Web Application Penetration Testing Methodology

3 Hr 28 Min Remaining

Instructions Resources Help  100%

Exercise 6: Performing Dictionary Attack on a WordPress Web Application using Burp Suite

Scenario

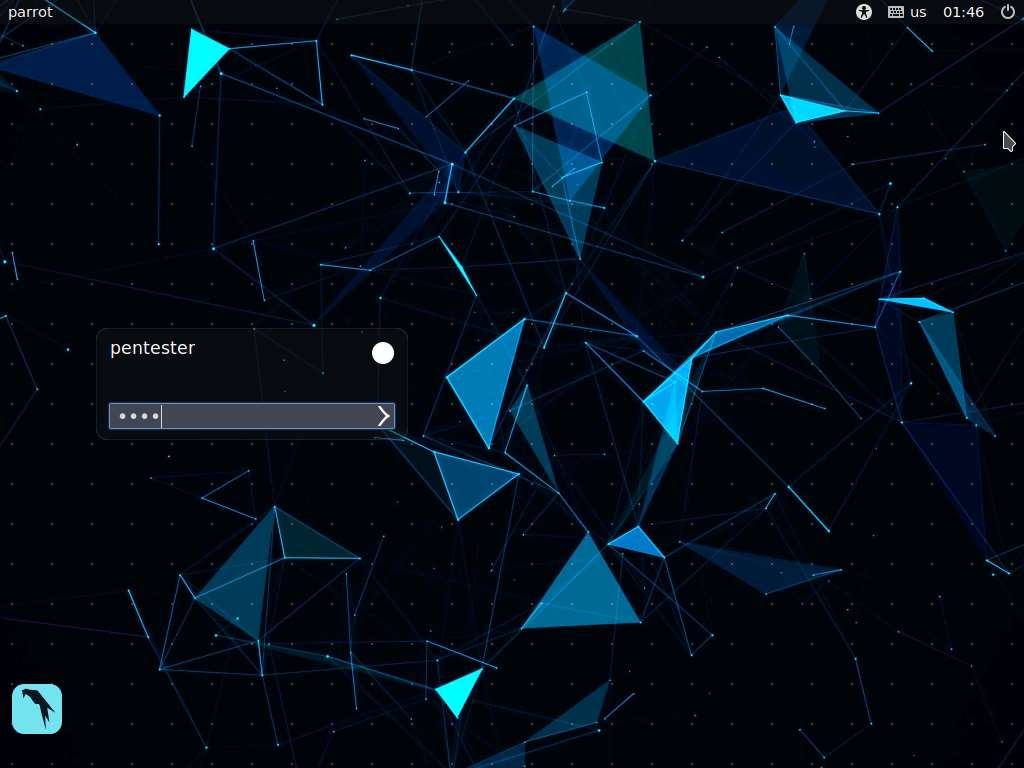
Using weak username/password combinations to log in to web applications might allow attackers to brute-force them and gain access to them. This leads to unrestricted access to user accounts and manipulation of data in those accounts.

As a penetration tester, you should be able to identify weak username-password combinations in web applications. In this lab, you are going to learn how to perform a dictionary attack on WordPress web application using Burp Suite.

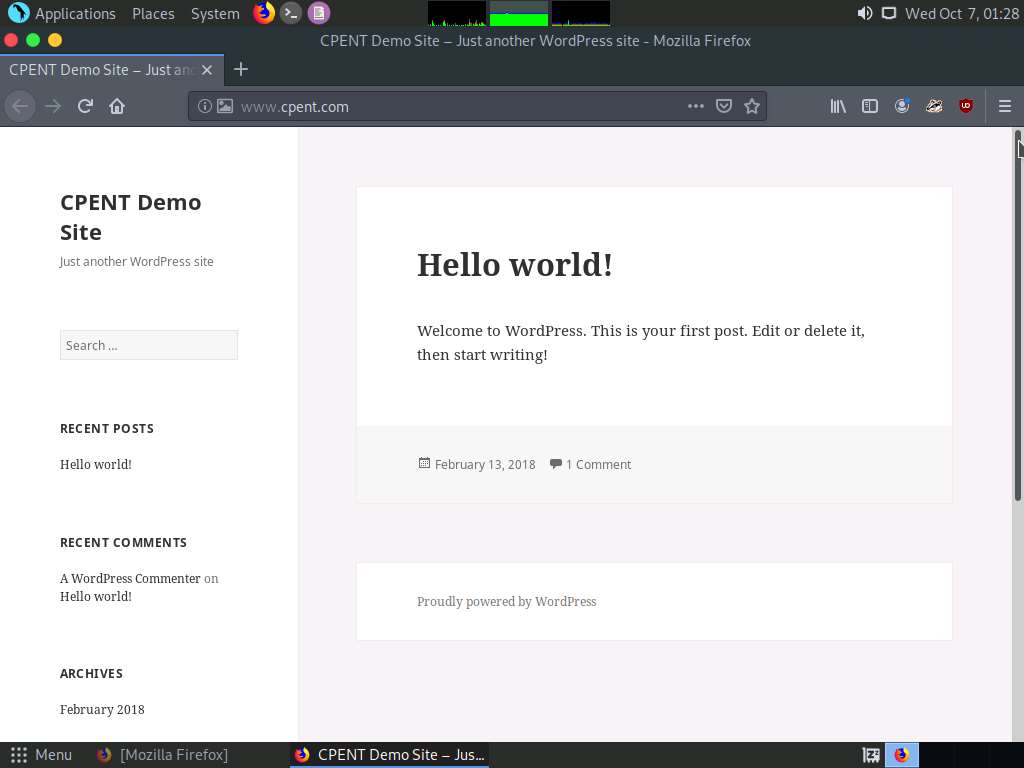
**Lab Duration**: **30** Minutes

1. Click [Parrot](https://labclient.labondemand.com/Instructions/24205116-eb0d-48aa-9936-8931f0fd5efc?rc=10). Type **toor** in the **Password** field and press **Enter**.

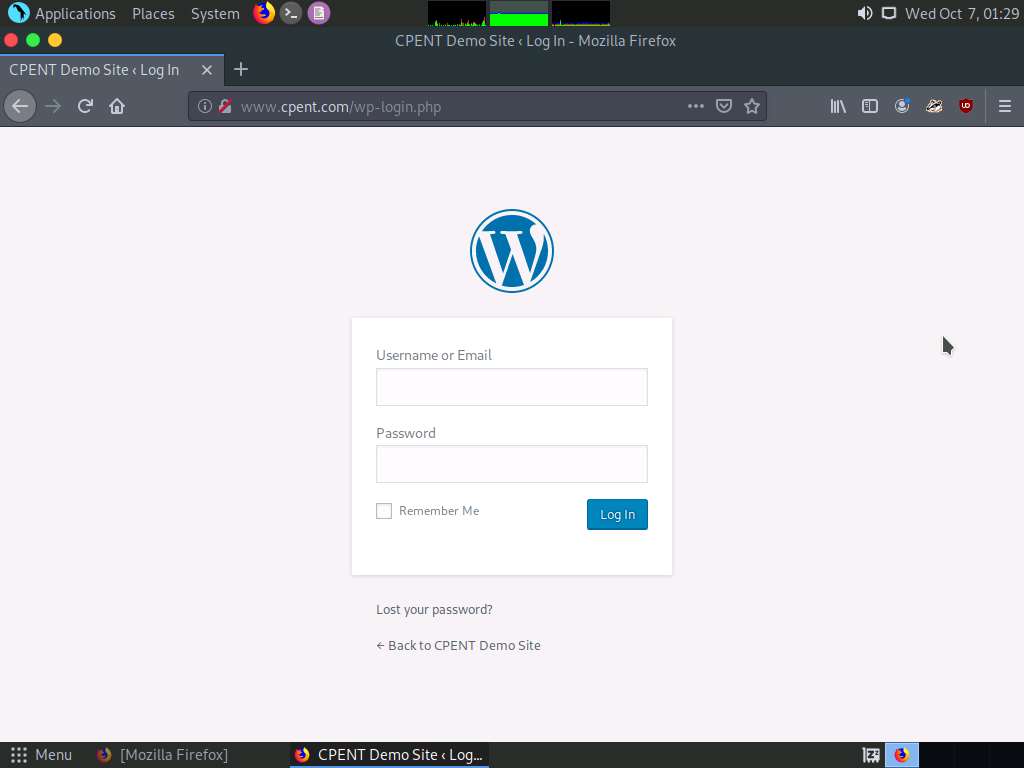
If you are already logged in skip to step **2**.



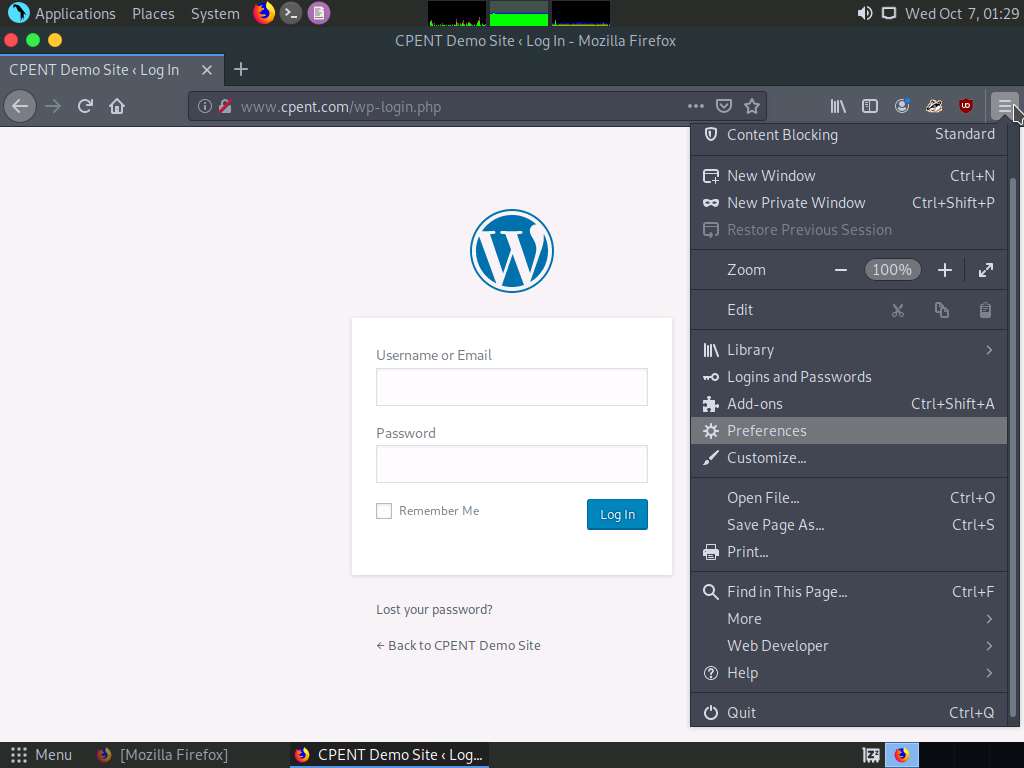
1. In this lab, we will target a web application with the URL **http://www.cpent.com**. So, launch a web browser, type the URL **http://www.cpent.com** and press **Enter**. CPENT Demo Site appears as shown in the screenshot.



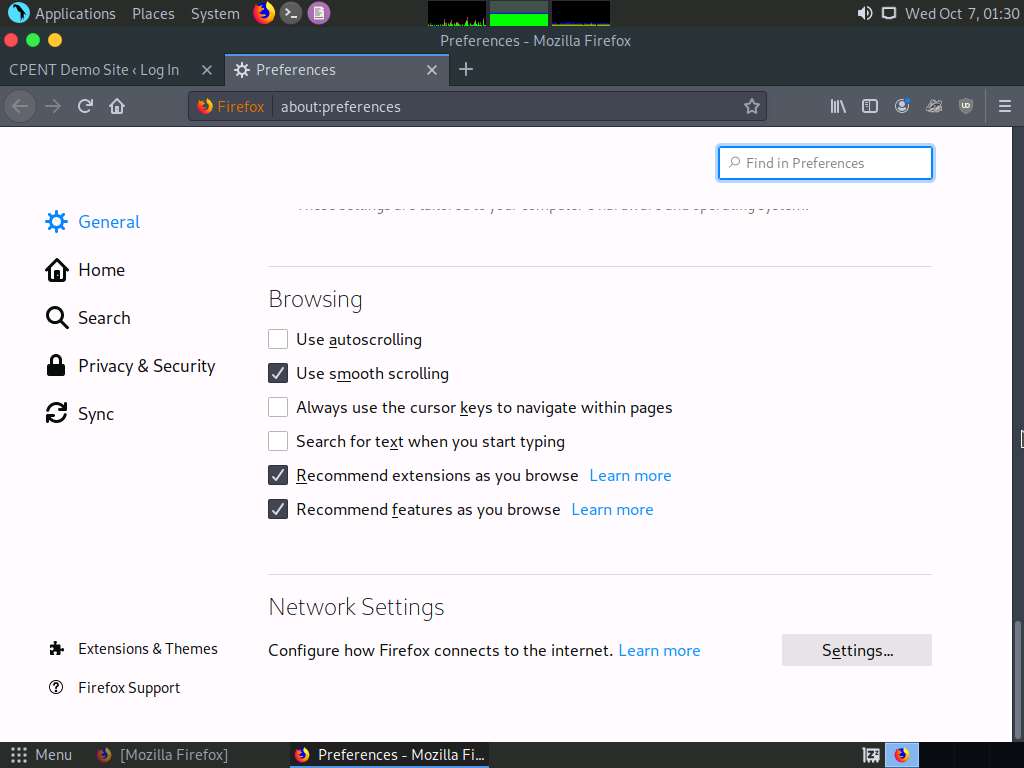
1. In this lab, we will be launching a dictionary attack on the website to see if there are any weak username/password combinations. Here, we will enter random user credentials on the login page, capture the login request and use it in Burp Suite to perform a dictionary attack on the website. Type the URL **http://www.cpent.com/wp-login.php** in the address bar and press **Enter**. This displays the CPENT Demo Site login page.



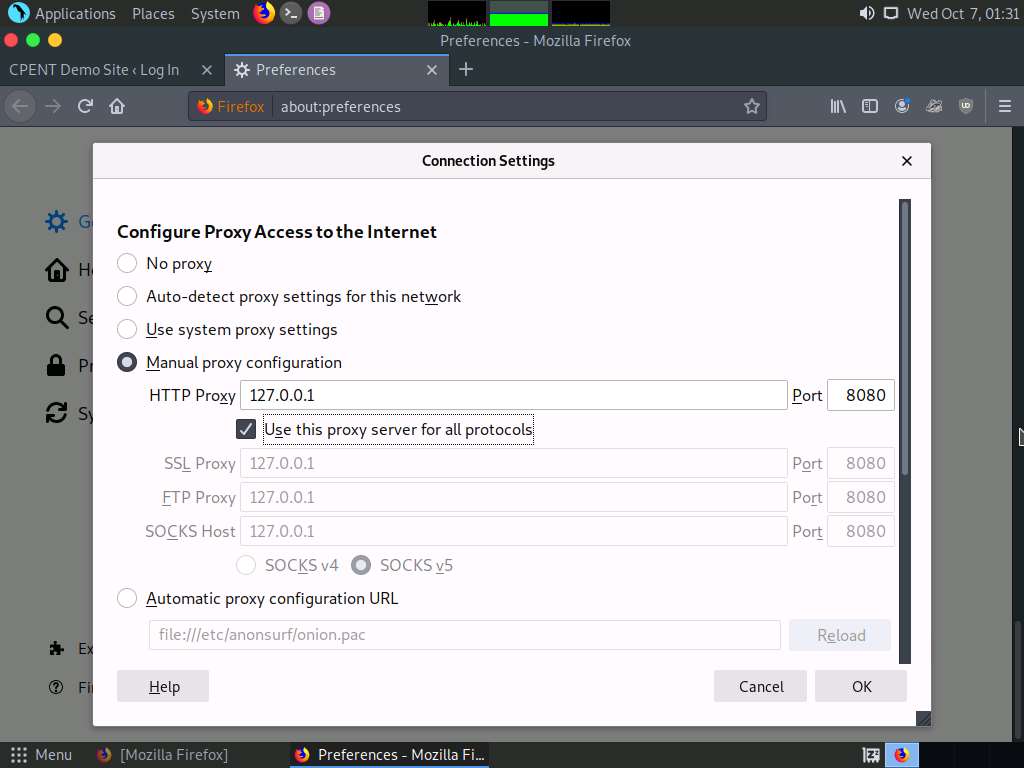
1. Open **Firefox** menu and click **Preferences** as shown in the screenshot.



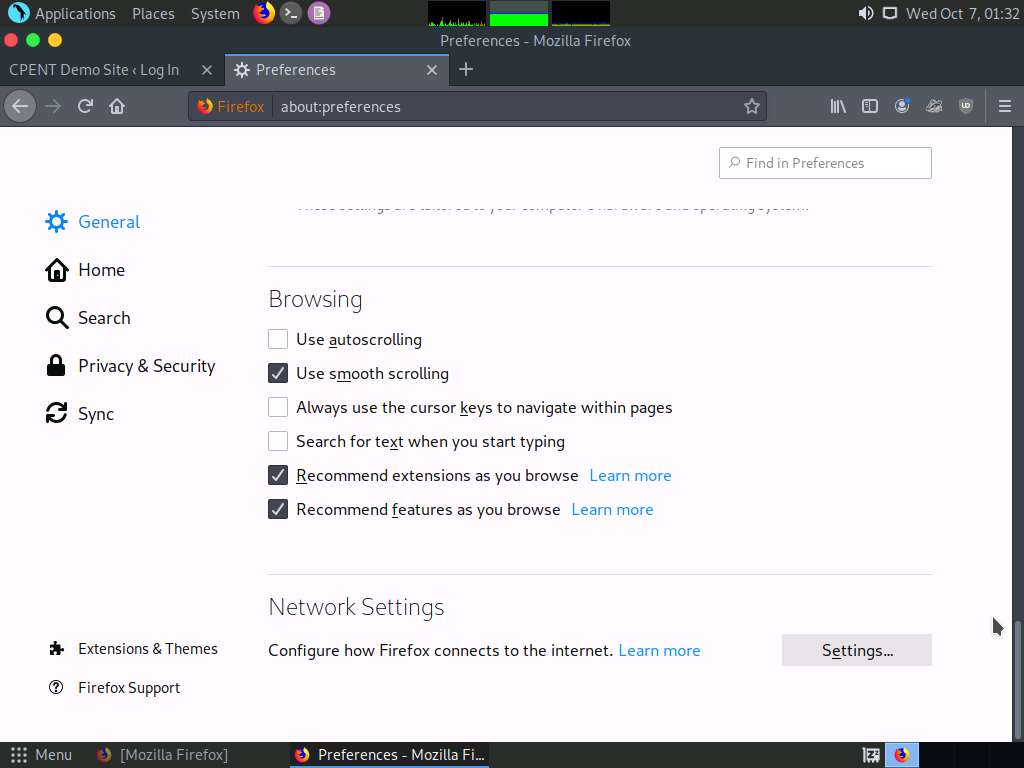
1. **Preferences** window appears, with **General** settings. Scroll down and click **Settings** under **Network Settings**.



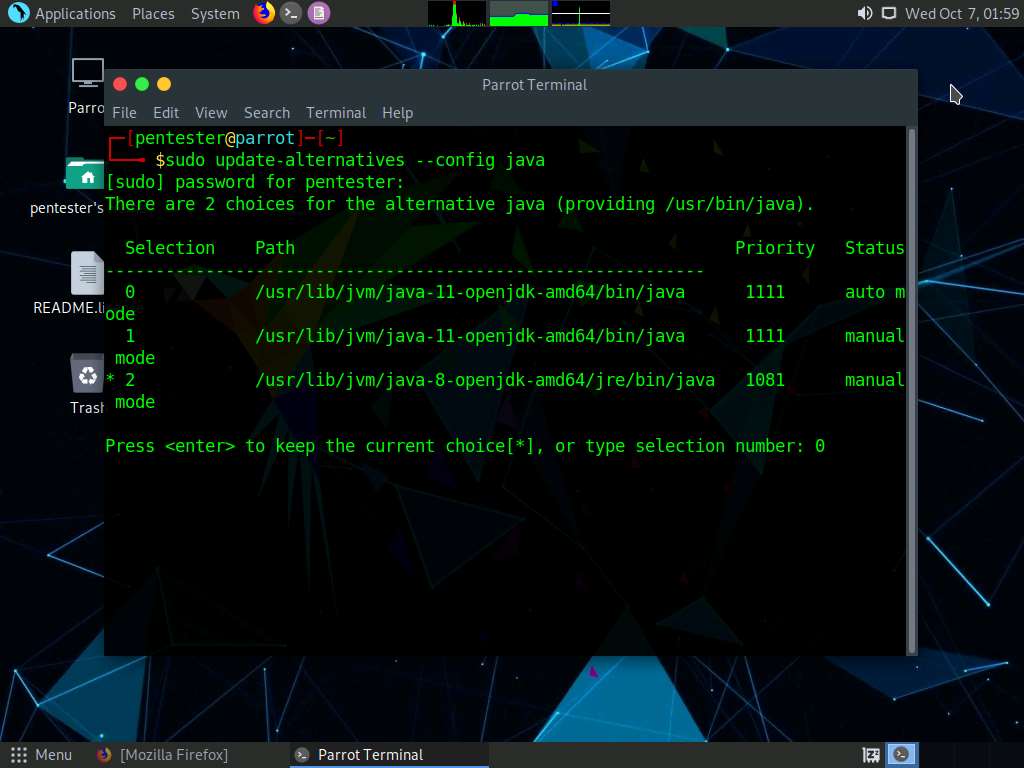
1. **Connection Settings** window appears, click **Manual proxy configuration** radio button. Enter the IP address **127.0.0.1** in the **HTTP Proxy** field, specify the port number **8080** in the Port field, check **Use this proxy server for all protocols** and click **OK**.



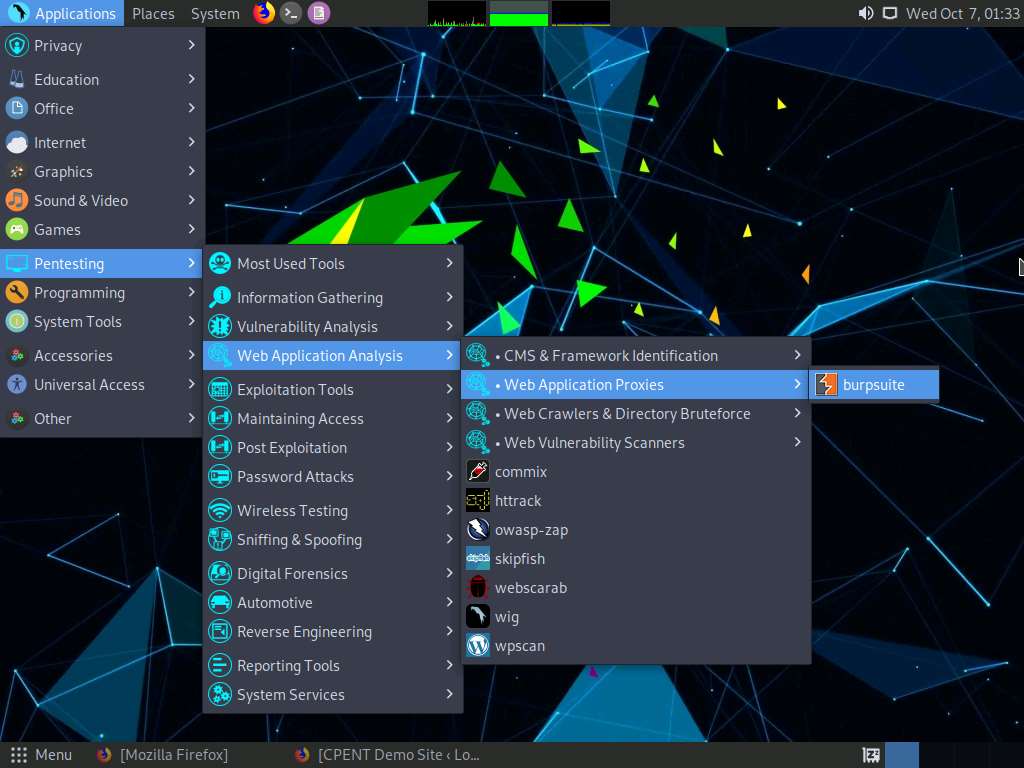
1. Close the **Preferences** tab and minimize the web browser.



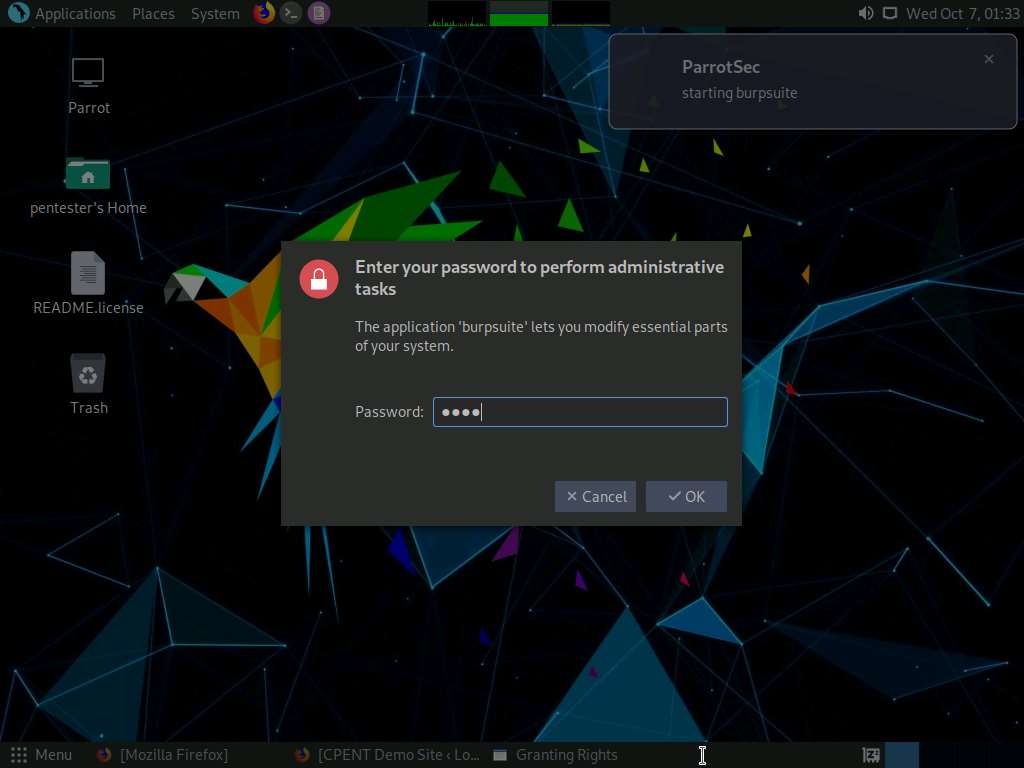
1. Open a terminal, and type **sudo update-alternatives --config java** and press **Enter**. Type **toor** and press **Enter**. There are 2 choices for the alternative java appears, type **0** and press **Enter**. Close the terminal window.



1. Navigate to **Applications** | **Pentesting** | **Web Application Analysis** | **Web Application Proxies** and click **burpsuite** to launch the application.

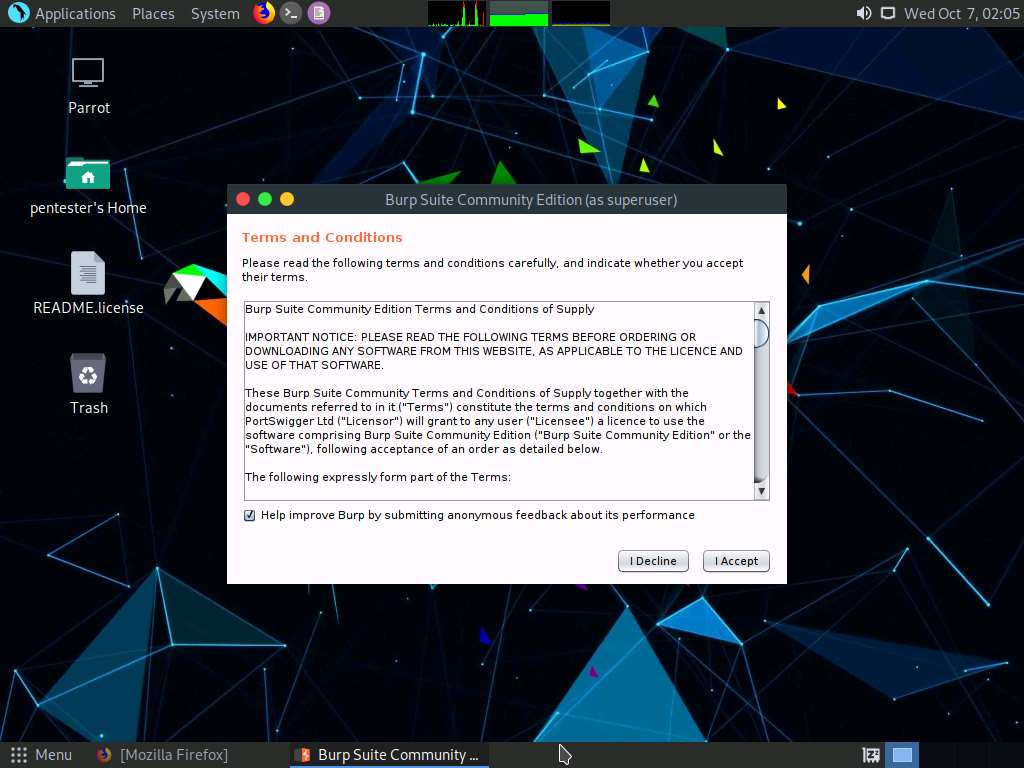


1. Enter your password to perform administrative tasks pop-up appears, type toor and click **OK**.



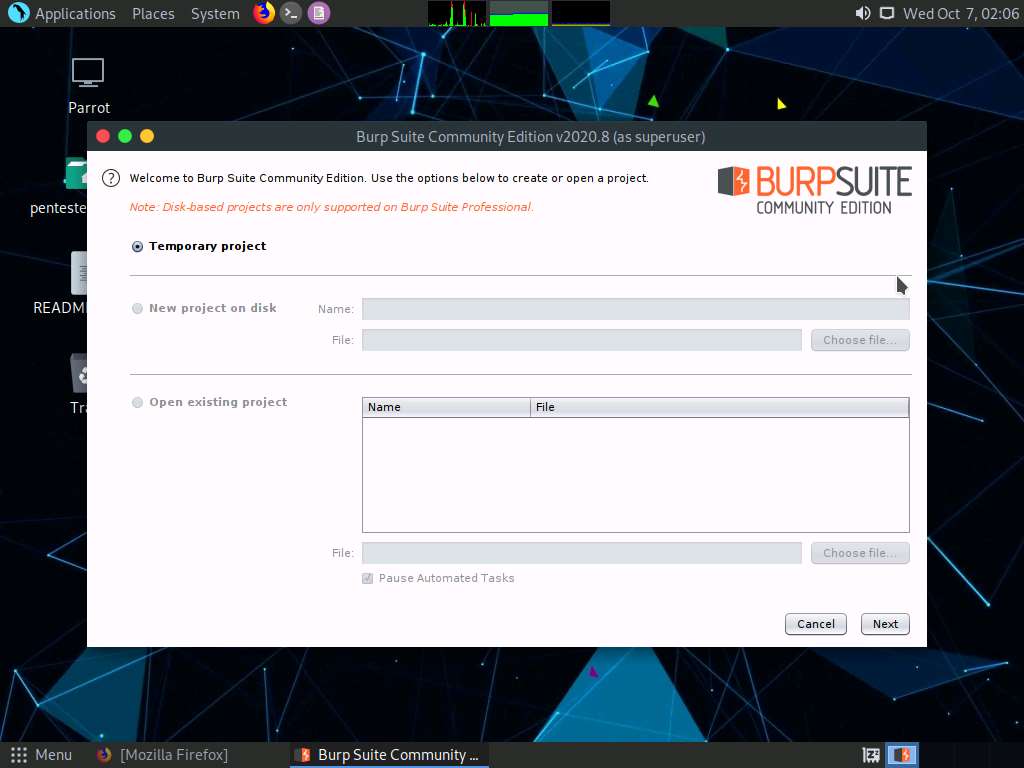
1. **BURPSUITE COMMUNITY EDITION** appears, it will take some time load. displaying the **License Agreement**. Click **I Accept** button to accept the license agreement.

Burp Suite Community Edition pop-up appears, click **OK**.

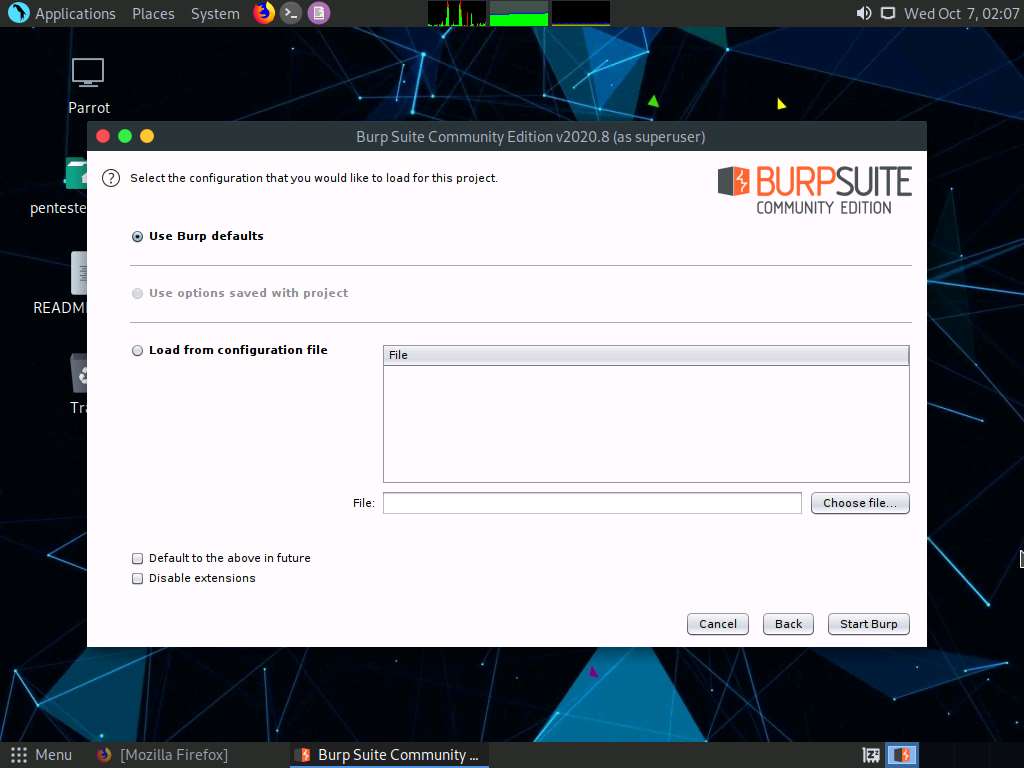


1. Burp Suite **projects** window appears with **Temporary project** radio button selected by default. Click **Next** to proceed with the **Temporary Project**.

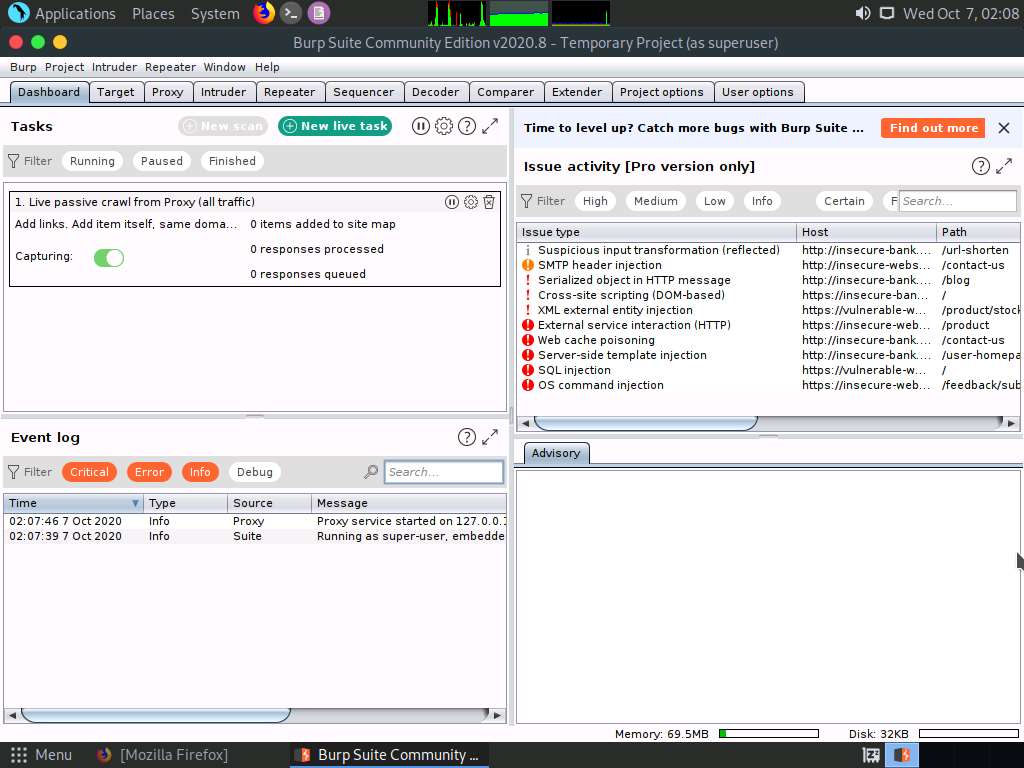
An update is available pop-up appears, click **Close**.



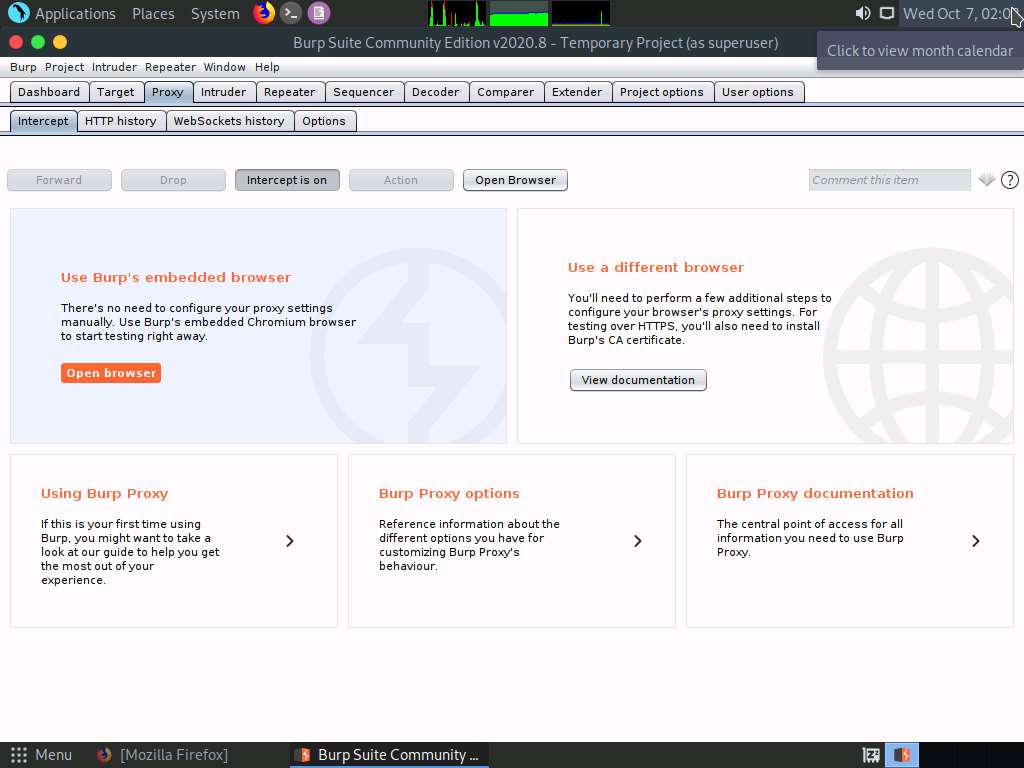
1. Burp Suite project configuration window appears, click **Use Burp defaults** radio button, since we will be using the default project configuration to run the application. Click **Start Burp** to start the application.



1. Burp Suite main window appears, click **Proxy** tab.

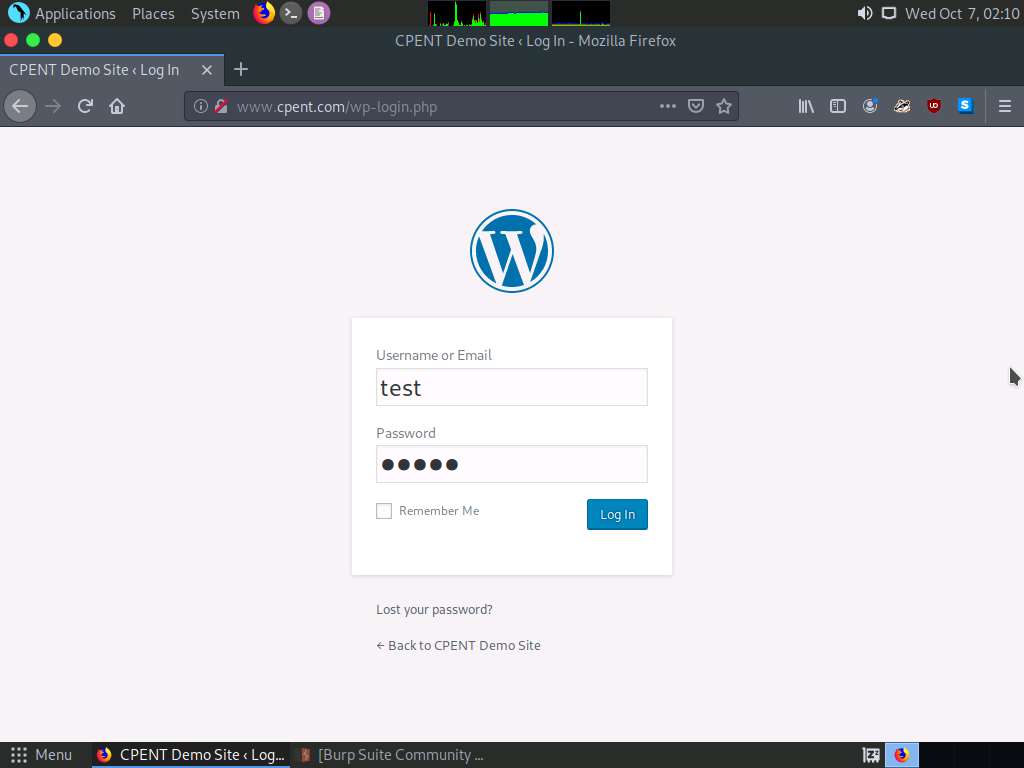


1. Burp Suite **Proxy** window appears displaying the Intercept section. Ensure that the **Intercept is on** button is activated.

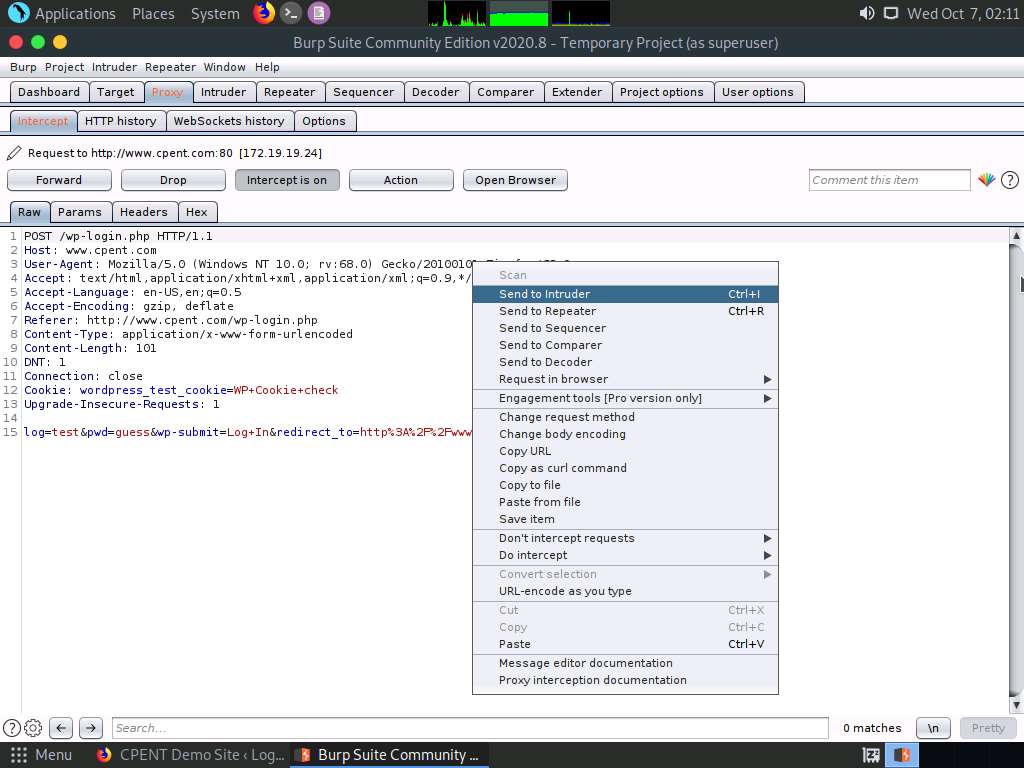


1. Now, maximize the web browser and switch to the **WordPress** login page. We do not know a password to log in. So, type random credentials and click **Log In**.

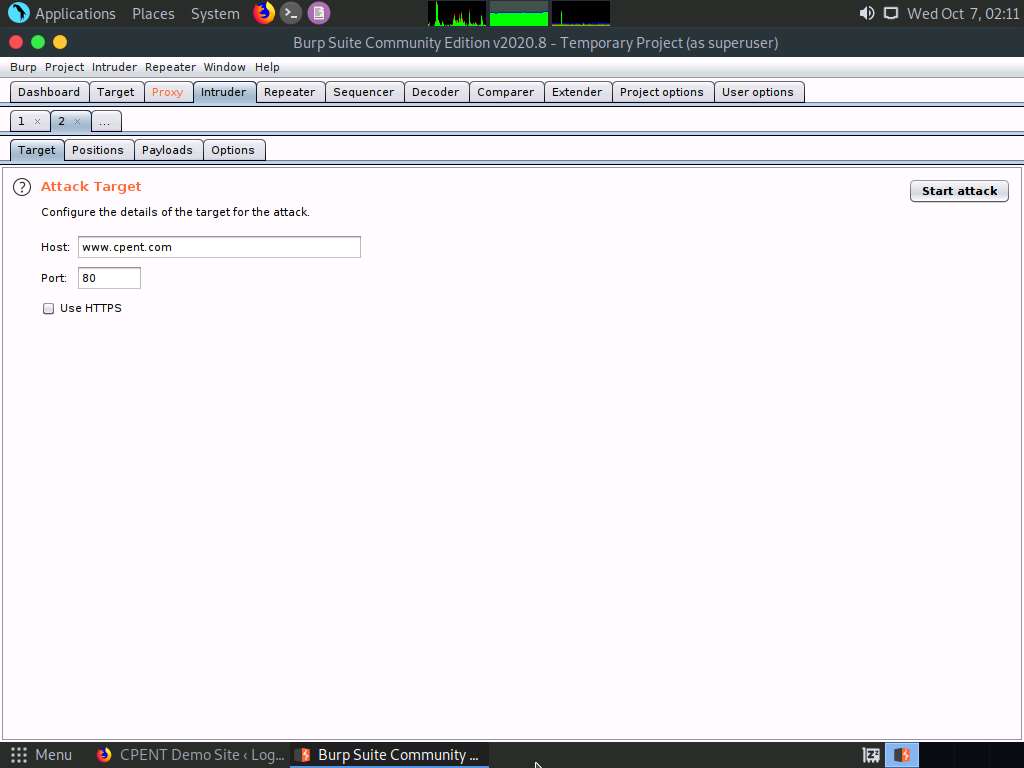
The username and password issued in this lab are **test** and **guess**.



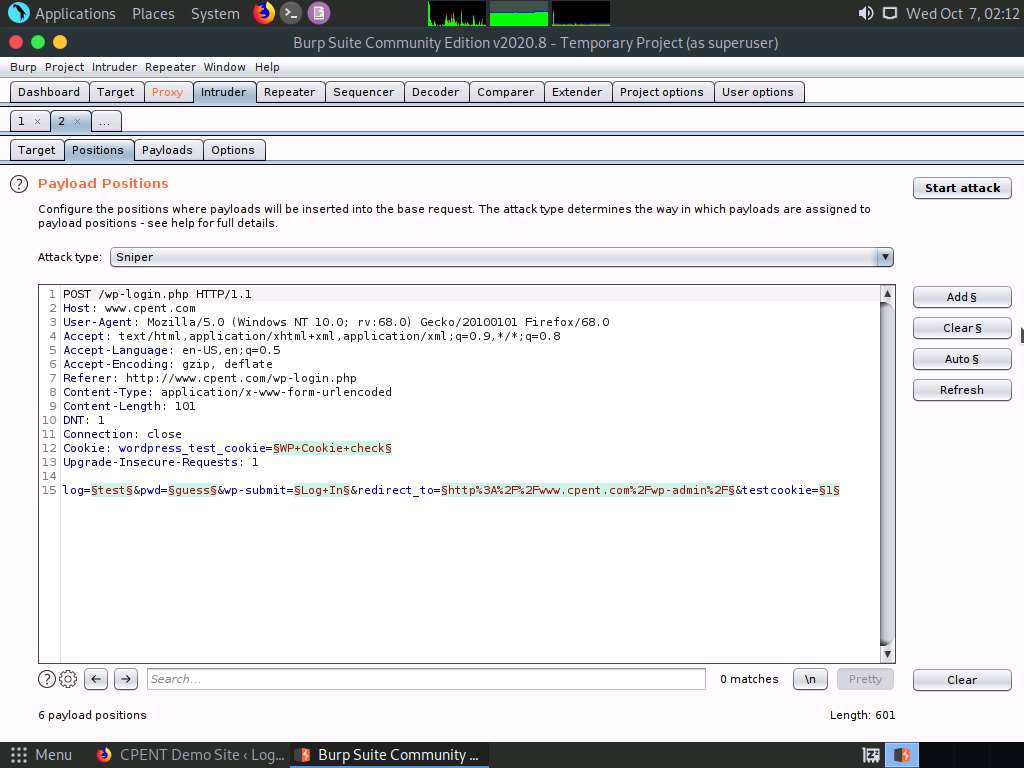
1. Switch to **Burp Suite**. You will observe that the application has intercepted the login request. We will try a set of usernames and passwords on the username and password fields of this request. To try, right-click on the request and click **Send to Intruder** option from the context menu.



1. Click **Intruder** tab. Burp Suite **Intruder** window appears, click **Positions** tab.

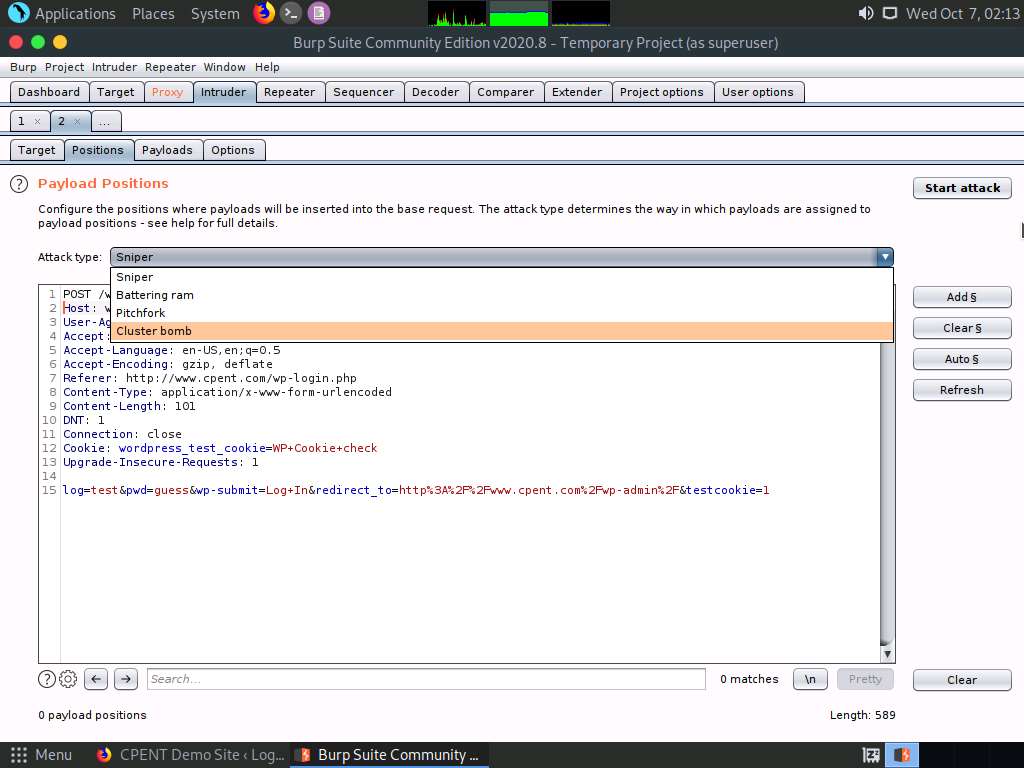


1. Burp Suite sets target positions by default. Click the **Clear §** button on the right side of the **Payload Positions** section to clear the payload positions.

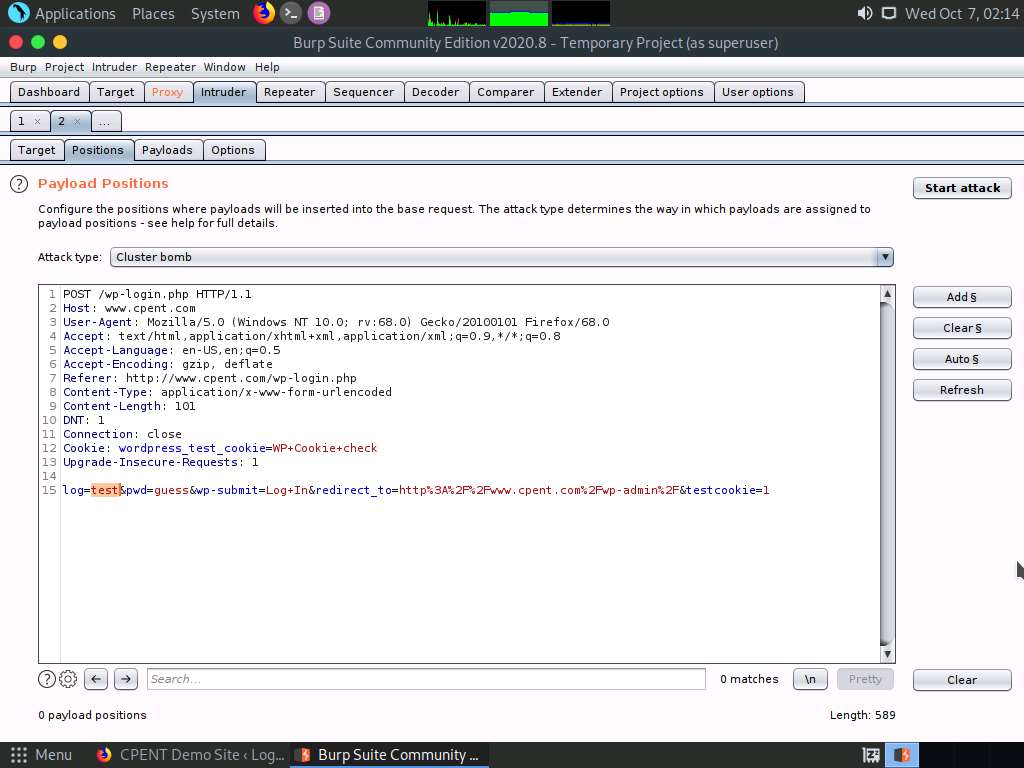


1. Once you clear the payload positions, select **Cluster bomb** from the **Attack type** drop-down list.

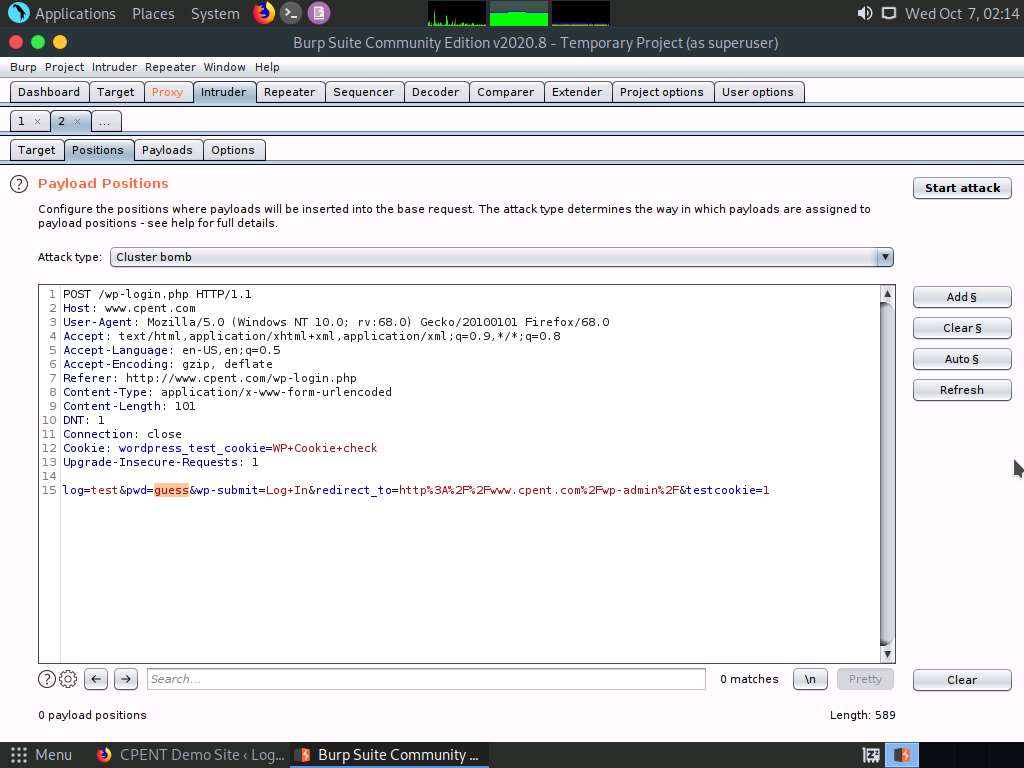
Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested. I.e., if there are two payload positions, the attack will place the first payload from payload set 2 into position 2, and iterate through all the 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. This attack type is useful where an attack requires different and unrelated or unknown input to be inserted in multiple places within the request (e.g. when guessing credentials, a username in one parameter, and a password in another parameter). The total number of requests generated in the attack is the product of the number of payloads in all defined payload sets - this may be extremely large.



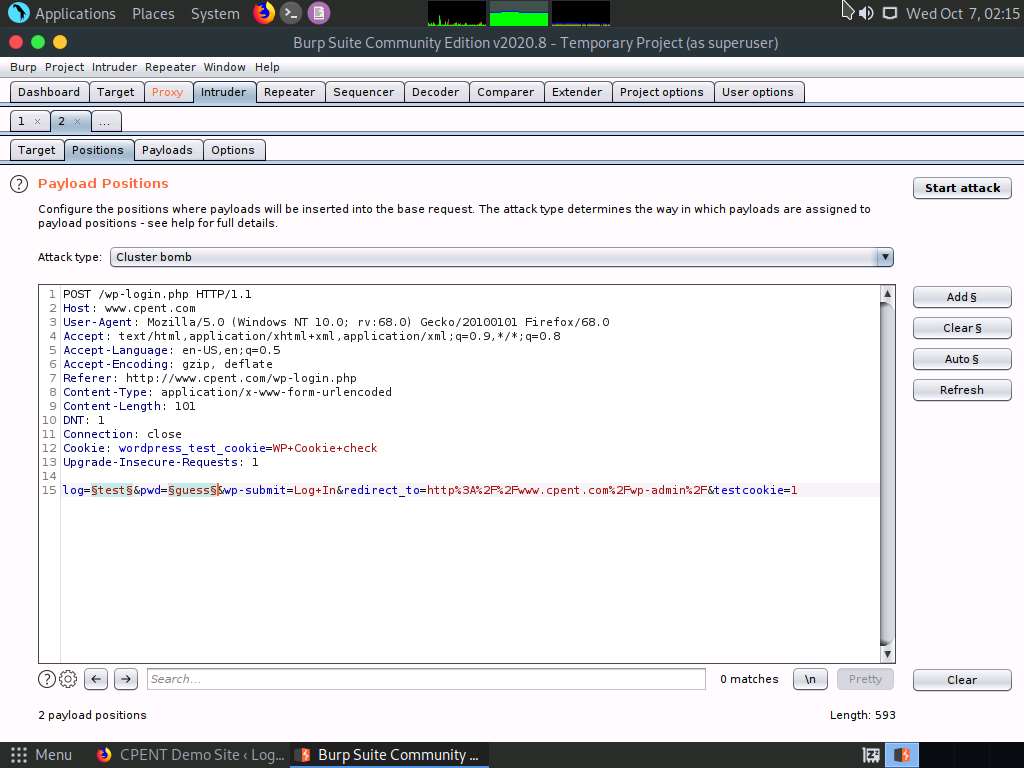
1. Now, we will be setting the username and password as the payload positions. To set the username you entered in the **Task no. 16**, highlight **test** and click **Add §**.



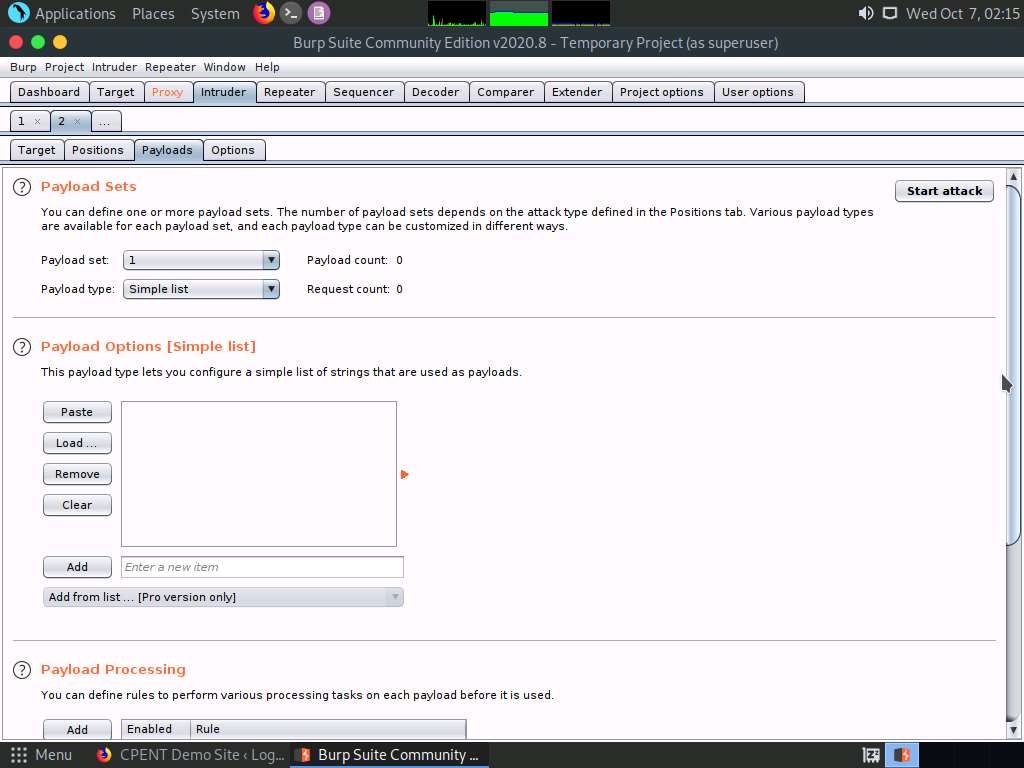
1. To set the password you entered in the **Task no. 16**, highlight **guess** and click **Add §**.



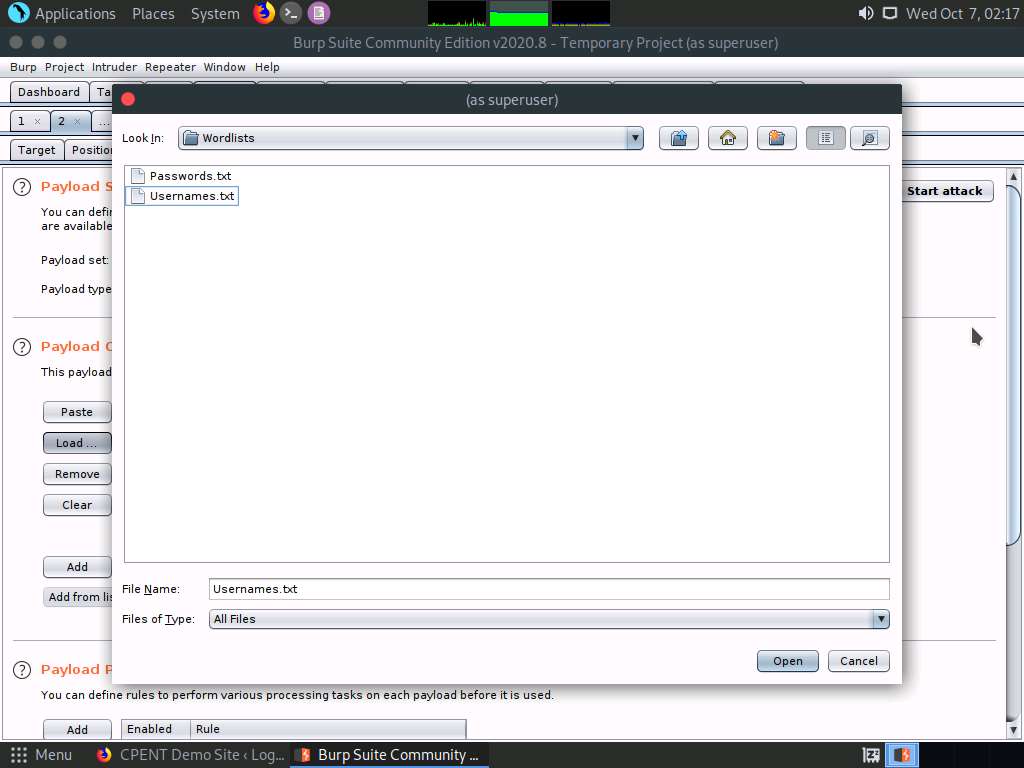
1. You will now observe that the username and password positions are set. To set the payloads, click the **Payloads** tab.



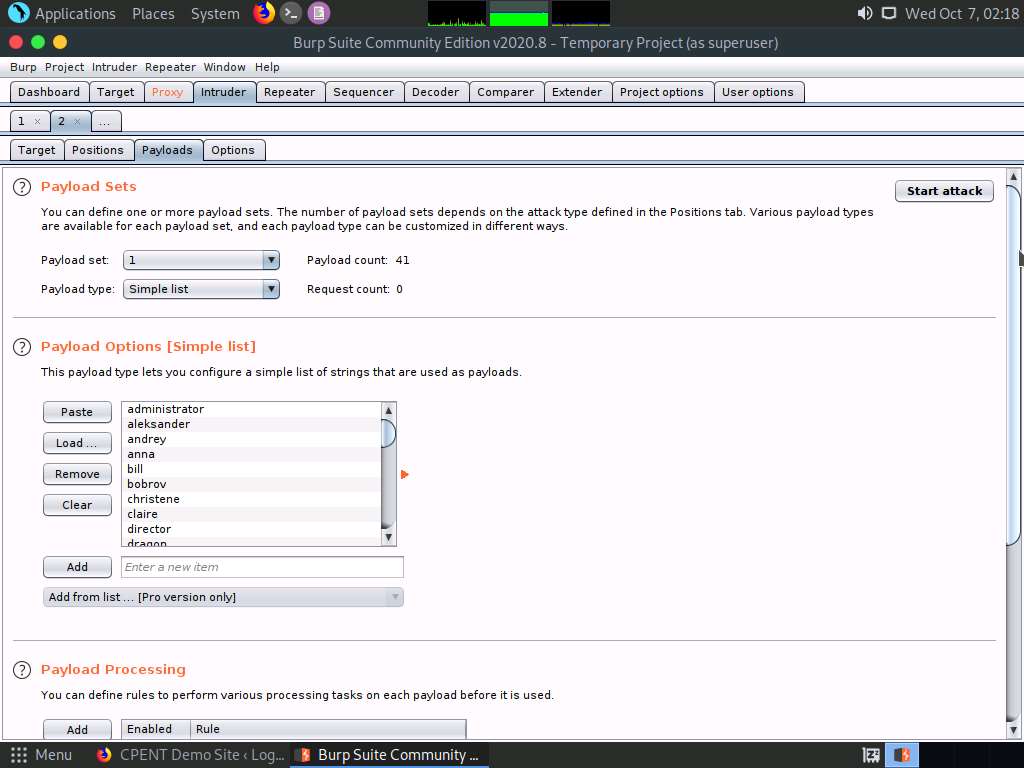
1. **Payloads** section appears with **Payload set 1** selected. Click **Load …** button in the **Payload Options [Simple list]** section.



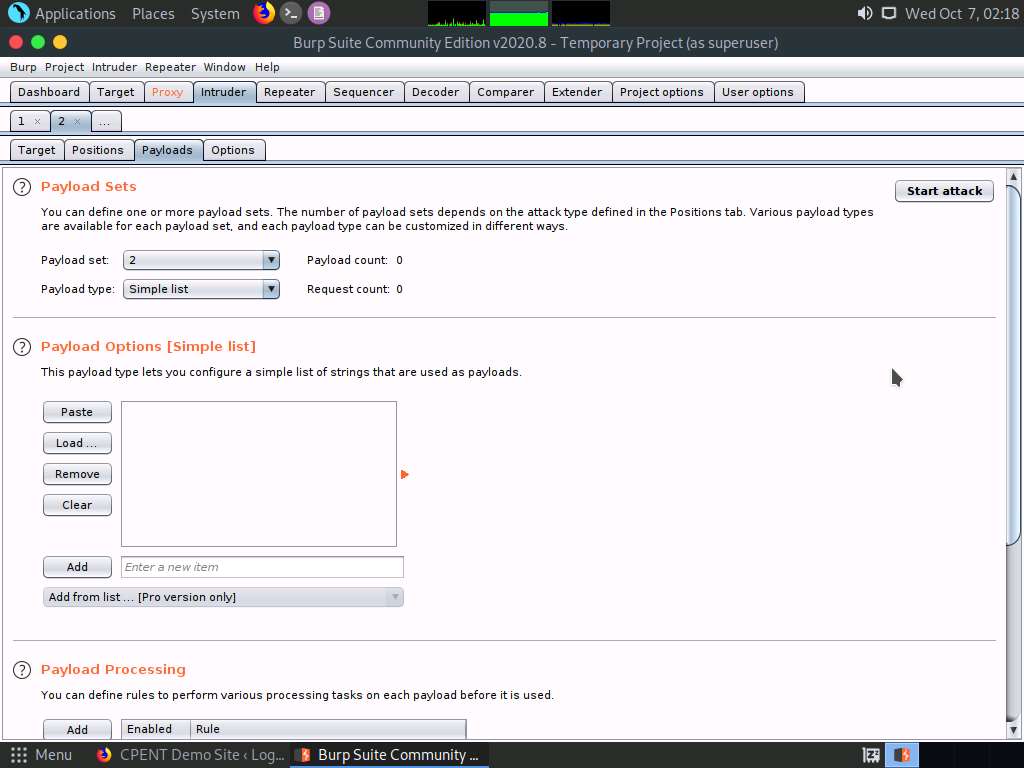
1. A pop-up appears displaying the file structure. Navigate to **/home/pentester/Wordlists** in the **Look In** field, select **Usernames.txt** and click **Open**.



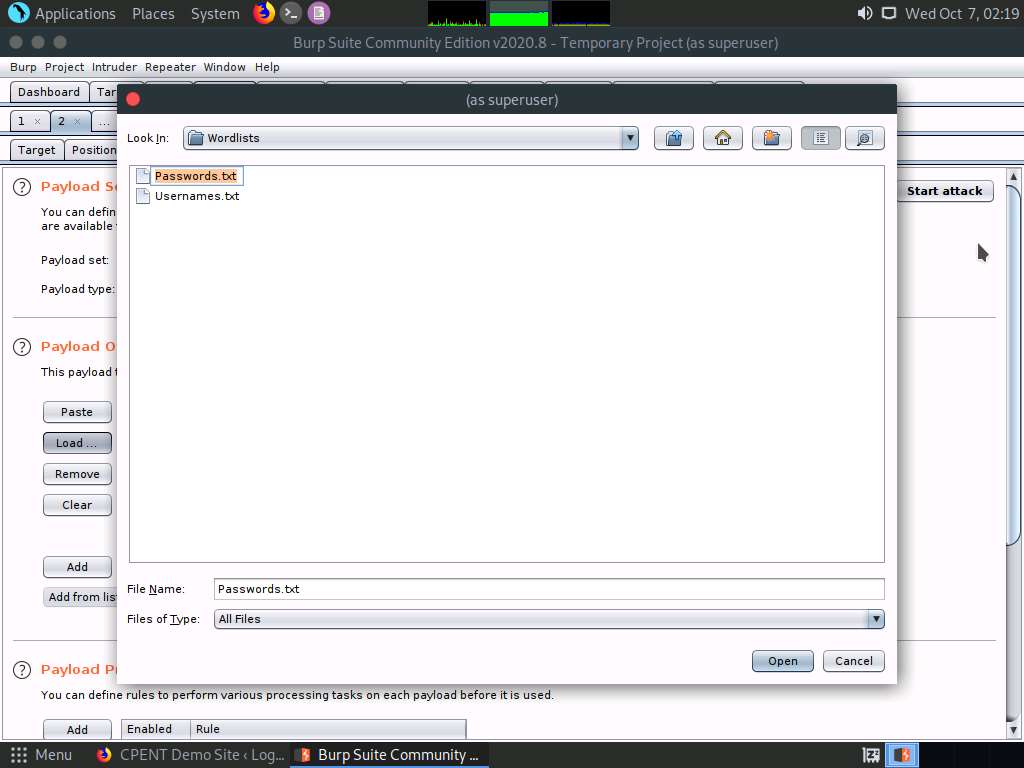
1. You will observe that the usernames inside the text file are loaded in the **Payload Options [Simple list]** section as shown in the screenshot:



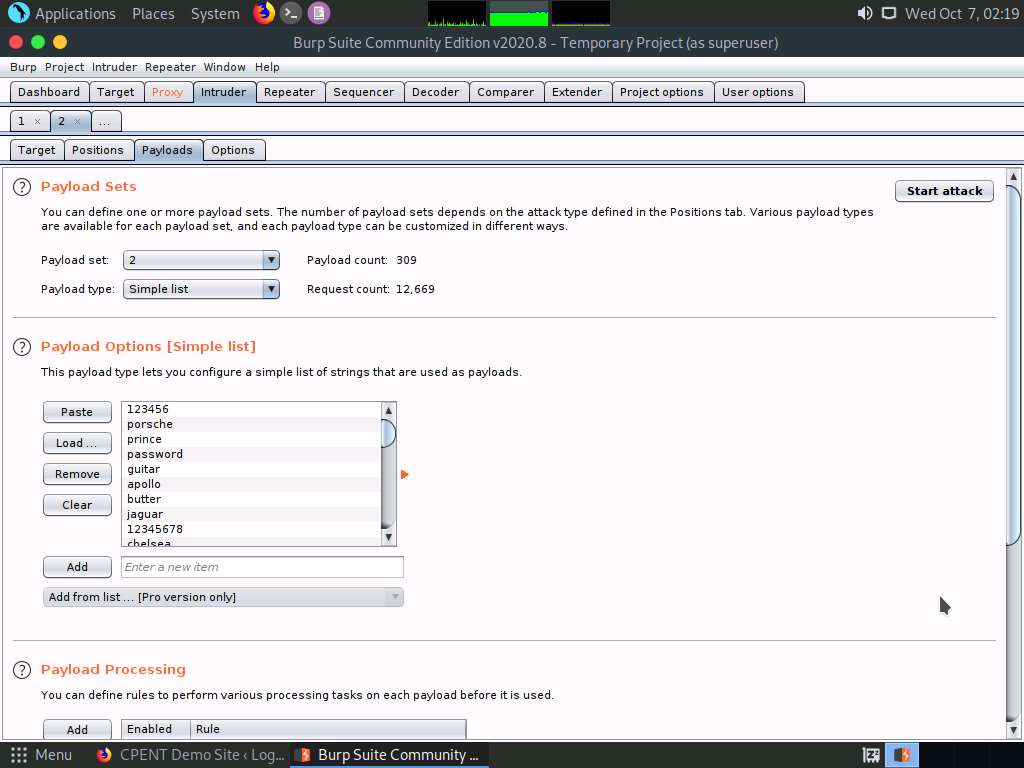
1. Now, under the **Payload Sets** section, select **2** from **Payload set** drop-down list. Click **Load …** button in the **Payload Options [Simple list]** section.



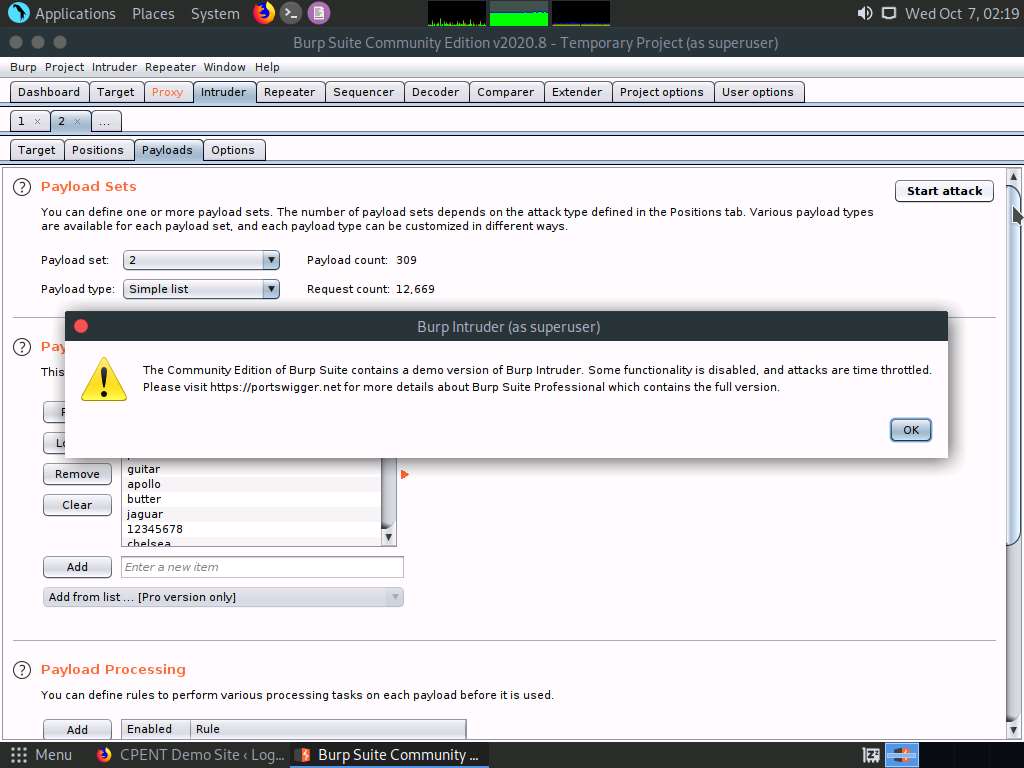
1. A pop-up appears displaying the file structure. Navigate to **/home/pentester/Wordlists** in the Look In field, select **Passwords.txt** and click **Open**.



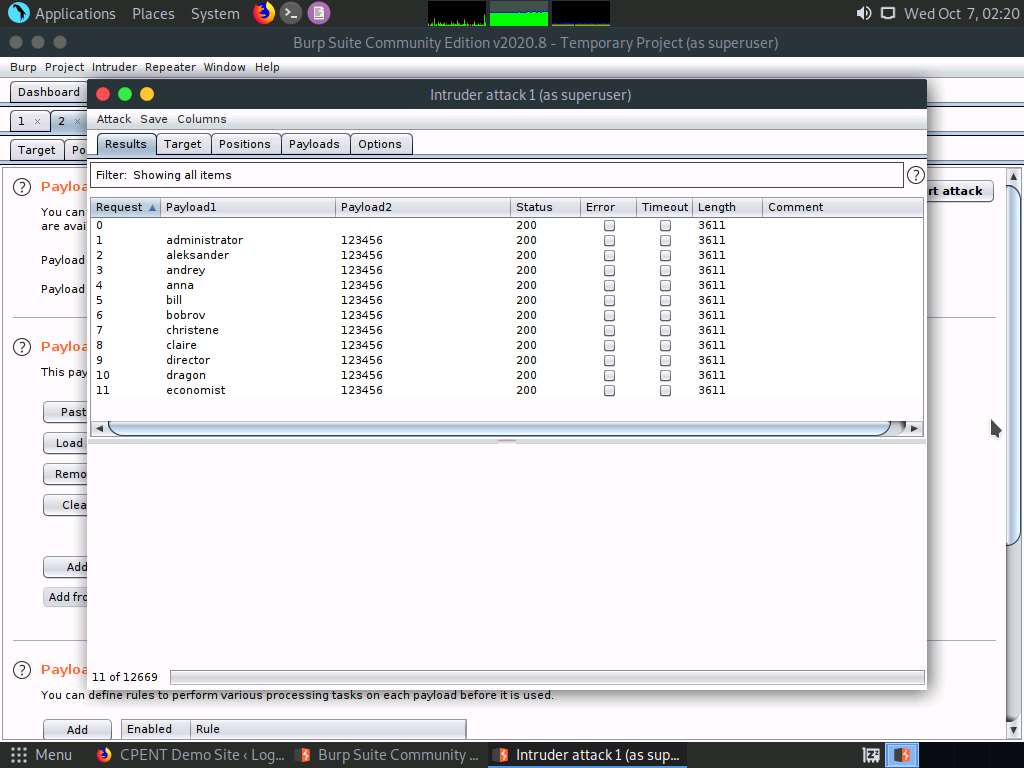
1. You will observe that the passwords inside the text file are loaded in the **Payload Options [Simple list]** section as shown in the screenshot. Now, click **Start attack** button.



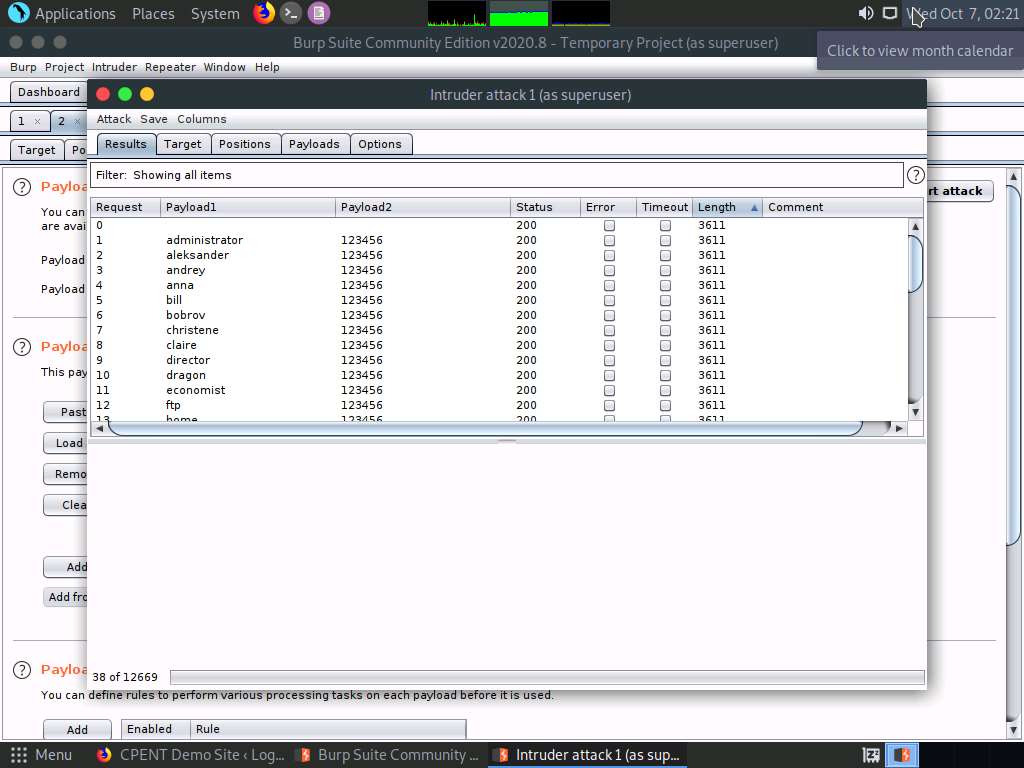
1. **Burp Intruder** pop-up appears, click **OK**.



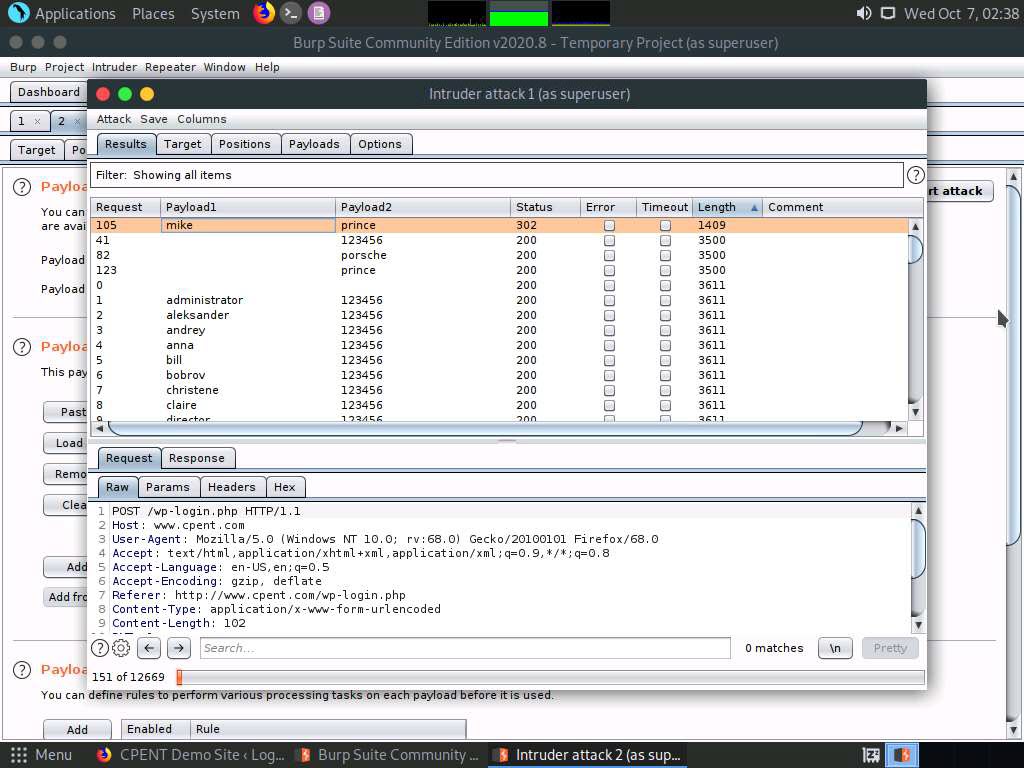
1. **Intruder attack 1** window appears, displaying the various username-password combinations along with the **Length** of the response and **Status**. Wait for **2-3** minutes for Burp Suite to try various username-password combinations.



1. Burp Suite tries all the username-password combinations and records the response for each request sent to the WordPress website. The length of the response remains almost the same for all the requests containing wrong username-password combination. When burp suite tries the correct username-password combination on the website, the length of the response differs a lot from the other responses and the status also varies accordingly. Click **Length** in the **Filter** section to sort the lengths of the responses in ascending order.

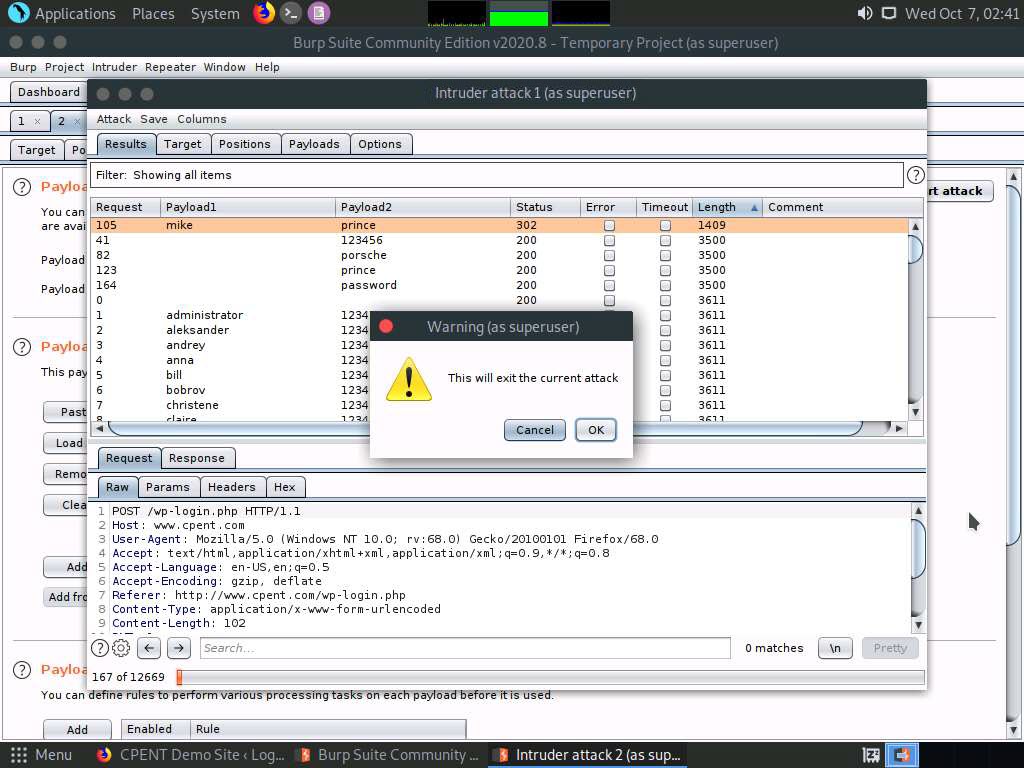


1. Upon clicking **Length** in the **Filter** section, Burp Suite arranges the lengths of the responses in ascending order. The length and status of the response for the username-password combination **mike** - **prince** is different compared to the other responses, which shows that it is a valid combination.



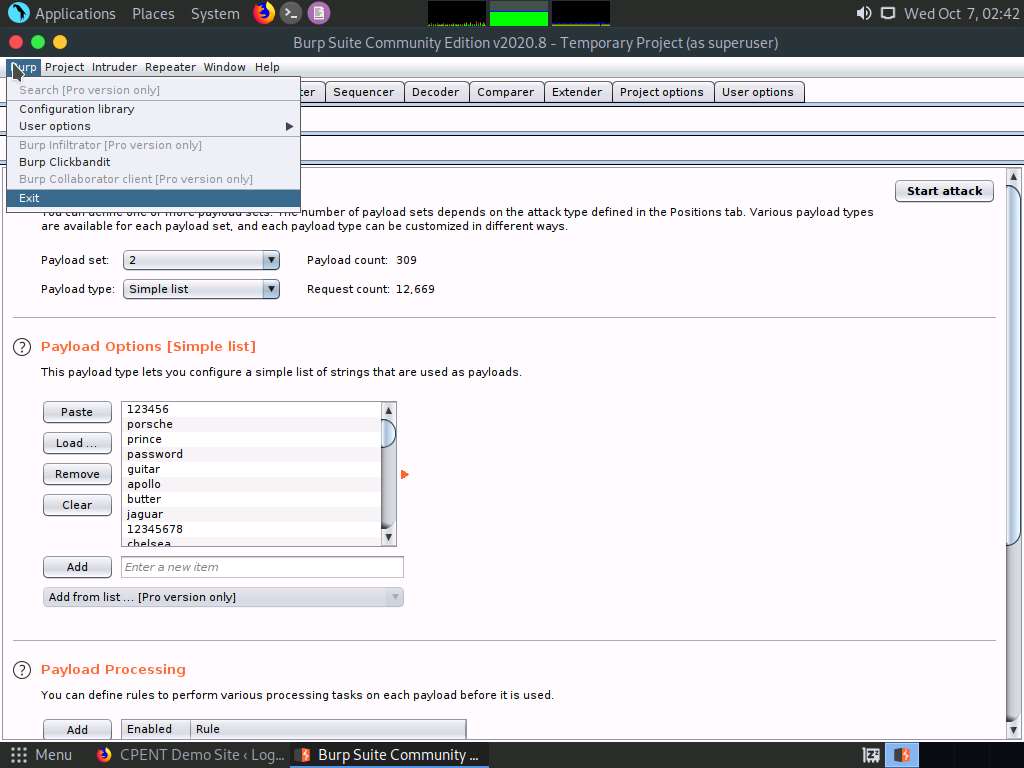
1. Close the **Intruder Attack** window.

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

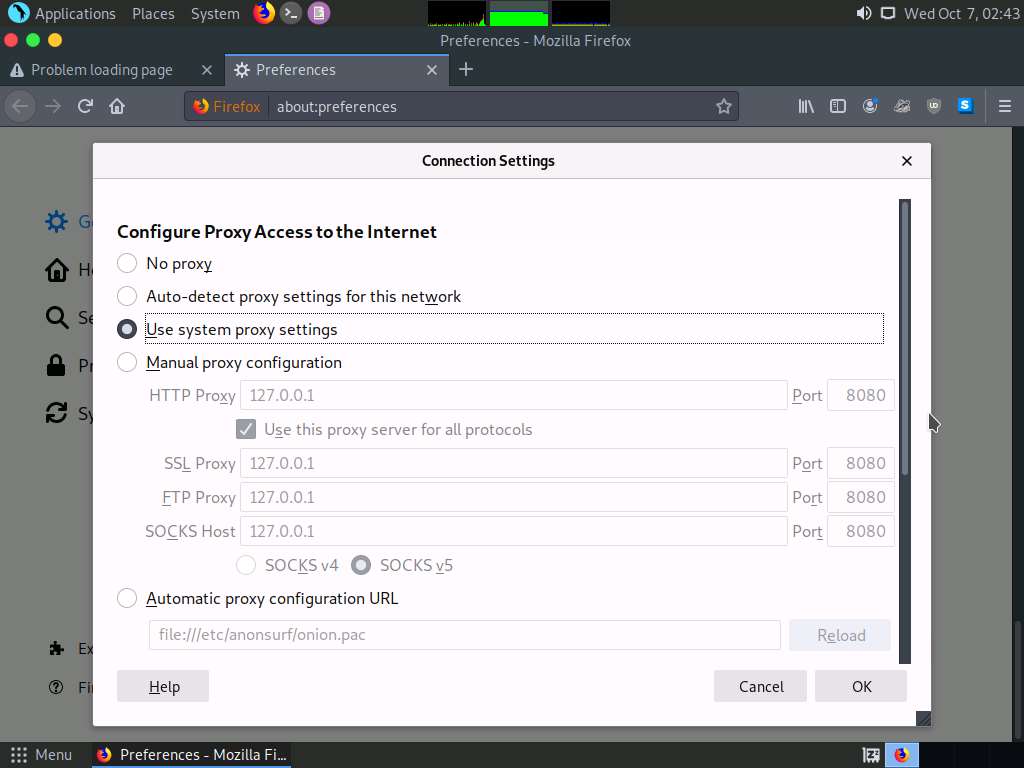


1. Go to **Burp** menu and click **Exit** to close the application.

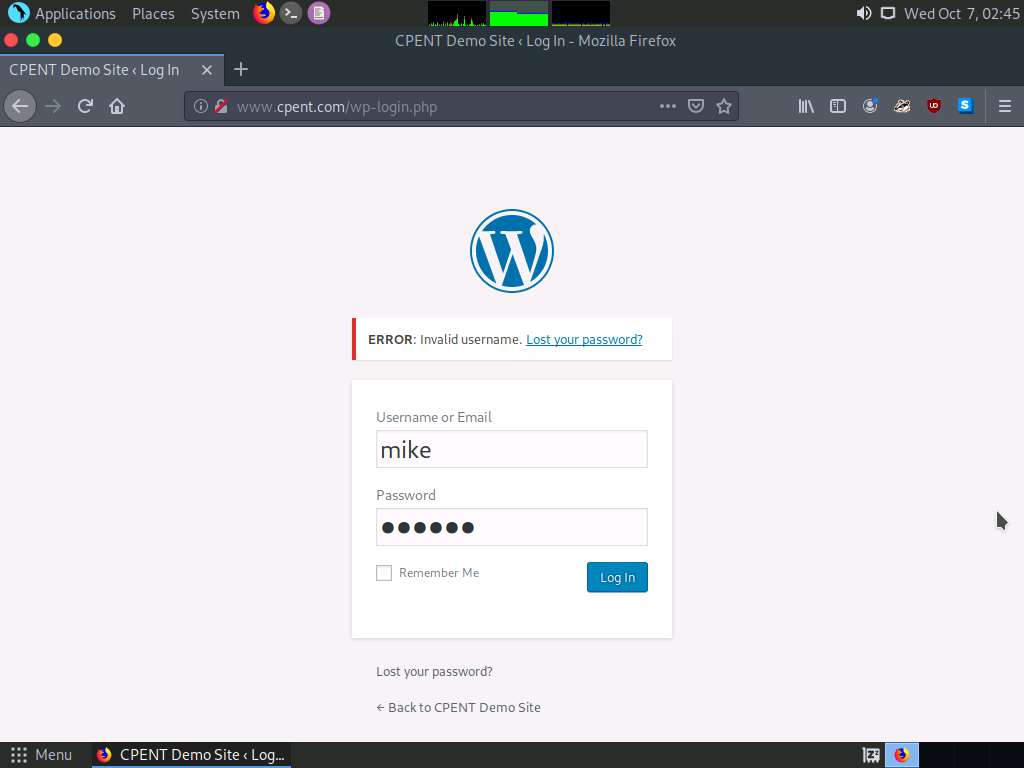
**Confirm** pop-up appears, click **Yes**.



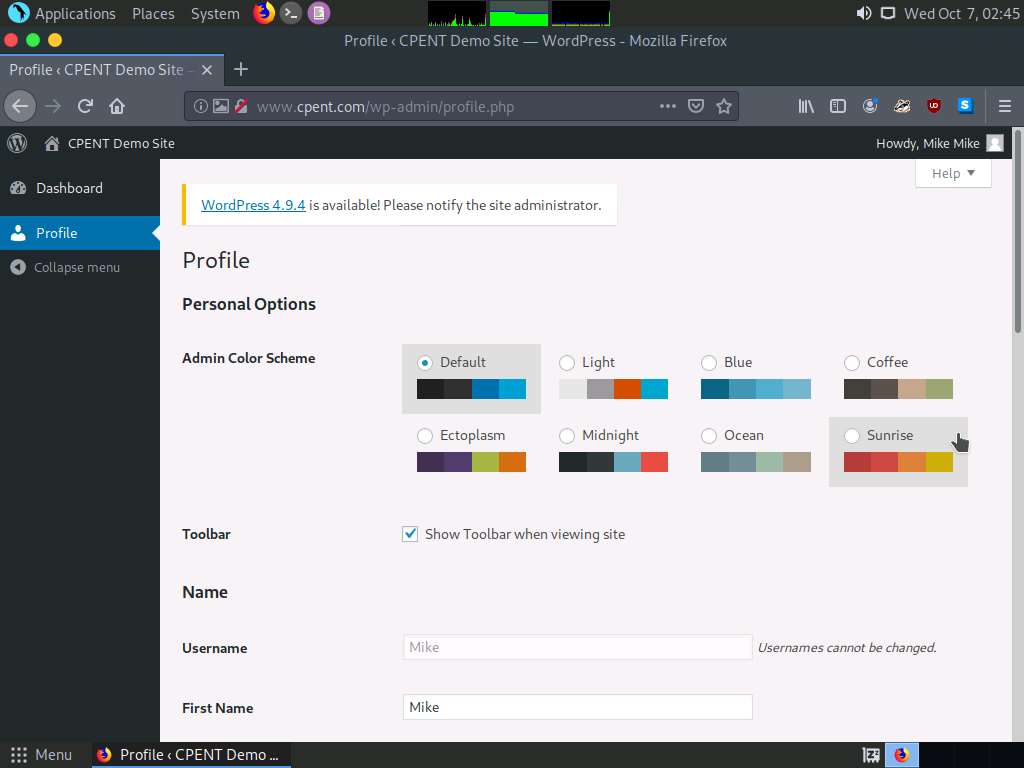
1. Now, open the **Firefox** web browser and switch to the **Preferences** window. Go to Proxy **Connection Settings**, select the **Use system proxy settings** radio button and click **OK**. Close the **Preferences** tab.



1. Switch to the CPENT Demo Site and refresh the page. Login page appears, type **mike**/**prince** in the username and password fields and click **Log In**.



1. You have successfully logged into the CPENT Demo Site, meaning that the dictionary attack using Burp Suite was successful.



1. Now, we shall upload a shell into the web application to gain unrestricted access to the machine hosting the website in the next lab exercise.

In this lab, you have learned how to perform a dictionary attack on WordPress web application using Burp Suite.