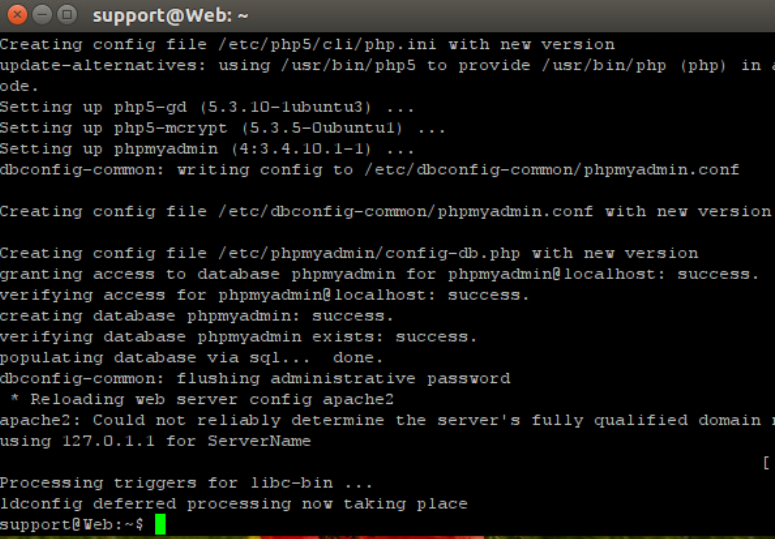
**CS547 – Secure Systems and Programs**

**SQL Injection (SQLi)**

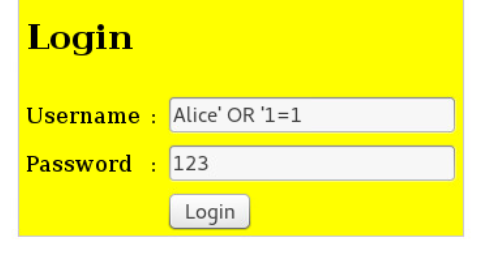
The requirements for this lab is to capture the screenshot of the below steps from given sections and submit in the word document.

**Part1**

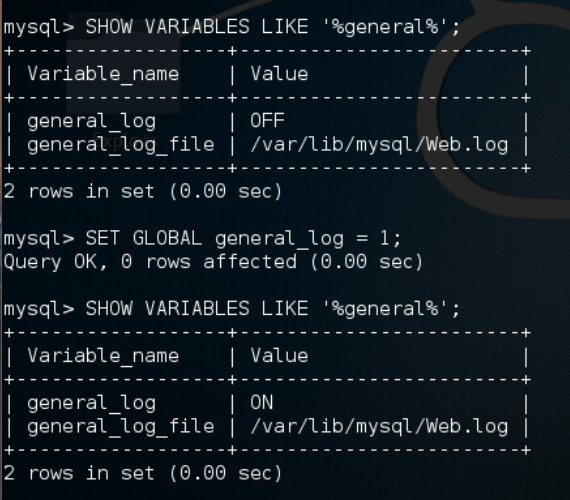
**SETTING UP THE VIRTUAL ENVIRONMENT**

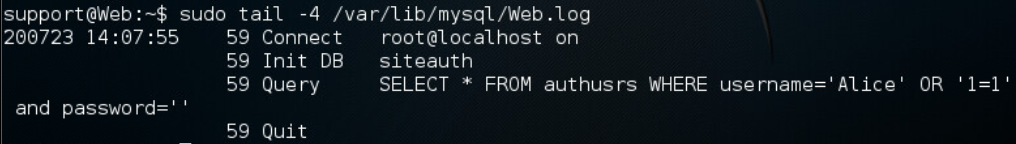


**SQLI PASSWORD BYPASS**

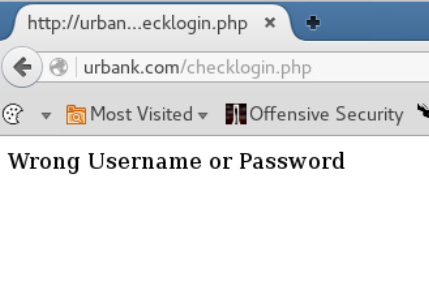


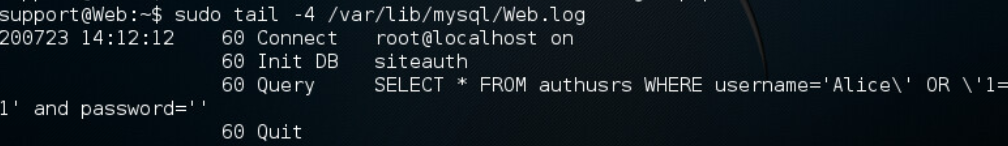
**ANALYSIS OF THE VULNERABILITY**





**ATTACK MITIGATION**

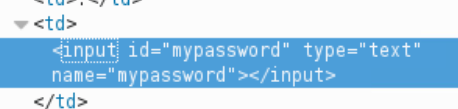




**PART 2**

Putty is a program that allows us to SSH into a windows server. We use that to SSH into the windows server as “login”. And we run the LAB03A script in the server remotely.

First of all, when I typed into the password field, I was able to read my characters. So I guessed that it wasn’t a password field, it was a text field. I checked the html code and I was right.



Pressing enter when we have the Username or Password textfields selected executes the “Login” button. Which means in the html code, the both text fields are in the same form.

After fixing the php code, we were not longer able to login without knowing the password.