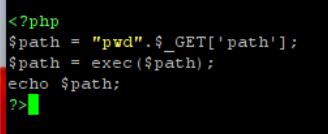
**CS547 – Secure Systems and Programs**

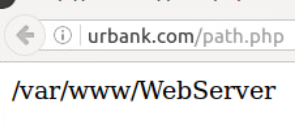
**Lab 8: Command Injection**

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

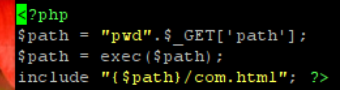
**Part 1**

**RUNNING THE PHP CODE**



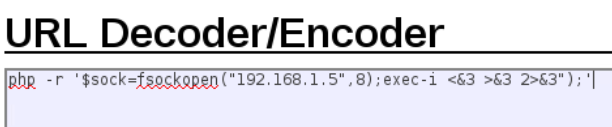


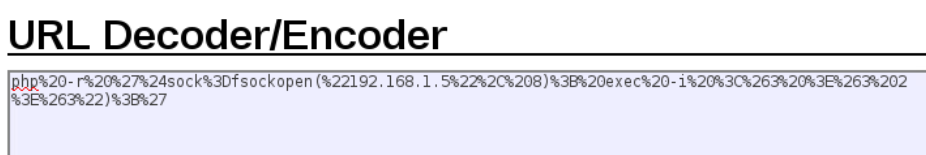
**ADDING THE CODE**





**REMOTE SHELL**





**PENTESTING ASSIGNMENT**

* **skip it**

**PART 2**

We first ssh into the server using putty in order to set it up for the lab.

We create a php file called path.php in the path “var/www/WebServer/” in the server that echoes the path of the file to the user and we test it with a browser.

We ssh into the server and add this php code to the php file on the server instead of just testing it on our local machine.

Now we log in to the kali machine. We set up the mahine to listen to traffic on port 8. Then we write a malicious code and url encode it and then use it as a parameter to the legitimate website. Using the link to the legitimate website with this malicious parameter will cause a socket to be opened between our kali machine and the machine of our victim.