Web Application Penetration Testing Methodology

3 Hr 27 Min Remaining

Instructions Resources Help  100%

Exercise 8: Directory Browsing a WordPress Website using DirBuster and Accessing Shell

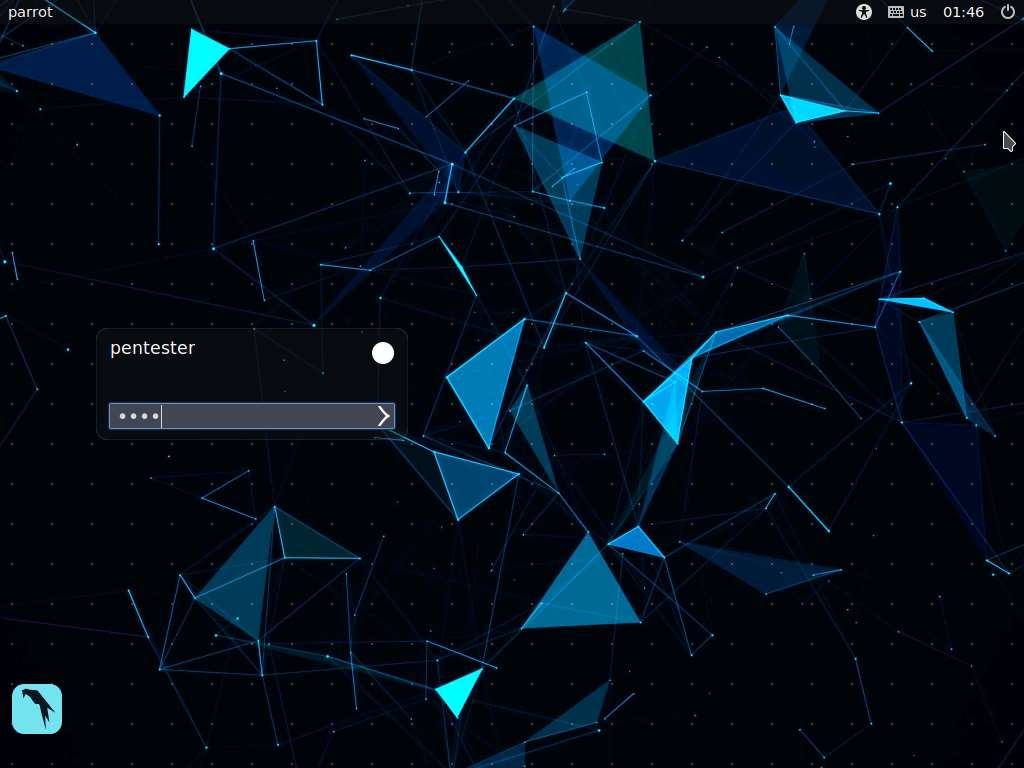
Scenario

This lab is a continuation of the previous lab exercise.  
In the previous lab exercise, you have learned how to create a shell and upload it. It is essential for a pentester to determine the directory structure of a web application in order to browse them and find out if there are any unnecessary/sensitive folders that are browsable.  
In this lab, you are going to learn how to browse directories using dirbuster, determine the location of the shell (uploaded in the previous lab exercise), browse it and gain access to the server.

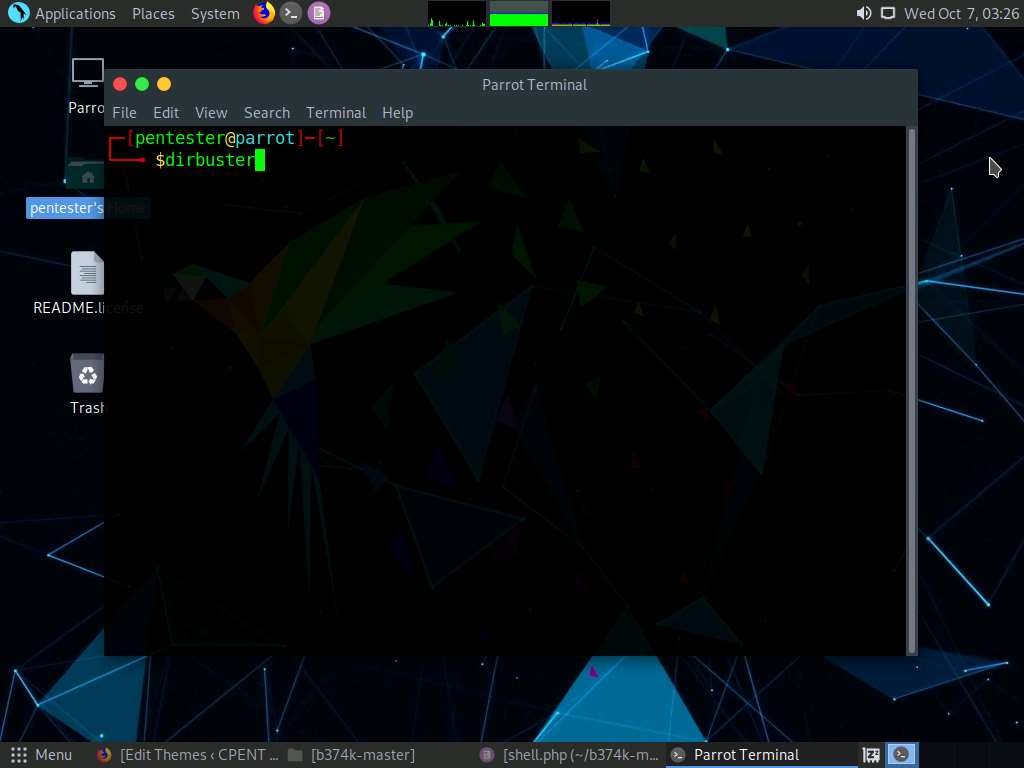
**Lab Duration**: **25** Minutes

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

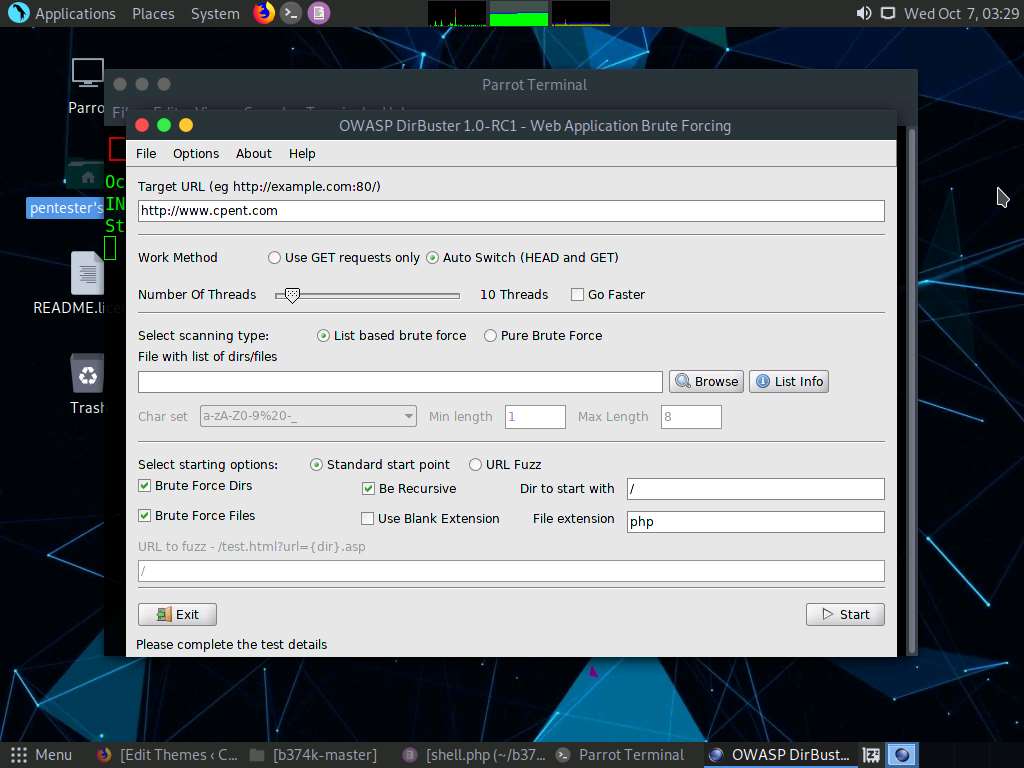
If you are already logged in skip to step **2**.



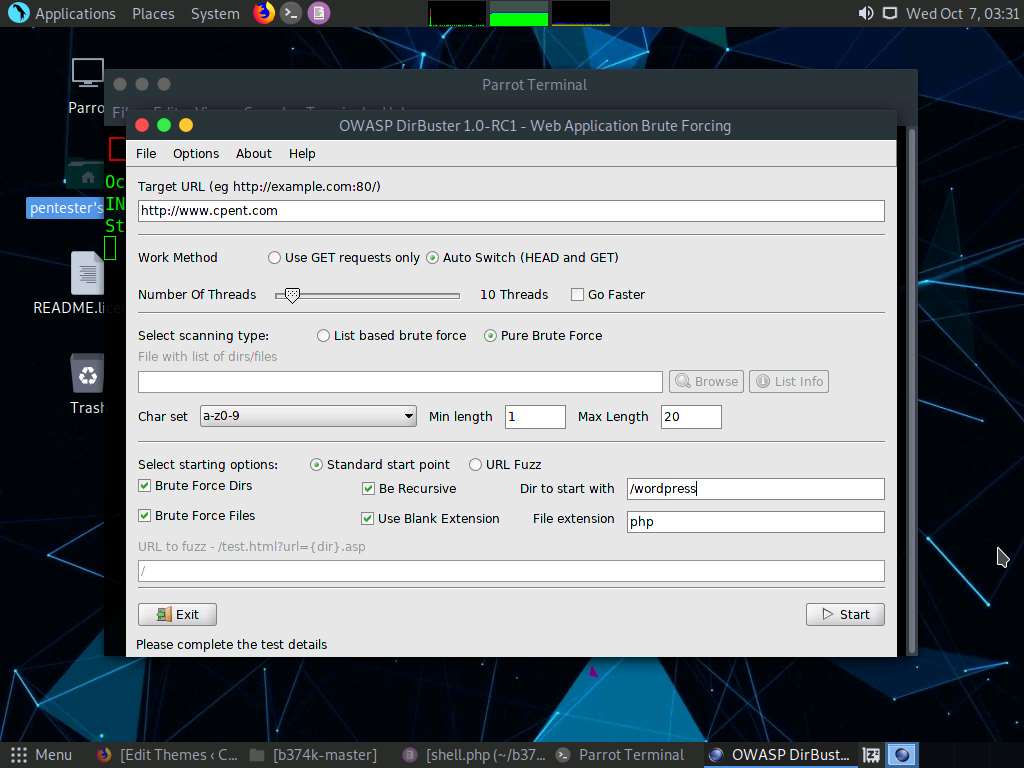
1. Once you log in to the machine, launch a command line terminal, type **dirbuster** and press **Enter**.



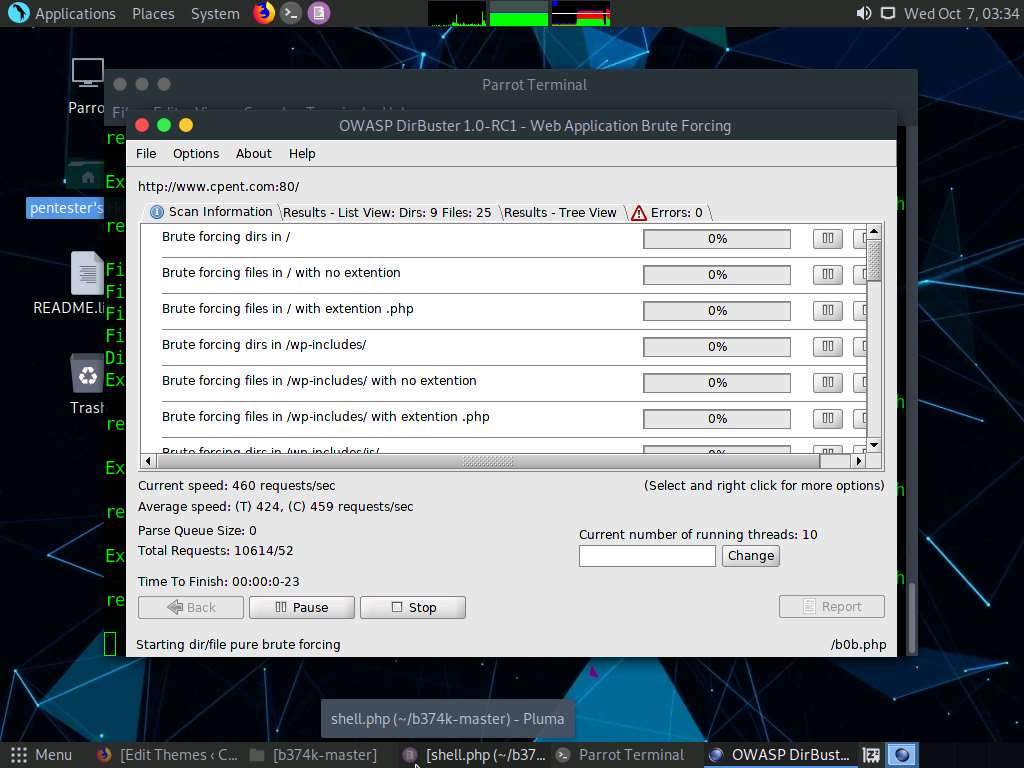
1. DirBuster main window appears. Type **http://www.cpent.com** in the **Target URL** field.



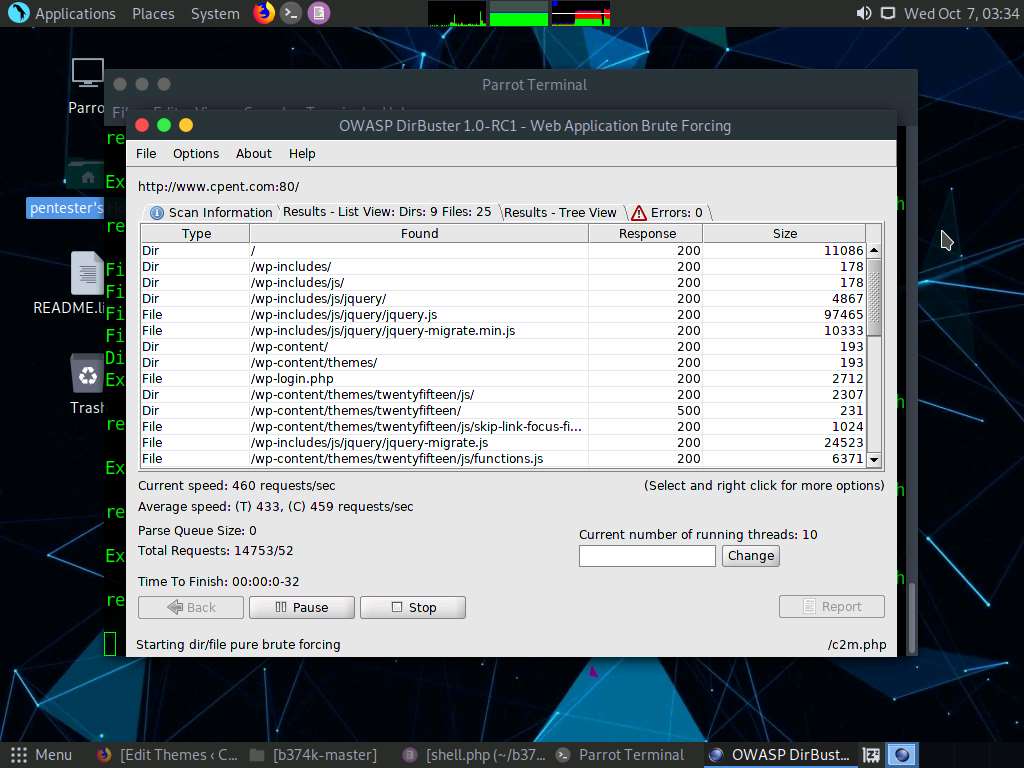
1. Select **Pure Brute Force** radio button in the **Select scanning type** section, select **a-z0-9** from the **Char set** drop-down list, set the **Min Length** to **1** and **Max Length** to **20** and check **Use Blank Extention** option and type **wordpress** in the **Dir to start with** field.
2. Click **Start** button to initiate the brute force attack.



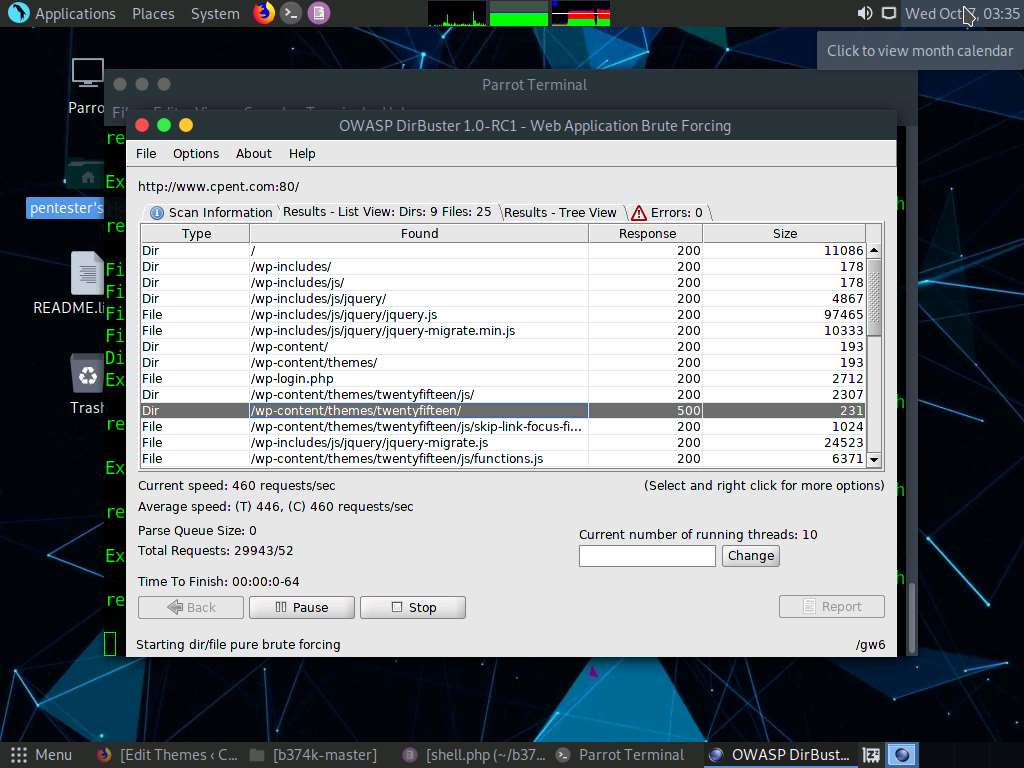
1. DirBuster begins to brute force the directories and files, and displays the scan status in the **Scan Information** tab as shown in the screenshot:



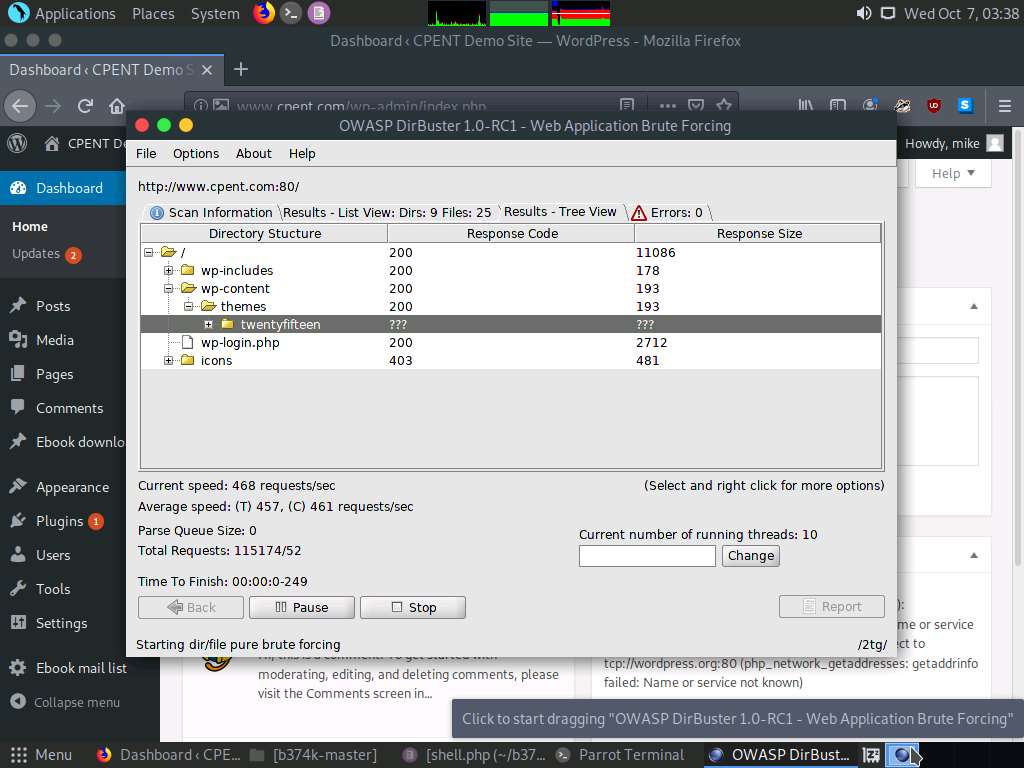
1. Click the **Results - List View** tab to view the brute forced files and directories.



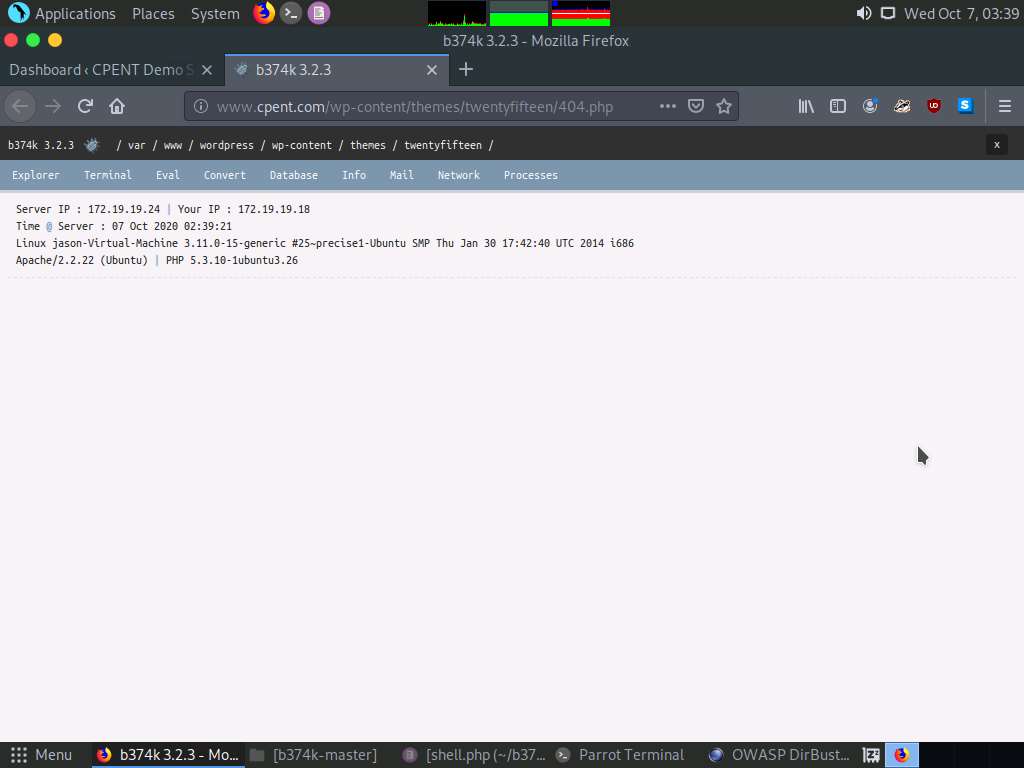
1. Scroll down the **Results - List View** tab. You will observe a directory named **twentyfifteen**, which is possibly the location where the **404.php** file is stored.



1. Click the **Results - Tree View** tab to view the directory structure in tree view. It is found that the location of twentyseventeen theme is **/wp-content/themes/twentyfifteen/**. Therefore, we will be entering the URL **http://www.cpent.com/wp-content/themes/twentyfifteen/404.php** in the web browser.



1. Launch a web browser, type the URL **http://www.cpent.com/wp-content/themes/twentyseventeen/404.php** in the address bar and press **Enter**.
2. **b374k shell** is successfully launched in the web browser as shown in the screenshot.



1. Thus, we have successfully launched a php shell by finding the directory structure using DirBuster. Close all the windows.

In this lab, you have learned how to browse directories using dirbuster, determine the location of the shell, browse it and gain access to the server.