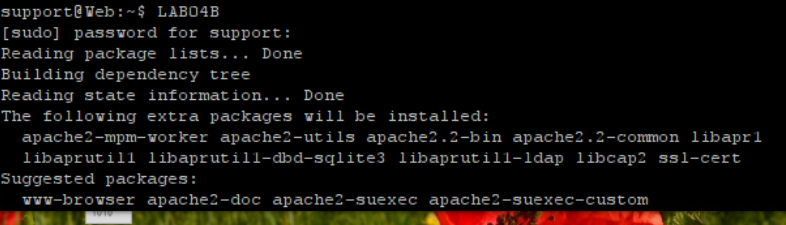
**CS547 – Secure Systems and Programs**

**Module 5 - Lab 4: HTMLi Vulnerability and Mitigation**

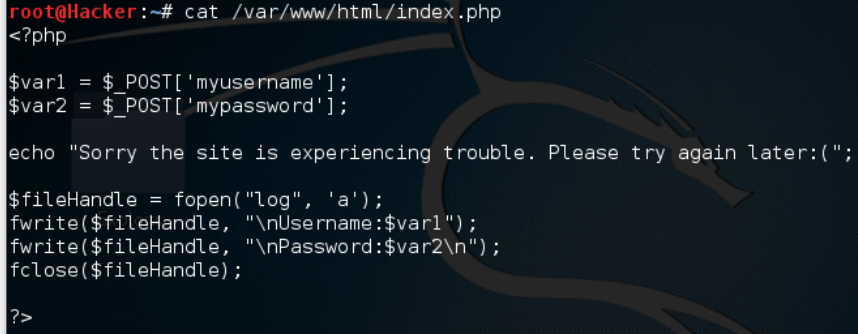
The requirements for this lab is to capture the screenshot of the below steps from given sections and submit in the word document.

**Part 1**

**SETTING UP THE VIRTUAL ENVIRONMENT**



**DESCRIBING THE ACTION SCRIPT (INDEX.PHP)**



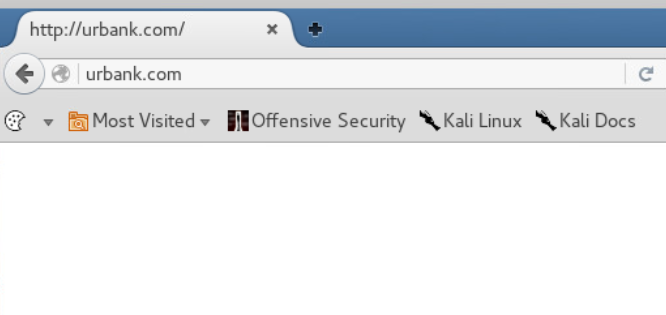
**ANALYSIS OF THE VULNERABILITY**



**IMPLEMENTING A SECURITY CONTROL**



**VERIFYING THE CONTROL WORKS**



**PENTESTING ASSIGNMENT**

* **Skip it**

**PART 2**

We first SSH into the server using putty and set up the server for the lab.

We then check the content of the ondex.php file. The php code takes the two variables submitted by the client’s post and assign them to php variables. Then prints an error message to the http response to the user, then logs the two variables to a file in server.

Now that we are in the kali linux machine, we can go ahead and SSH into a server without the need for putty. We edit the index.php to use get method instead of request method. We start capturing packets with wireshark. We first request the original website. We request the website with parameters in the url. We go and check the wireshark to see how the communication happened.

For some reason my kali’s internet connection went down. I cant reach any websites from it. So I couldn’t test the last version of the website.