PSP0201
Week 3
Writeup

Group Name: Hacktocrats

Members

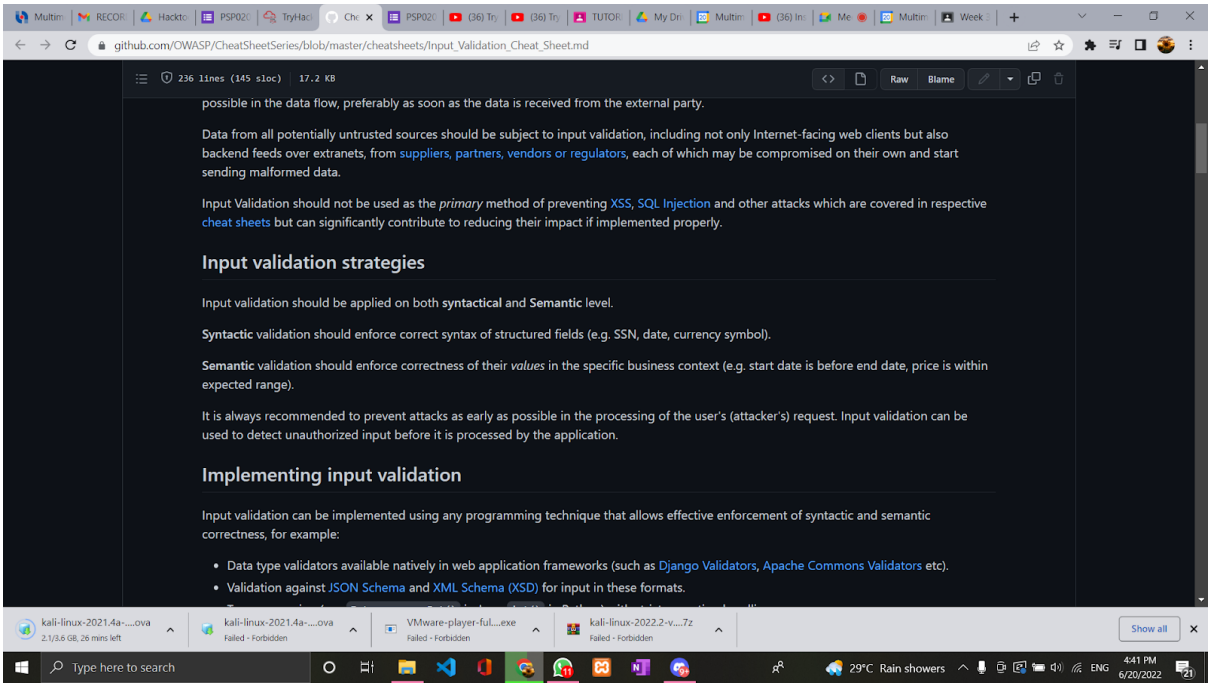
ID	Name	Role
1211103194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
1211103602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member
1211103430	AINA SOFEA BINTI AMIER HAMZAH	Member
1211103237	NURUL AIN BINTI KAMARUDIN	Member

DAY 6 : Web Exploitation - Be Careful With What You Wish On A Christmas Night

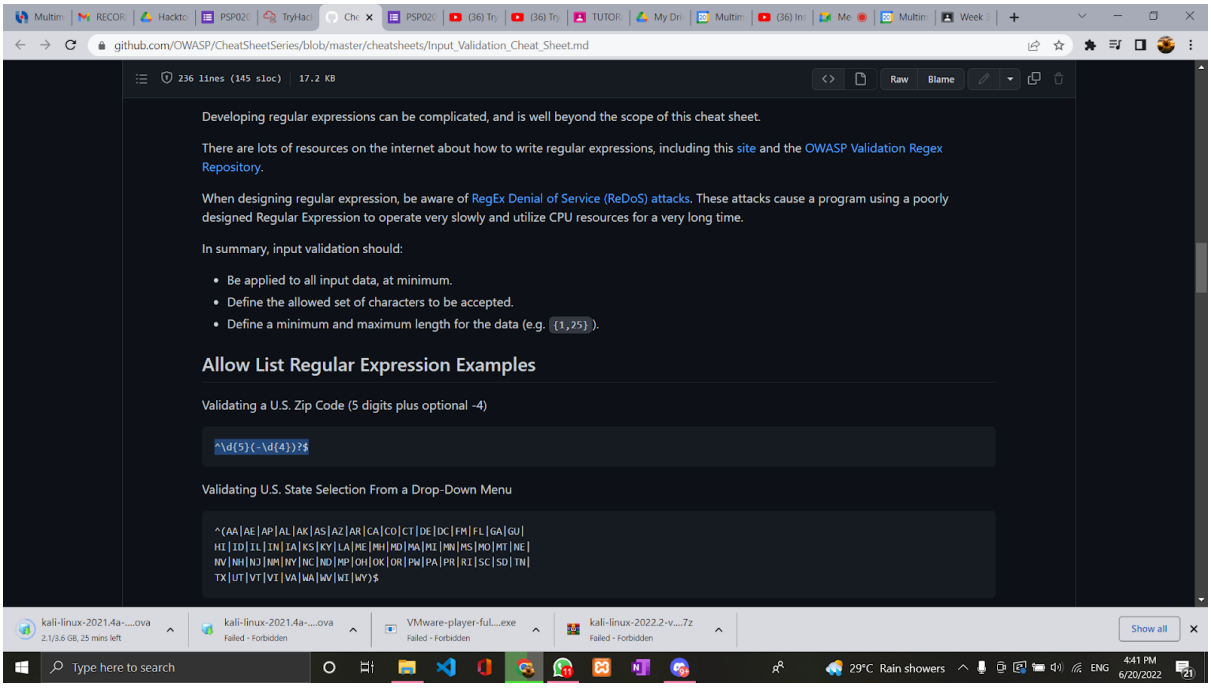
Tools used: Kali Linux, Firefox, Google Chrome

Solution/Walkthrough:

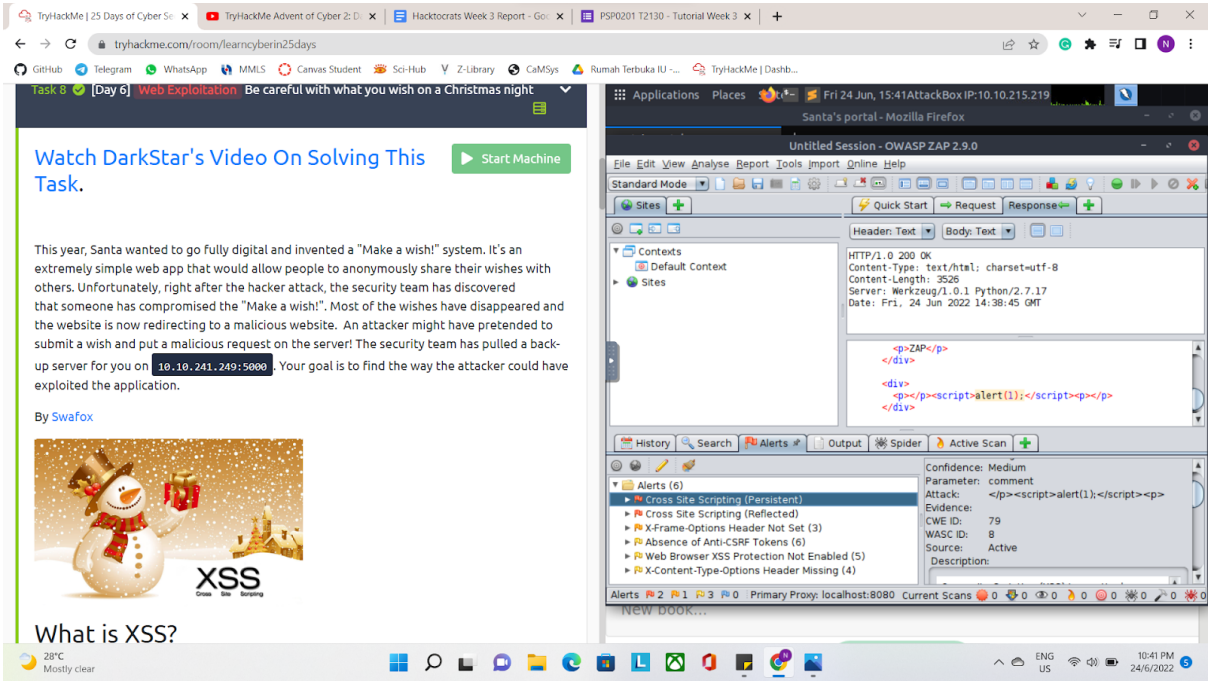
Question 1: Open OWASP Cheat Sheet on google chrome to read and match the correct description with its input validation level



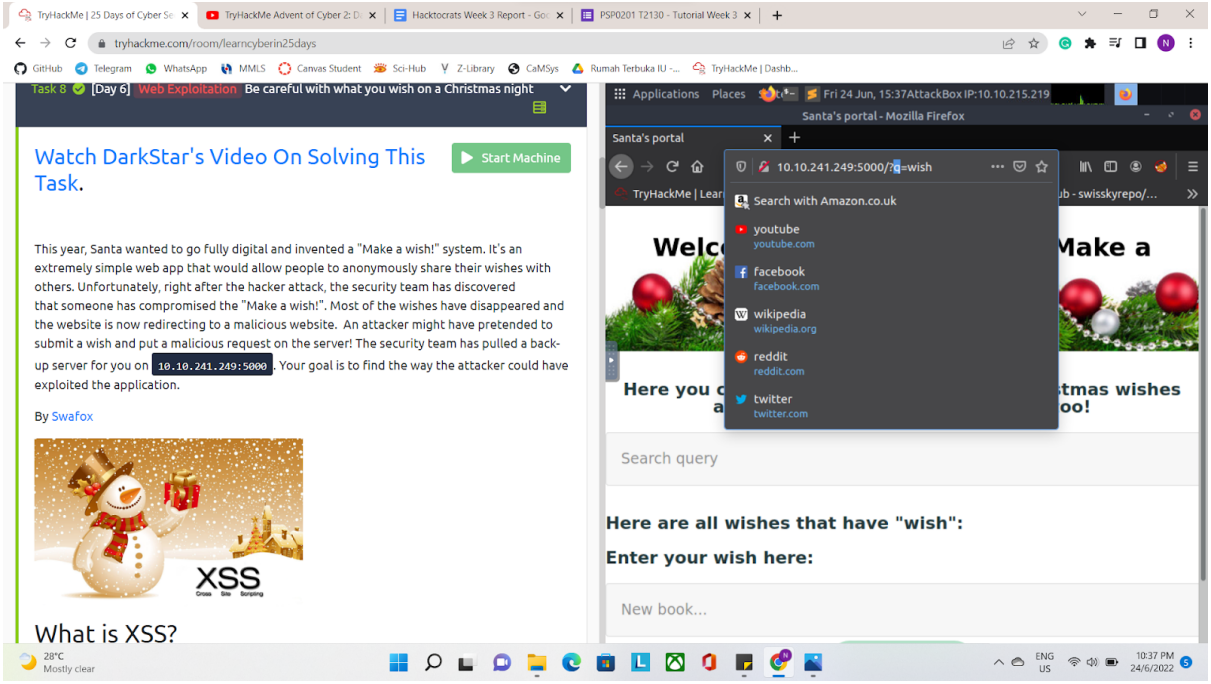
Question 2: Browse through OWASP Cheat Sheet to find the regular expression used to validate a US Zip code



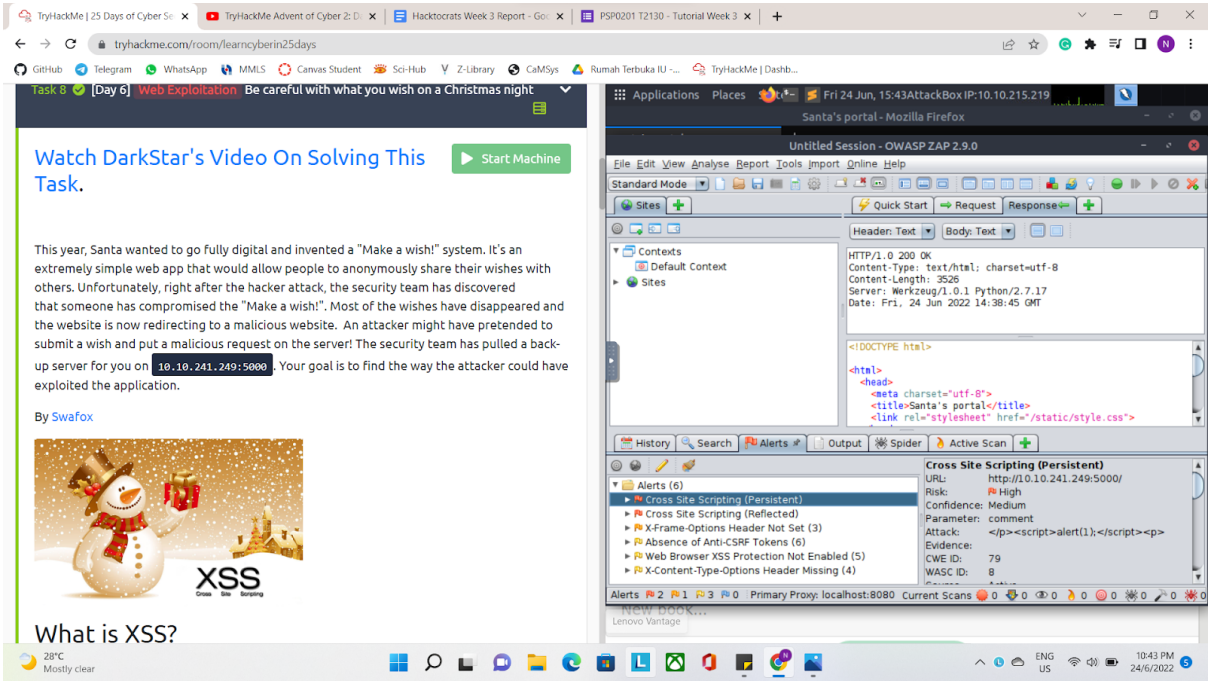
Question 3: Finding vulnerability type used to exploit the application using OWASP ZAP and found stored XSS inside <p> tag and <script> tag

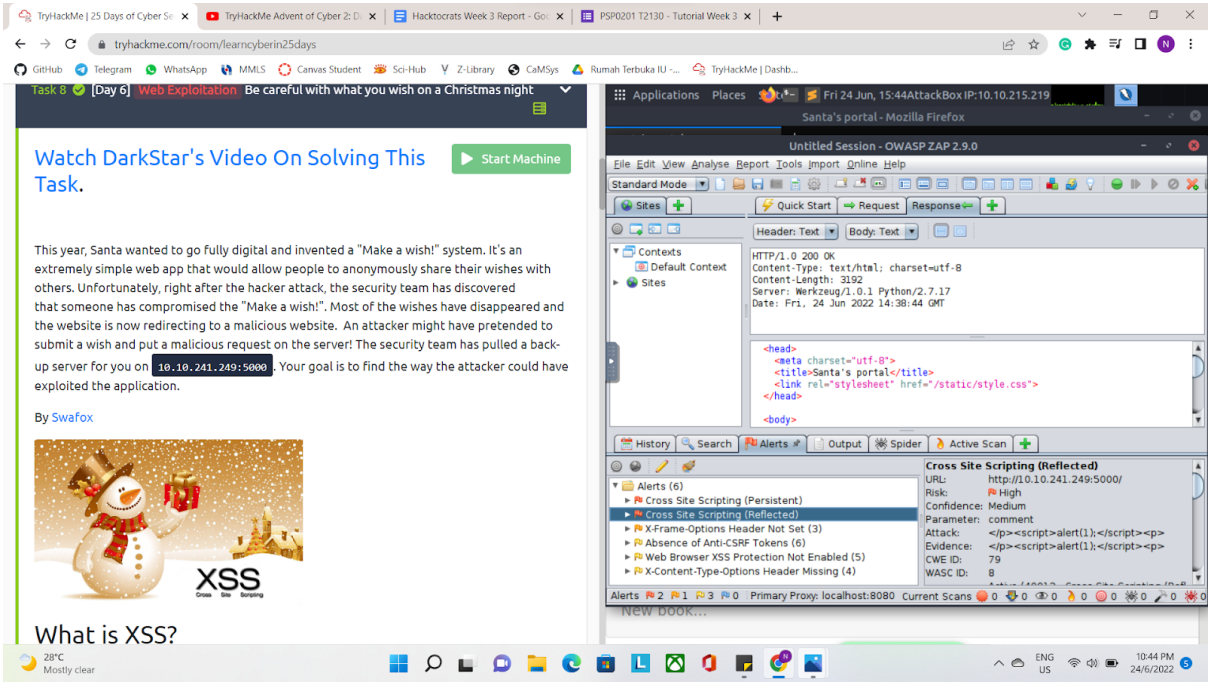


Question 4: Insert random words in christmas wish input and found the query string that can be abused to craft reflected XSS in the webpage

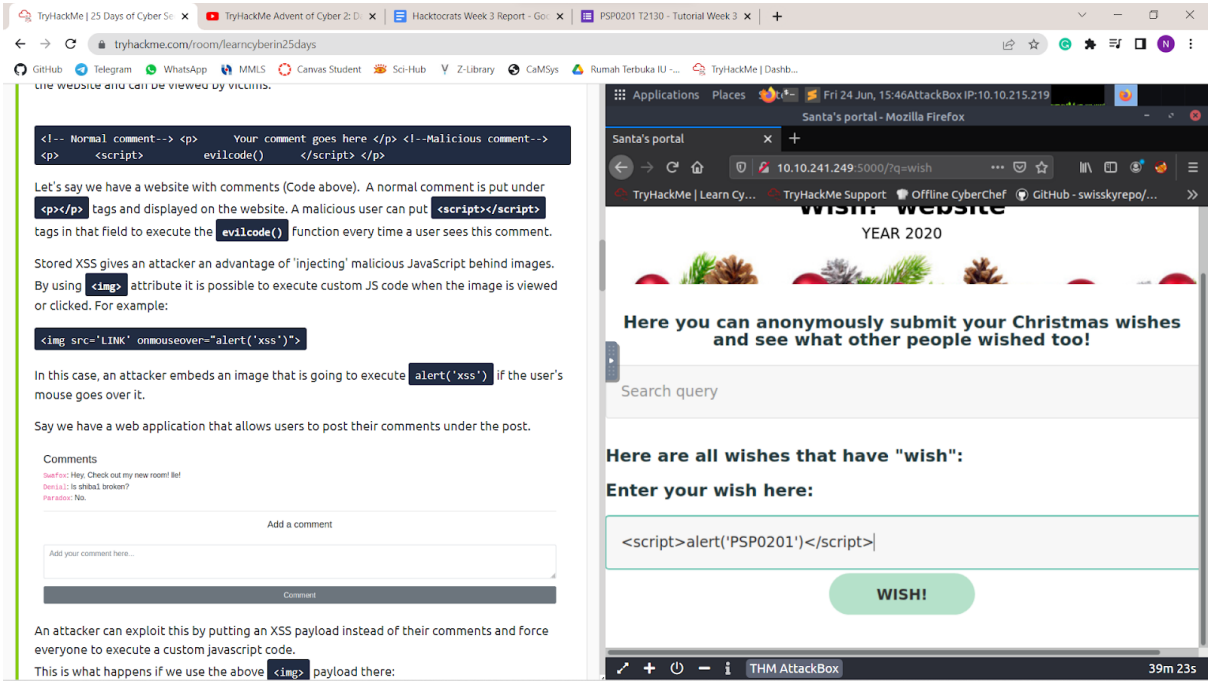


Question 5: After running automated scan on Zaproxy, two types of XSS alerts were found which is Persistent Cross Site Scripting (Stored XSS) and Reflected Cross Site Scripting

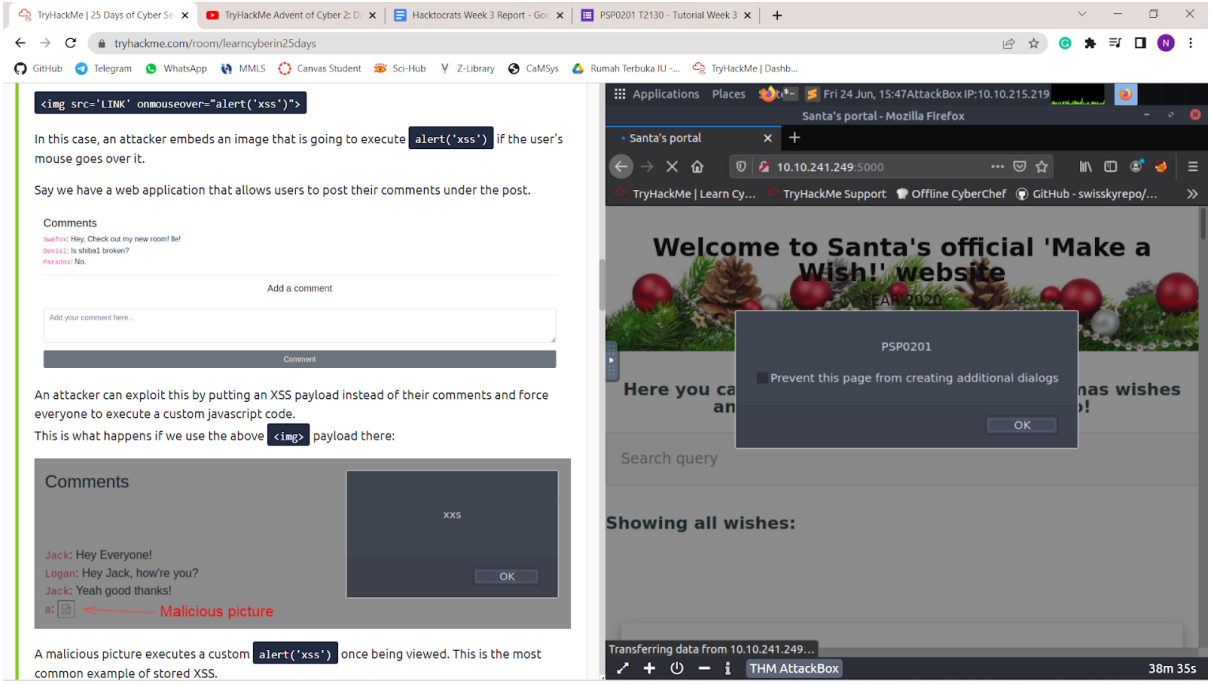




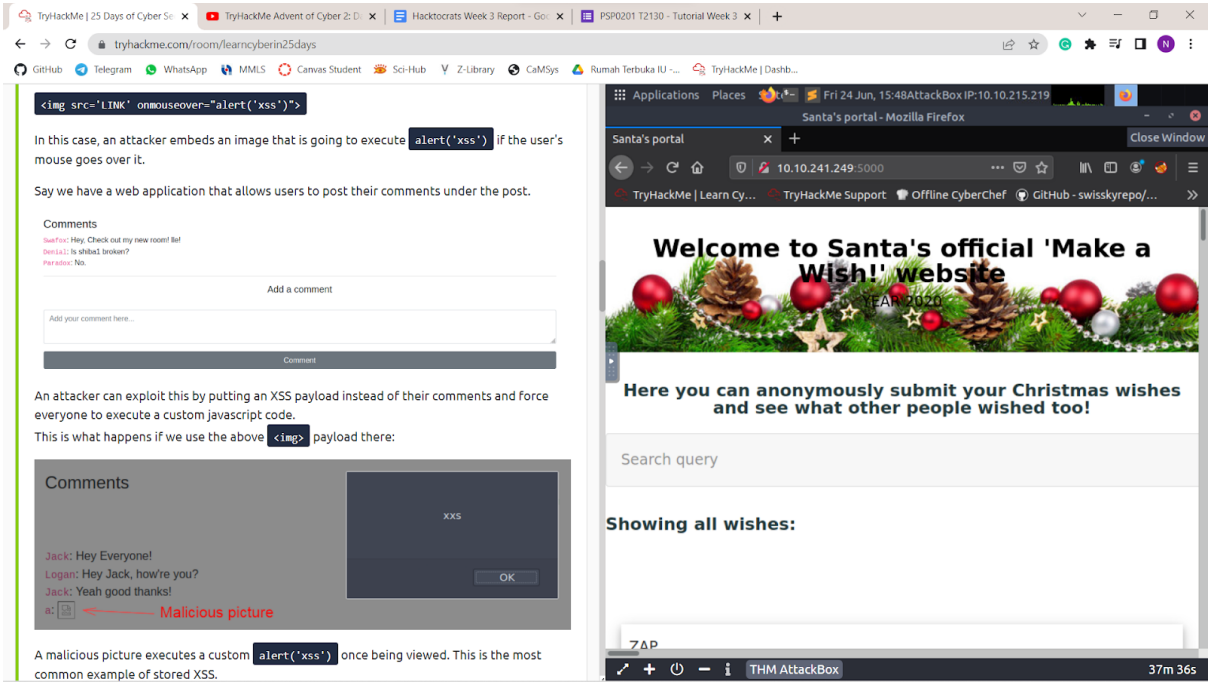
Question 6: Implementing stored XSS by inserting malicious Javascript code into Wish text box

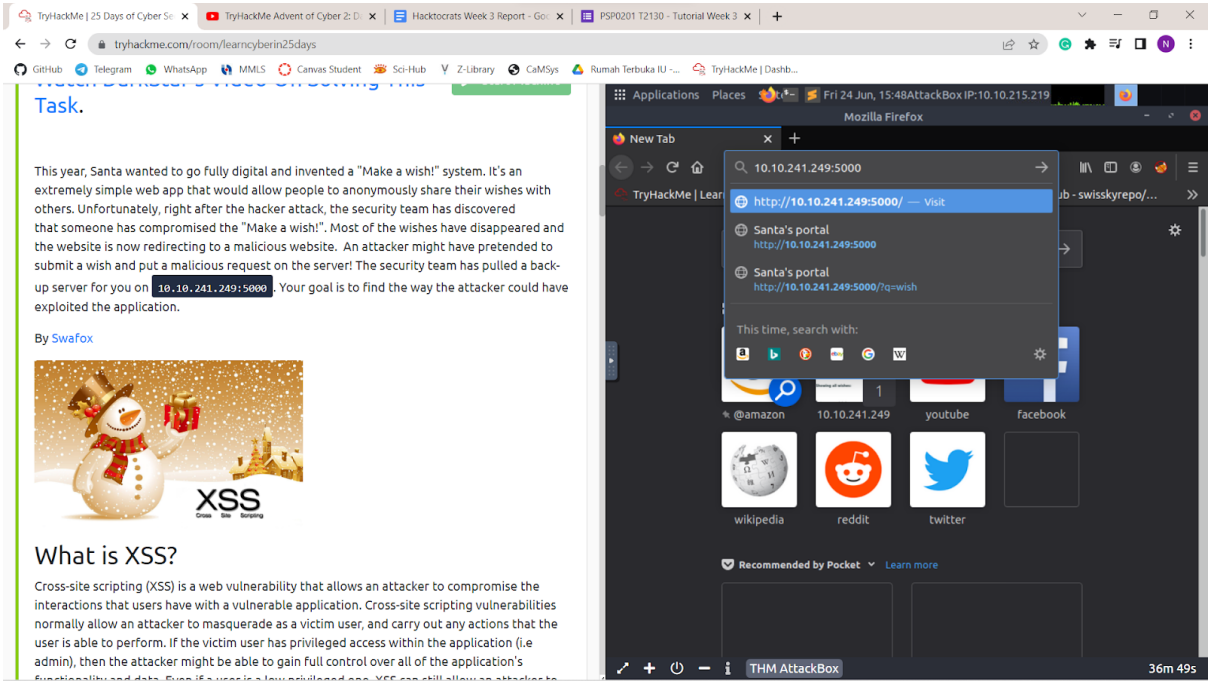


Once code entered, command was executed and alert box appeared on the screen

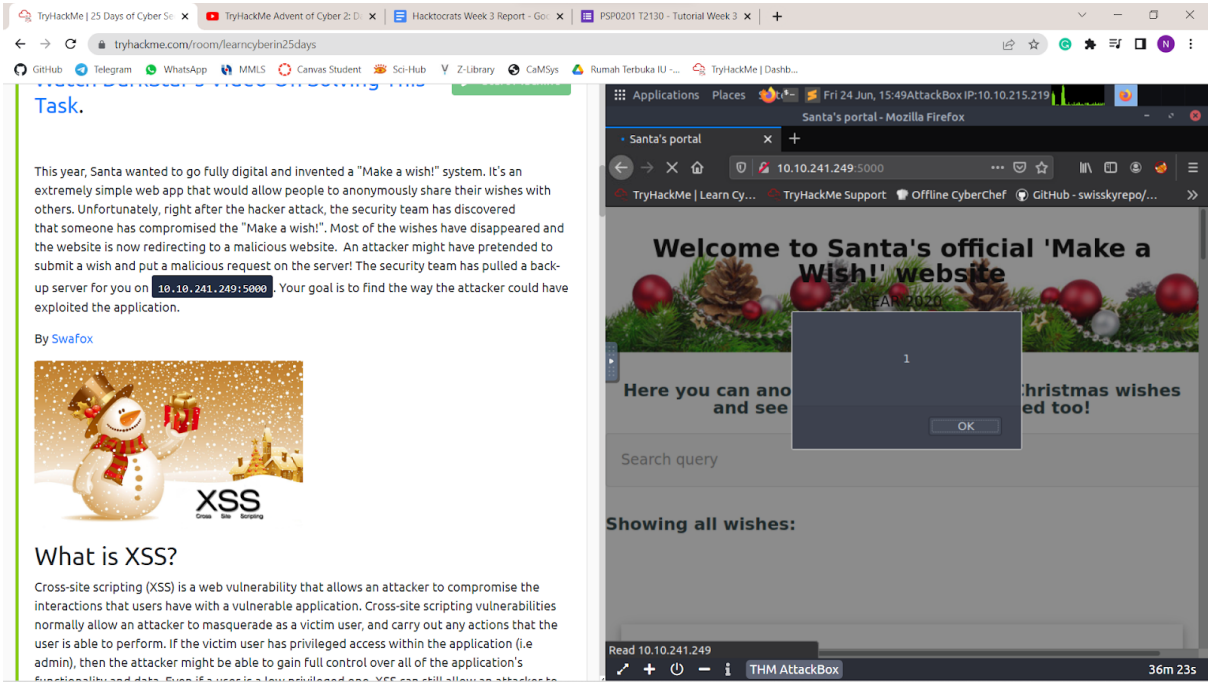


Question 7: Closing the browser and revisit the website





XSS attack persist by displaying alert box as soon as we revisit the webpage

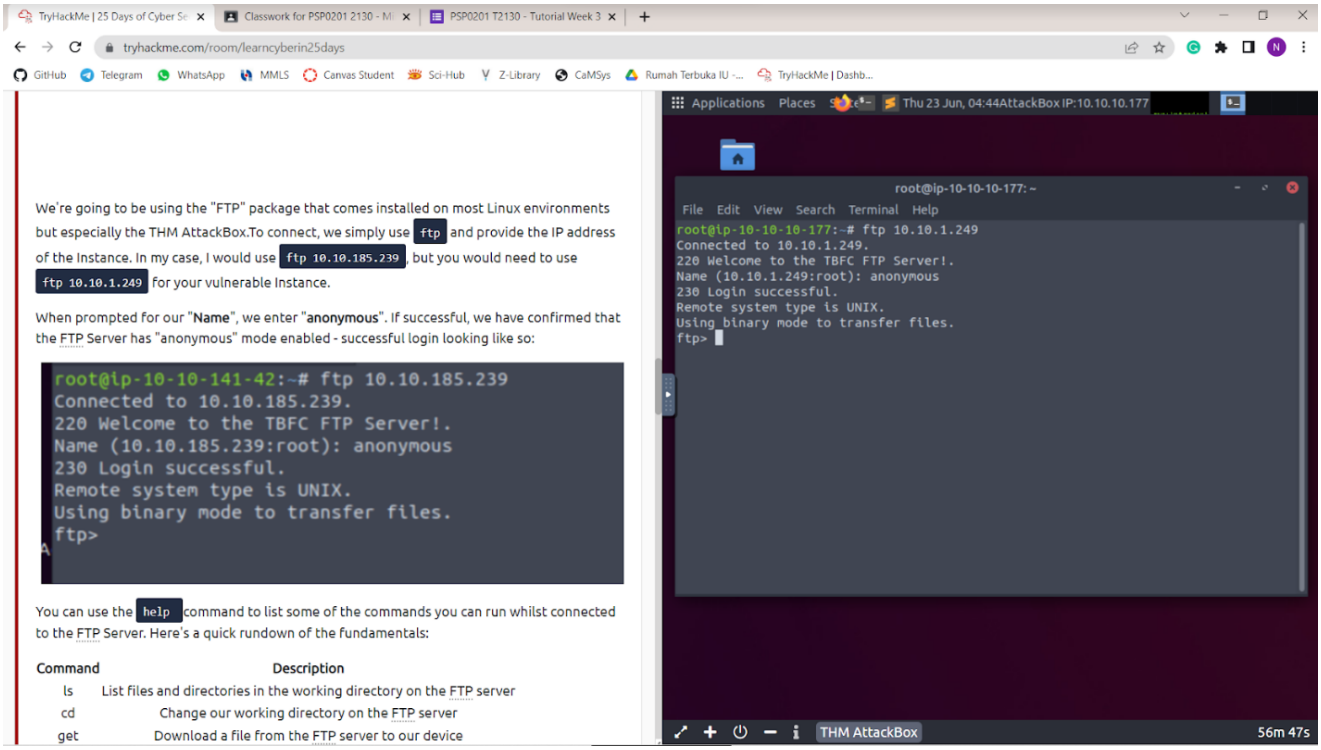


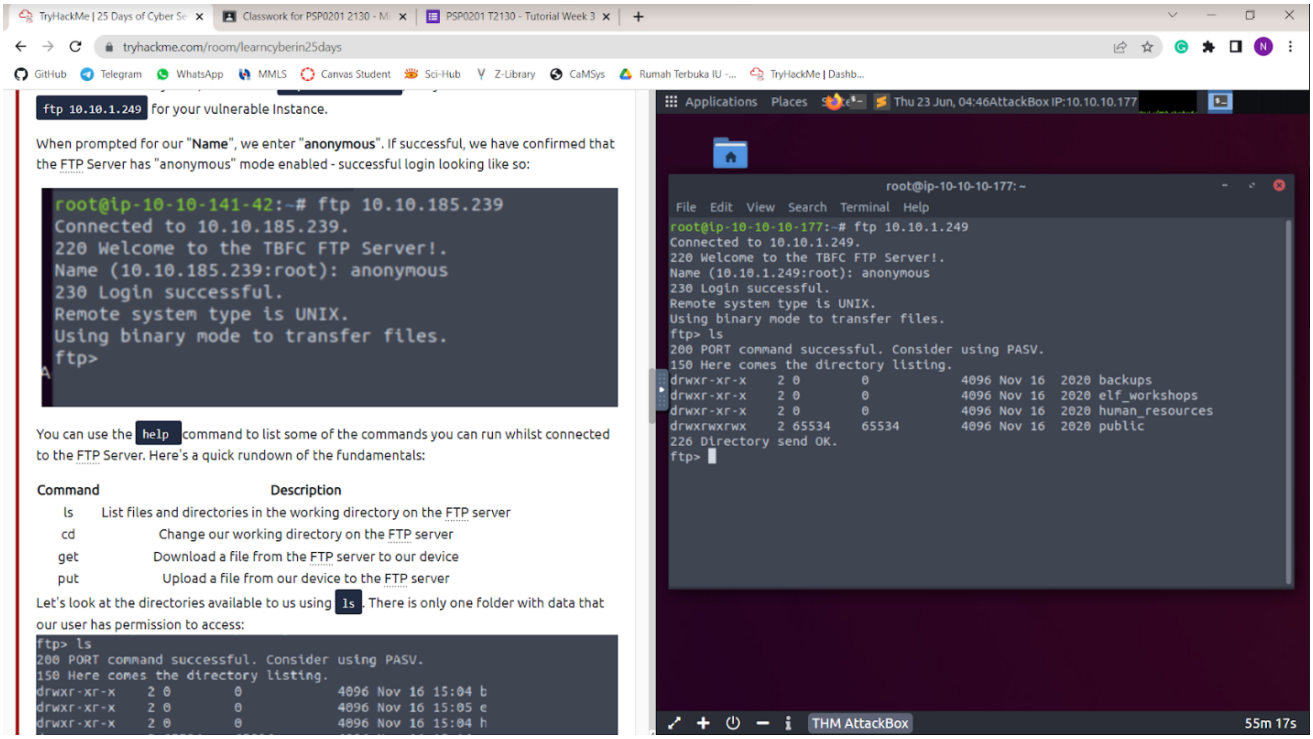
Thought methodology / process:
After gaining access to the backup server, we performed automated scan in OWASP Zaproxy to find vulnerabilities in the web application. The scan showed a few vulnerabilities inside the web application including Stored Cross-Site Scripting and Reflected Cross-Site Scripting. Both were classified as high risk vulnerabilities. By using OWASP Zaproxy, we also found XSS payload written inside comment parameter of the Javascript code. We wrote our own XSS payload in the wish text box and caused an alert box displaying ‘PSP0201’ to appear. This proved that a malicious code has been stored in the web application. After that, we close the web browser and revisit the webpage to see if the attack persist. An alert box popped up as soon as the web page load, signalling us that the XSS attack will continue even if we re-open the web application.

DAY 9: Anyone can be santa!

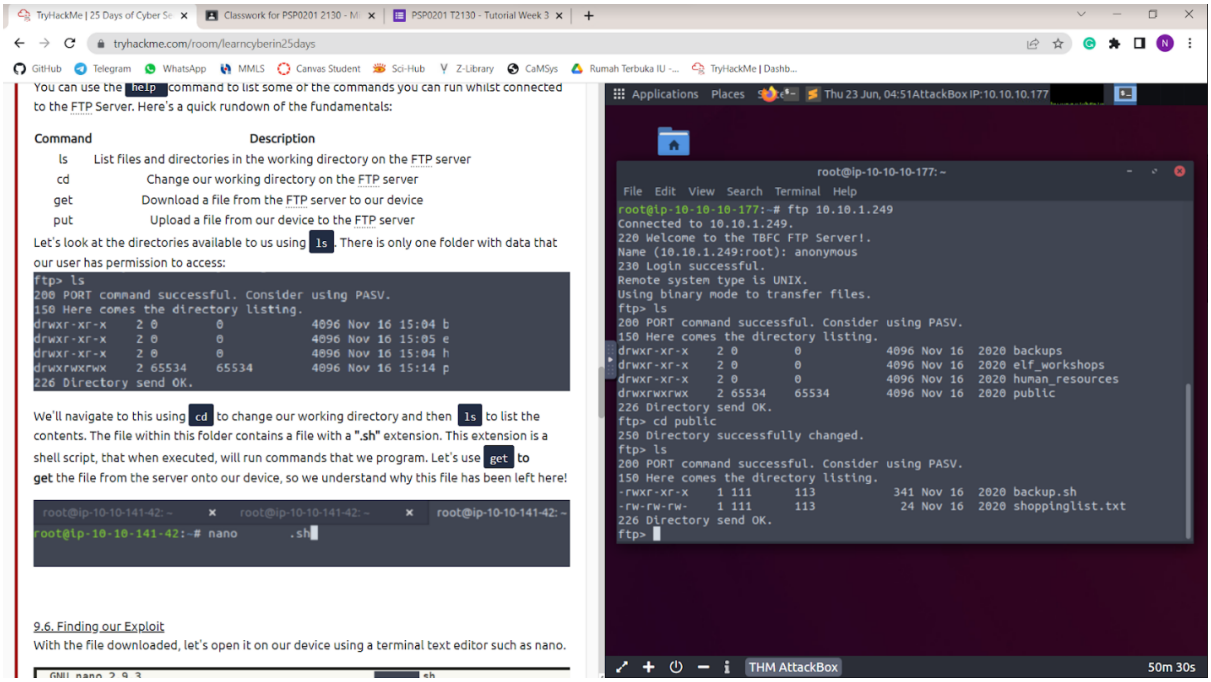
Question 1:

Get into the ftp server in the terminal and find the files using ‘ls’ command



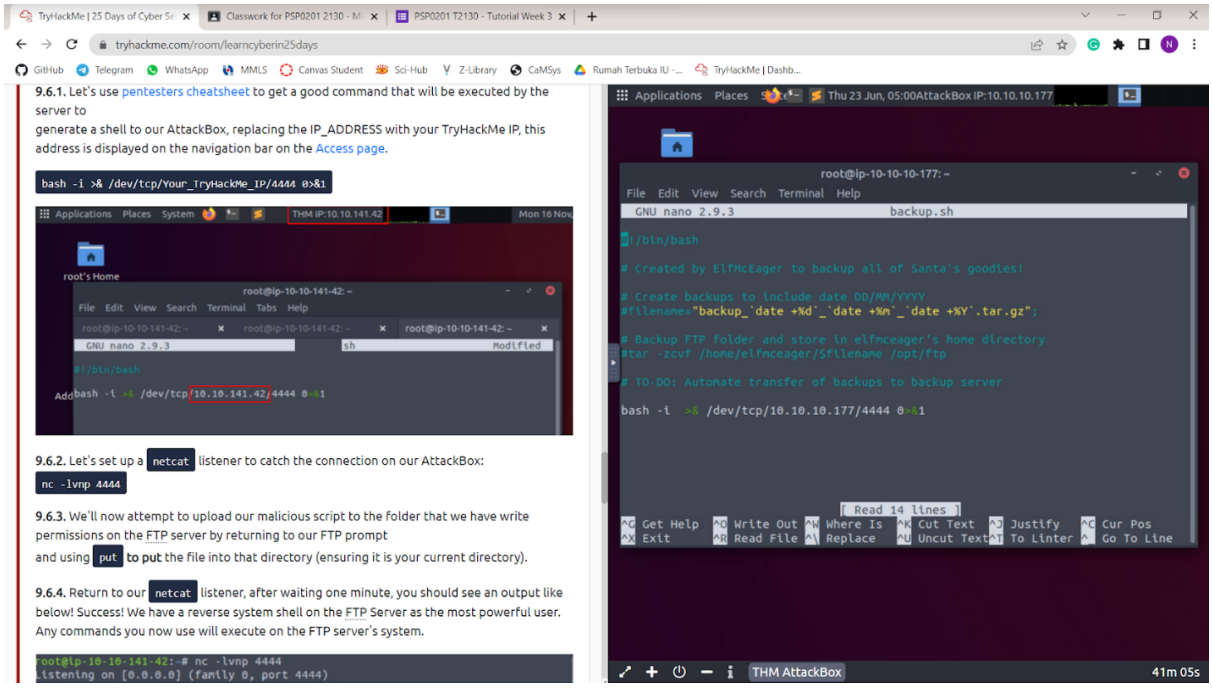


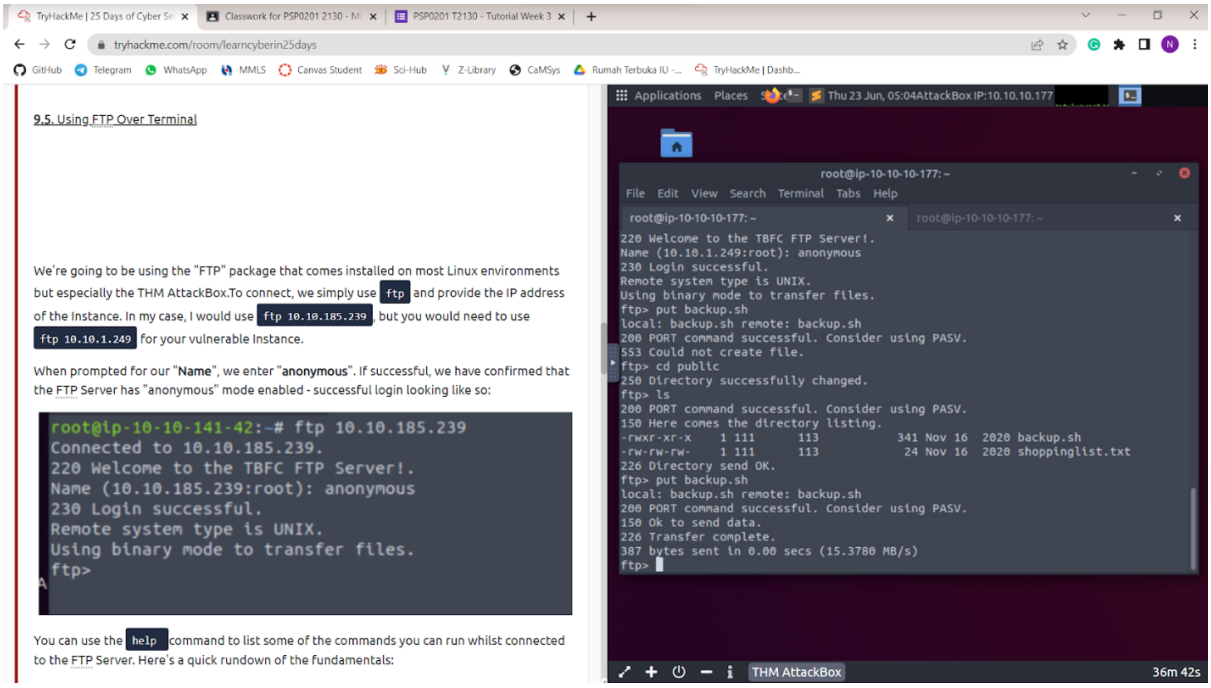
Question 2:
Try and error to find the FTP server that has data accessible by the “anonymous” user. Use the cd command to change the directory to the public, and use the “ls” command to get the list files and directories in the working directory.



Question 3:

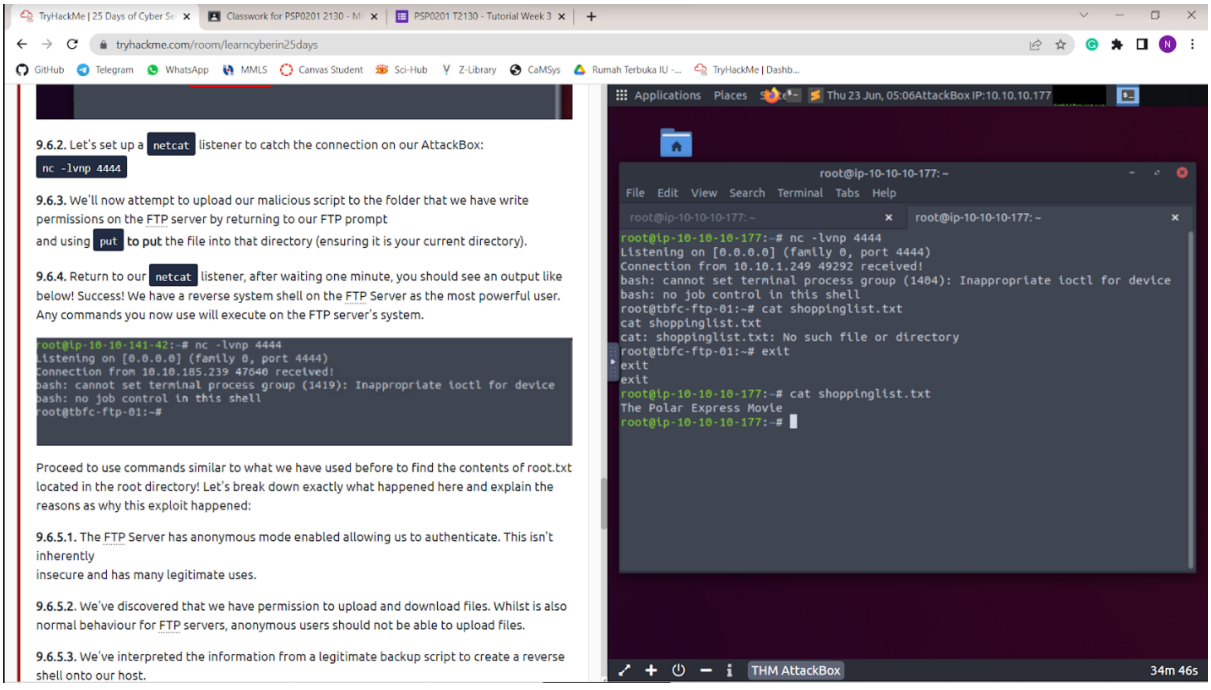
In the public directory, there are backup.sh and shoppinglist.txt files so to know which script can be executed within this directory, we use ‘get’ command.
The scripts that are executed within this directory are backup.sh. Open the backup.sh using nano text editor.



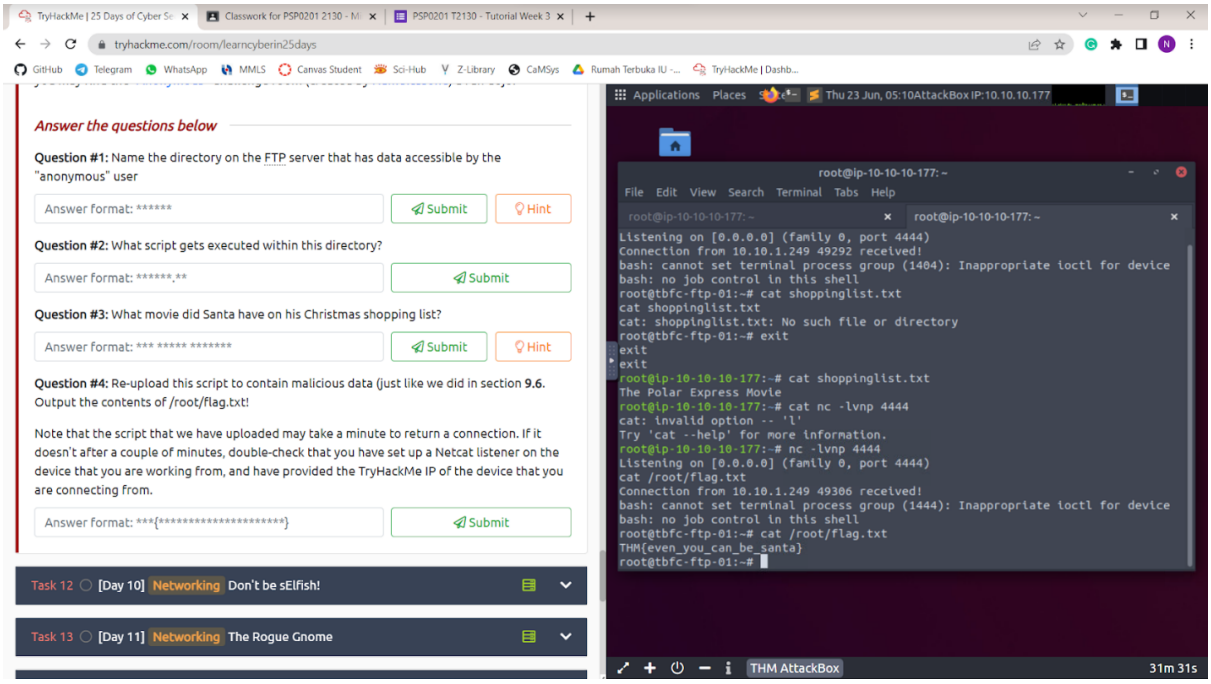


Question 4:

To know the movie name in the shoppinglist.txt file, we use the ‘cat’ command



Question 5:
Using cat command and the contents of /root/flag.txt, we get the secret flag!!



Thoughts methodology / process:
First and foremost, we get into the ftp server with our ip addresses and find the files using ‘ls’ command.