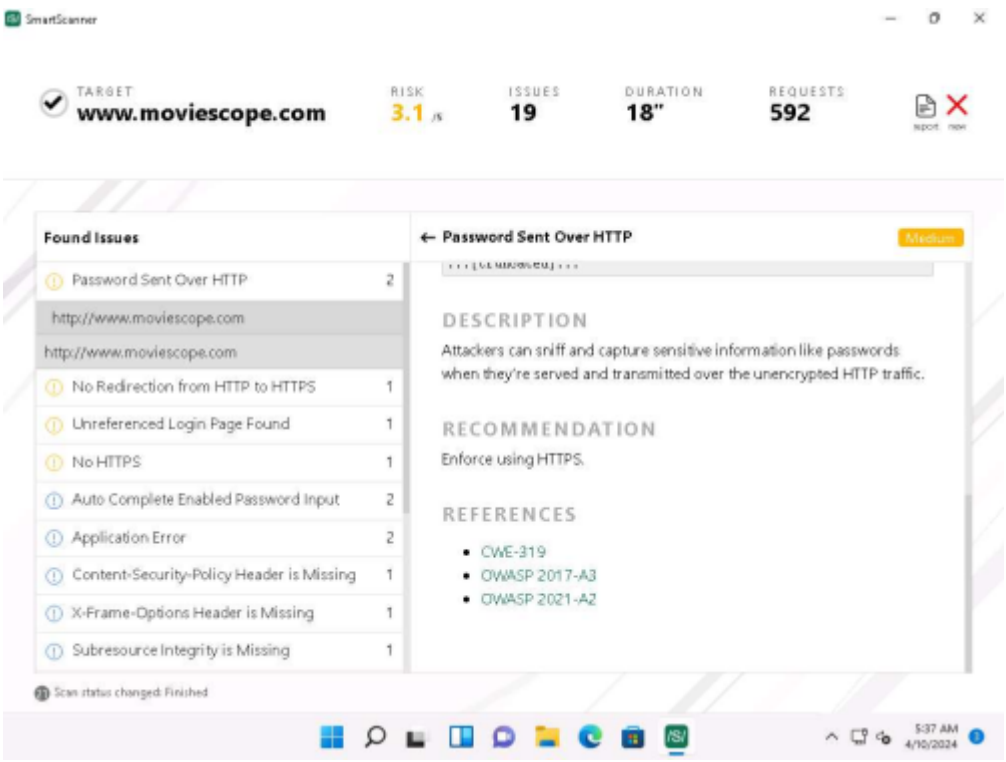


Severity of Issues.

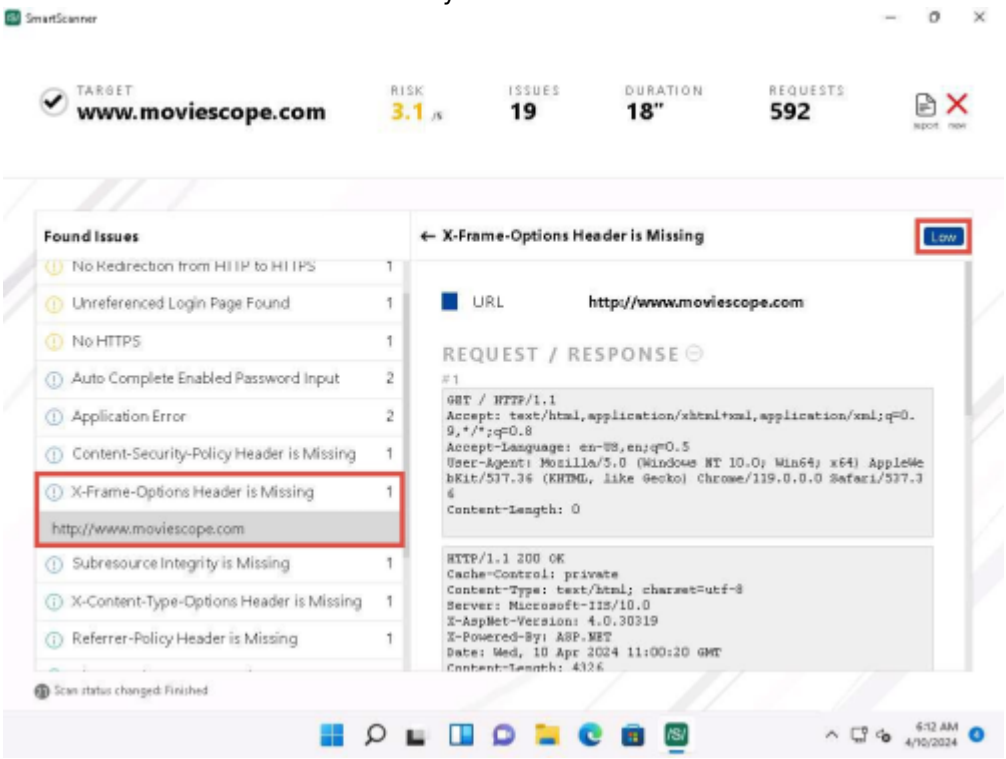
4. Now, expand Password Sent Over HTTP and click on first http://www.moviescope.com link from the left pane to view the details of the vulnerability.



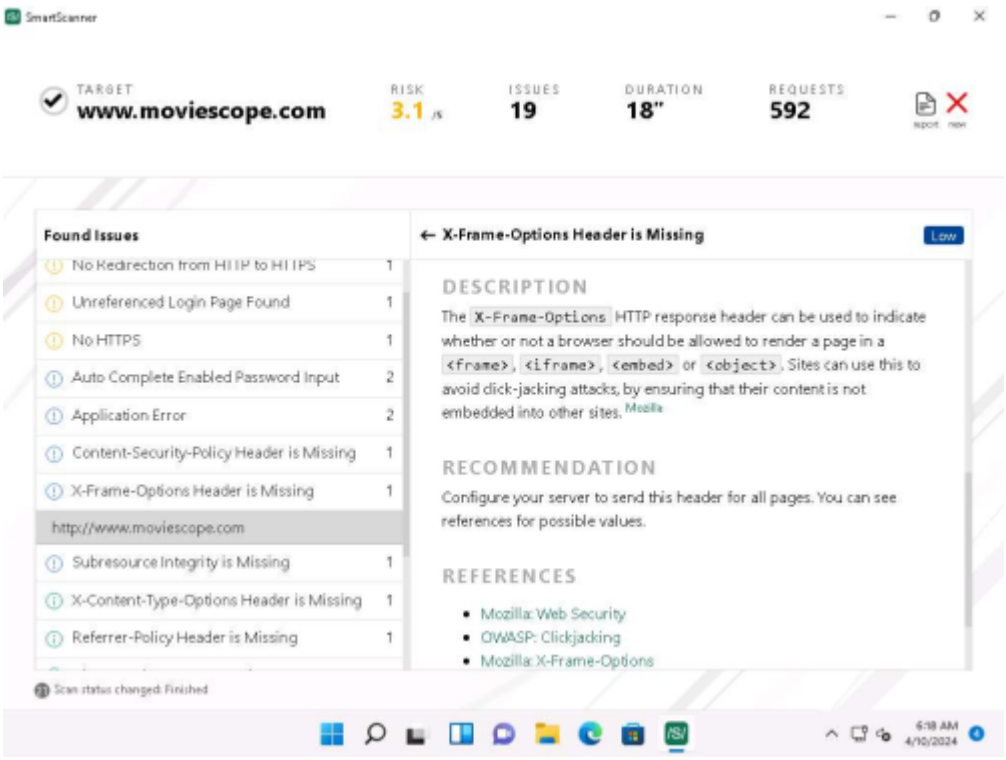
5. In the right pane, scroll down to the DESCRIPTION part. We can observe that this website contains a vulnerability, which could be exploited by attackers to intercept sensitive information like passwords during transmission over unencrypted HTTP traffic.



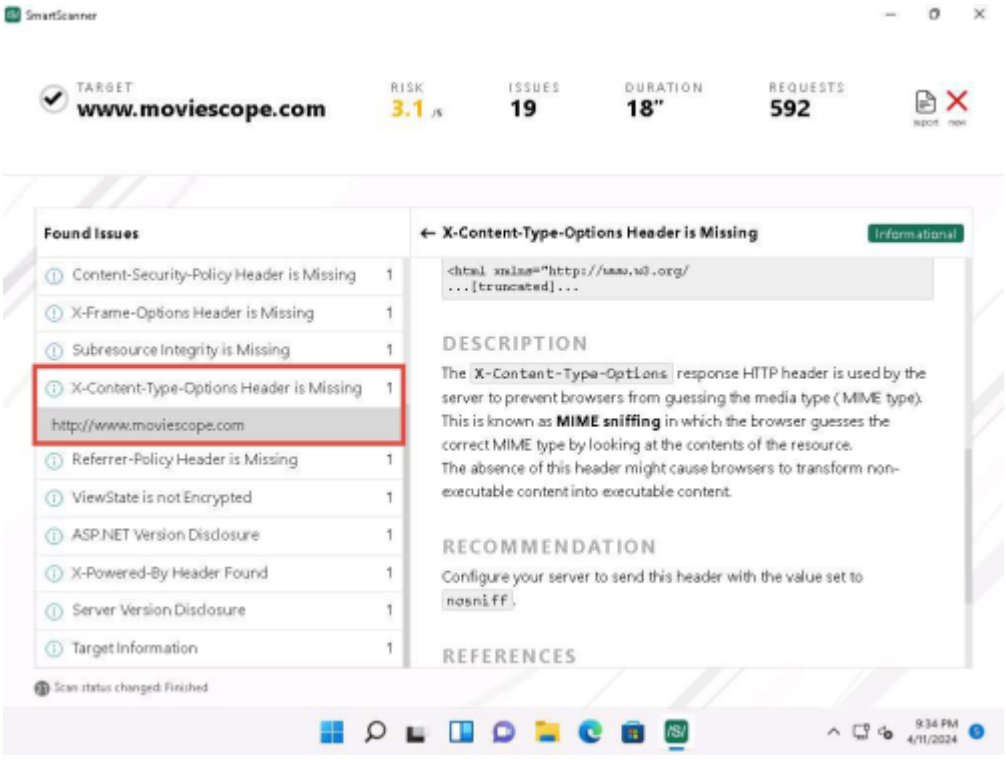
6. You can also go through the RECOMMENDATION section to check for the recommended actions to patch the vulnerability.
7. Now, under REFERENCES section, press Ctrl and click on CWE-319 hyperlink .
8. A CWE website appears in Microsoft Edge web browser, displaying the details of CWE-319 ClearText Transmission of Sensitive Information.
9. Similarly, click the http://www.moviescope.com link available under X-Frame-Options Header is Missing node which is termed as Low severity.



10. Scroll down to the DESCRIPTION here, we can observe that the X-Frame-Options Header is Missing which will make this site vulnerable to click-jacking.



11. Now, expand X-Content-Type-Options Header is Missing node and click on http://www.moviescope.com link to view its contents.
12. Under DESCRIPTION section we can observe that the browsers can perform MIME sniffing which can cause the browsers to transform non-executable content into executable content.

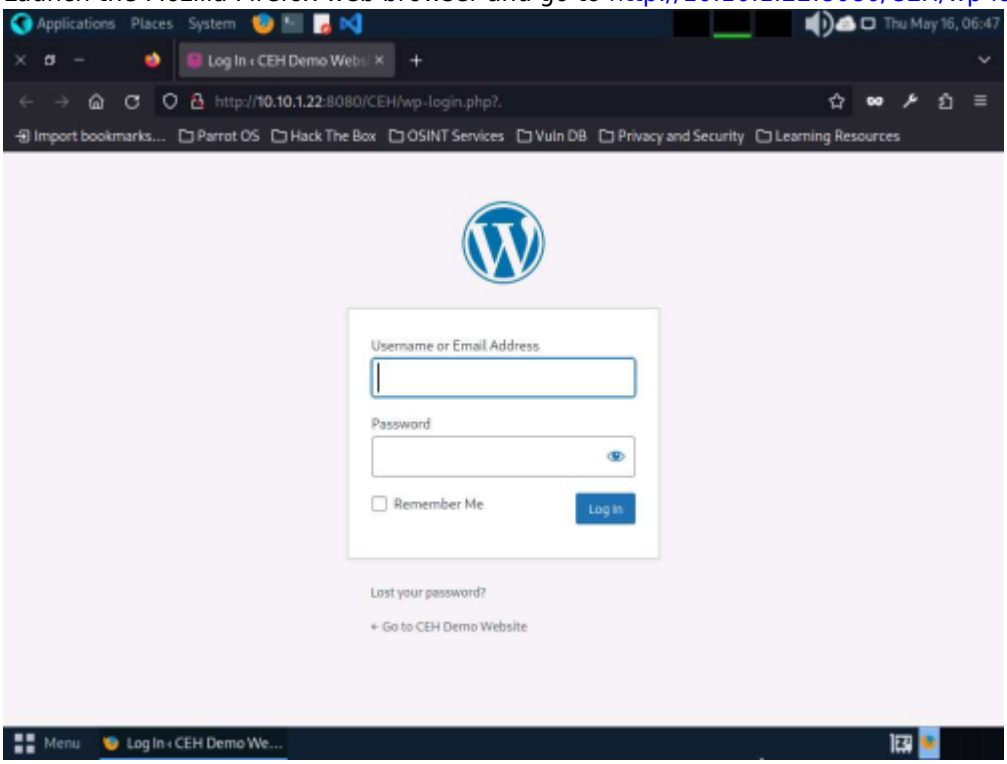


13. Similarly, you can view the the RECOMMENDATION section and click on the reference link under REFERENCES section.
14. You can also use other web application vulnerability scanning tools such as:
    1. WPScan Vulnerability Database (https://wpscan.com),
    2. Codename SCNR (https://ecsypno.com),
    3. AppSpider (https://www.rapid7.com),
    4. Uniscan (https://github.com),
    5. N-Stalker (https://www.nstalker.com).

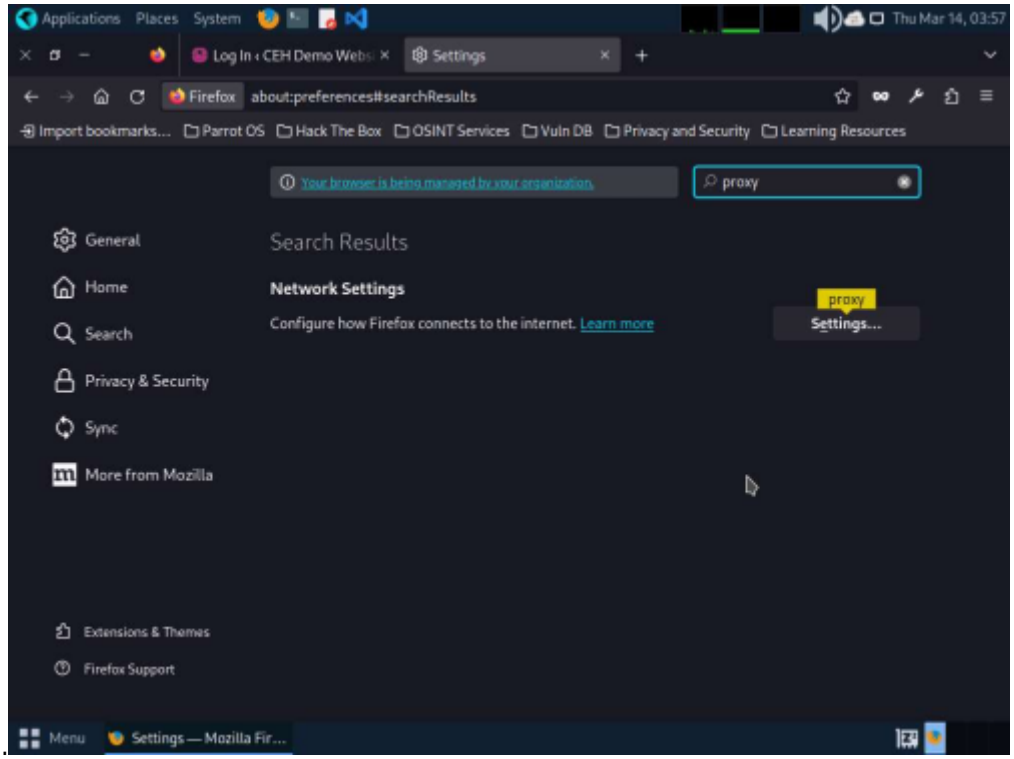
Lab 2 Module 14: Perform Web Application Attacks

Task 1: Perform a Brute-force Attack using Burp Suite

1. In this task, the target WordPress website (http://10.10.1.22:8080/CEH) is hosted by the victim machine, Windows Server 2022. Here, the host machine is the Parrot Security machine.
2. Ensure that the Wampserver is running in Windows Server 2022 machine. To run the WampServer, execute the following steps:
    1. Now, click Type here to search field on the Desktop, search for wampserver64 in the search bar and select Wampserver64 from the results.
    2. Click the Show hidden icons icon, observe that the WampServer icon appears.
    3. Wait for this icon to turn green, which indicates that the WampServer is successfully running.
3. Launch the Mozilla Firefox web browser and go to http://10.10.1.22:8080/CEH/wp-login.php?.

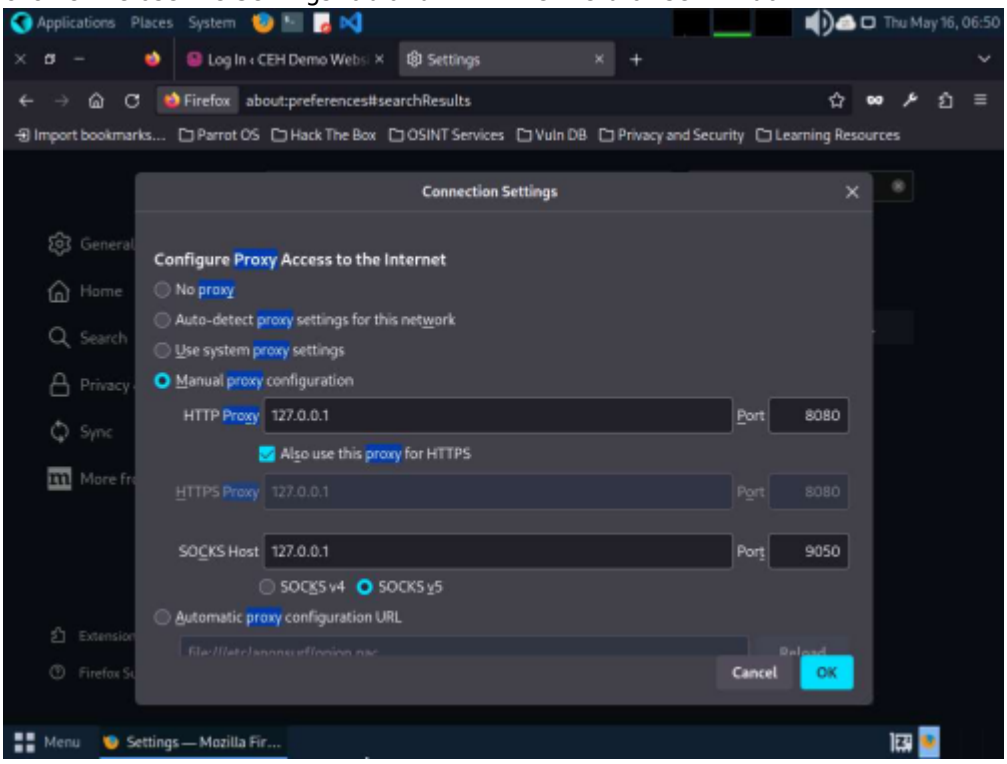


    1. Here, we will perform a brute-force attack on the designated WordPress website hosted by the Windows Server 2022 machine.
4. Now, we shall set up a Burp Suite proxy by first configuring the proxy settings of the browser.In the Mozilla Firefox browser, click the Open application menu icon in the right corner of the menu bar and select Settings from the drop-down list. The General settings tab appears. In the Find in Settings search bar, search for proxy and in the Search Results, click the Settings button under the Network Settings

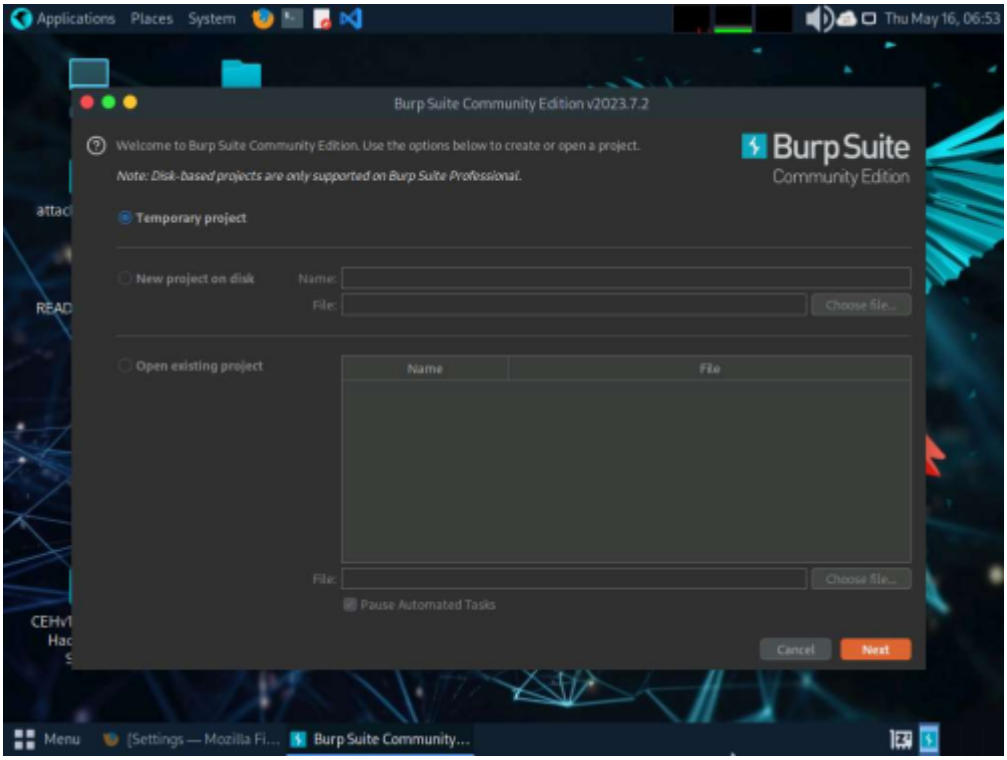


option.

5. The Connection Settings window appears; select the Manual proxy configuration radio button and specify the HTTP Proxy as 127.0.0.1 and the Port as 8080. Tick the Also use this proxy for HTTPS checkbox and click OK. Close the Settings tab and minimize the browser window.

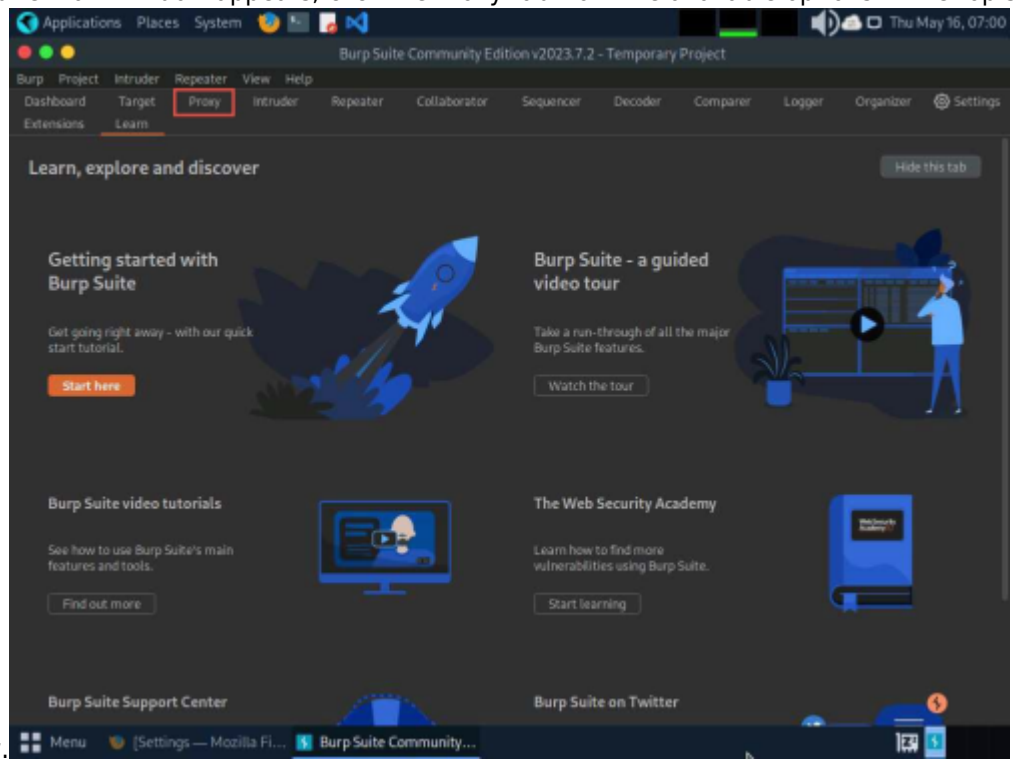


6. Now, minimize the browser window, click the Applications menu form the top left corner of Desktop, and navigate to Pentesting –> Web Application Analysis –> Web Application Proxies –> Burpsuite CE to launch the Burpsuite CE application.

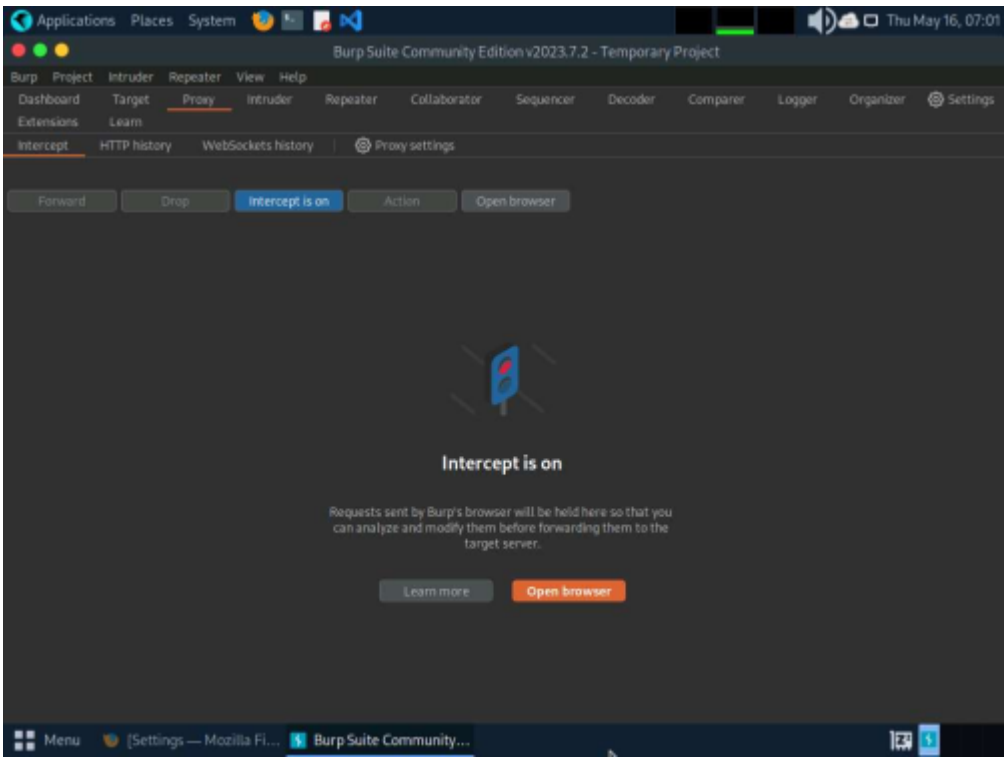


1. In the next window, select the Use Burp defaults radio-button and click the Start Burp button.

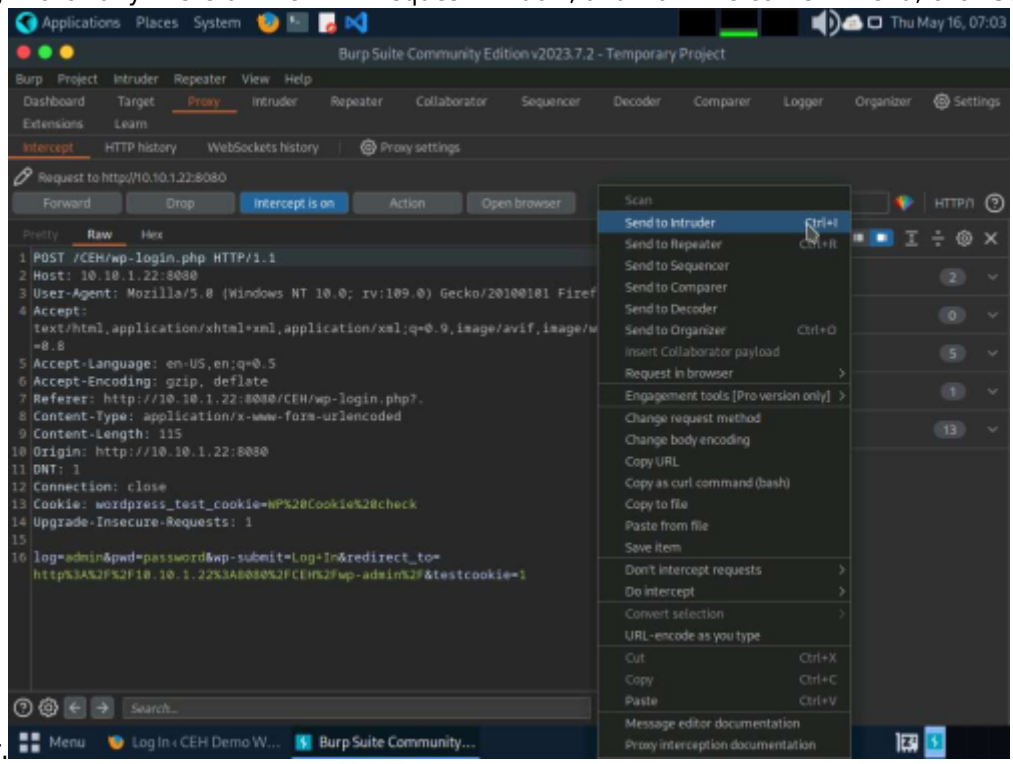
7. The Burp Suite main window appears; click the Proxy tab from the available options in the top section of the window.



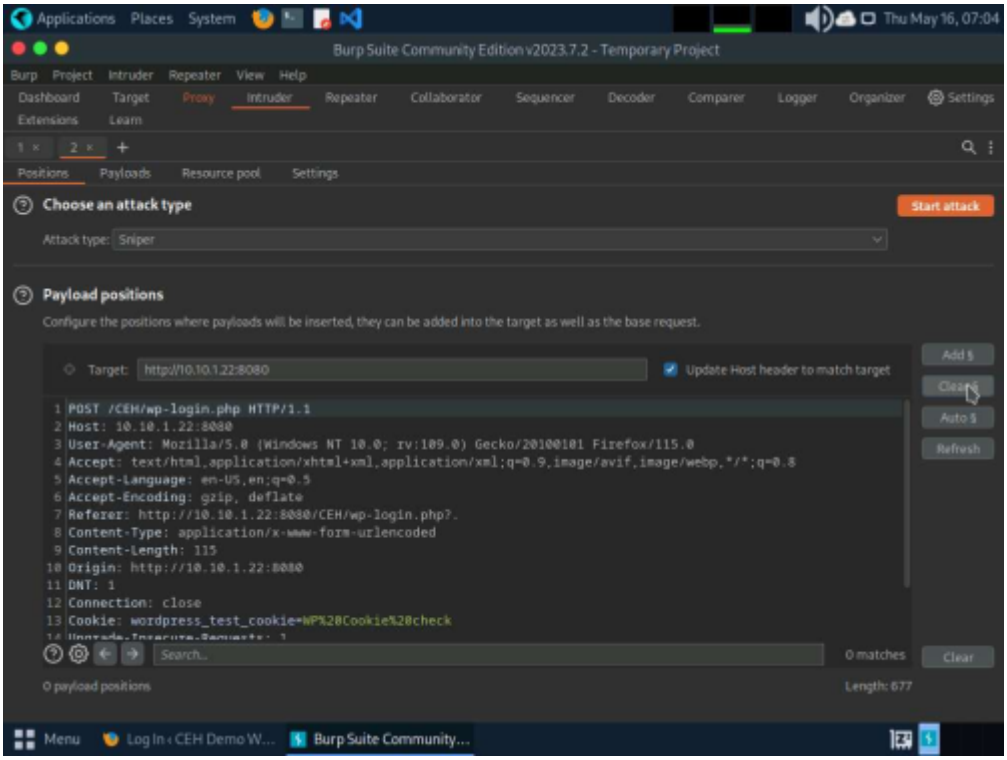
8. In the Proxy settings, by default, the Intercept tab opens-up. Observe that by default, the interception is active as the button says Intercept is on. Leave it running.



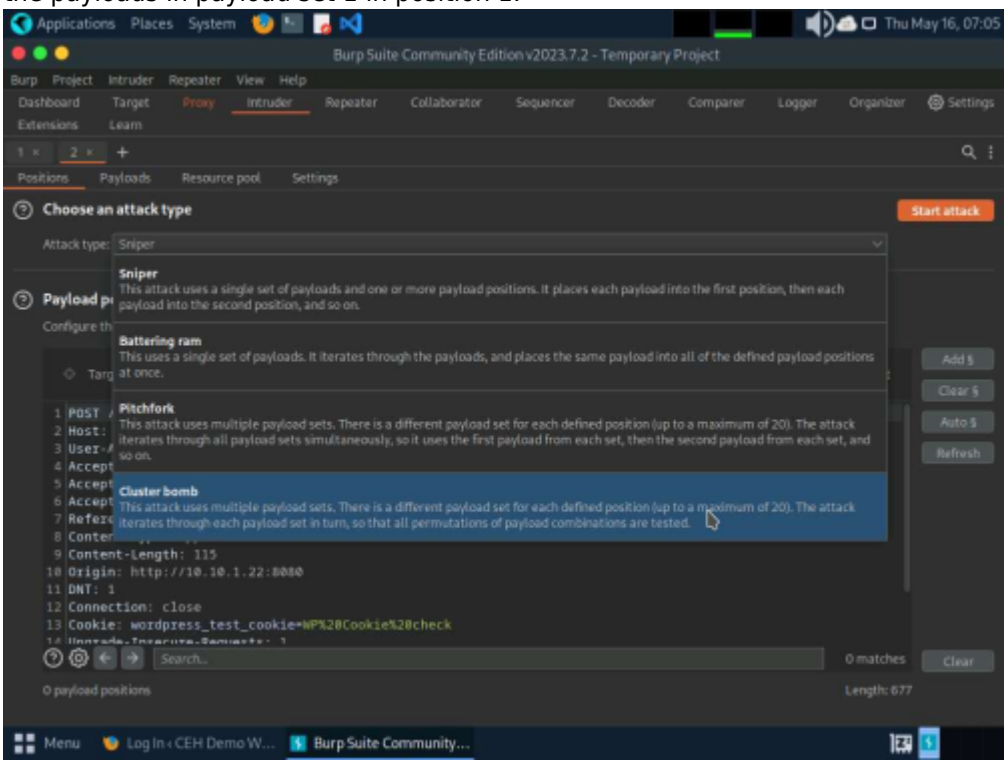
9. Switch back to the browser window. On the login page of the target WordPress website, type random credentials, here admin and password. Click the Log In button.
10. Switch back to the Burp Suite window; observe that the HTTP request was intercepted by the application.
11. Now, right-click anywhere on the HTTP request window, and from the context menu, click Send to Intruder.



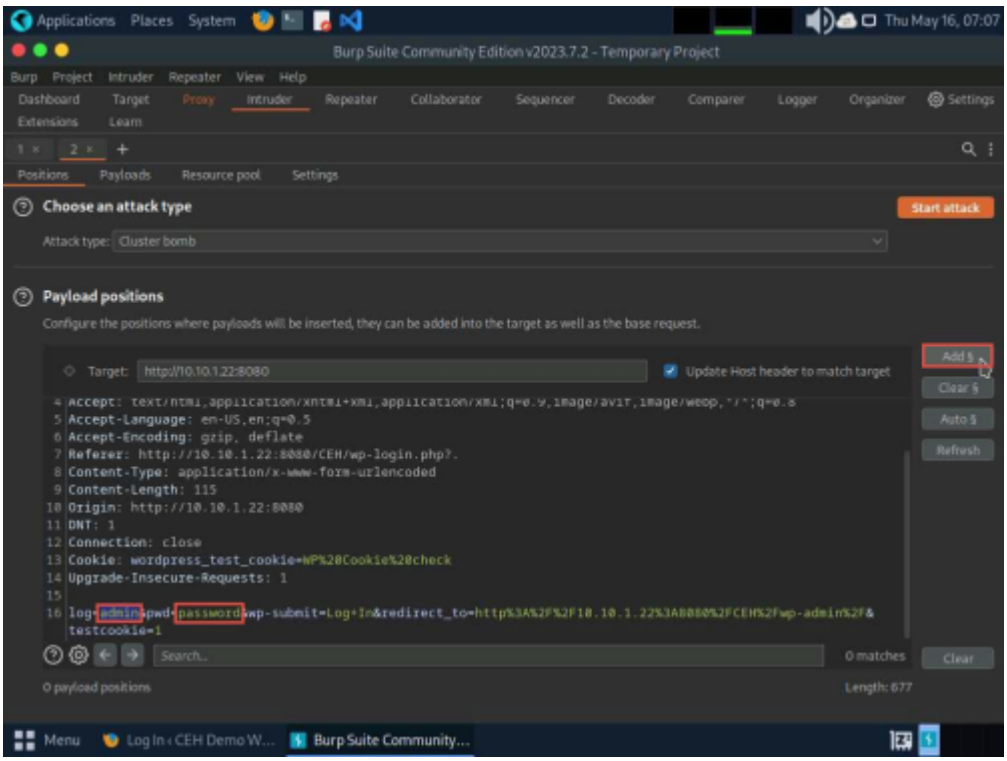
12. Now, click on the Intruder tab from the toolbar and observe that under the Intruder tab, the Positions tab appears by default. In the Positions tab under the Intruder tab observe that Burp Suite sets the target positions by default, as shown in the HTTP request. Click the Clear § button from the right-pane to clear the default payload values.



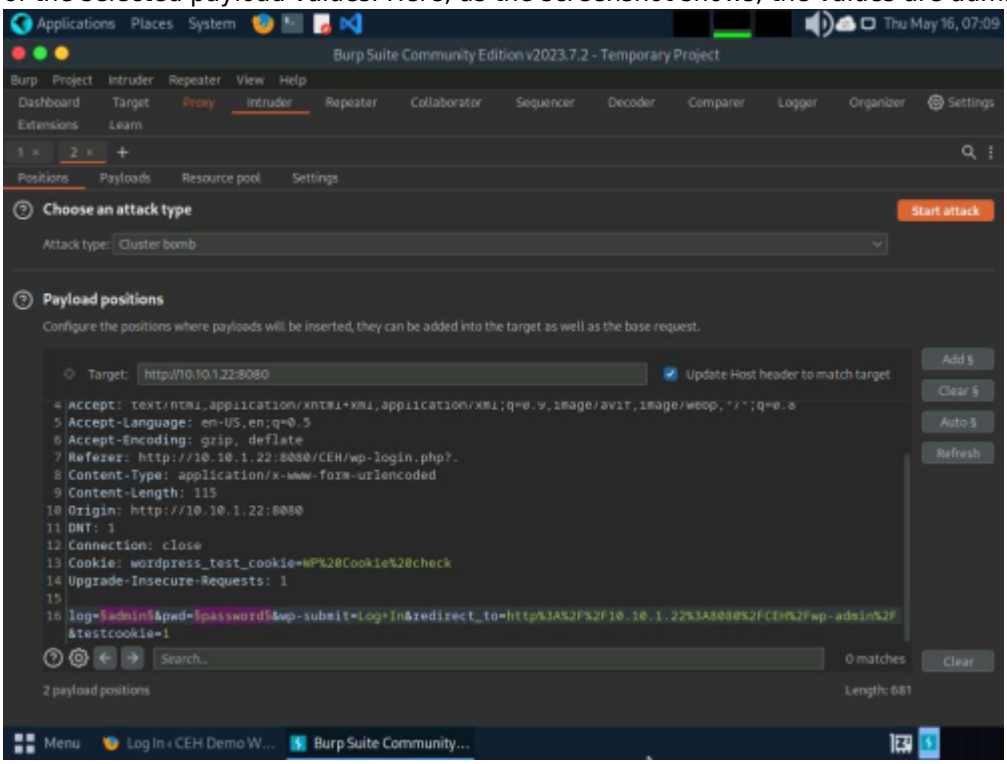
13. Once you clear the default payload values, select Cluster bomb from the Attack type drop-down list. Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will place the first payload from payload set 2 into position 2 and iterate through all payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2 and iterate through all the payloads in payload set 1 in position 1.



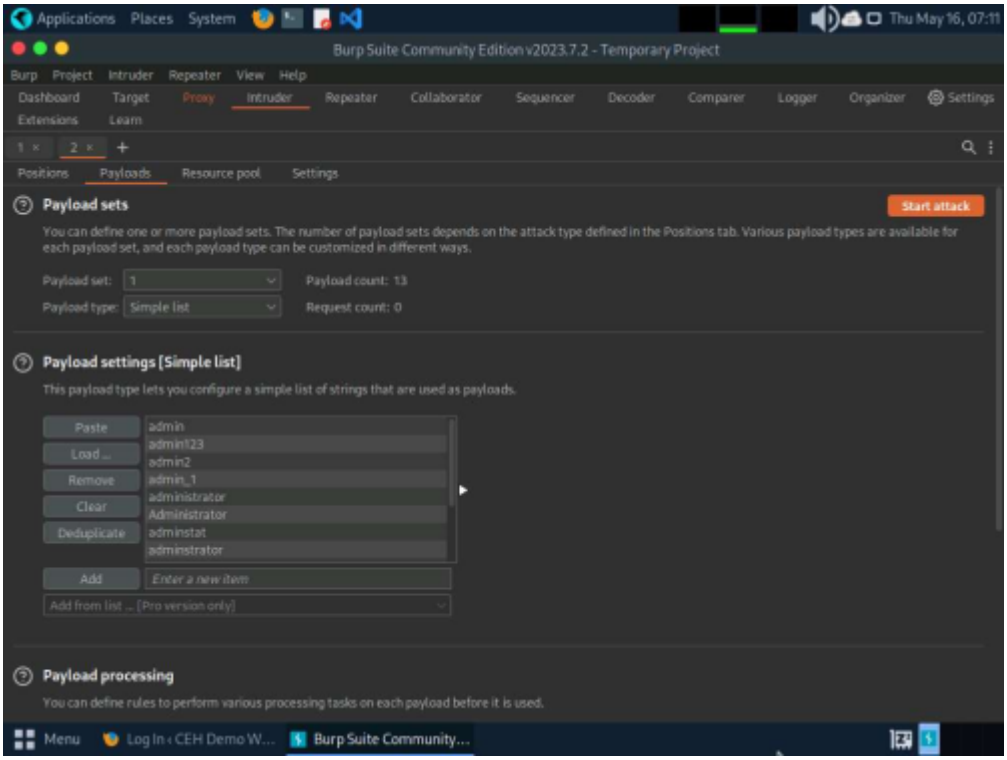
14. Now, we will set the username and password as the payload values. To do so, select the username value entered in Step#14 and click Add § from the right-pane. Similarly, select the password value entered in Step#14 and click Add § from the right-pane.



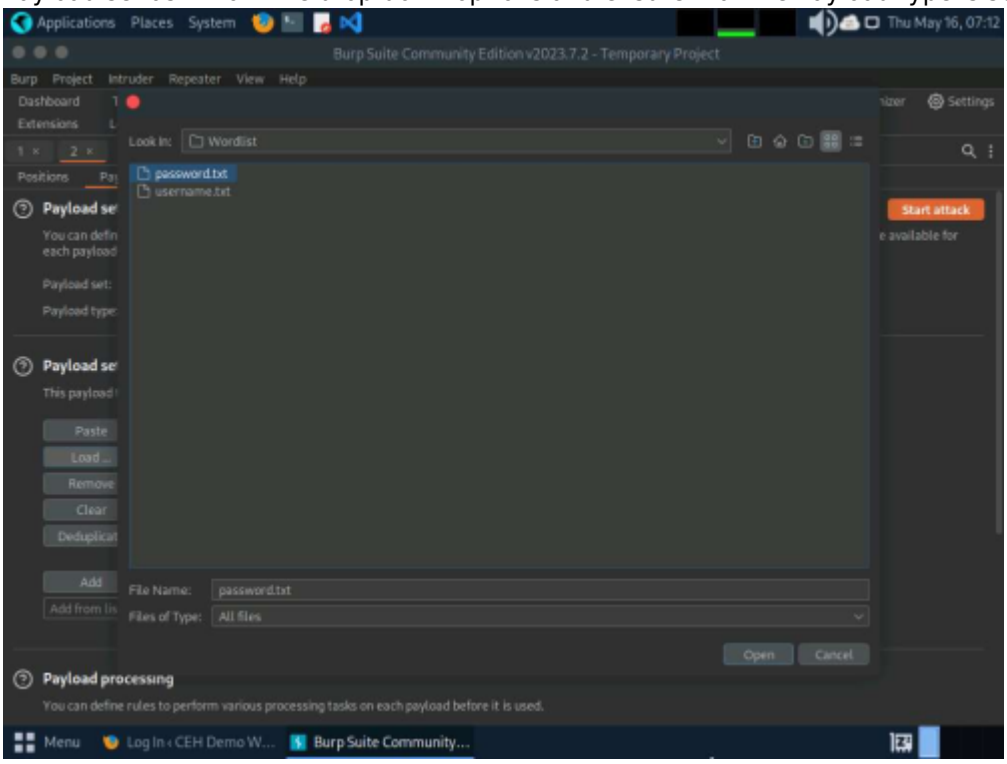
15. Once the username and password payloads are added. The symbol '§' will be added at the start and end of the selected payload values. Here, as the screenshot shows, the values are admin and password.



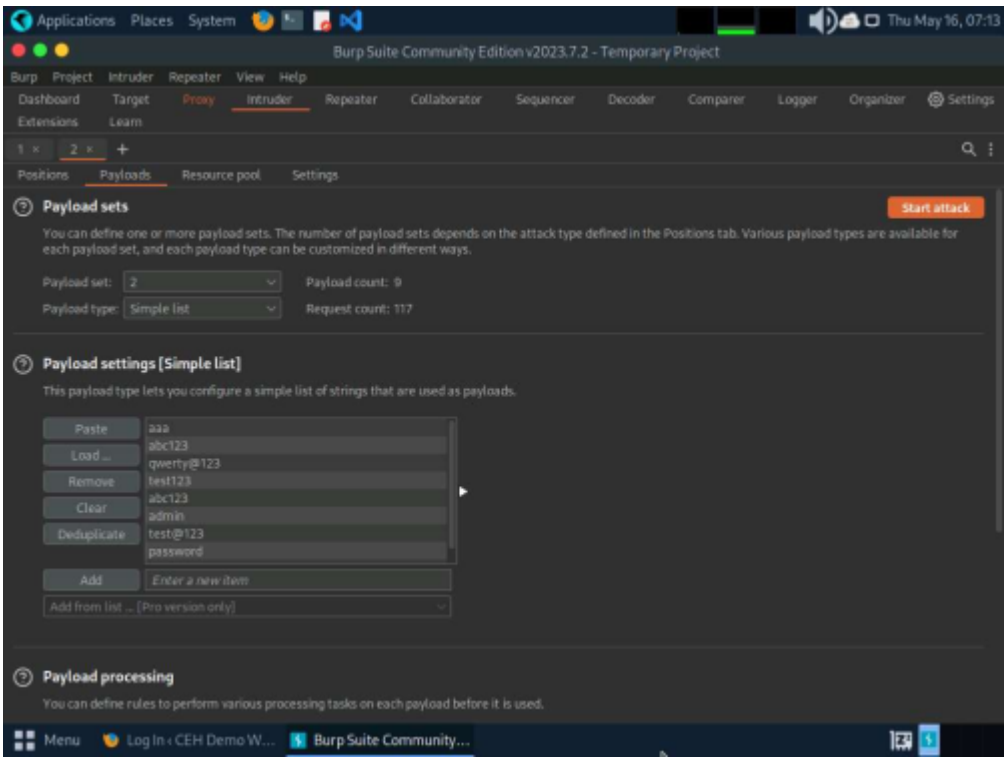
16. Navigate to the Payloads tab under the Intruder tab and ensure that under the Payload Sets section, the Payload set is selected as 1, and the Payload type is selected as Simple list. Under the Payload settings [Simple list] section, click the Load… button.
17. A file selection window appears; navigate to the location /home/attacker/Desktop/CEHv13 Module 14 Hacking Web Applications/Wordlist, select the username.txt file, and click the Open button.20250220-030614.png_500
18. Observe that the selected username.txt file content appears under the Payload settings [Simple list] section, as shown in the screenshot.



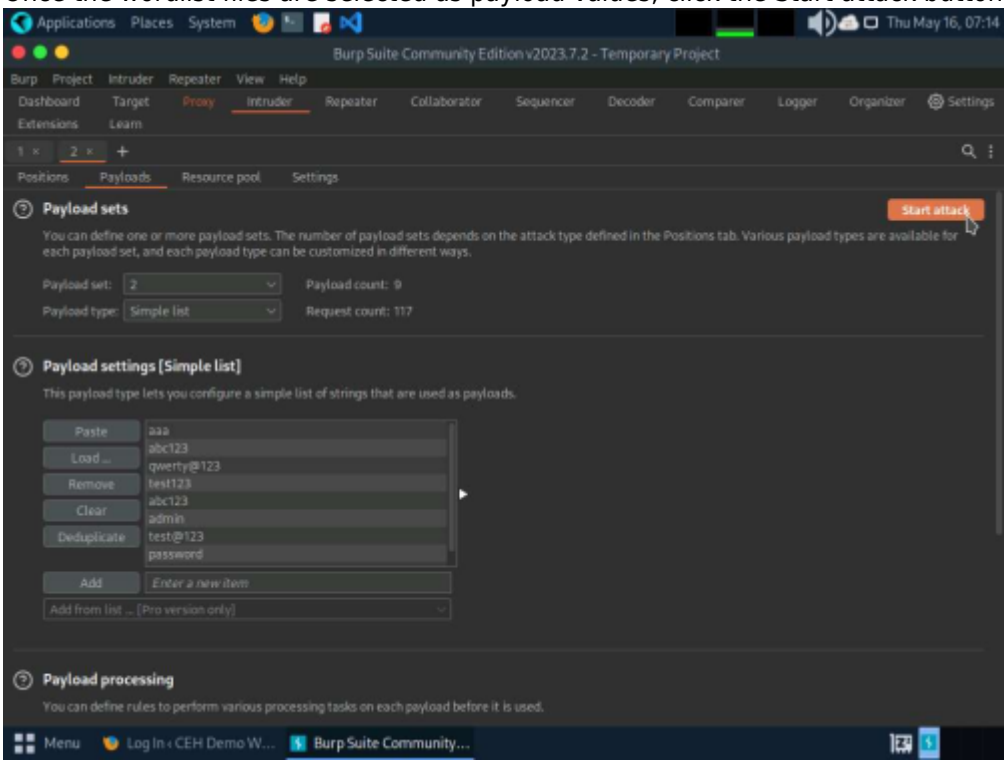
19. Similarly, load a password file for the payload set 2. To do so, under the Payload Sets section, select the Payload set as 2 from the drop-down options and ensure that the Payload type is selected as Simple list.



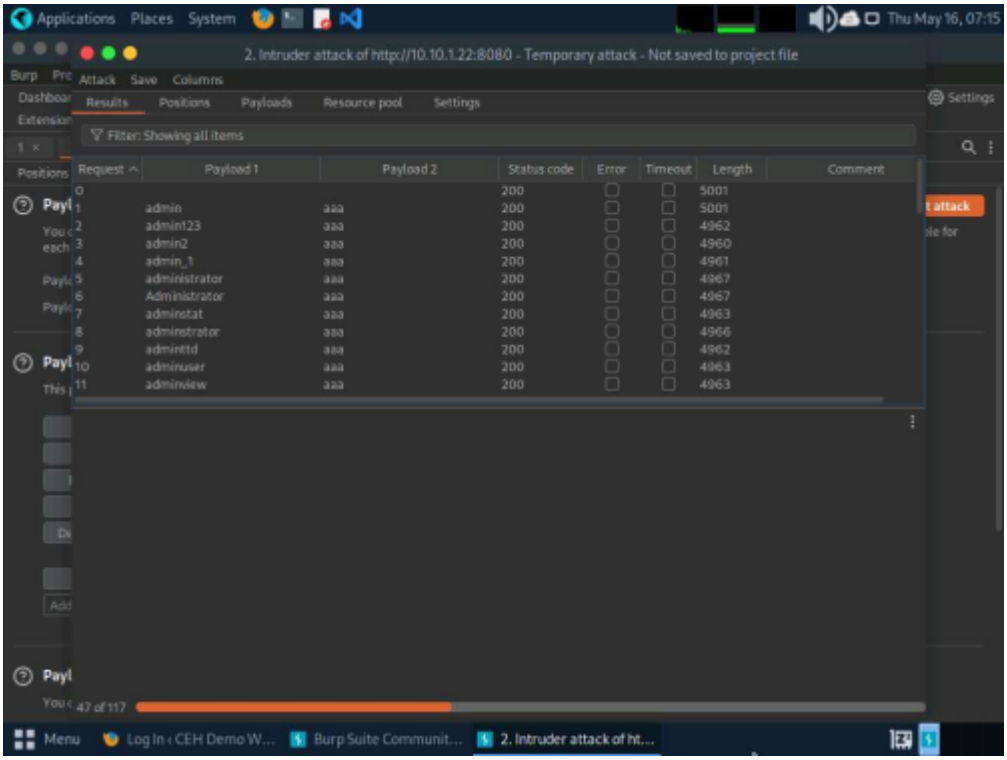
20. Observe that selected password.txt file content appears under the Payload settings [Simple list] section, as shown in the screenshot.



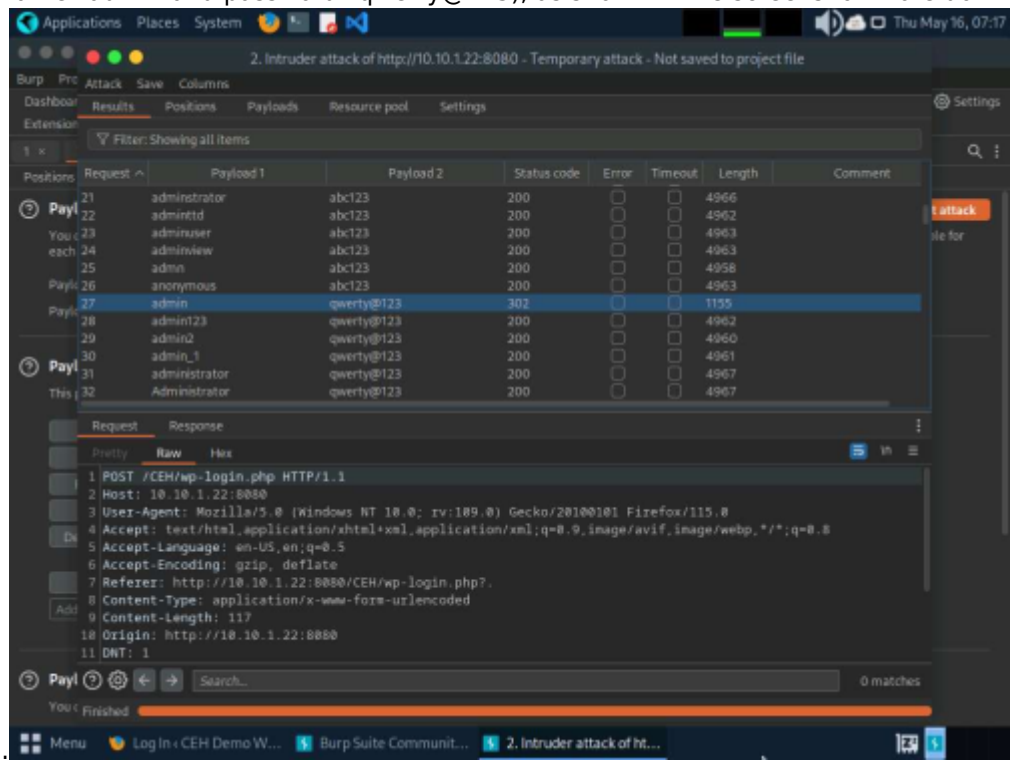
21. Once the wordlist files are selected as payload values, click the Start attack button to launch the attack.



22. The Intruder attack of 10.10.1.22 window appears as the brute-attack initializes. It displays various username-password combinations along with the Length of the response and the Status.



23. After the progress bar completes, scroll down and observe the different values of Status and Length. Here, Status=302 and Length= 1155.
24. In the Raw tab under the Request tab, the HTTP request with a set of the correct credentials is displayed. (here, username=admin and password=qwerty@123), as shown in the screenshot. Note down these user credentials.



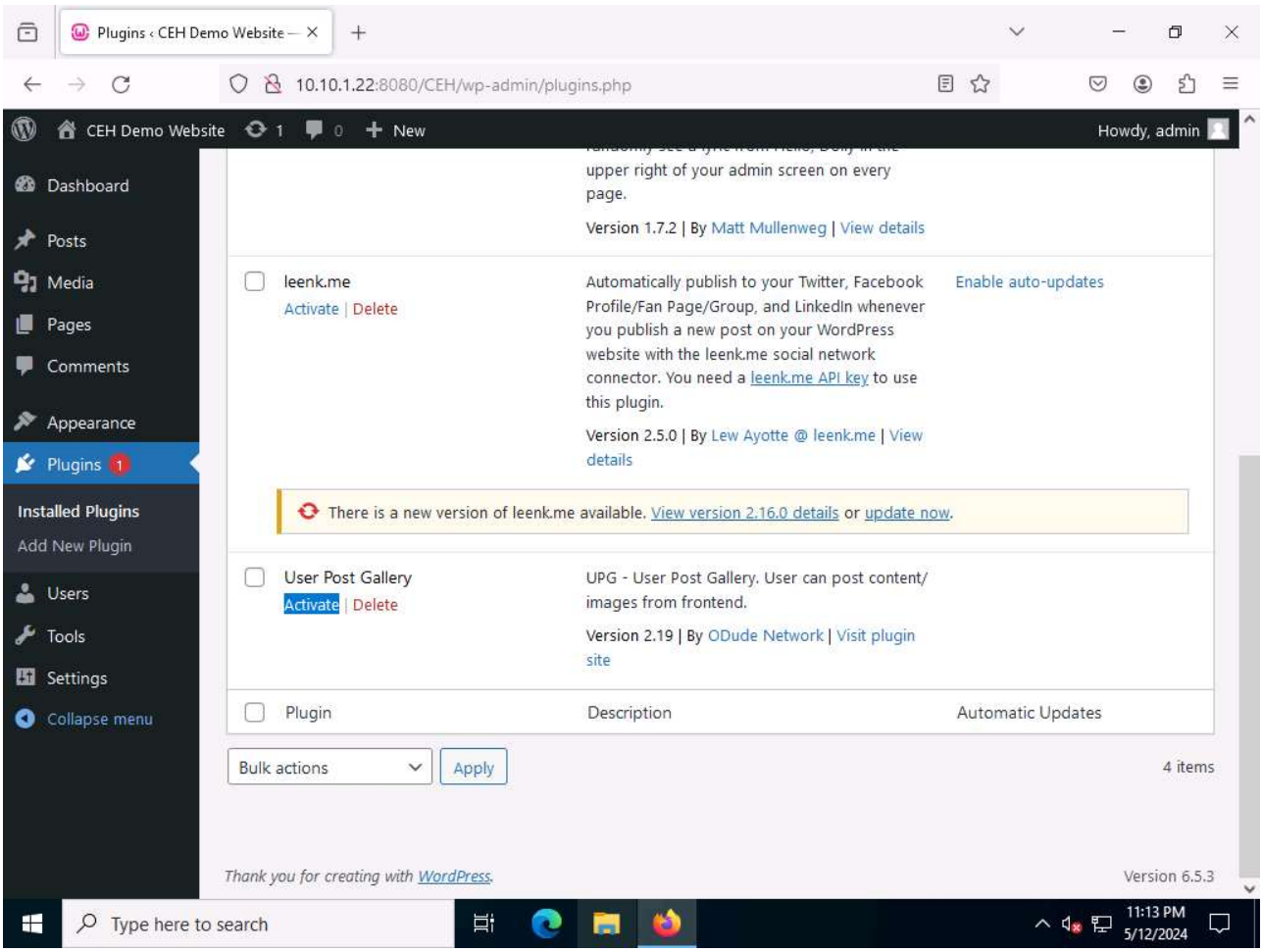
Task 2: Perform Remote Code Execution (RCE) Attack

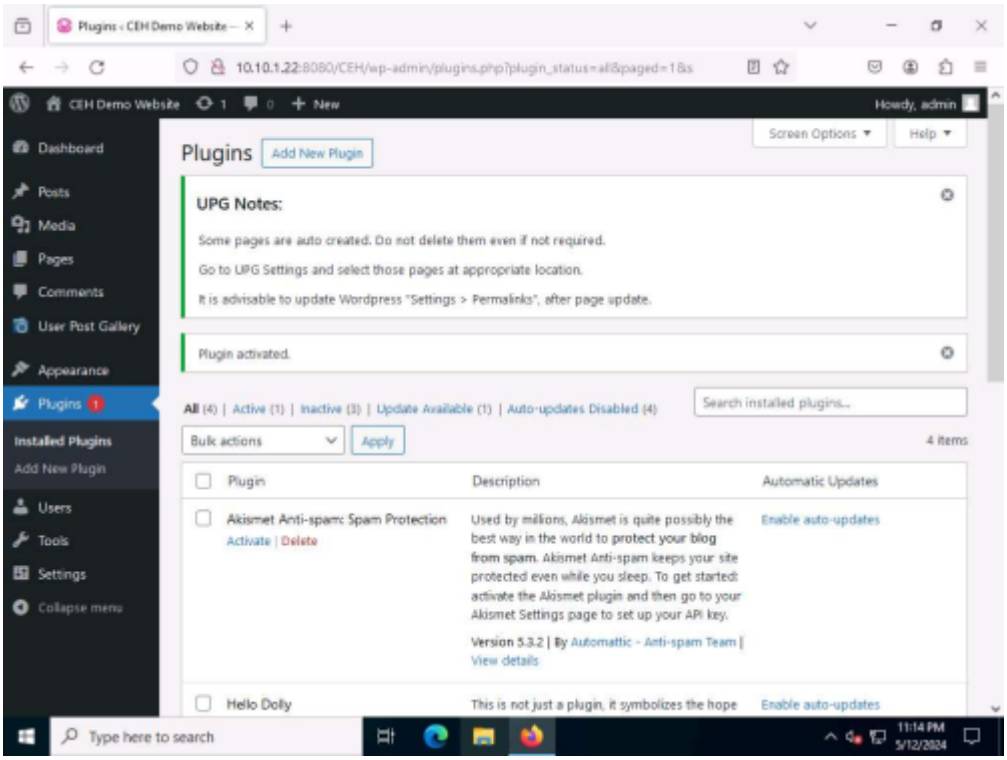
Remote Code Execution (RCE) Attack vulnerability is a critical security flaw that allows an attacker to execute arbitrary code on a target system remotely, without needing physical access to the system. This type of vulnerability is particularly dangerous because it enables attackers to take control of the target system, potentially gaining unauthorized access, stealing data, or causing damage to the system or network.

Attackers exploit these vulnerabilities by injecting malicious code into the target system through various means such as input fields, file uploads, or network protocols. Once the malicious code is executed, the attacker can gain control over the system and perform actions as if they were an authenticated user or system administrator.

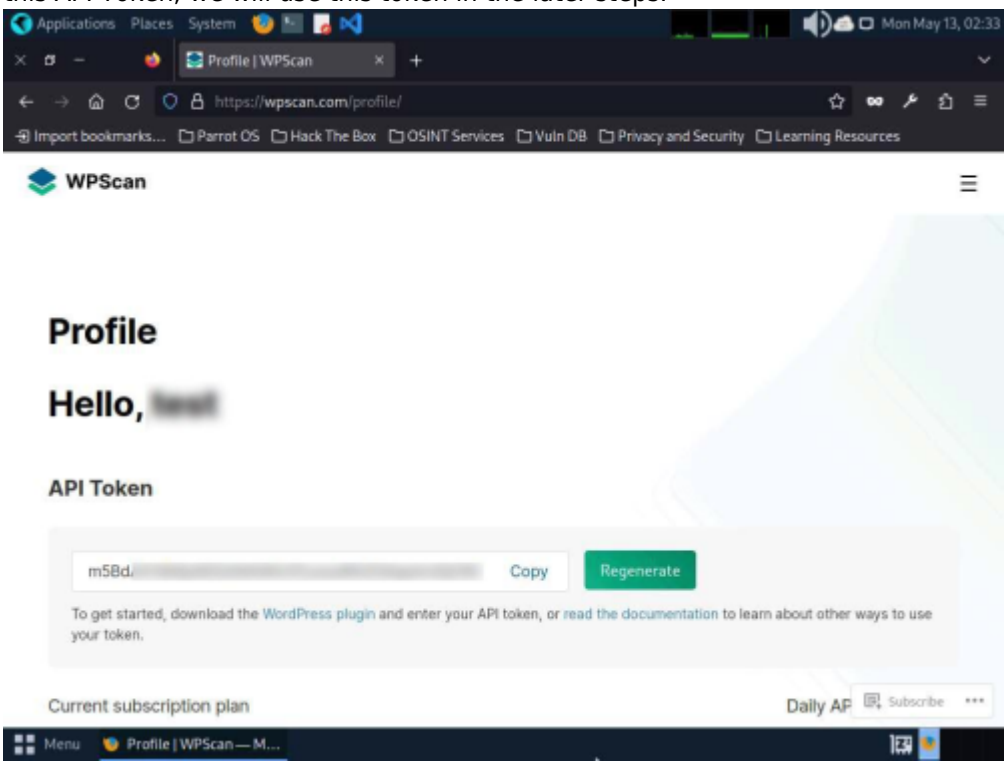
Here, we will perform a CSRF attack using vulnerability present in the wp-upg plugin.

1. Click Type here to search field on the Desktop, search for wampserver64 in the search bar and select Wampserver64 from the results.
2. Wait for this icon to turn green, which indicates that the WampServer is successfully running.
3. Now, open any web browser, and go to http://10.10.1.22:8080/CEH/wp-login.php? (here, we are using Mozilla Firefox).
4. A WordPress webpage appears. Type Username or Email Address and Password as admin and qwerty@123. Click the Log In button.
5. Hover your mouse cursor on Plugins in the left pane and click Installed Plugins, as shown in the screenshot.

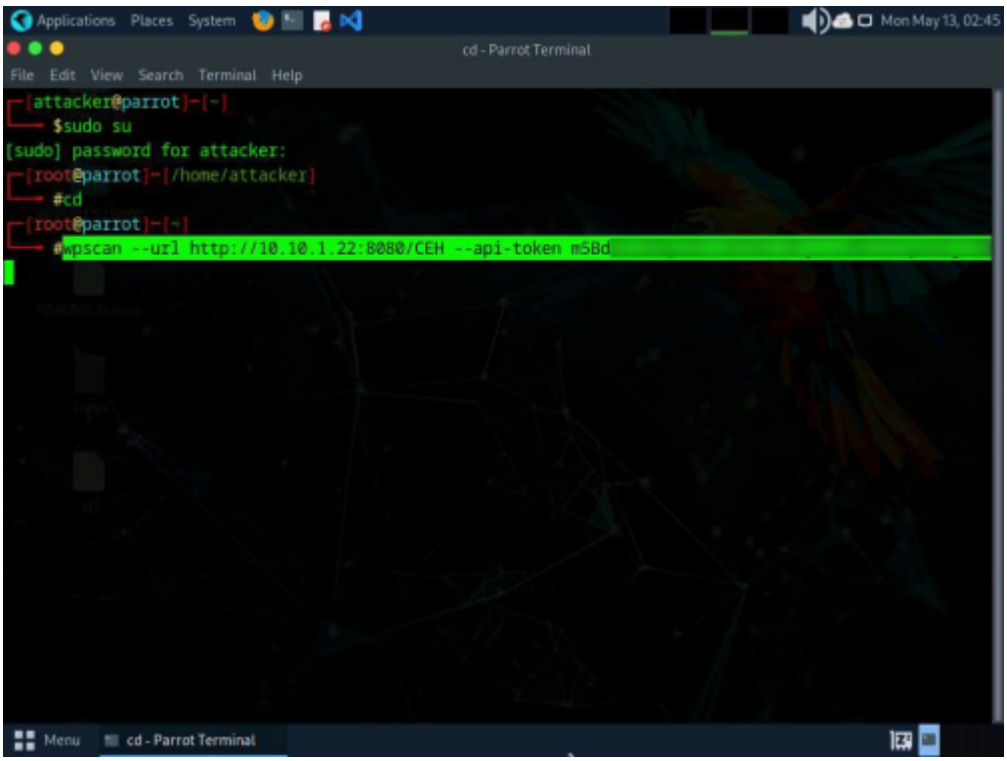




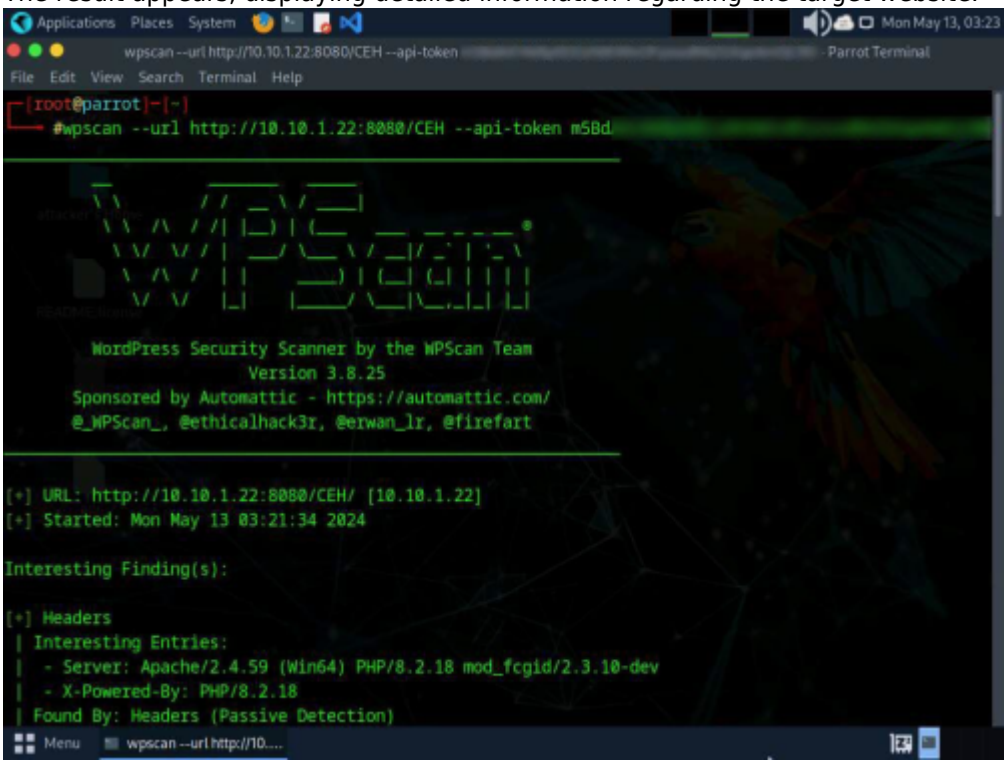
6. Open Mozilla Firefox web browser and go to https://wpscan.com/ and login to the wpscan account that you have created in previous task.
7. You get signed in successfully in the website. Now, click the Get Started button and click Start for free button under Researcher section.
8. The Edit Profile page appears; in the API Token section and observe the API Token. Note down or copy this API Token; we will use this token in the later steps.



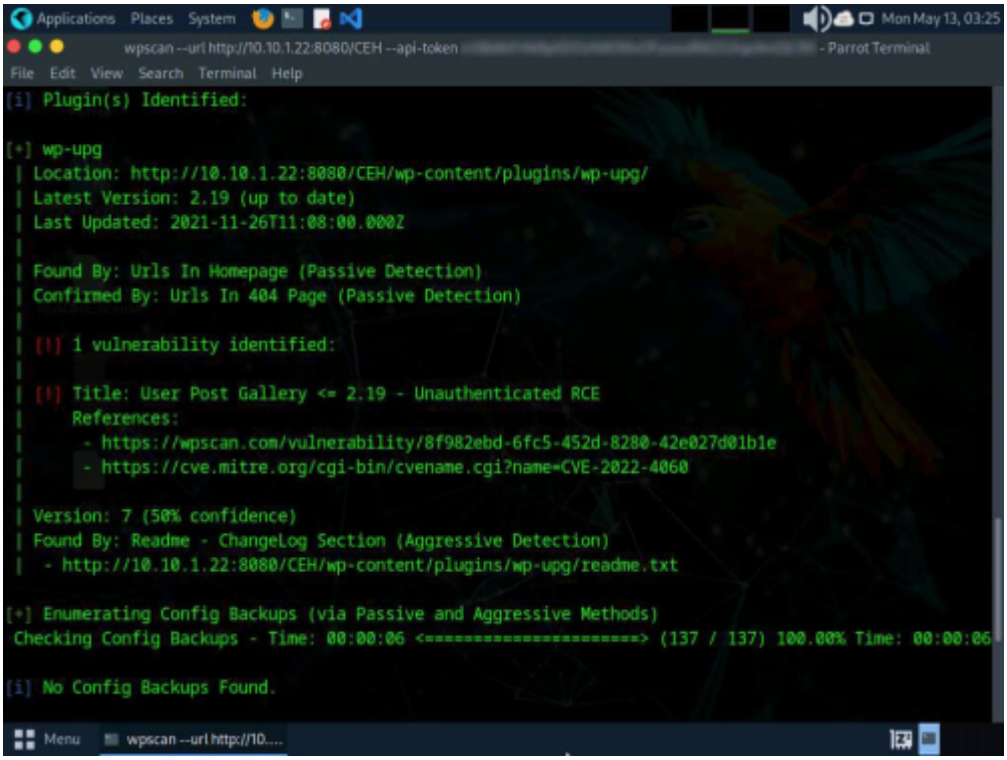
9. In the Parrot Security machine, open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).
10. In the Terminal window, run `wpscan –url http://10.10.1.22:8080/CEH –api-token [API Token from Step#13]` command.



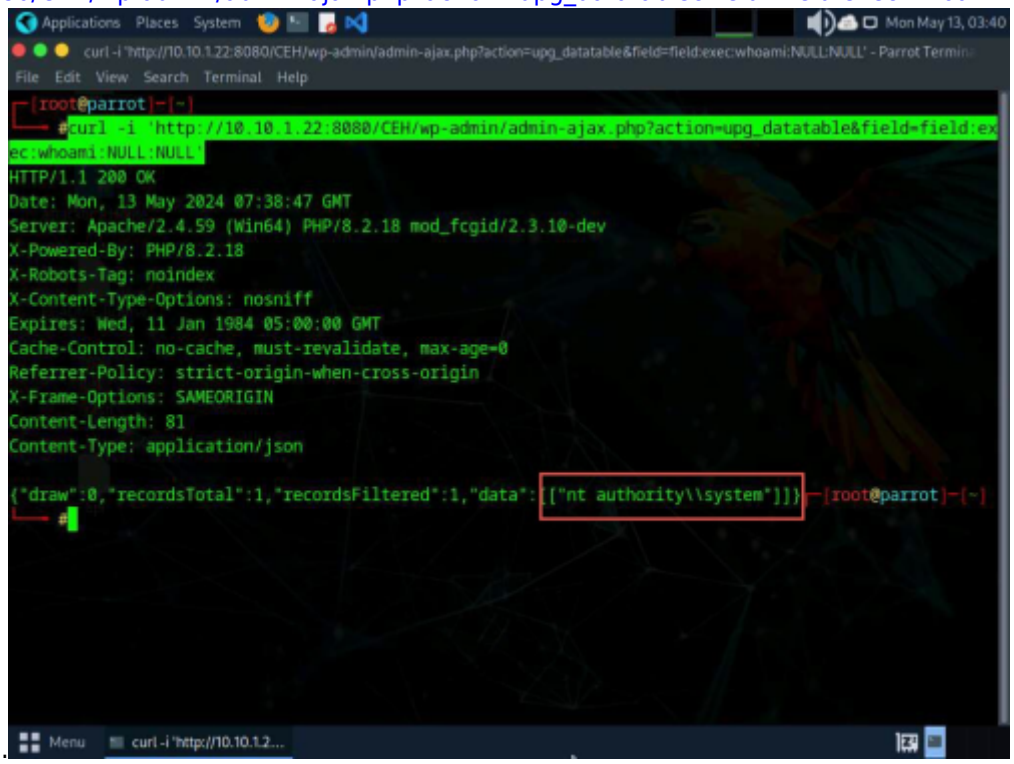
11. The result appears, displaying detailed information regarding the target website.



12. Scroll down to the Plugin(s) Identified section, and observe the installed vulnerable plugins (wp-upg) on the target website.
13. In the Plugin(s) Identified section, within the context of the wp-upg plugin, an Unauthenticated Remote Code Execution (RCE) vulnerability has been detected as shown in the screenshot.



14. To perform RCE attack, run curl -i 'http://10.10.1.22:8080/CEH/wp-admin/admin-ajax.php?action=upg_datatable&field=field:exec:whoami:NULL:NULL' command.



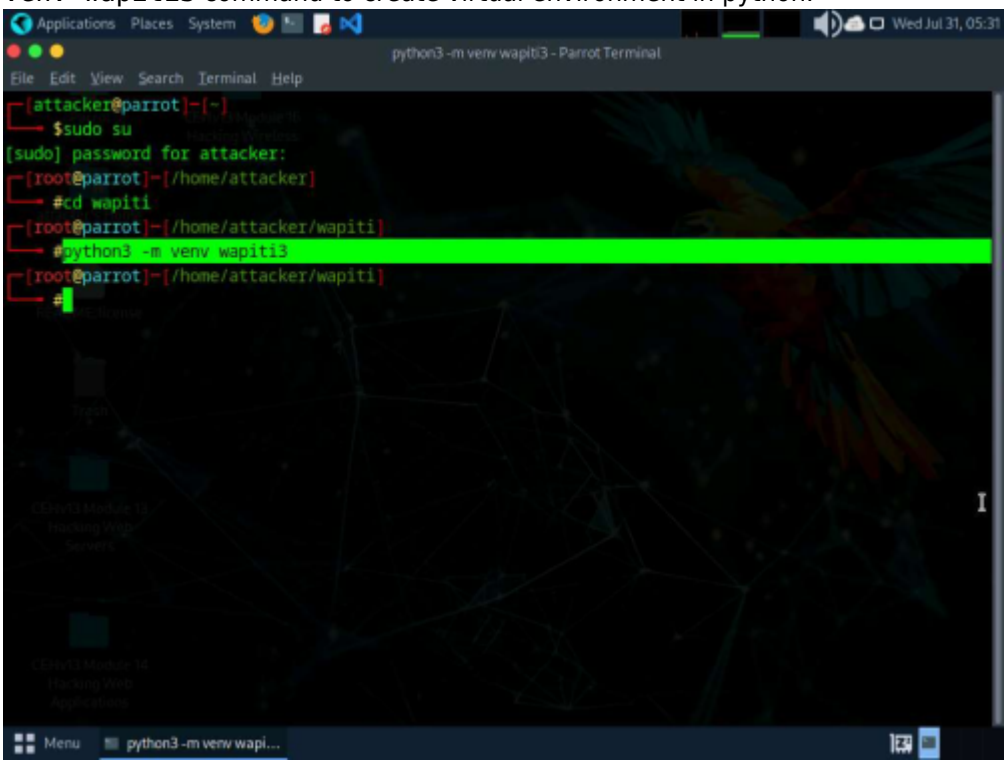
15. This curl command exploits a WordPress plugin vulnerability by sending a malicious request to the admin-ajax.php file, allowing an attacker to execute arbitrary system commands via the exec function, potentially leading to remote code execution.

Lab 3: Detect Web Application Vulnerabilities using Various Web Application Security Tools

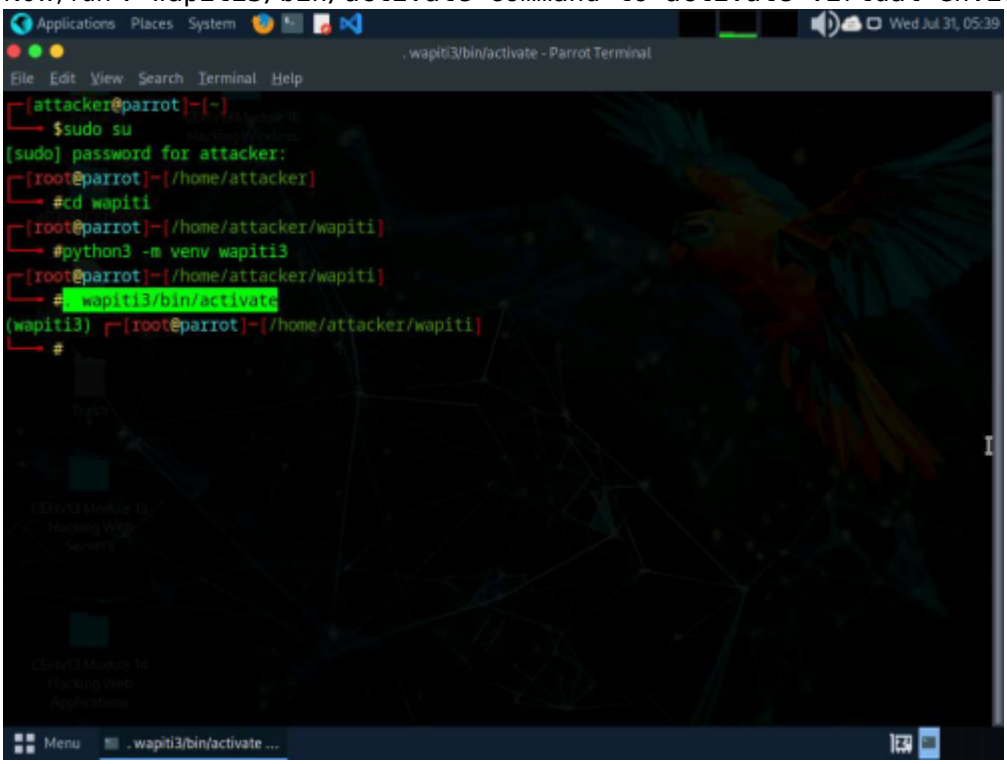
Task 1: Detect Web Application Vulnerabilities using Wapiti Web Application Security Scanner

1. In the terminal window run `cd wapiti` command to navigate into wapiti directory and run `python3 -m`

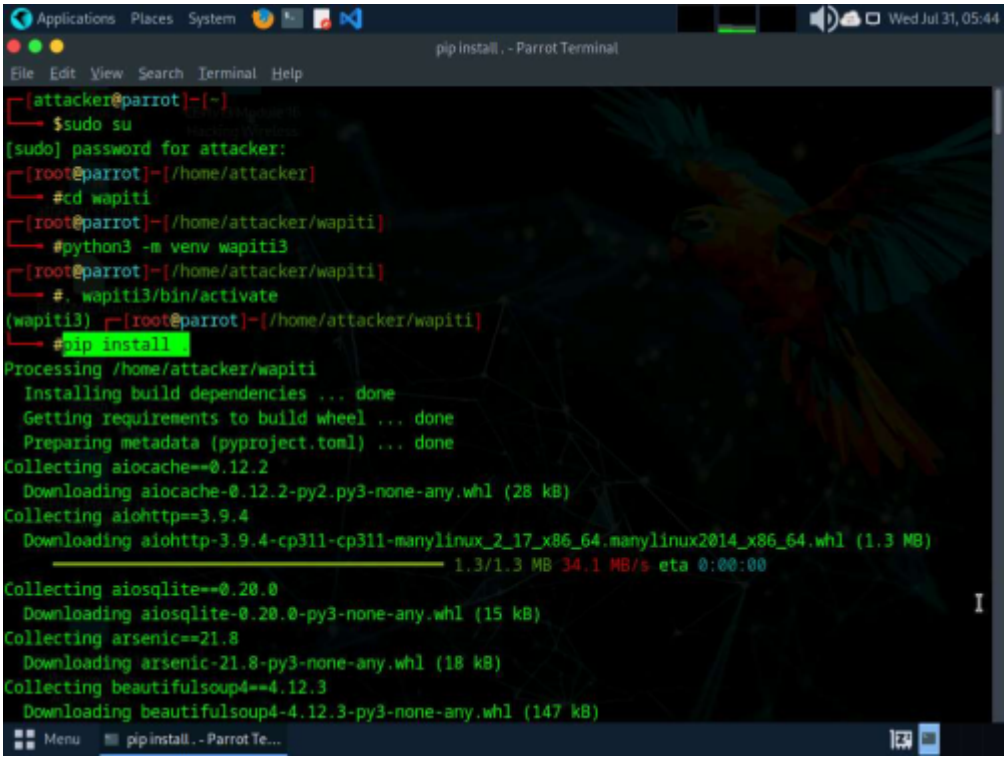
`venv wapiti3` command to create virtual environment in python.



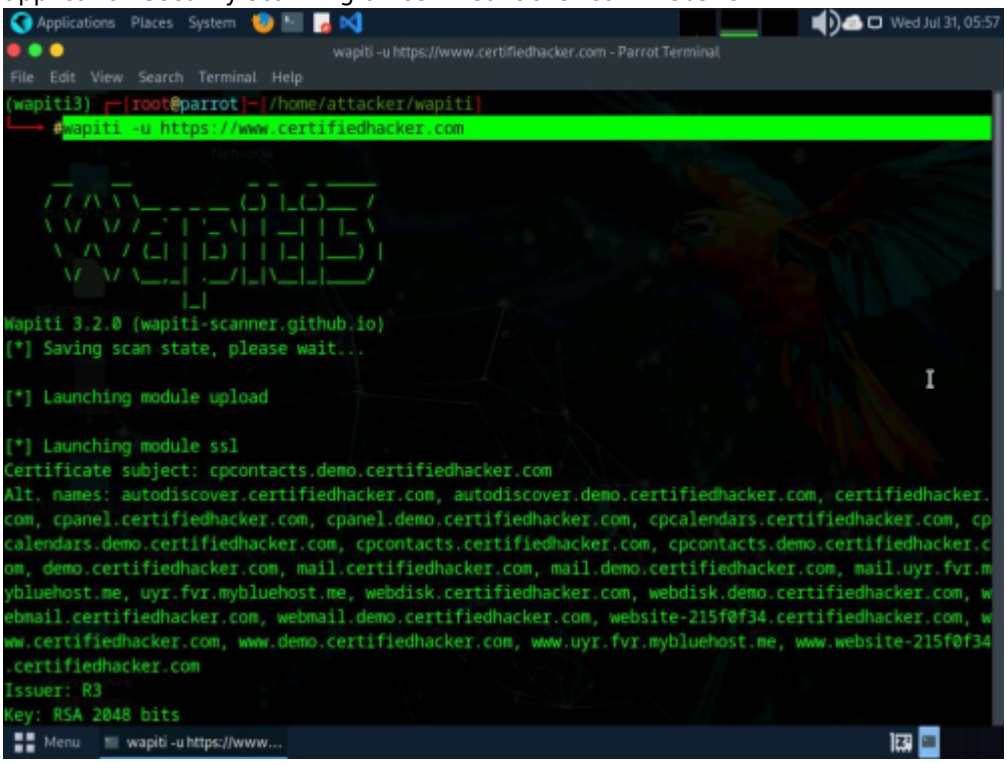
2. Now, run `. wapiti3/bin/activate` command to activate virtual environment.



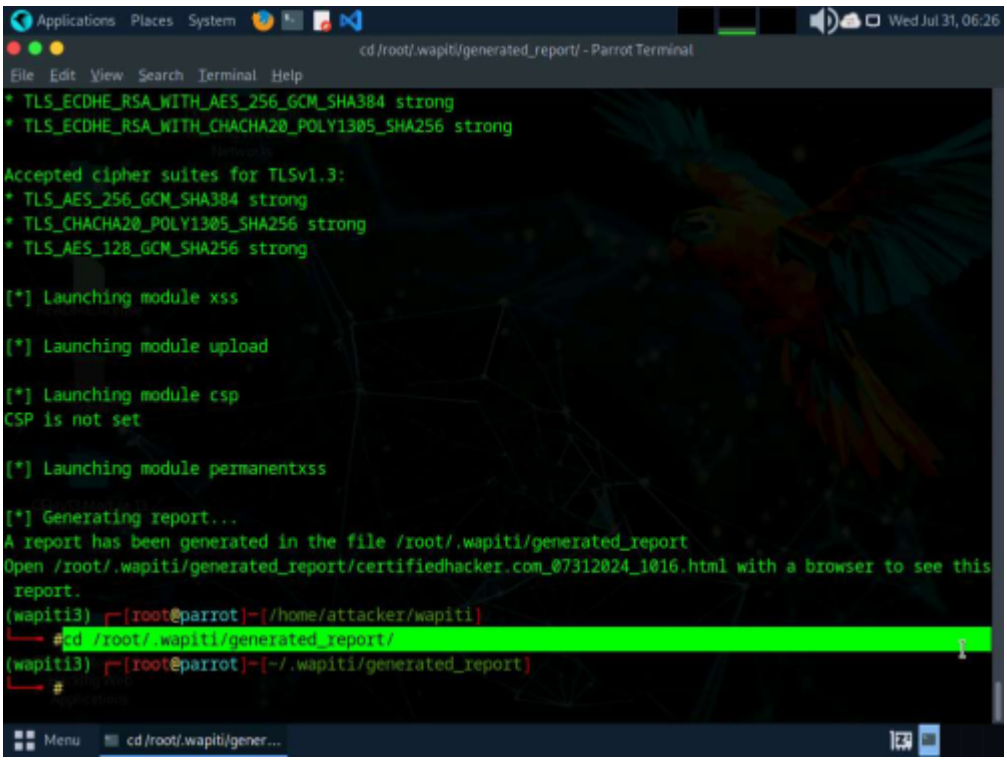
3. Run `pip install .` command to install wapiti web application security scanner.



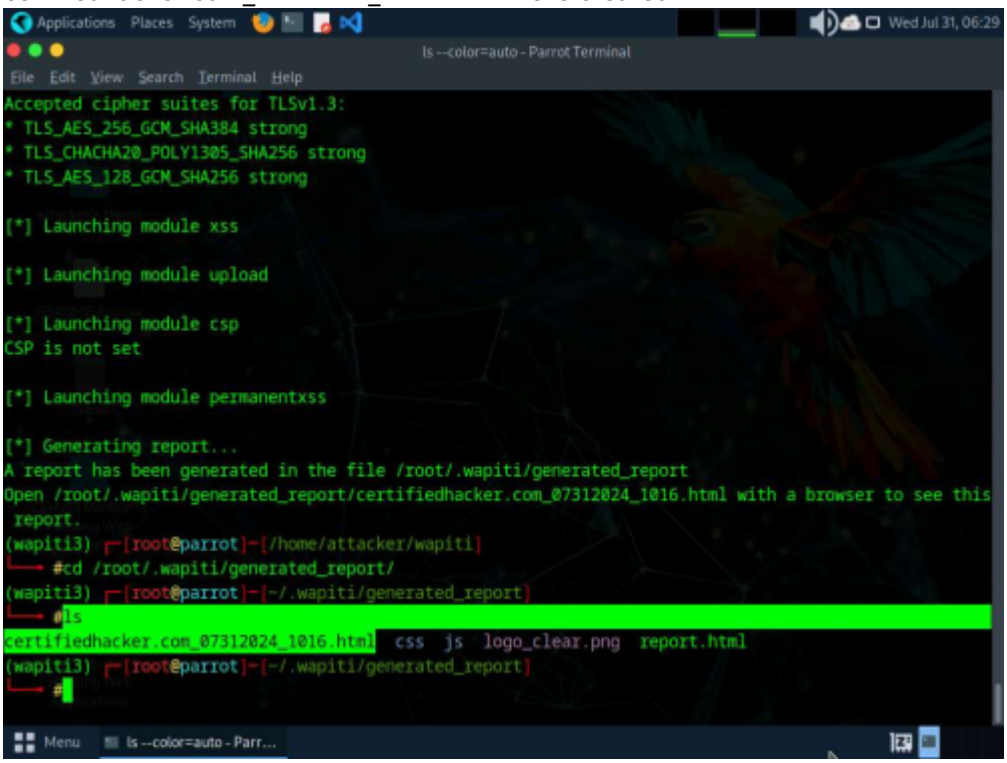
4. After installing the tool run wapiti -u https://www.certifiedhacker.com command to perform web application security scanning on certifiedhacker.com website.



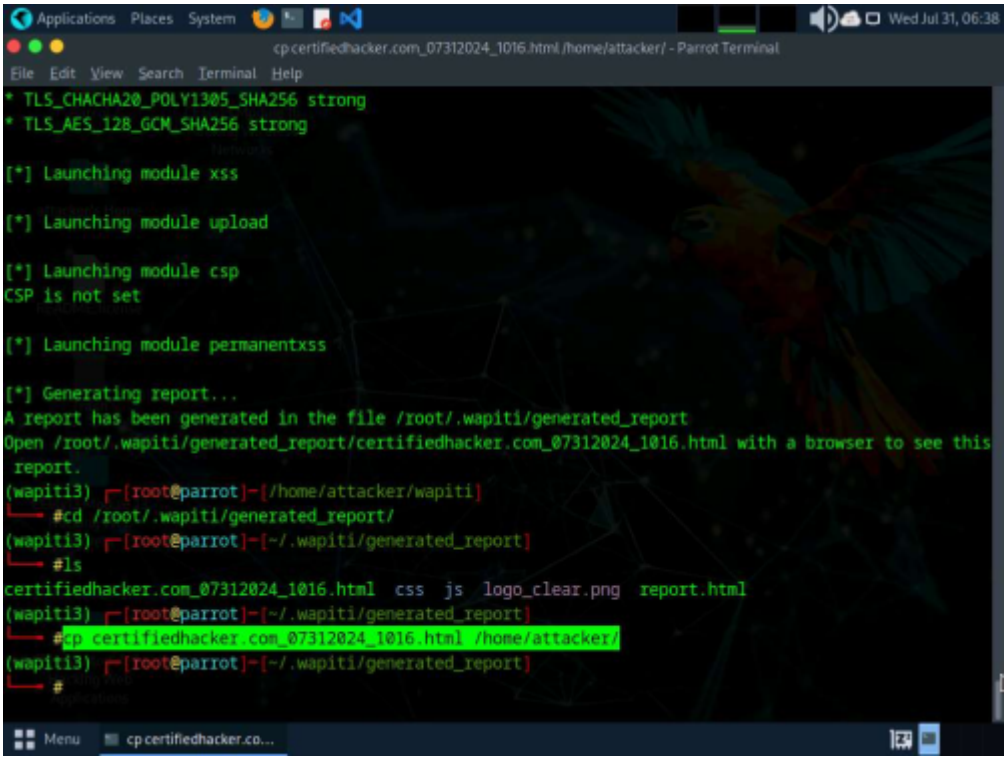
5. Now, in the terminal run cd /root/.wapiti/generated_report/ to navigate to generated_report directory.



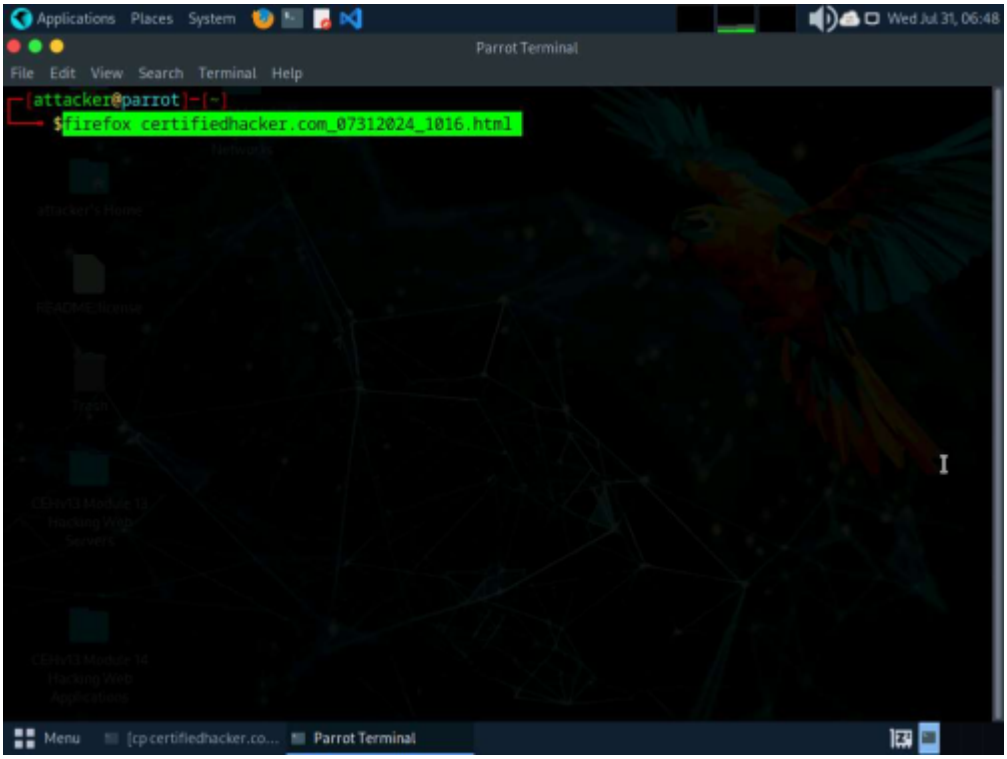
6. Run ls command to view the contents of the directory. we can see that the certifiedhacker.com_xxxxxxxx_xxxx.html file is created.



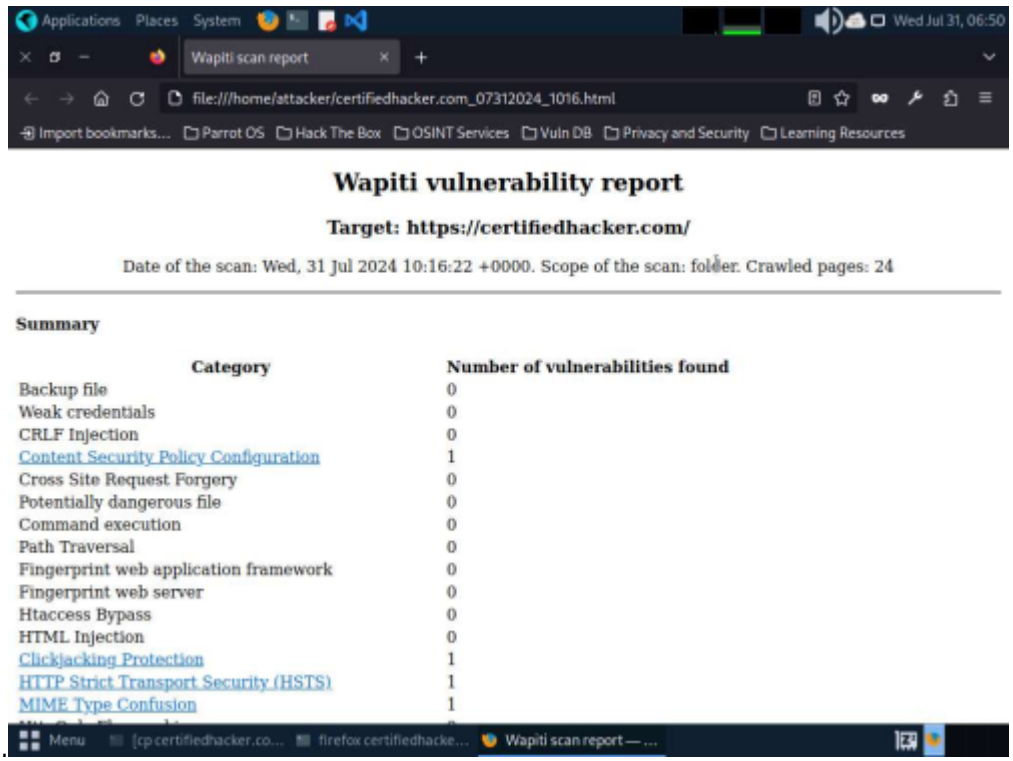
7. Run cp certifiedhacker.com_xxxxxxxx_xxxx.html /home/attacker/ command to copy the .html file to /home/attacker location.



8. Open a new terminal and run firefox certifiedhacker.com_xxxxxxxx_xxxx.html command to open the .html file in Firefox browser.

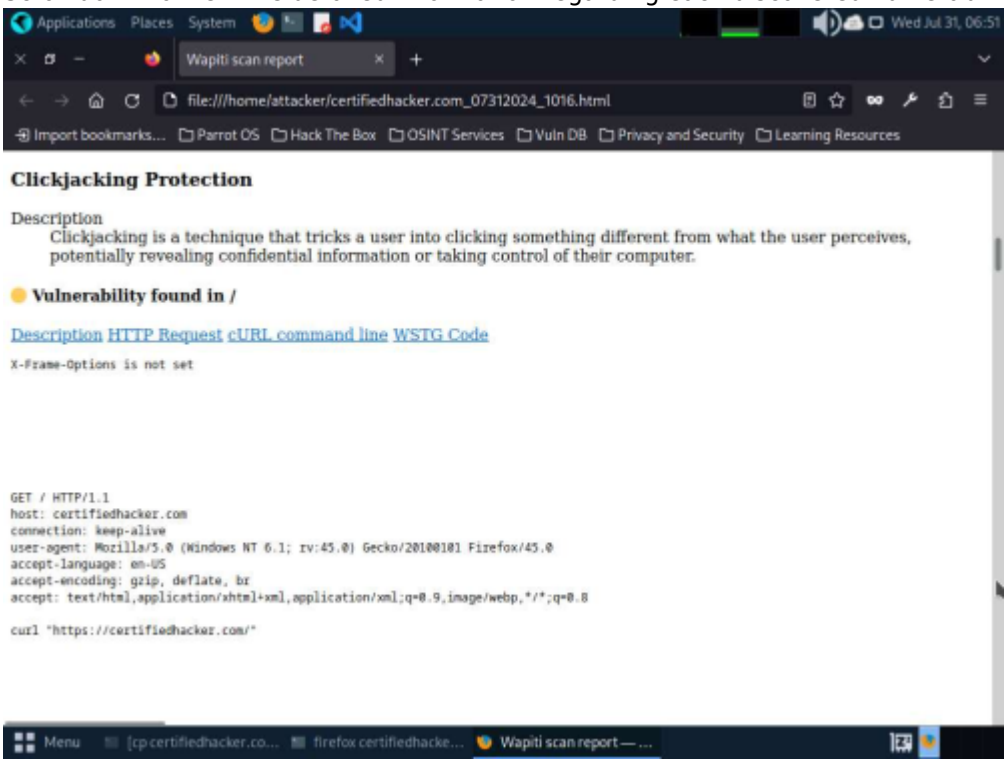


9. Wapiti scan report opens upp in Firefox browser, you can analyze the scan result with the discovered



vulnerabilities.

10. Scroll down to view the detailed information regarding each discovered vulnerability.



Lab 4: Perform Web Application Hacking using AI

Task 1: Perform Web Application Hacking using ShellGPT

Module 15: SQL Injection

apuntes fernando

- https://owasp.org/www-community/attacks/SQL_Injection - Recursos en Inglés
- FUN:
  - https://es.xkcd.com/strips/exploits-de-una-madre/ - SQL Injection
  - https://xkcd.com/1253/ - Otro SQL Injection
  - https://computerhoy.com/noticias/life/pone-nombre-null-matricula-hacerse-invisible-cobran-12000-dolares-multas-defectuosas-473645 - Le pone a su matricula «NULL» y le caen decenas de multas pendientes de cobrar.
  - https://www.xataka.com/otros/internet-tu-nombre-puede-convertirse-tu-peor-pesadilla-1 - Jennifer Null
  - https://i.kinja-img.com/gawker-media/image/upload/s--UzcqSr8_--/c_fill,fl_progressive,g_center,h_900,q_80,w_1600/18mpenleoksq8jpg.jpg - SQL Injection
  - https://sqlpd.com/ - Para aprender SQL jugando
  - https://dvwa.co.uk/ - Damm Vulnerable web application ←- Aprenderás jugando
  - https://portswigger.net/web-security/sql-injection/union-attacks - Cómo detectar número de columnas en una query, para poder utilizar el operador UNION

extras

- bash: usar – y comillas para crear ficheros que no deja (igual para borrar)

```
touch -- '*'
rm -- '*'
```

sección 1

- `UNION`: mismo número de campos

sección 2

- inband: hago y veo el resultado en la misma web
- out-of-band: respuesta por otro cana
- provocar errores para ver si es accesible via SQL injection o si los errores son descriptivos
- usar `UNION`
- Blind/inferial
- `WAITFOR DELAY`:

```
IF EXISTS(SELECT * FROM users) waitfor delay '00:00:10'
```

- Testing strings SQL Injection
  - Material de Alumnos: Modulo15_SQL_Injection_Cheat_Sheet.pdf
- `OPENROWSHEET`
- `LOAD_FILE()`
- `INTO OUTFILE()`
- Herramientas
  - sqlmap
  - Mole
  - noSQLMap
- Evasión
- Contramedidas

Lab 1 Modulo 15: Perform SQL Injection Attacks

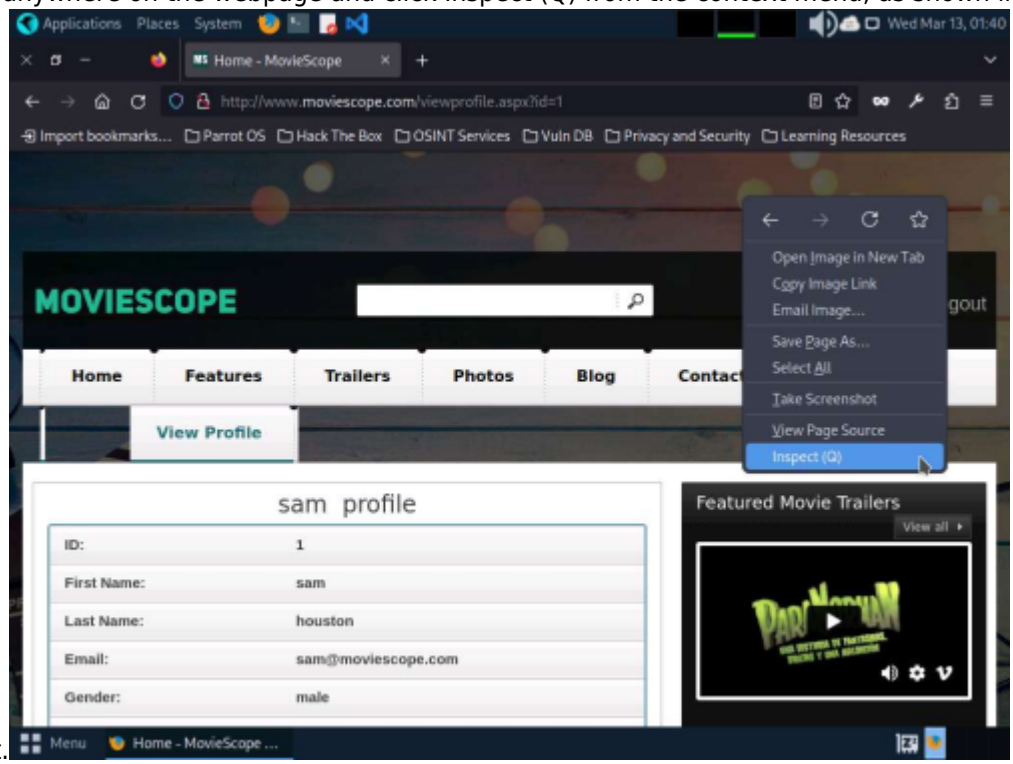
Task 1: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

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.

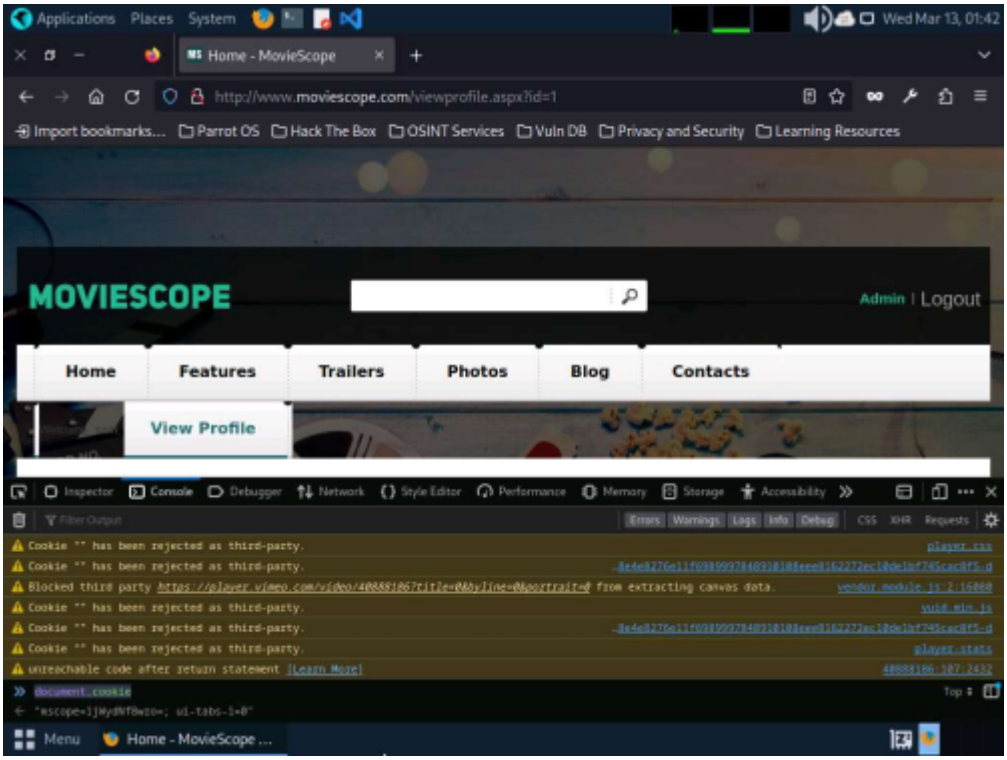
You can use sqlmap to perform SQL injection on a target website using various techniques, including Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band SQL injection.

In this task, we will use sqlmap to perform SQL injection attack against MSSQL to extract databases.

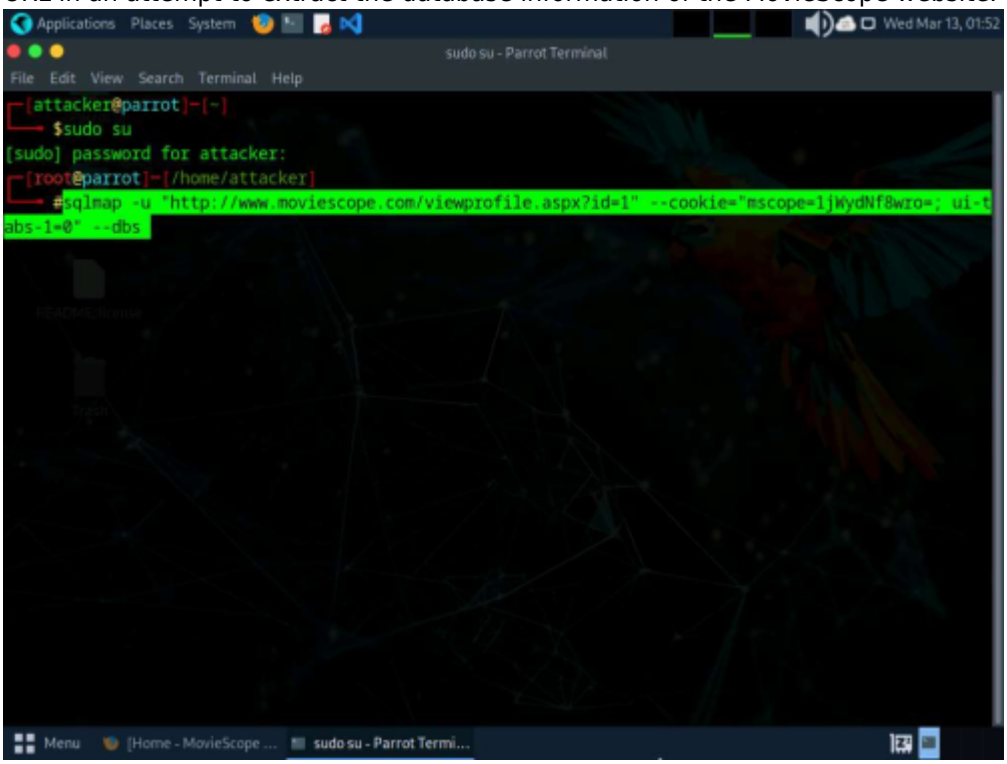
1. Navigate to http://www.moviescope.com/. A Login page loads; enter the Username and Password as sam and test, respectively.
2. Once you are logged into the website, click the View Profile tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.
3. Right-click anywhere on the webpage and click Inspect (Q) from the context menu, as shown in the screenshot.



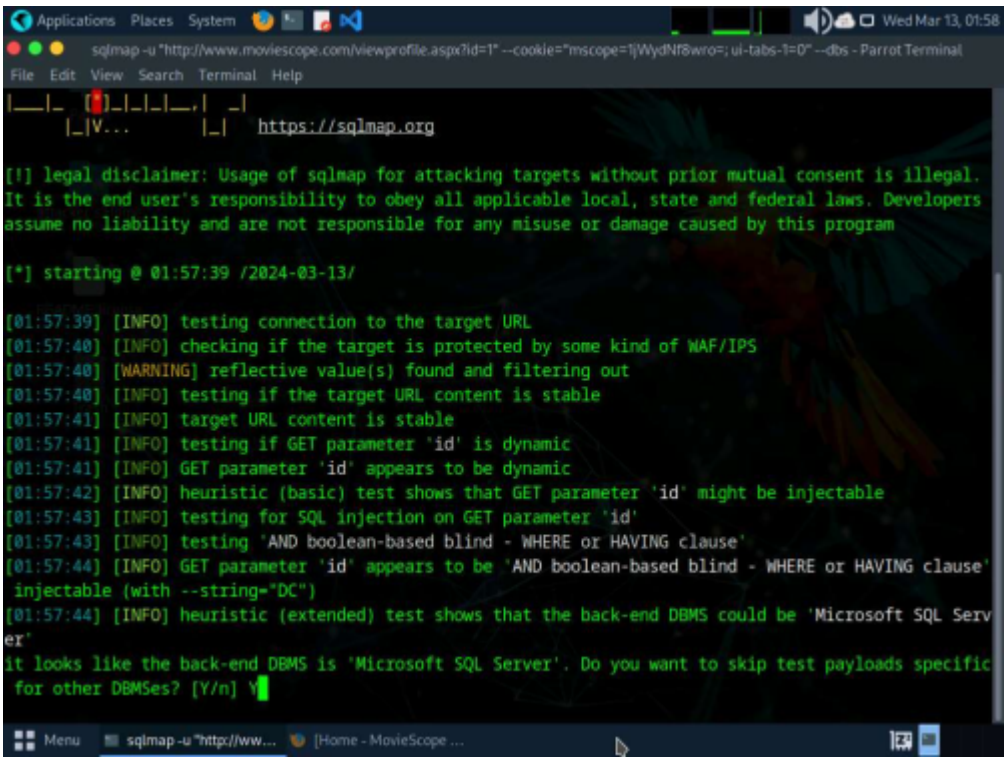
4. The Developer Tools frame appears in the lower section of the browser window. Click the Console tab, type document.cookie in the lower-left corner of the browser, and press Enter.



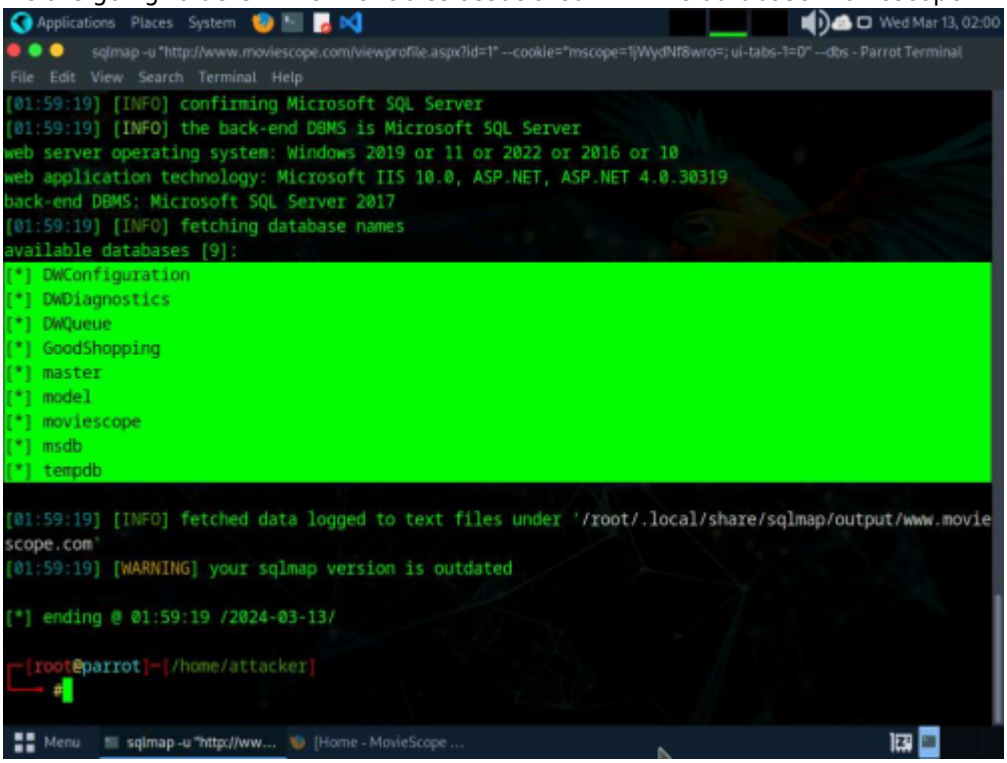
5. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser. Note down the URL of the web page.
6. As root, Run `sqlmap -u «http://www.moviescope.com/viewprofile.aspx?id=1» --cookie=«[cookie value that you copied in Step#7]» --dbs` command.
    1. In 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.
7. 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.



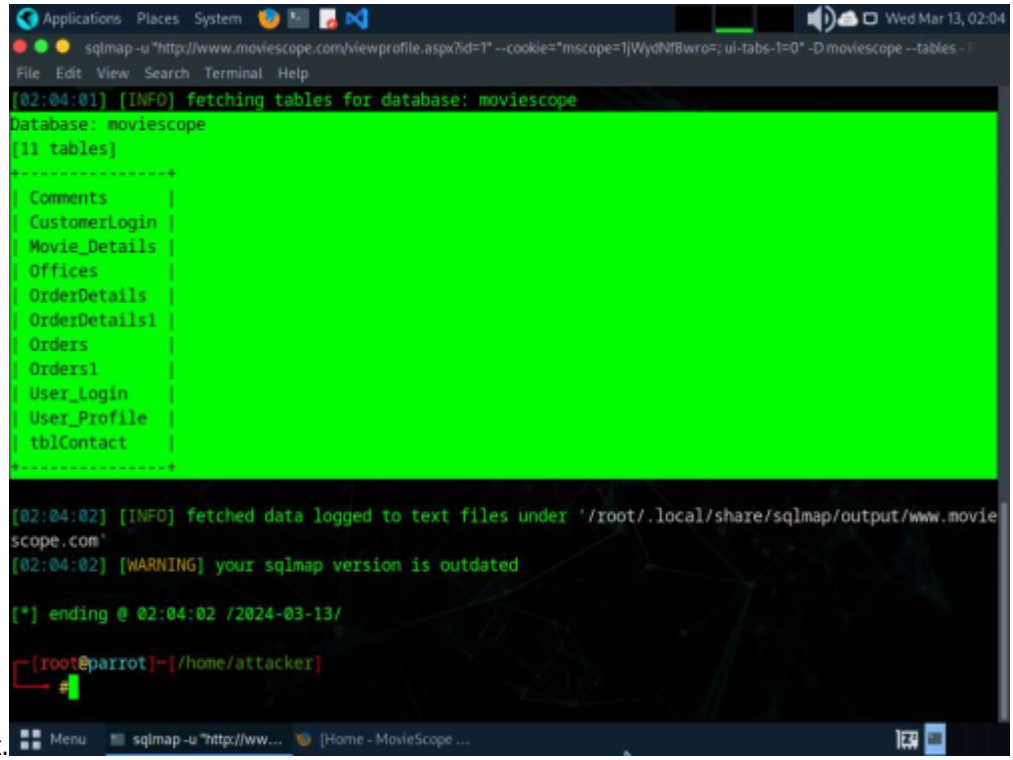
8. If the message Do you want to skip test payloads specific for other DBMSes? [Y/n] appears, type Y and press Enter.
9. If the message for the remaining tests, do you want to include all tests for ‘Microsoft SQL Server’ extending provided level (1) and risk (1) values? [Y/n] appears, type Y and press Enter.



10. 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.
11. 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.

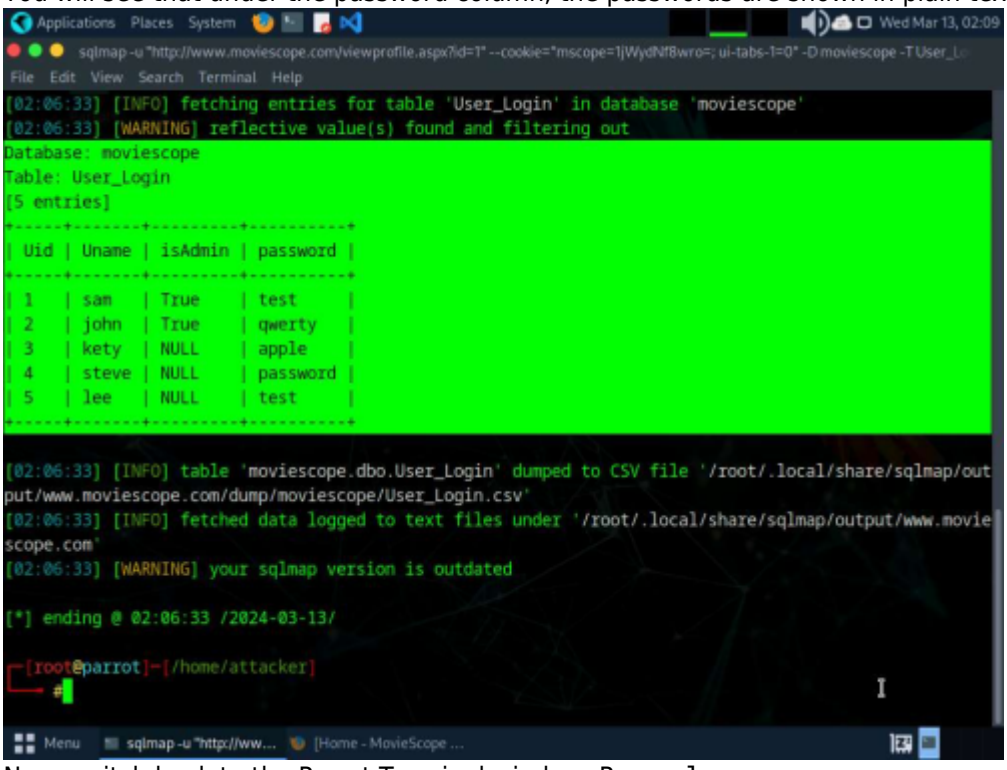


12. Run `sqlmap -u «http://www.moviescope.com/viewprofile.aspx?id=1» –cookie=«[cookie value which you have copied in Step#7]» -D moviescope –tables` command.
    1. In this query, -D specifies the DBMS database to enumerate and –tables enumerates DBMS database tables.
13. sqlmap retrieves the table contents of the moviescope database and displays them, as shown in

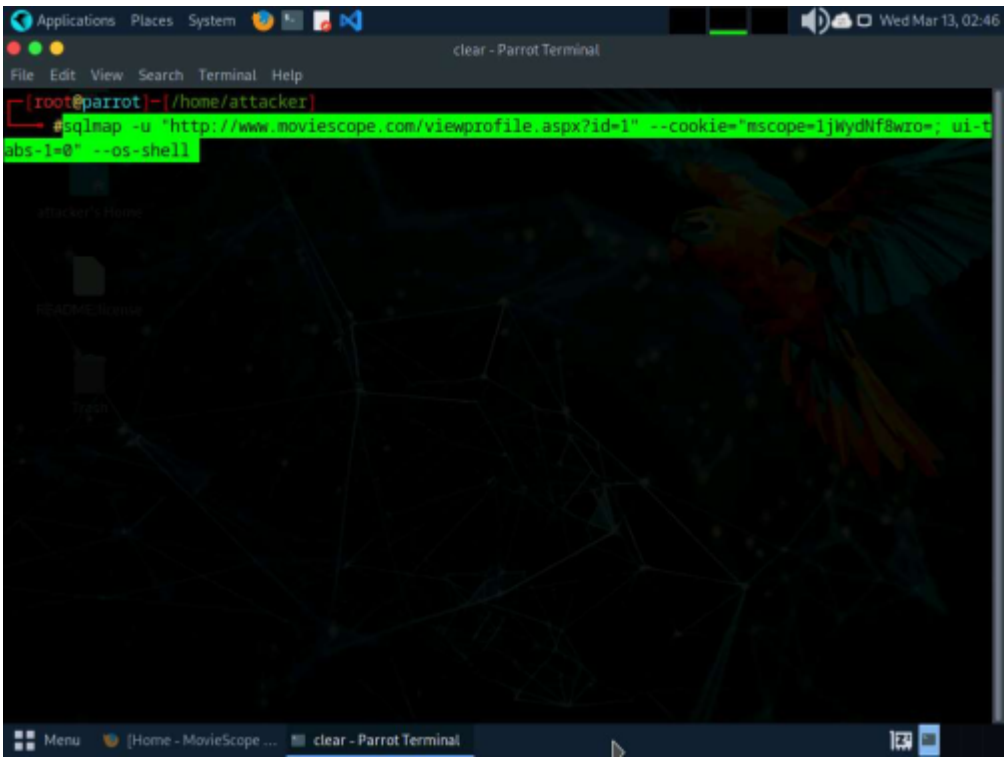


screenshot.

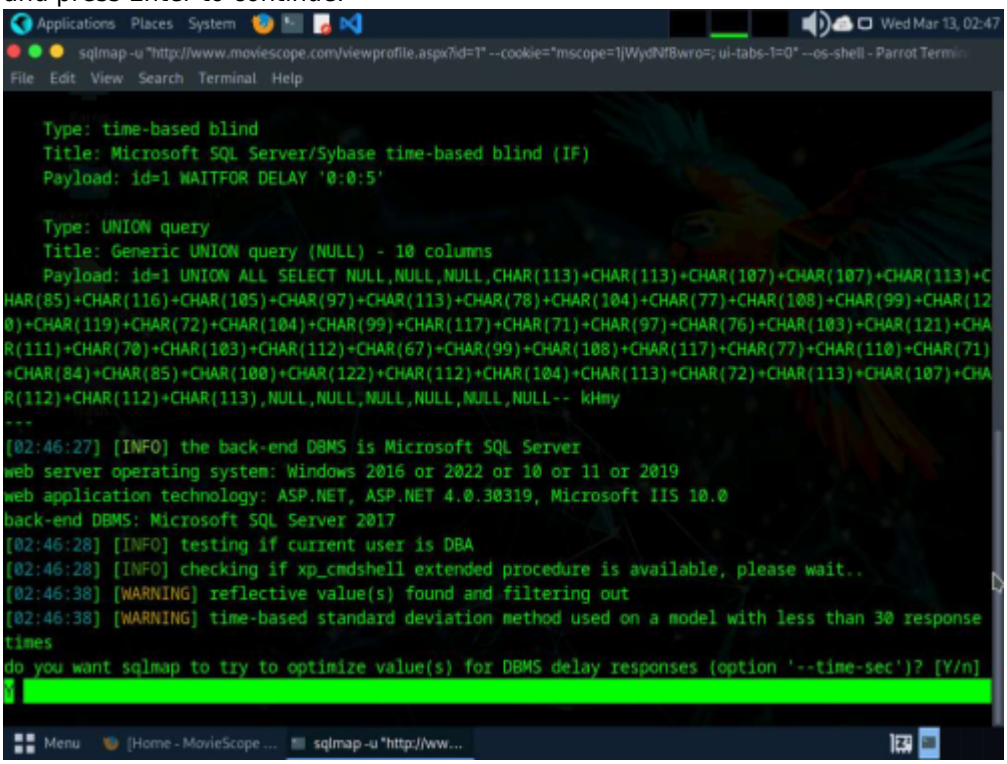
14. Now, you need to retrieve the table content of the column User_Login.
15. Run `sqlmap -u «http://www.moviescope.com/viewprofile.aspx?id=1» –cookie=«[cookie value which you have copied in Step#7]» -D moviescope -T User_Login –dump` command to dump all the **User_Login** table content.
16. sqlmap retrieves 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.
17. You will see that under the password column, the passwords are shown in plain text form.



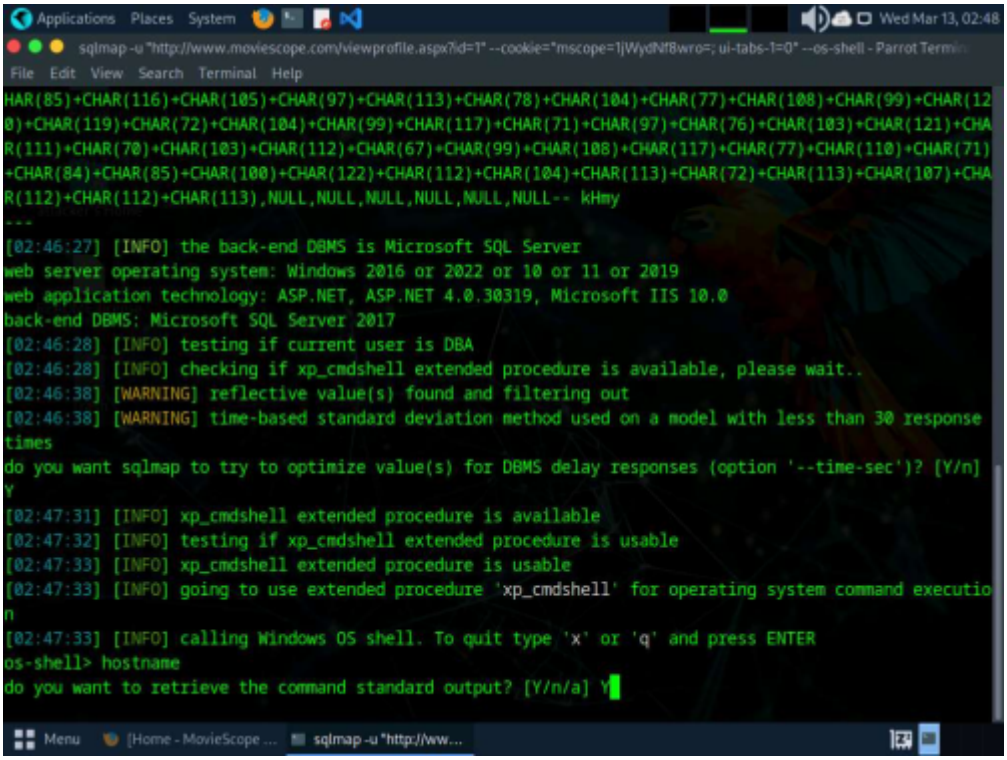
18. Now, switch back to the Parrot Terminal window. Run `sqlmap -u «http://www.moviescope.com/viewprofile.aspx?id=1» –cookie=«[cookie value which you have copied in Step#7]» –os-shell`.



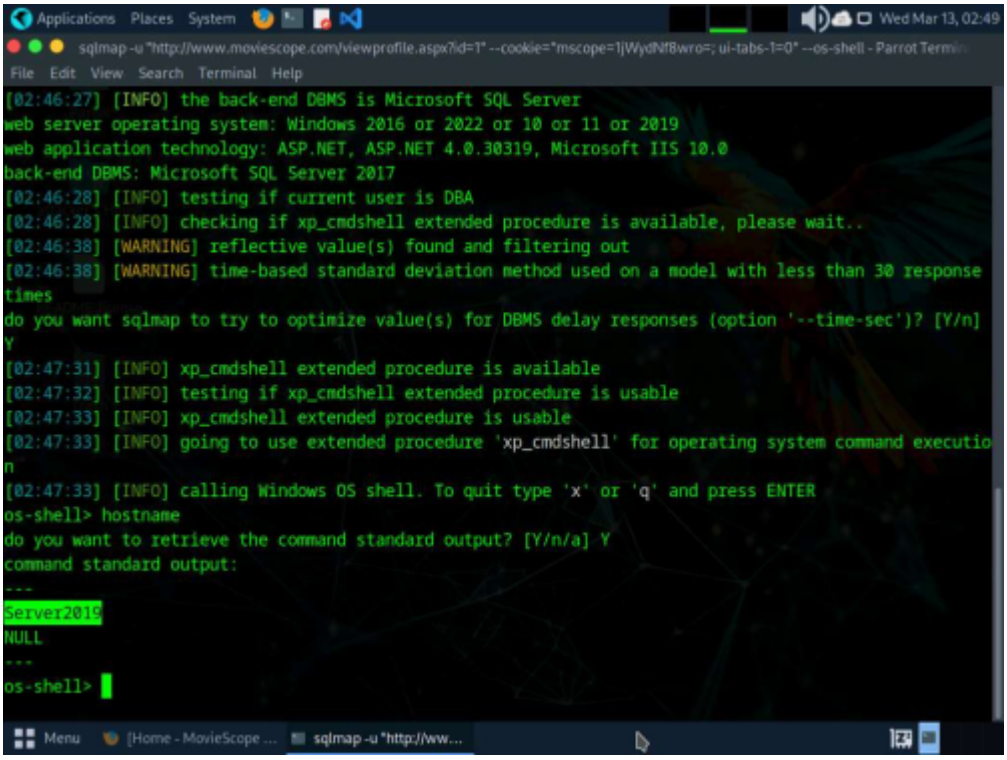
19. If the message do you want sqlmap to try to optimize value(s) for DBMS delay responses appears, type Y and press Enter to continue.



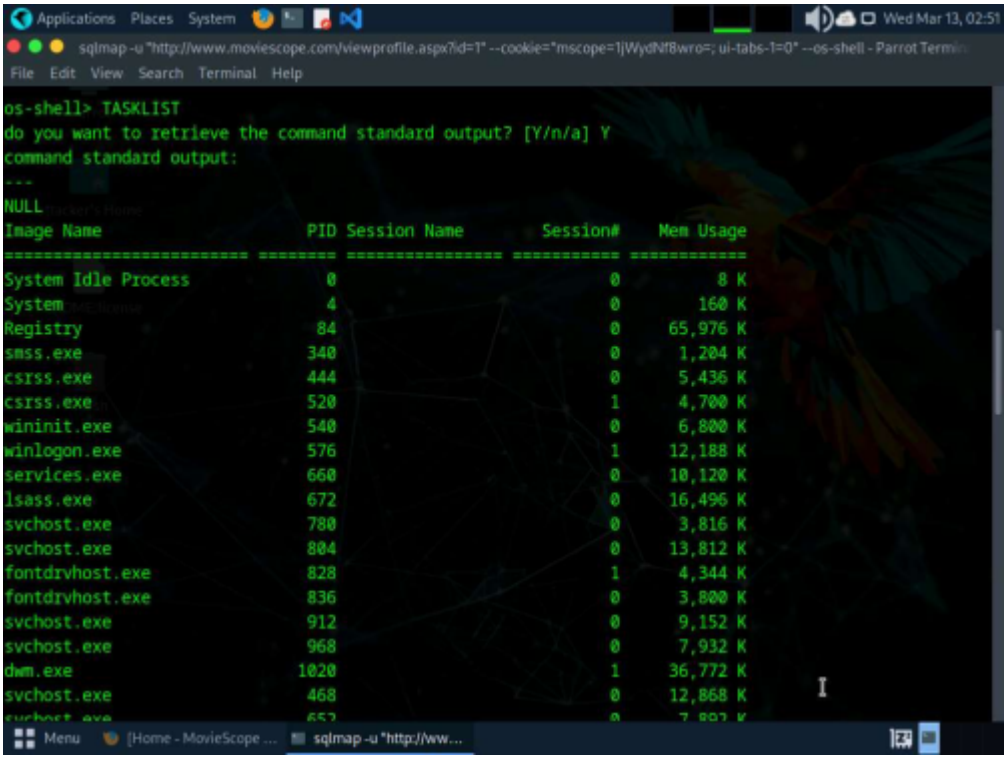
20. Once sqlmap acquires the permission to optimize the machine, it will provide you with the OS shell. Type hostname and press Enter to find the machine name where the site is running. If the message do you want to retrieve the command standard output? appears, type Y and press Enter.



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



22. Type **TASKLIST** and press Enter to view a list of tasks that are currently running on the target system.
23. If the message do you want to retrieve the command standard output? appears, type Y and press Enter. The above command retrieves the tasks and displays them under the command standard output section, as shown in the screenshots below.

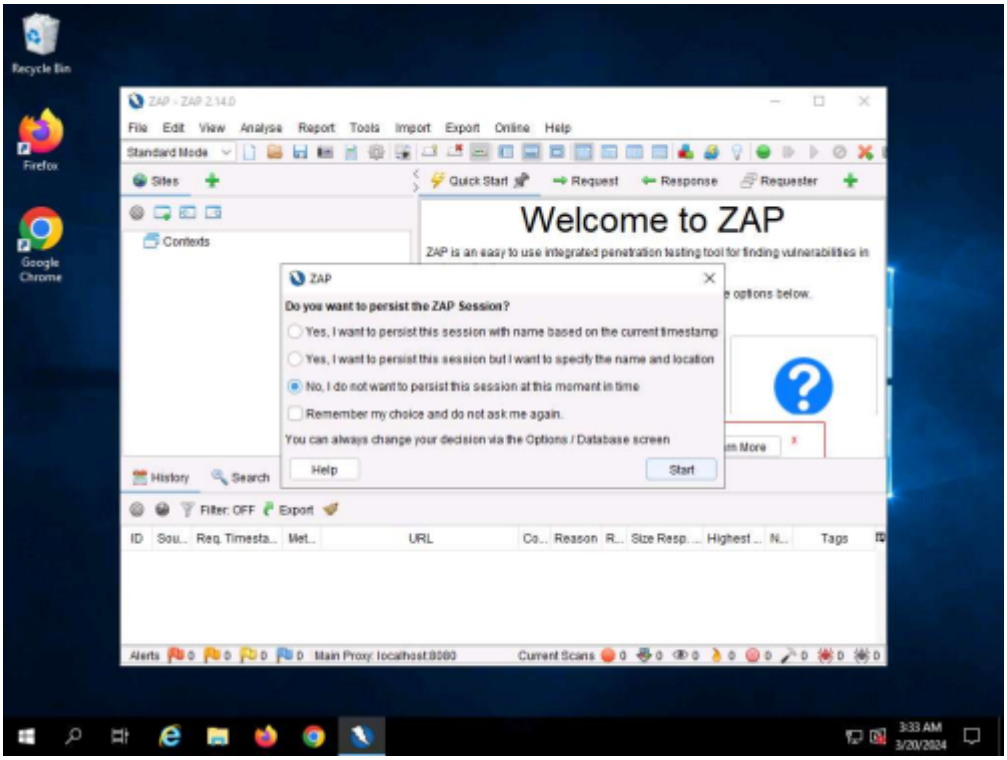


24. To view the available commands under the OS shell, type help and press Enter.
25. You can also use other SQL injection tools such as:
    1. Mole (https://sourceforge.net),
    2. jSQL Injection (https://github.com),
    3. NoSQLMap (https://github.com),
    4. Havij (https://github.com) and
    5. blind_sql_bitshifting (https://github.com).

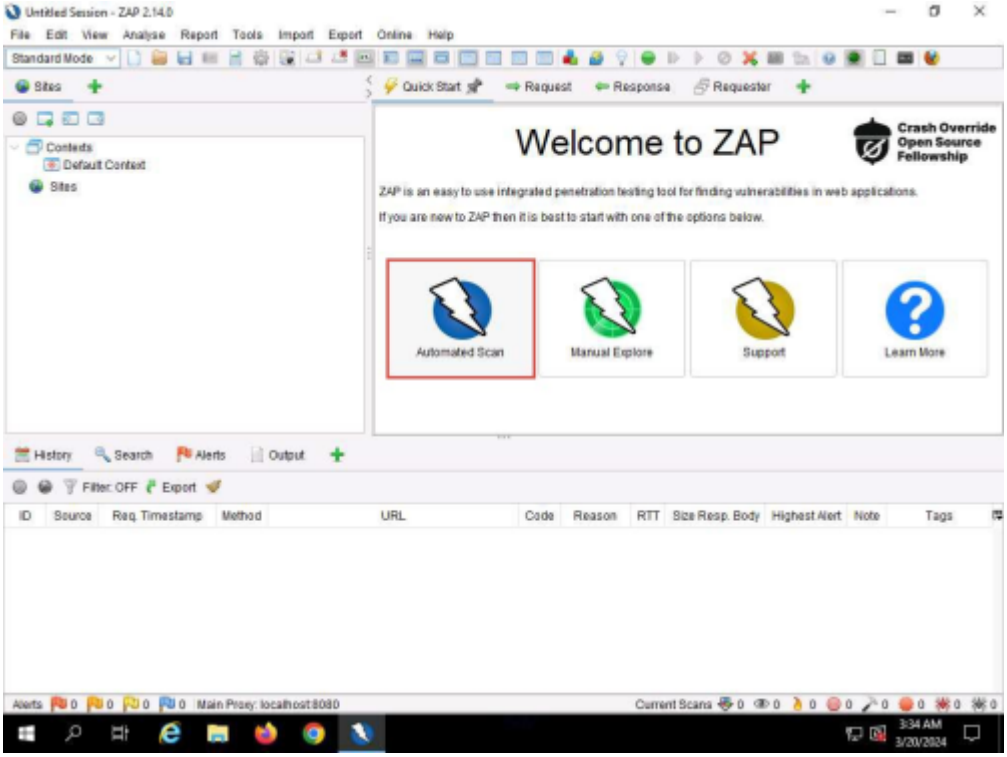
Lab 2 Modulo 15: Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools

Task 1: Detect SQL Injection Vulnerabilities using OWASP ZAP

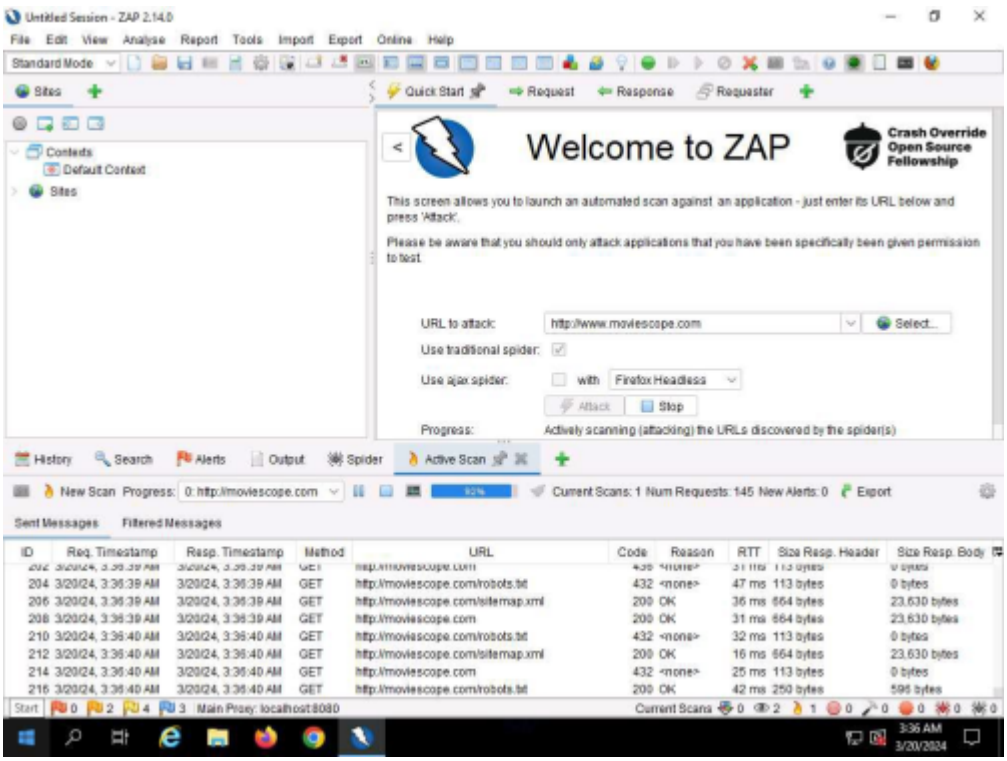
1. OWASP ZAP initialized and a prompt that reads Do you want to persist the ZAP Session? appears; select the No, I do not want to persist this session at this moment in time radio button, and click Start.



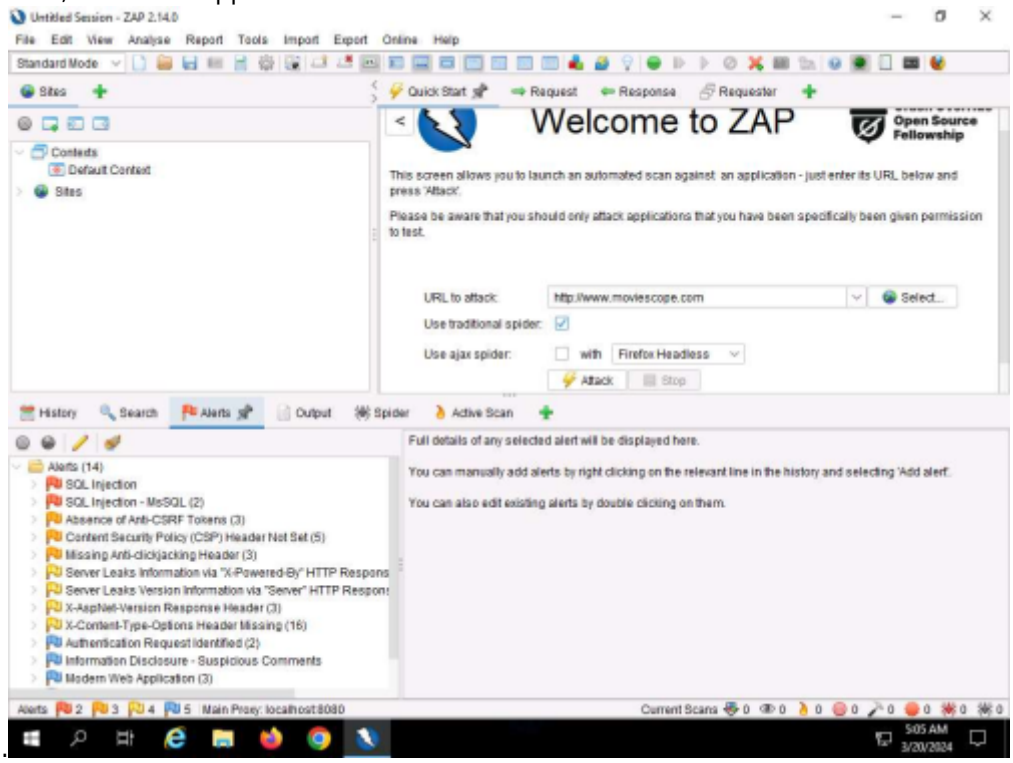
2. The OWASP ZAP main window appears; under the Quick Start tab, click the Automated Scan option.



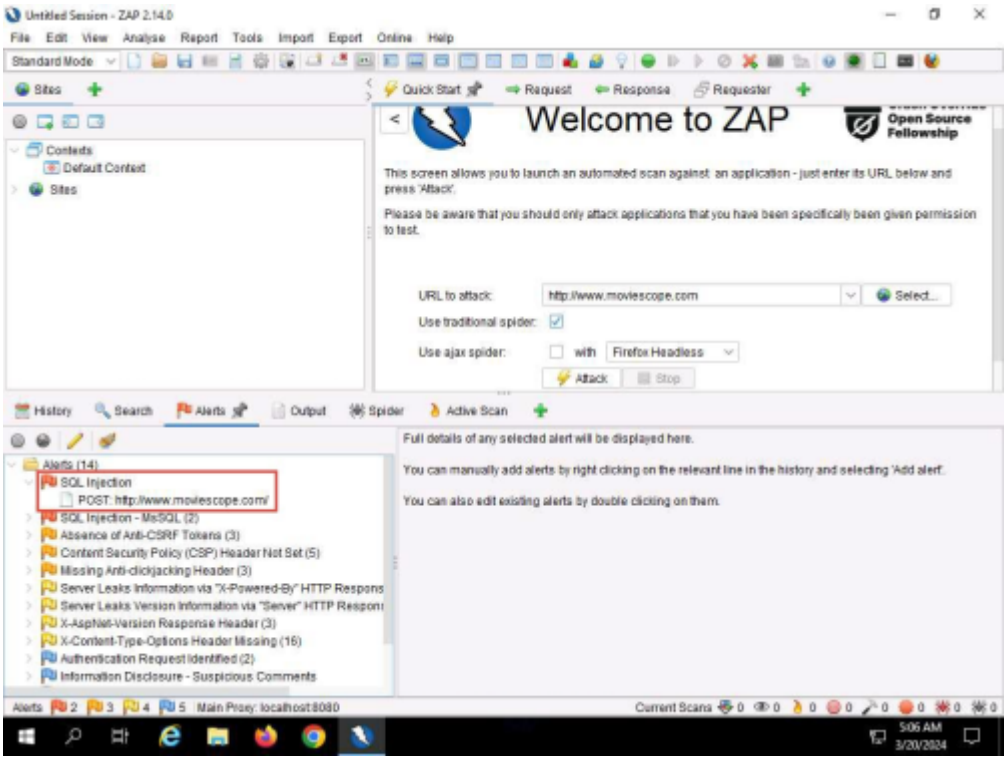
3. The Automated Scan wizard appears, enter the target website in the URL to attack field (in this case, http://www.moviescope.com). Leave other options set to default, and then click the Attack button. OWASP ZAP starts performing Active Scan on the target website, as shown in the screenshot.



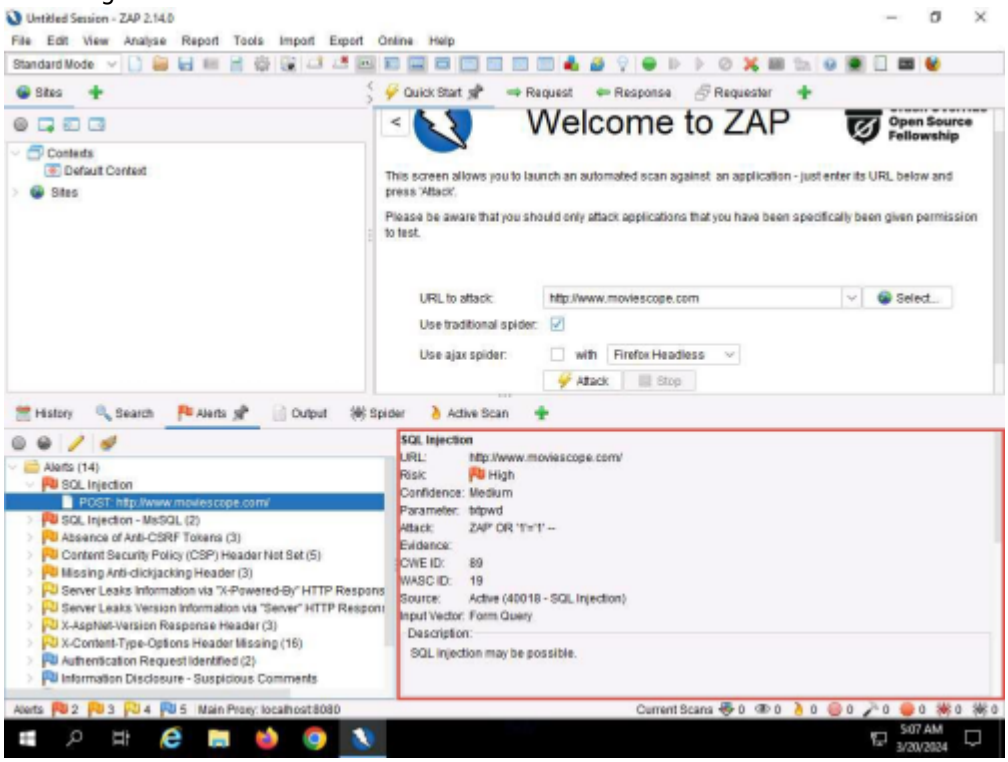
4. After the scan completes, Alerts tab appears. You can observe the vulnerabilities found on the website under the Alerts tab.



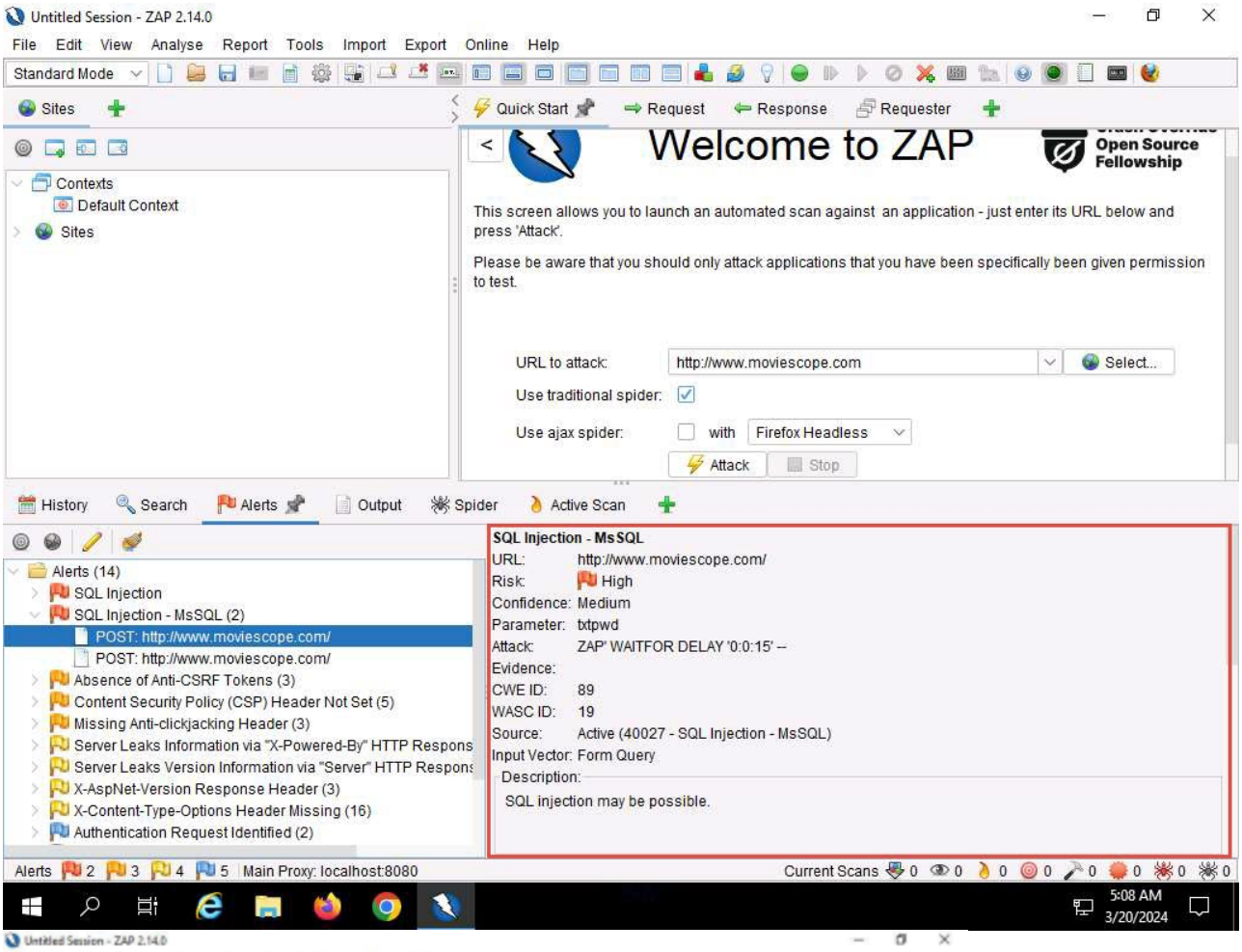
5. Now, expand the SQL Injection vulnerability node under the Alerts tab.

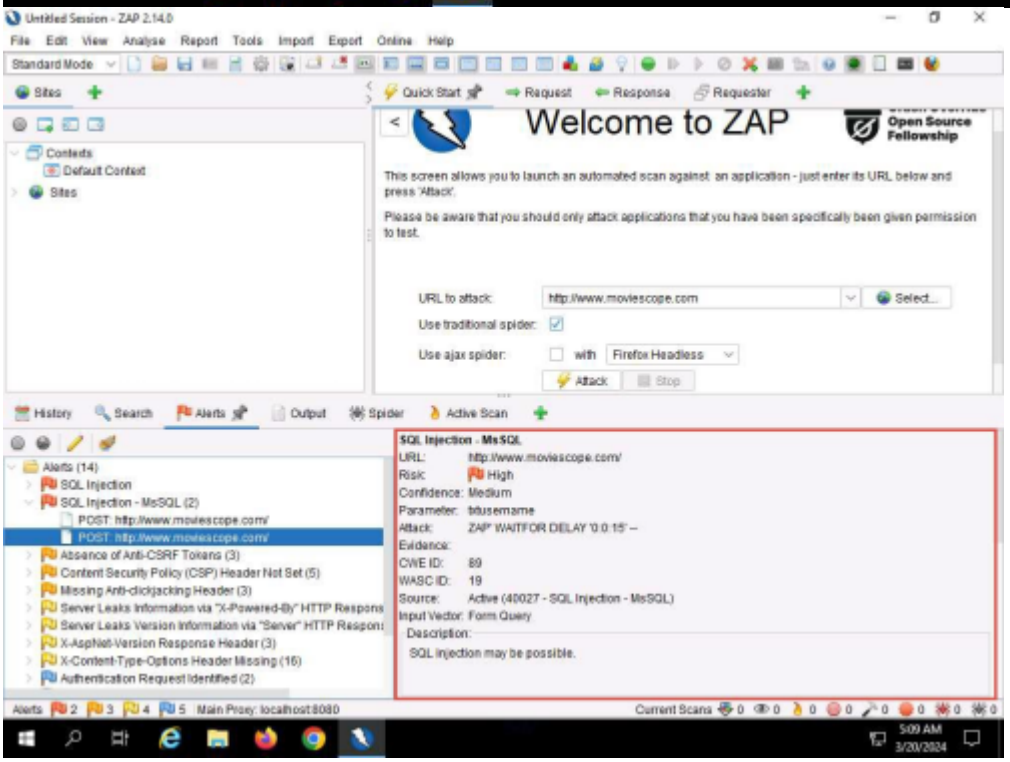


6. Click on the discovered SQL Injection vulnerability and further click on the vulnerable URL.
7. You can observe the information such as Risk, Confidence, Parameter, Attack, etc., regarding the discovered SQL Injection vulnerability in the lower right-bottom, as shown in the screenshot.
    1. Red Flag: High risk
    2. Orange Flag: Medium risk
    3. Yellow Flag: Low risk
    4. Blue Flag: Provides details about information disclosure vulnerabilities



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



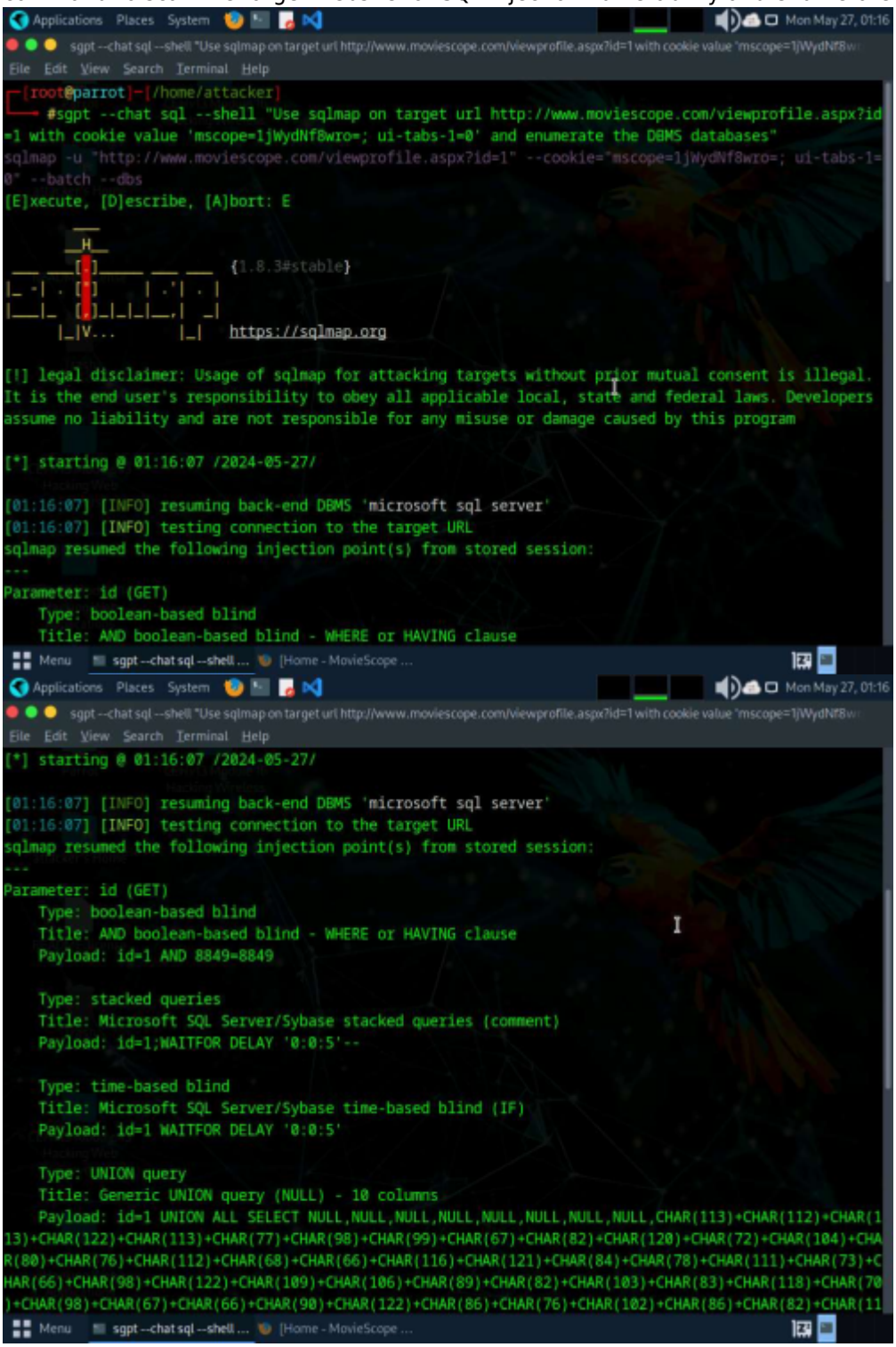


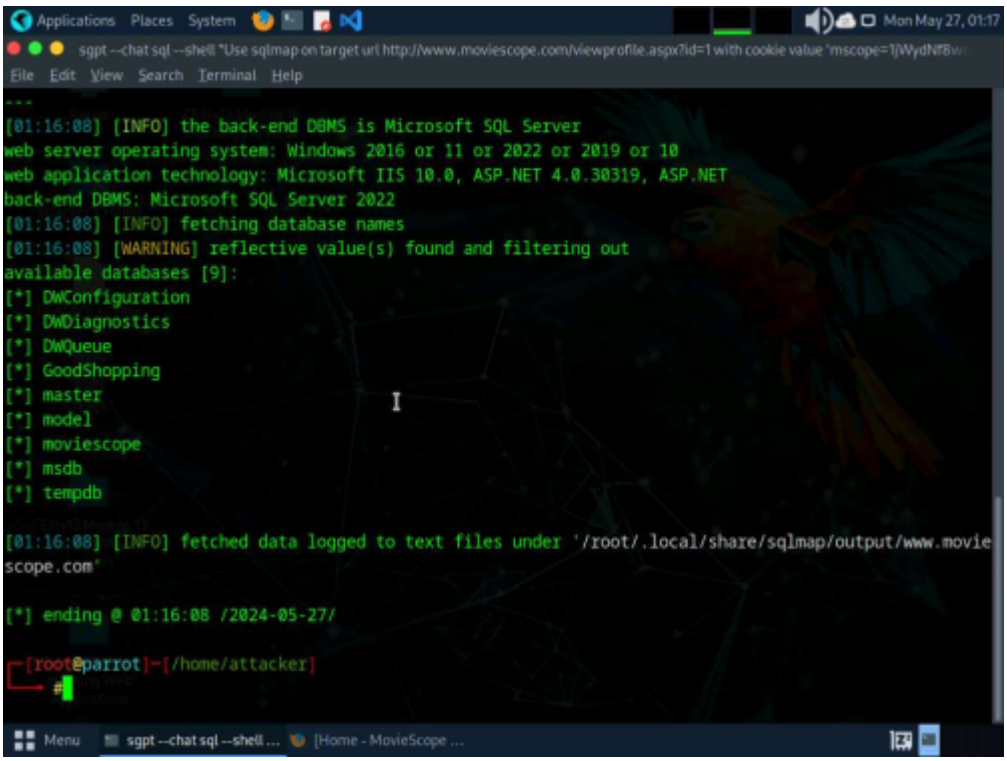
9. You can also use other SQL injection detection tools such as:
    1. Damn Small SQLi Scanner (DSSS) (https://github.com),
    2. Snort (https://snort.org),
    3. Burp Suite (https://www.portswigger.net),
    4. HCL AppScan (https://www. hcl-software.com) etc. to detect SQL injection vulnerabilities.

Lab 3: Perform SQL Injection using AI

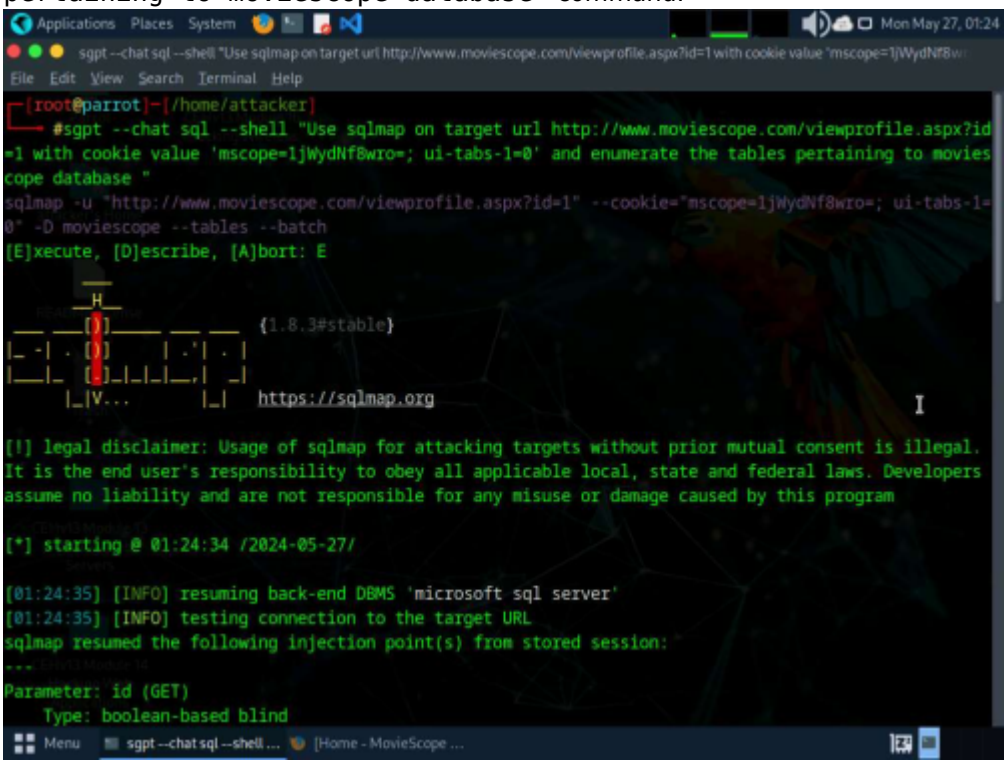
Task 1: Perform SQL Injection using ShellGPT

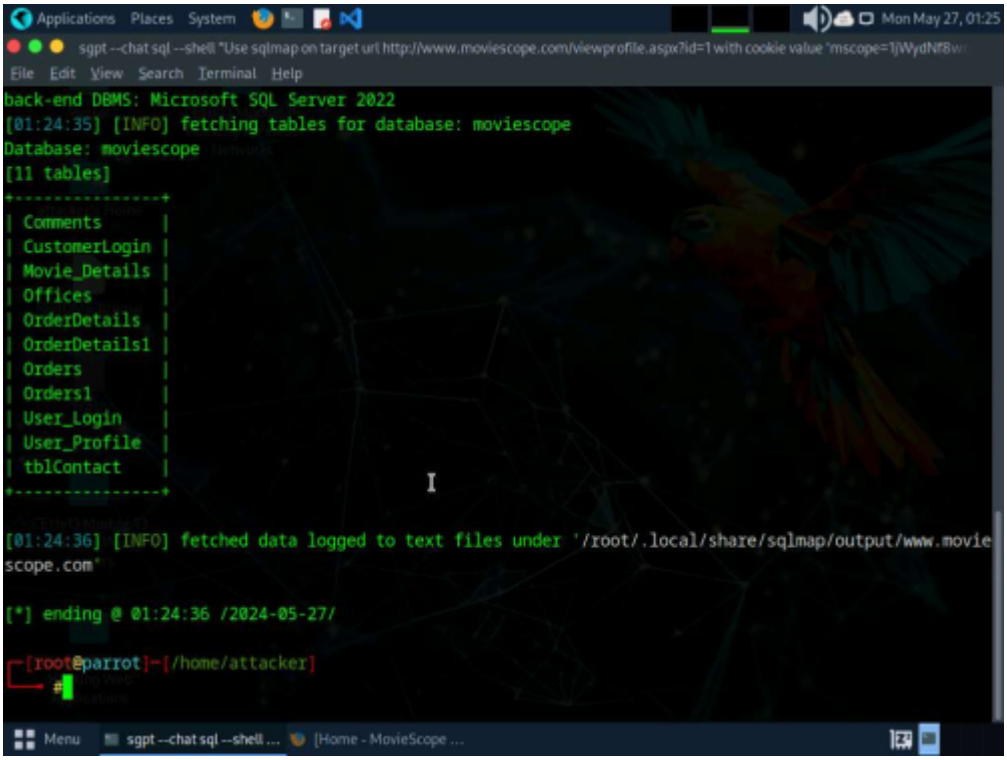
1. enumerate the database of the target website to do so, switch to the terminal window and run `sgpt –chat sql –shell “Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value '[cookie value which you have copied in Step#3]' and enumerate the DBMS databases”` command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



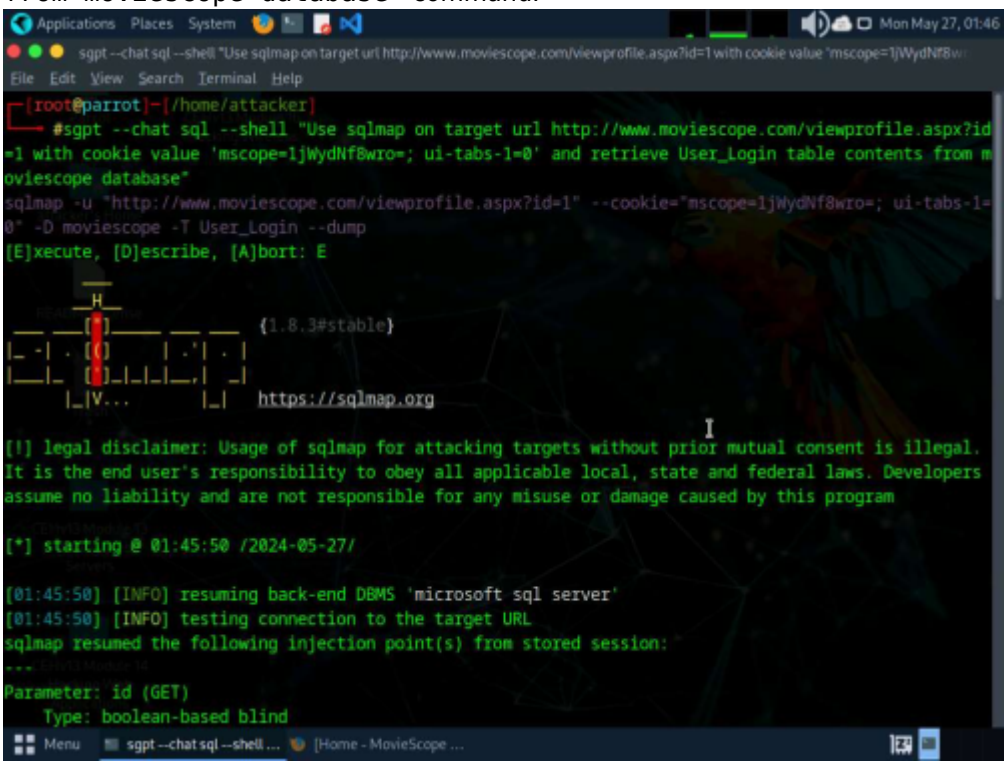


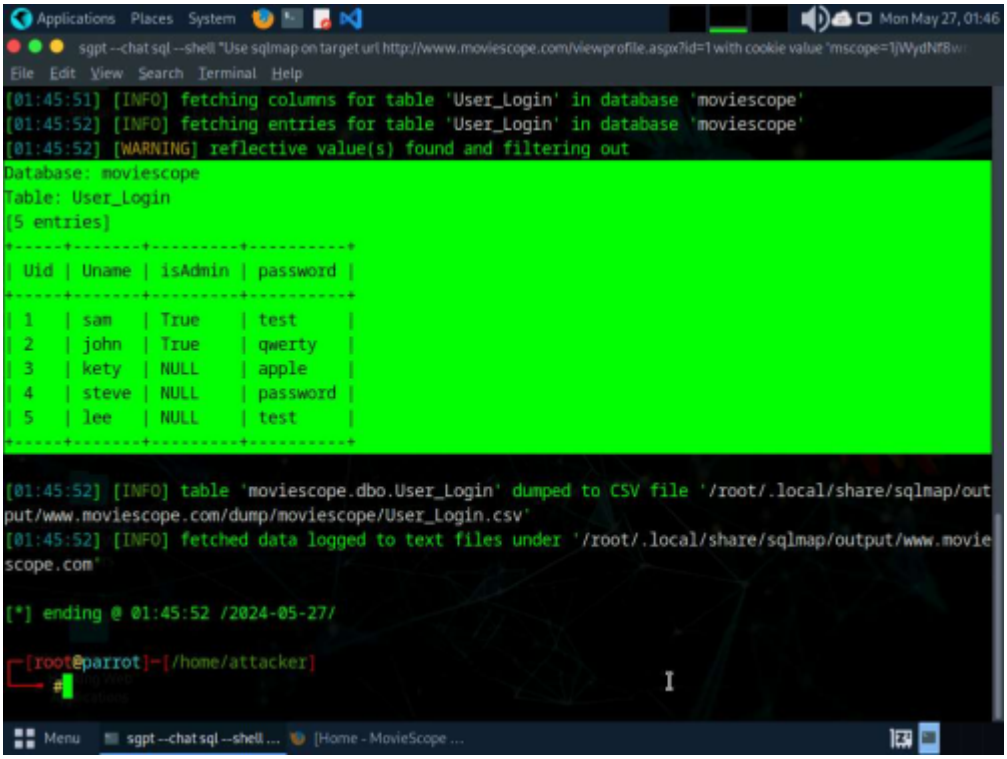
2. We have successfully enumerated the databases from the target website, we will now enumerate the tables pertaining to the database moviescope. To do so run `sgpt –chat sql –shell “Use sqlmap on target url http://www.moviescope.com/viewprofile.aspx?id=1 with cookie value '[cookie value which you have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





3. After enumerating the database tables we will dump the contents of the User_Login table to view the login information of the target website.
4. 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.





5. 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.

Module 16: Hacking Wireless Networks

```
-------------------------------------------------------------------------------
-----------------------------
Generation     IEEE Standard       Maximum Linkrate
Wi-Fi 7     802.11be          46 Gbit/s
Wi-Fi 6E    802.11ax          11 Gbit/s  Añade la banda de los 6GHz
Wi-Fi 6     802.11ax          11 Gbit/s  2,4GHz y 5GHz
Wi-Fi 5     802.11ac    680–6933 Mbit/s  2,4GHz y 5GHz
Wi-Fi 4     802.11n       72–600 Mbit/s  2,4GHz y 5GHz
Wi-Fi 3     802.11g         3–54 Mbit/s  2,4GHz
Wi-Fi 2     802.11b    1.5 to 54 Mbit/s  2,4GHz
Wi-Fi 1     802.11a      1 to 11 Mbit/s  3,7GHz y 5GHz
-------------------------------------------------------------------------------
-----------------------------
```

- WIFI 802.11bf: detección de movimiento (incloso frecuencia respiratoria) - WLAN sensing
  - https://www.genbeta.com/actualidad/detectar-movimiento-e-incluso-nuestra-frecuencia-respiratoria-asi-funcionaran-routers-nuevo-estandar-wifi-802-11bf
- Material Alumnos CEH (pCloud) → ZAC_FRTG_2024 2.pdf
- Algortimos:
  - RC4: algoritmo simétrico de tipo streaming
    - aún se usa en IoT, algoritmo rápido y poco consumo
  -

```
-------------------------------------------------------------------------------
-------------------------------------------------
Tecn.      <-------- IV ---------->      Alg.      Longitud key     Int.
Check Alg.      Key Management     Año
```

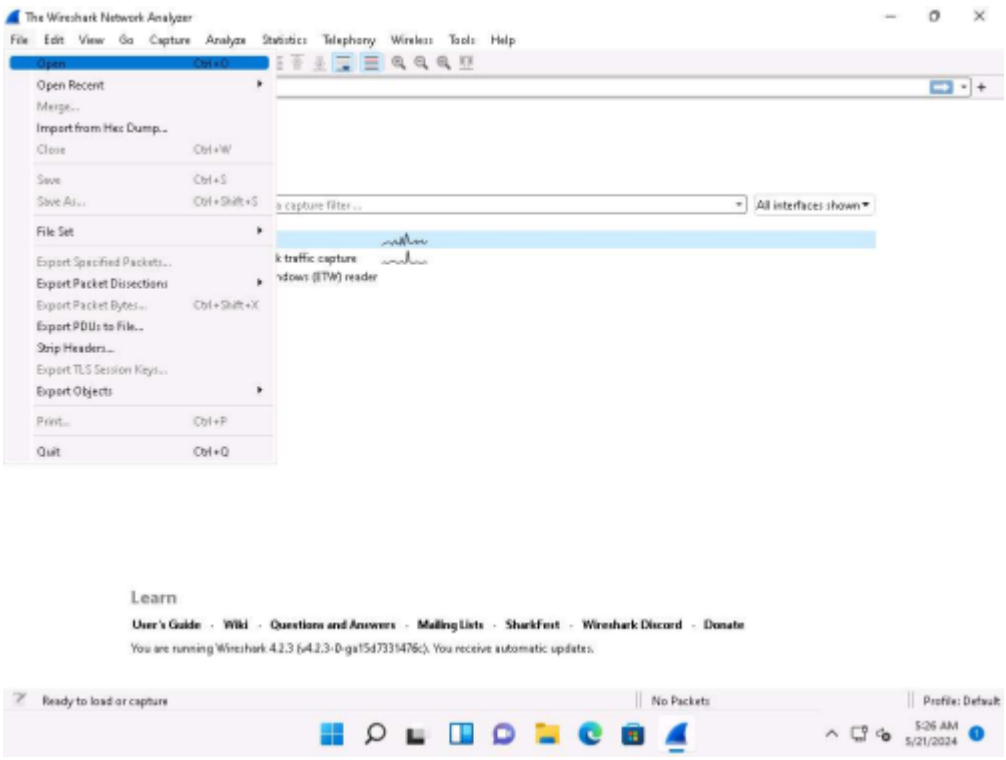
```
WEP       RC4  24 bits   EAP  40/104 bits    CRC-32       No
1997
WPA       RC4  48 bits   TKIP    128 bits  MA & CRC-32    4way Handshake
1999
WPA2      AES  48 bits   CCMP    128 bits   CBC-MAC       4way Handshake
2004
WPA3  AES-256 1-64 bits  GCMP    192 bits  BIP-GMAC-256   ECDH and ECDSA
2018
------------------------------------------------------------------------
-------------------------------------------------
```

    - Todos crackeables, contraseña lo más larga
- Ataques
    - Control de acceso
    - De integridad
    - de confidencialidad
    - Disponibilidad
    - Autenticación
    - KRACK → WPA2
- WPS → PIN numérico
    - incibe, guía para securizar router
    - https://www.redeszone.net/tutoriales/redes-wifi/metodos-crackear-wps-routers-wifi/
    - https://www.redeszone.net/tutoriales/redes-wifi/wps-que-es-como-funciona/
- https://www.incibe.es/sites/default/files/docs/guia_router/osi-guia-tu-router-tu-castillo.pdf
- Modo promíscuo = modo monitor
    - no todas las tarjetas → alpha wifi ASUS036ACH
    - ojo drivers OS
- Suite aircrack-ng
    - poner tarjeta en modo monitor
    - `airdump-ng`
- aLTEr Attack - error de diseño de 4G, antena falsa
- Contramedidas: VPN
- Hasta telefonia 4G, antena multidireccional. Varias antenas para triangular
- en 5G, unidireccional. Geolocalización con una sola antena, más precisión (hasta 50cm de margen)
- móviles anuncian su MAC al detectar una WIFI → seguimiento
    - los móviles ahora rotan la MAC para evitar el seguimiento
    - se puede forzar a usar la real (mirando en la WIFI)
    - https://computerhoy.com/noticias/moviles/papeleras-espia-rastrean-transeuntes-londres-5593
- Sidewalk → red WIFI de medio/largo alcance
    - red MESH
    - https://www.redeszone.net/reportajes/tecnologias/sidewalk-que-es-wifi-amazon-como-funciona/
    - Solo EEUU, no UE

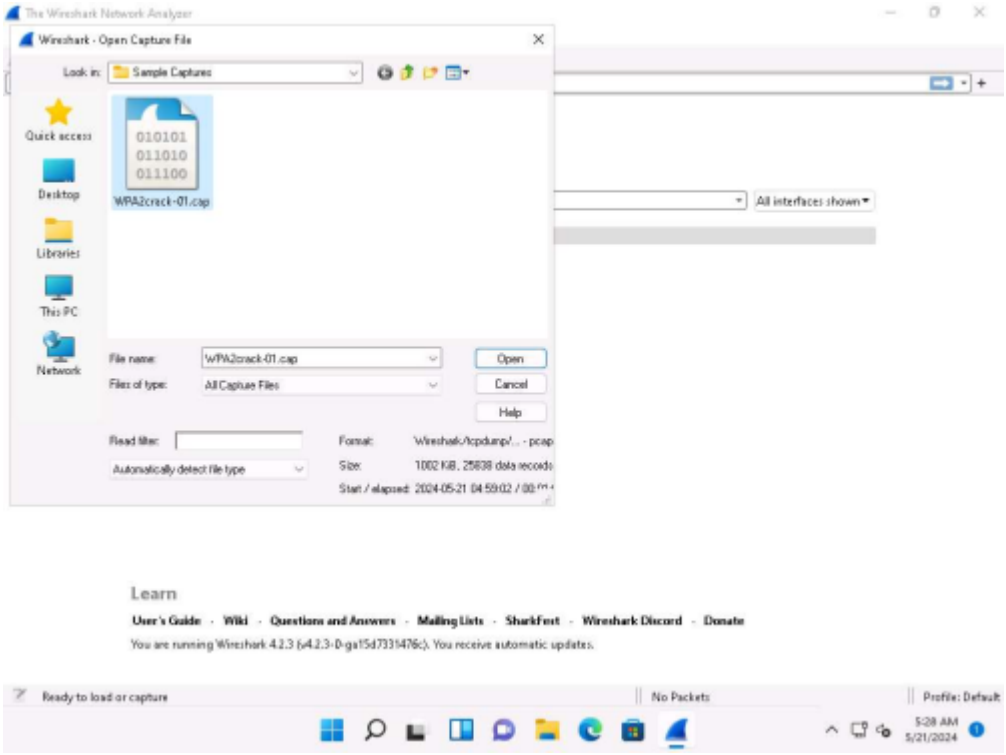
Lab 1 Modulo 16: Perform Wireless Traffic Analysis

Task 1: Wi-Fi Packet Analysis using Wireshark

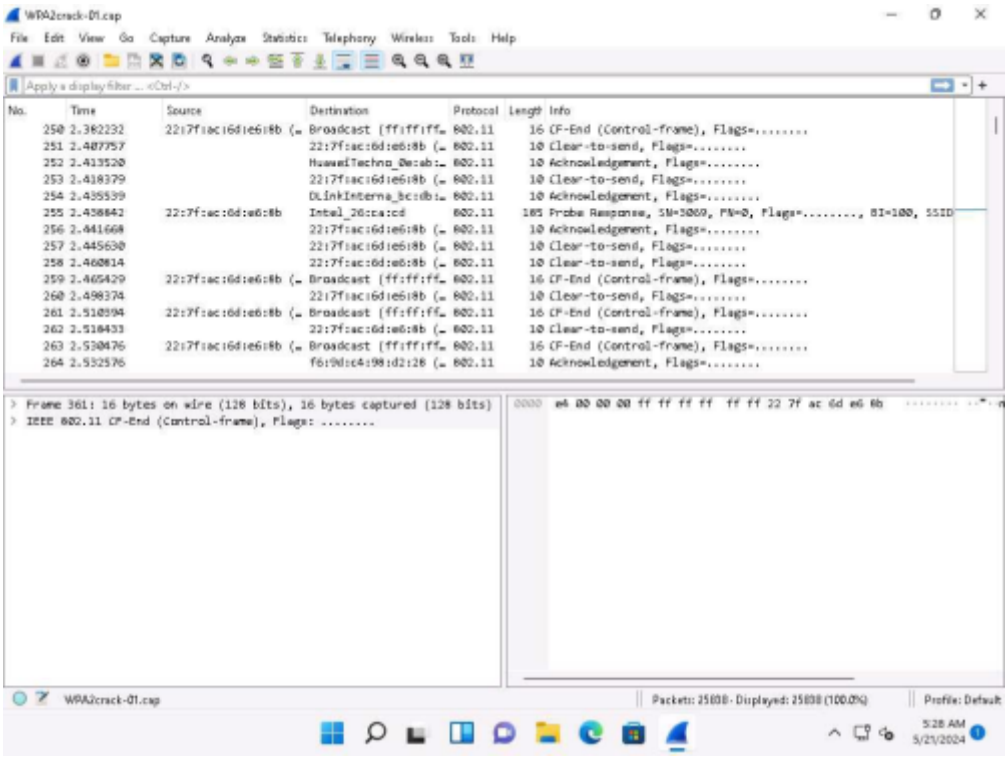
1. The **Wireshark** Network Analyzer window appears.
2. In the menu bar, click File and click Open option from the drop-down list.



3. Wireshark: Open Capture File window appears, navigate to E:\CEH-Tools\CEHv13 Module 16 Hacking Wireless Networks\Sample Captures, select WPA2crack-01.cap and click Open.



4. The WPA2crack-01.cap file opens in Wireshark window showing you the details of the packet for analysis. Here you can see the wireless packets captured which were otherwise masked to look like ethernet traffic.
5. Here 802.11 protocol indicates wireless packets.
6. You can access the saved packet capture file anytime, and by issuing packet filtering commands in the Filter field, you can narrow down the packet search in an attempt to find packets containing sensible information.
7. In real time, attackers enforce packet capture and packet filtering techniques to capture packets containing passwords (only for websites implemented on HTTP channel), perform attacks such as session



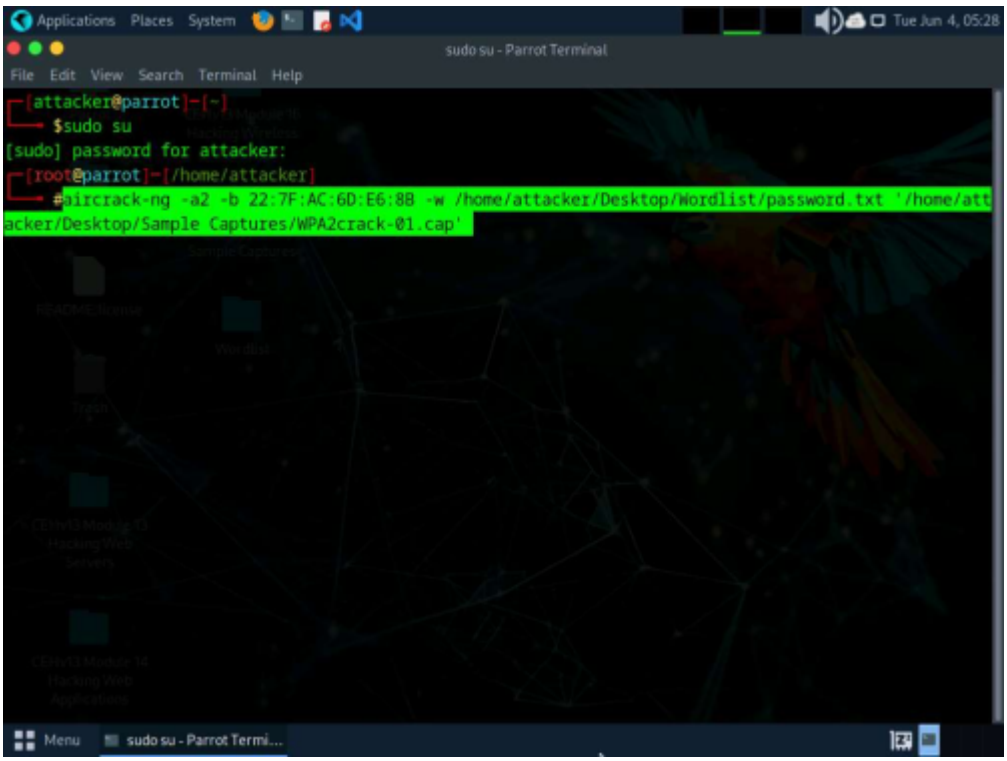
hijacking, and so on.

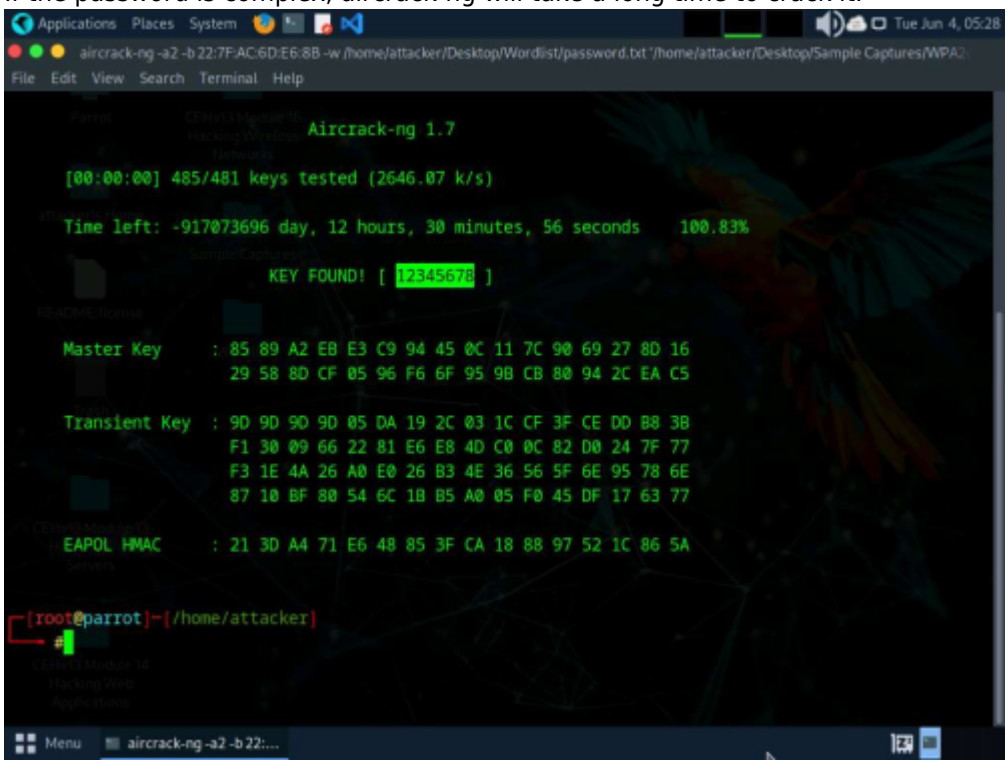
8. You can also use other wireless traffic analyzers such as:
    1. AirMagnet WiFi Analyzer PRO (https://www.netally.com),
    2. SteelCentral Packet Analyzer (https://www.riverbed.com),
    3. Omnipeek Network Protocol Analyzer (https://www.liveaction.com),
    4. and CommView for Wi-Fi (https://www.tamos.com) to analyze Wi-Fi traffic.

Lab 2: Perform Wireless Attacks

Task 1: Crack a WPA2 Network using Aircrack-ng

1. In the Parrot Terminal window, run `aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt «/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap»`. Here, the BSSID of the target is 22:7F:AC:6D:E6:8B.
    1. -a is the technique used to crack the handshake, 2=WPA technique.
    2. -b refers to bssid; replace with the BSSID of the target router.
    3. -w stands for wordlist; provide the path to a wordlist.

2. 

3. The result appears, showing the WPA handshake packet captured with airodump-ng. The target access point's password is cracked and displayed in plain text next to the message KEY FOUND!, as shown in the screenshot.
    1. If the password is complex, aircrack-ng will take a long time to crack it.


    2. You can also use other tools such as:
        1. hashcat (https://hashcat.net),
        2. Portable Penetrator (https://www.secpoint.com),
        3. WepCrackGui (https://sourceforge.net) to crack WEP/WPA/WPA2 encryption.

Module 17: Hacking Mobile Platforms