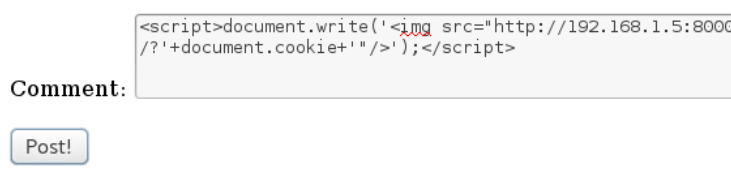
**CS547 – Secure Systems and Programs**

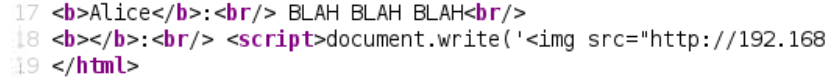
**Lab 7: Session Stealing (Stored XSS)**

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**

**REFLECTING SESSION IDS**

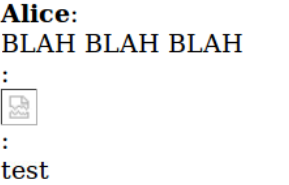




**SETTING UP A COLLECTION SERVER**

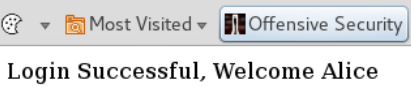


**ALICE LOGS IN**



**ALICE GETS OWNED**





**PART 2**

We first ssh into the server and set it up to get it ready for the lab.

We copy the malicious script and go to urbank.com. We type the malicious code into the comment section and click the post button. This script is supposed to take the cookies of the client and send it to our ip and the port we decided. The website takes all the comments and adds it as part of the website. So when someone else loads this website, they will also load the javascript we inserted and the javascript will run on their computer which will cause their cookies to be send to our ip and the port we determined.

We check our ip from console. Then we run a python code to start listening for traffic at the port 8000.

Now we log in to the alice’s computer to simulate her behaviour.

We go back to the kali machine to check the results. We can see the ip, date and time, sessionid for each request.

We go back to urbank.com from the kali machine. We open a cookie manager. We change our sessionid with alice’s session id. When we refresh the page, we send a request to the server with the new session id and the server responds with the appropriate content for the sessionID it got which is the sessionID of alice. We successfully logged into alice’s account.