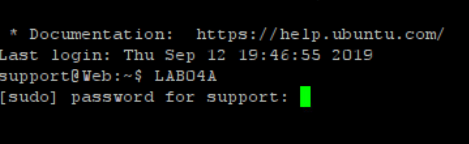
**CS547 – Secure Systems and Programs**

**Module 4 - Lab 3: HTML Injections (HTMLi)**

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

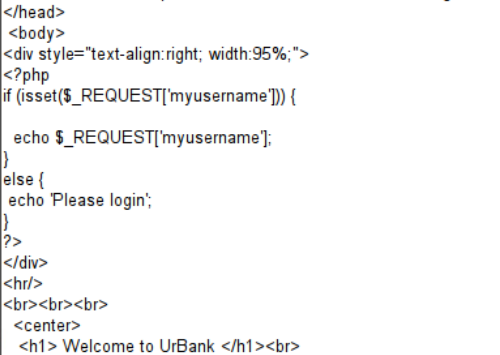
**Part 1**

**SETTING UP THE VIRTUAL ENVIRONMENT**



**ADDING VULNERABLE CODE**





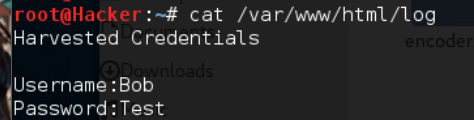
**EXPLOITING THE VULNERABLE CODE USING HTMLI**



**FORM STEALING**



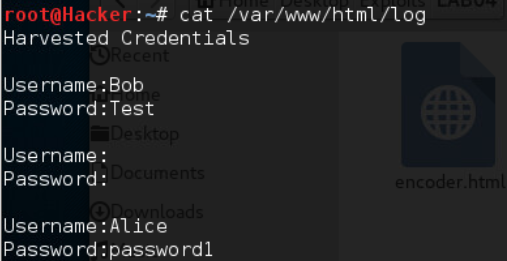
**SETTING UP A COLLECTION SERVER**



**SOCIAL ENGINEERING**



**FALLING VICTIM TO A SPEAR PHISHING ATTACK**



**PART 2**

Putty is a program that allows us to SSH into a server. We use it to SSH into urbank.com and we execute the required files to get the server ready for this lab.

We use the WinSCP program to upload files to the server using SCP instead of FTP. We copy display\_name.php to the server. And then we edit the index.php file to change which file is called by the html form. We do this by changing the value of the action attribute.

We have to point out that we are able to pull off this attack because we have full access to the server. Normally we would need to work to get access to the server first.

If we look at display\_name.php, we see that it takes the myusername parameter that was sent with the HTTP post request, and prints it as part of the HTTP response.

We also sent a get request using the url. We used the username “<input ‘radio’>”.

Then we sent the entire edited html page as the myusername value. Which caused the actualy page to get commented out and the server showed the user the edited html page that sends the form to our ip.

We then sent an email with an edited hyperlink to our victim. The edited hpyerlink pointed at our ip.