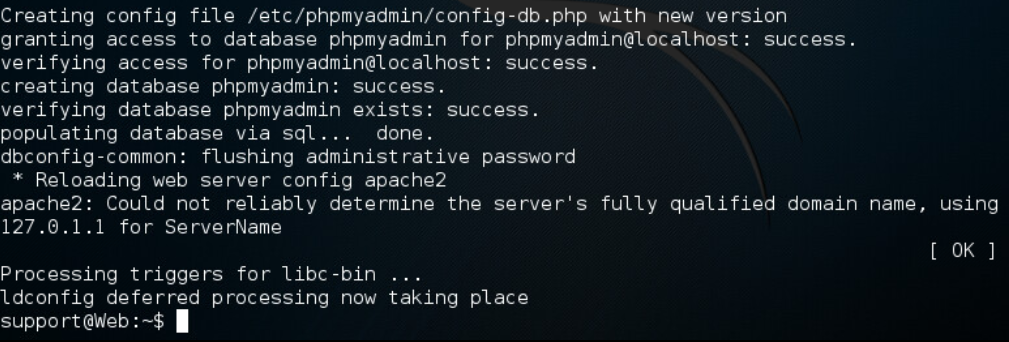
**CS547 – Secure Systems and Programs**

**Lab 2: Lab 2: SQLi Vulnerabilities and Pentesting Steps**

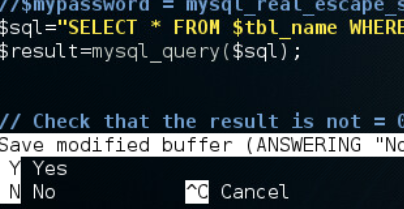
The requirements for this lab is to capture the screenshot of the below steps from given sections and submit in the word document.

**Part 1**

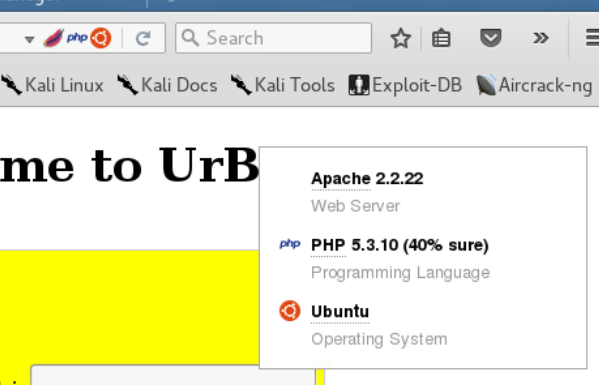
**PROVISIONING THE VIRTUAL ENVIRONMENT**



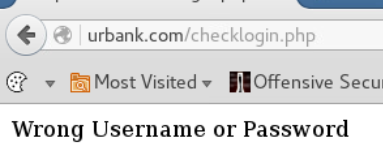
**ANALYSIS OF THE VULNERABILITY**



**WHERE TO PENTEST?**



**HOW TO PENTEST?**



## PENTESTING ASSIGNMENT

* **Skip it.**

**PART 2**

The client computer we use is a linux machine so we can ssh into the server directly without needing putty like a windows machine.

The way the virtual lab takes the time to go through the php code and explain what is going on what why there is a security vulnerability is very informative. It doesn’t skip over the subject. It actually teaches what causes the problem and how to fix it. In this case the problem is caused by not properly escaping certain characters in the input.

When we check the source code of the web page, we see that the form is being submitted(action) to a php file called checklogin.php. I have experience with the Servlet API of Java and Java can be used in the same manner where you pass an html form to a Servlet class and the Servlet class handles the http request and returns a http response.