Information Security

Assignment # 04

XSS Lab In SEED's Lab

Mam Hina Binte Haq

Course Instructor
CS- 3002
SE- S
Due Date: May 14, 2023

Group Members:

Zeeshan Ali	20i-2465
Ans Zeeshan	20i-0543

Assignment # 04

XSS Lab using SEED's Lab

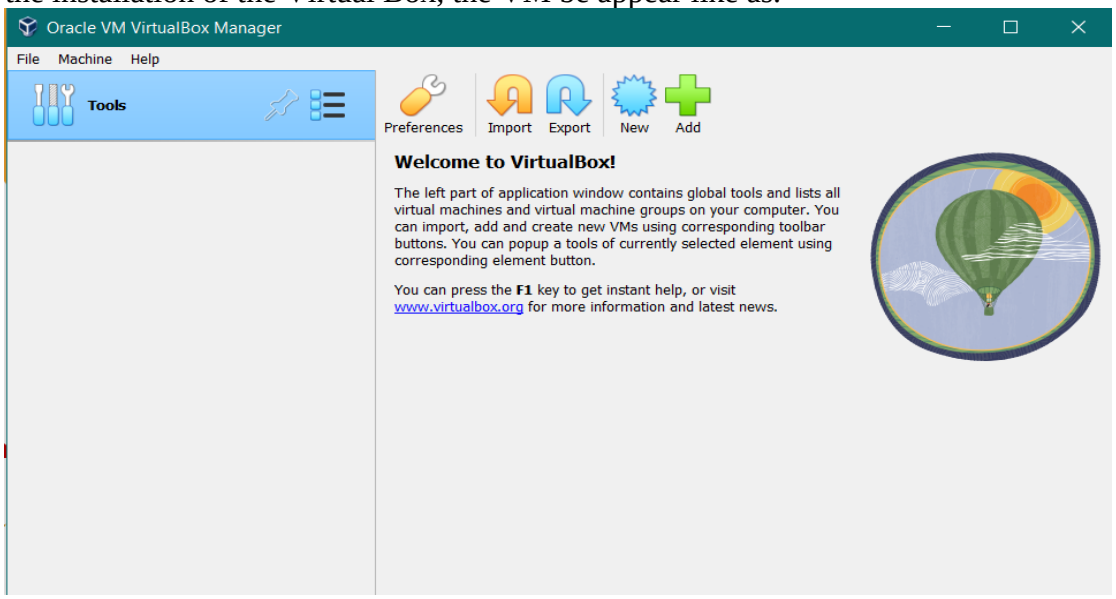
1- XSS Lab:

Description:

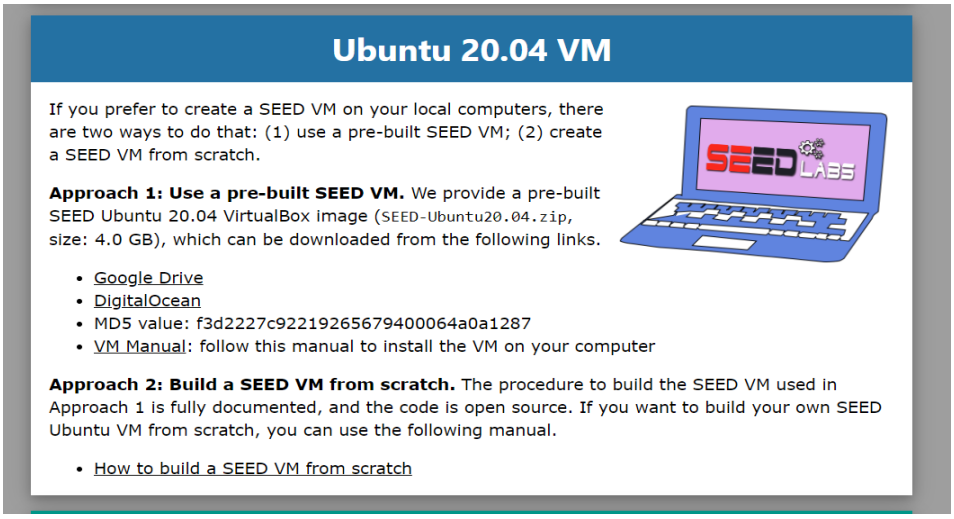
To starting, the Installation requirements are.

1- Oracle VM Virtual Box
2- SEED'S Ubuntu 20.04

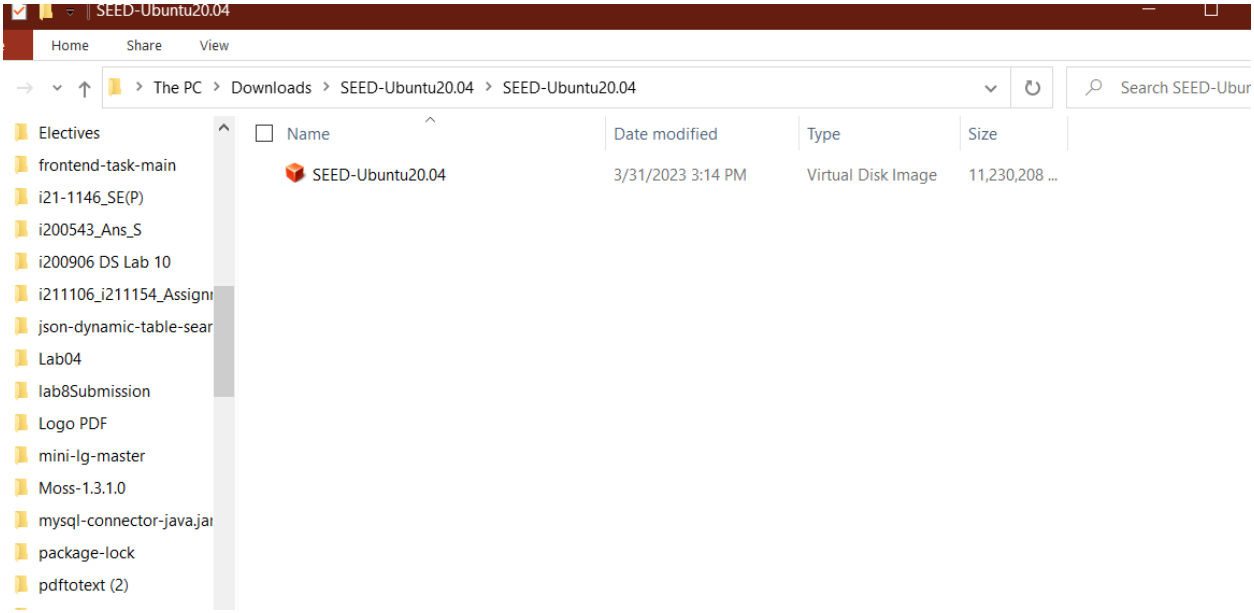
After the installation of the Virtual Box, the VM be appear like as.



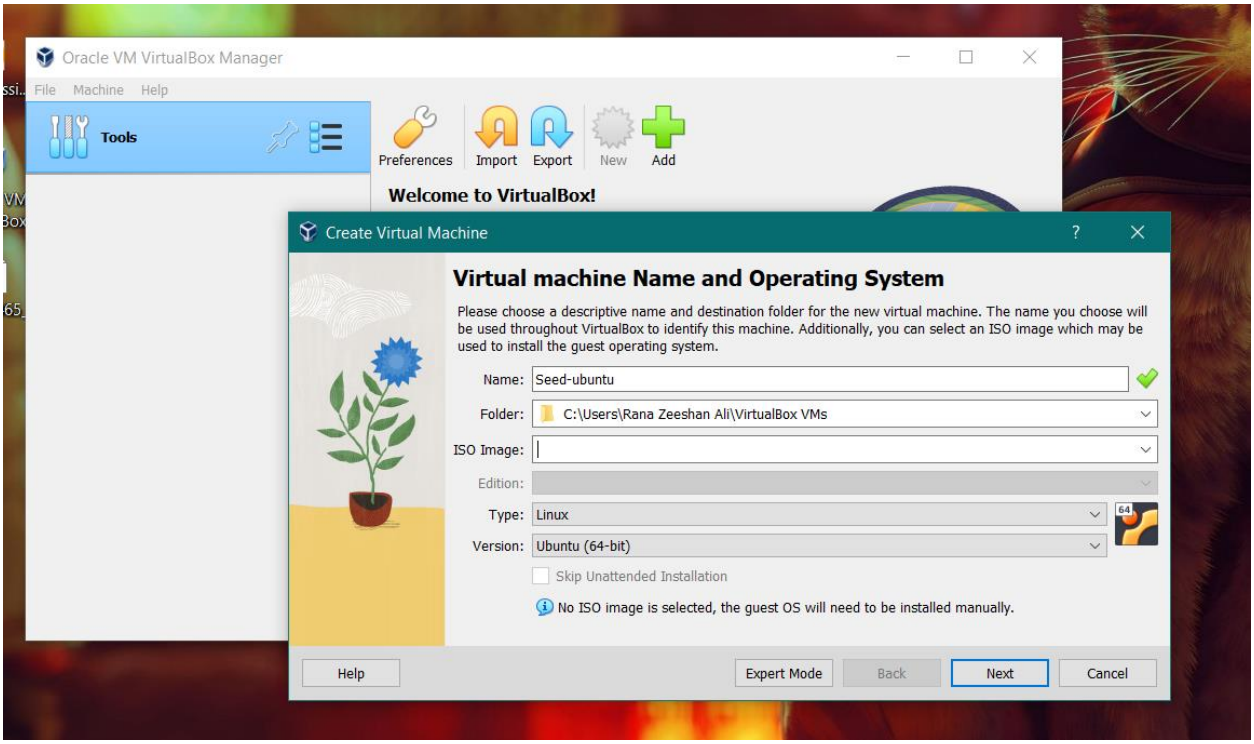
Now, Installing the Seed's Ubuntu, we have selected the version such as Ubuntu 20.04 VM as per requirements in the manual.



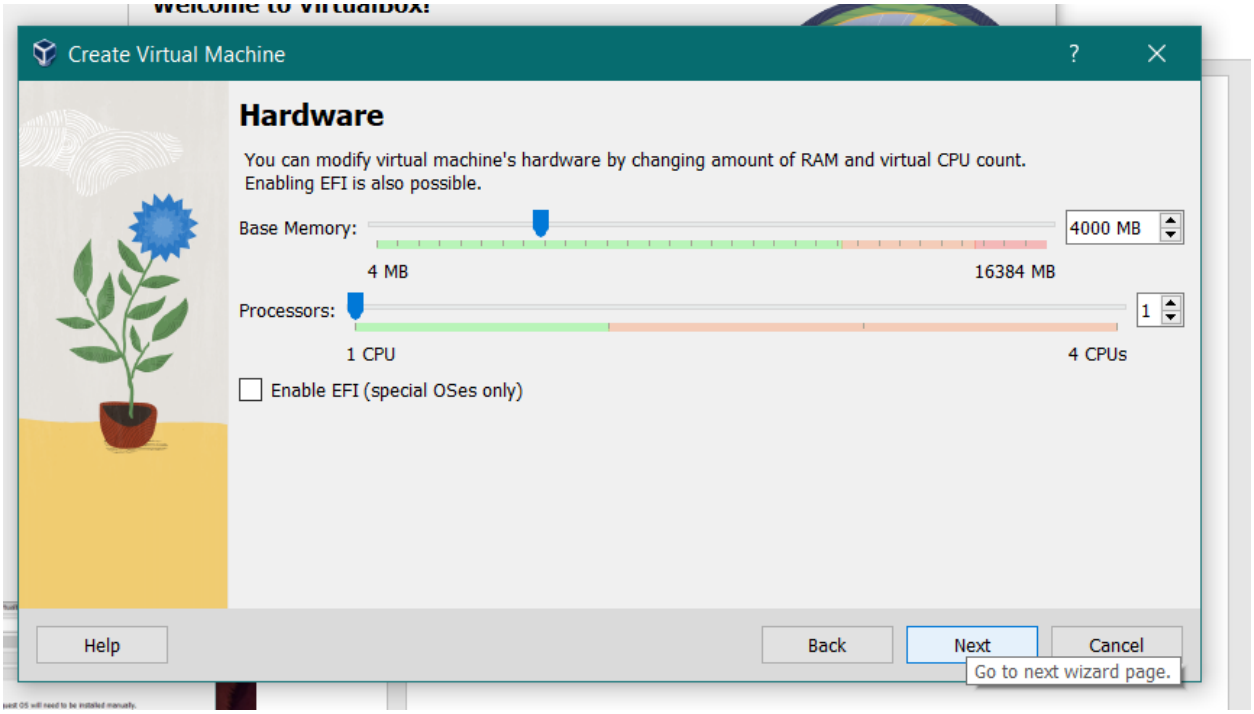
After Downloading and Extracting the zip file of the Ubuntu 20.04, it looks likes.



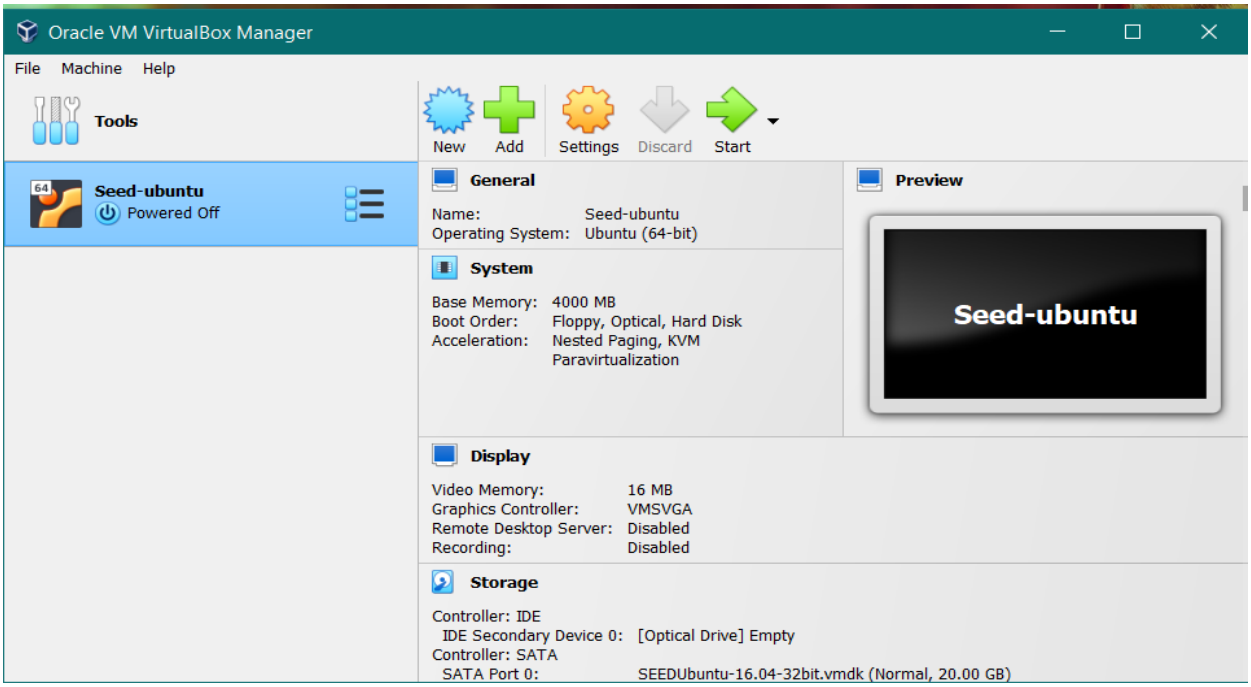
Now, to host the Ubuntu in VM box



Set the Memory Configurations

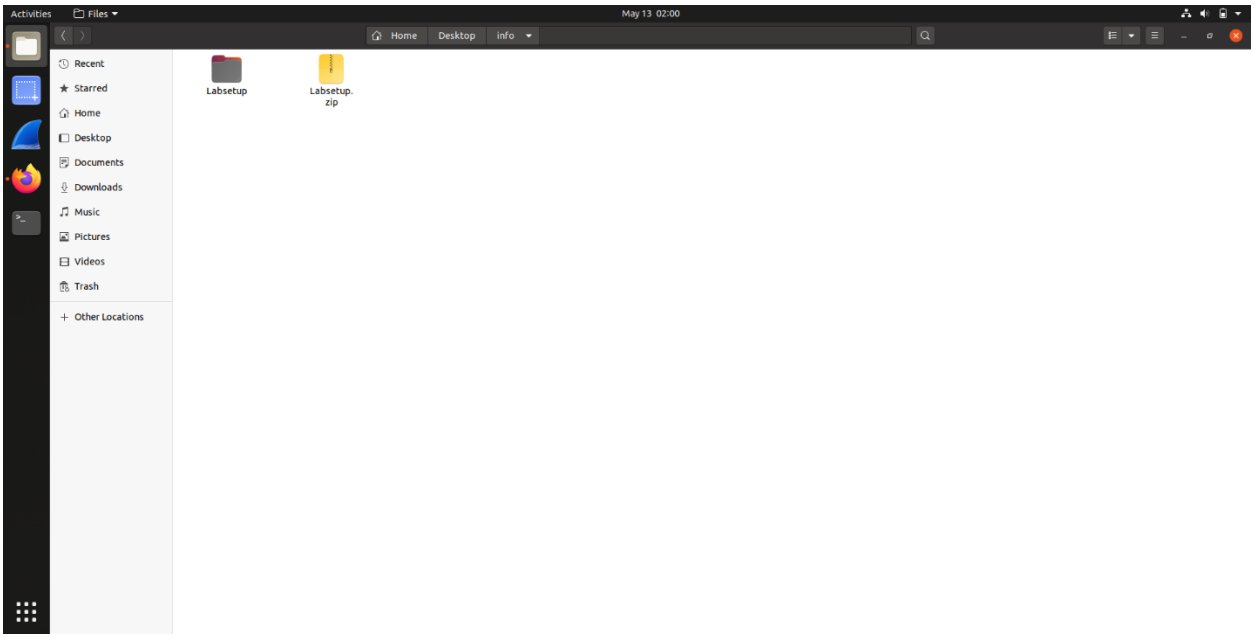


Now, the Ubuntu is successfully hosted.

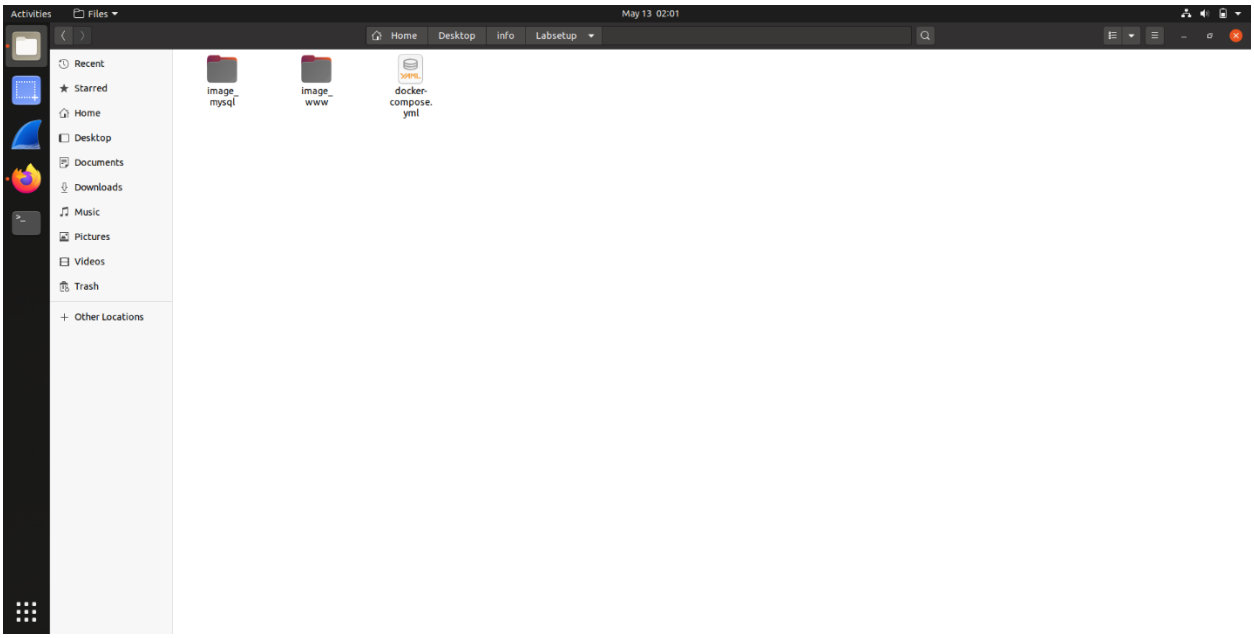


Lab Pre-Requisite Task:

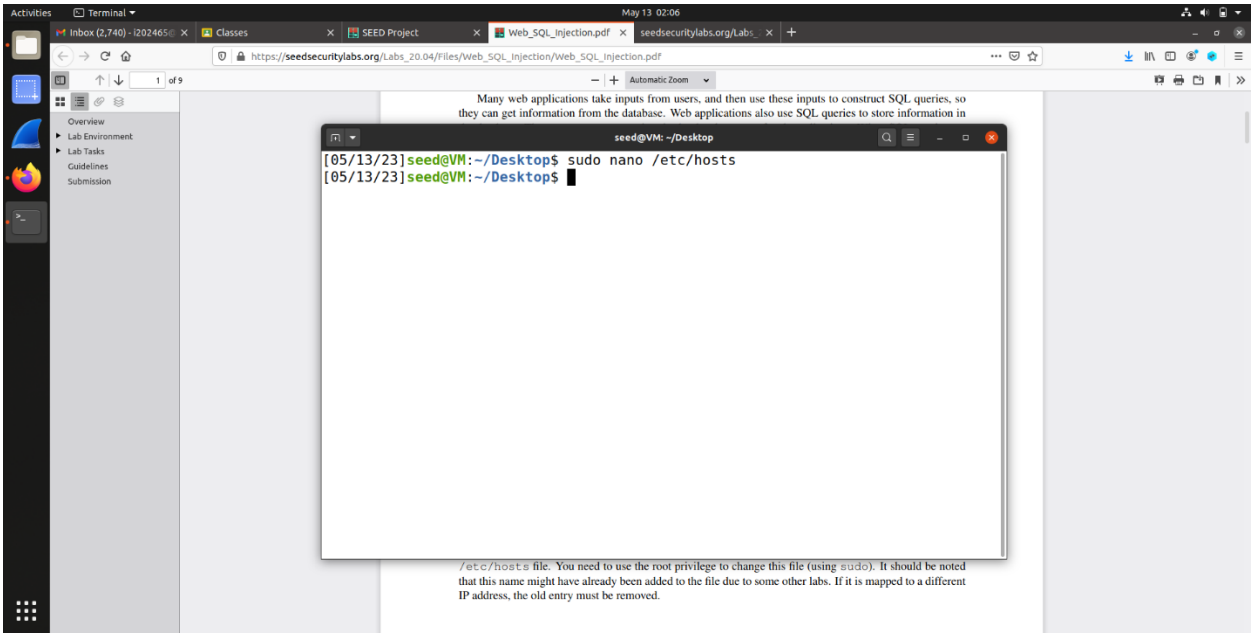
Download the Lab Setup file and extract it.



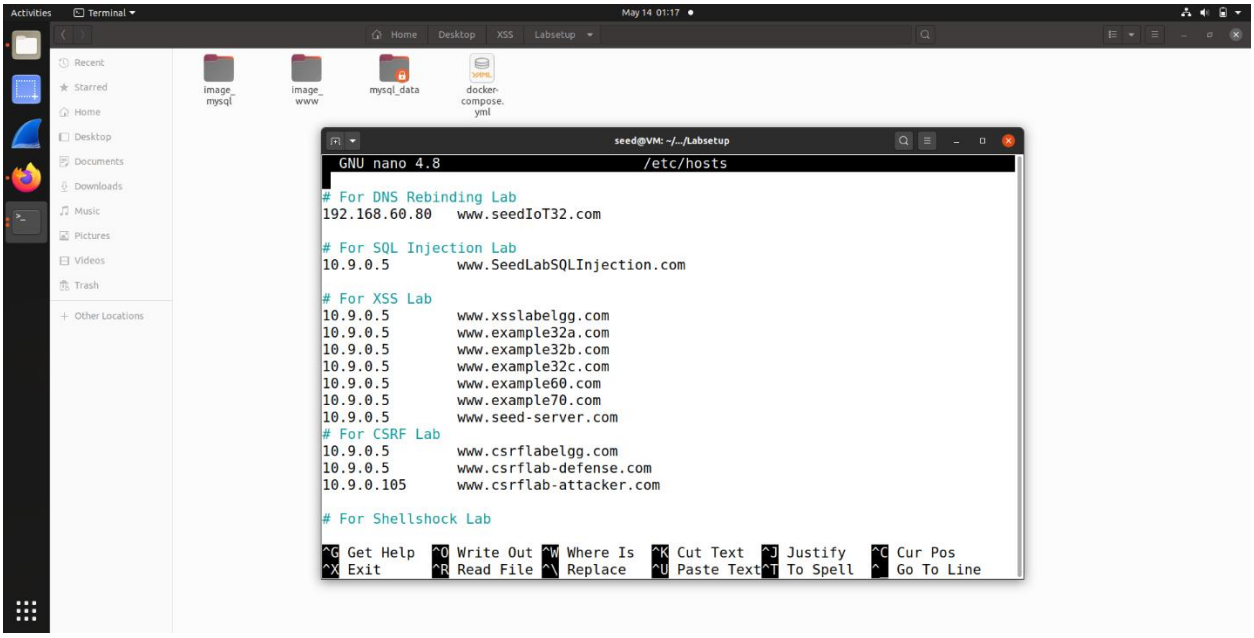
After Extracting, it shows all the file and folders in it.



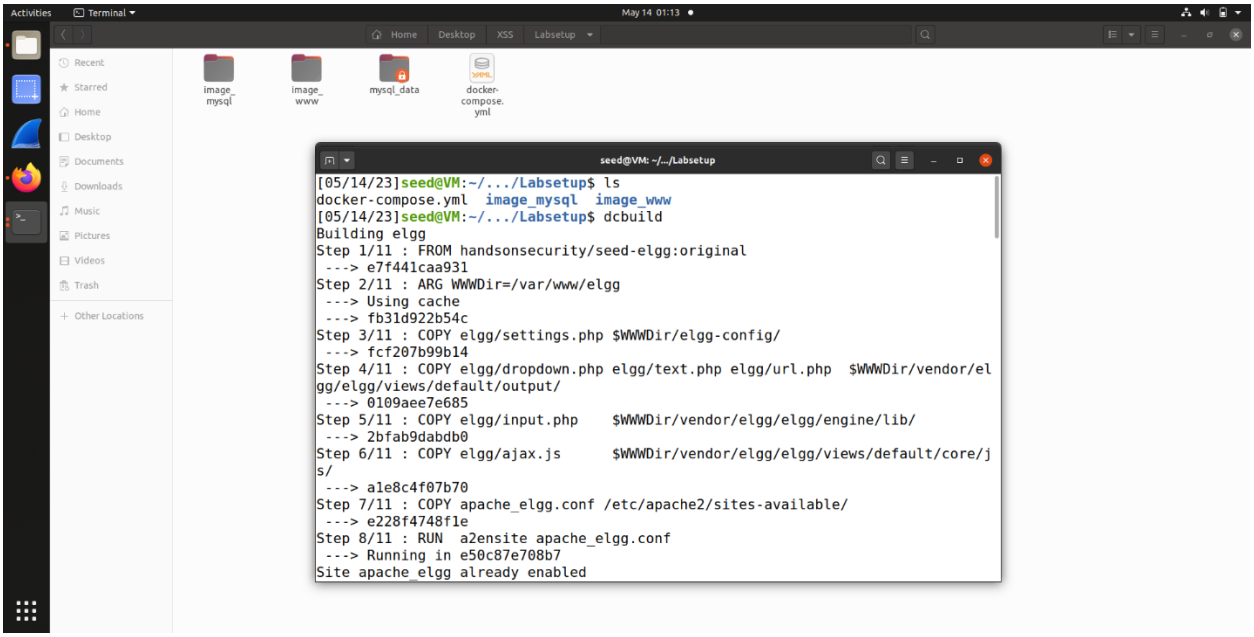
To Assign Ip of seed-server website to run on chrome easily.



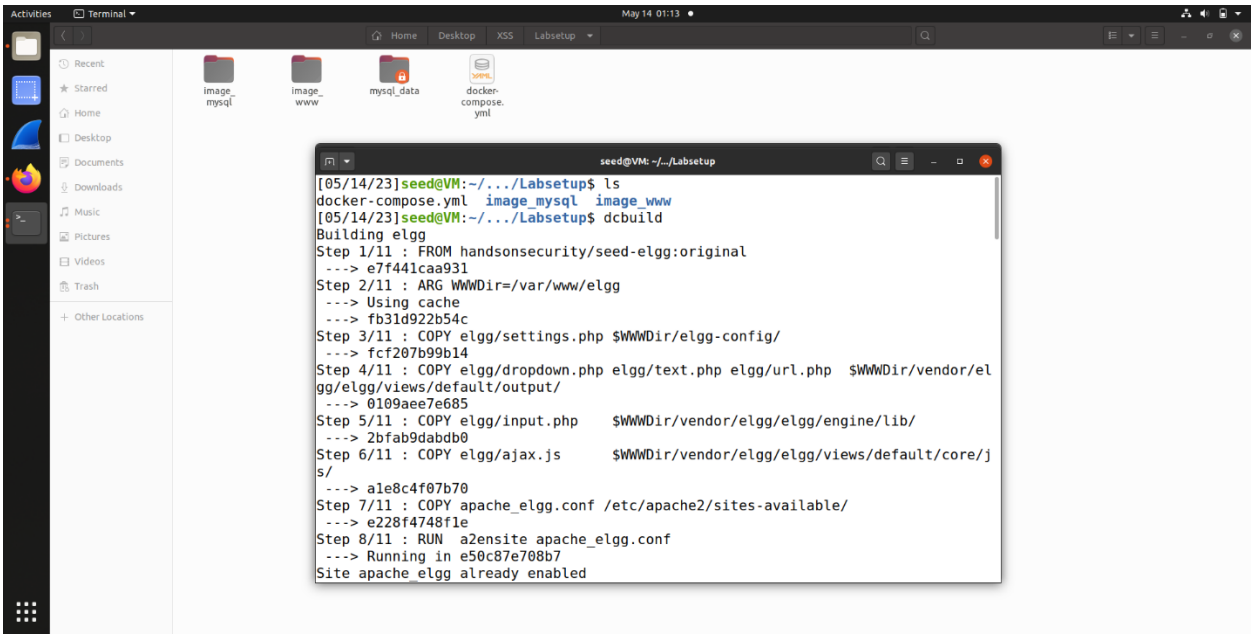
Add manually 10.9.0.5 www.seed-server.com in the file using the command line interface.



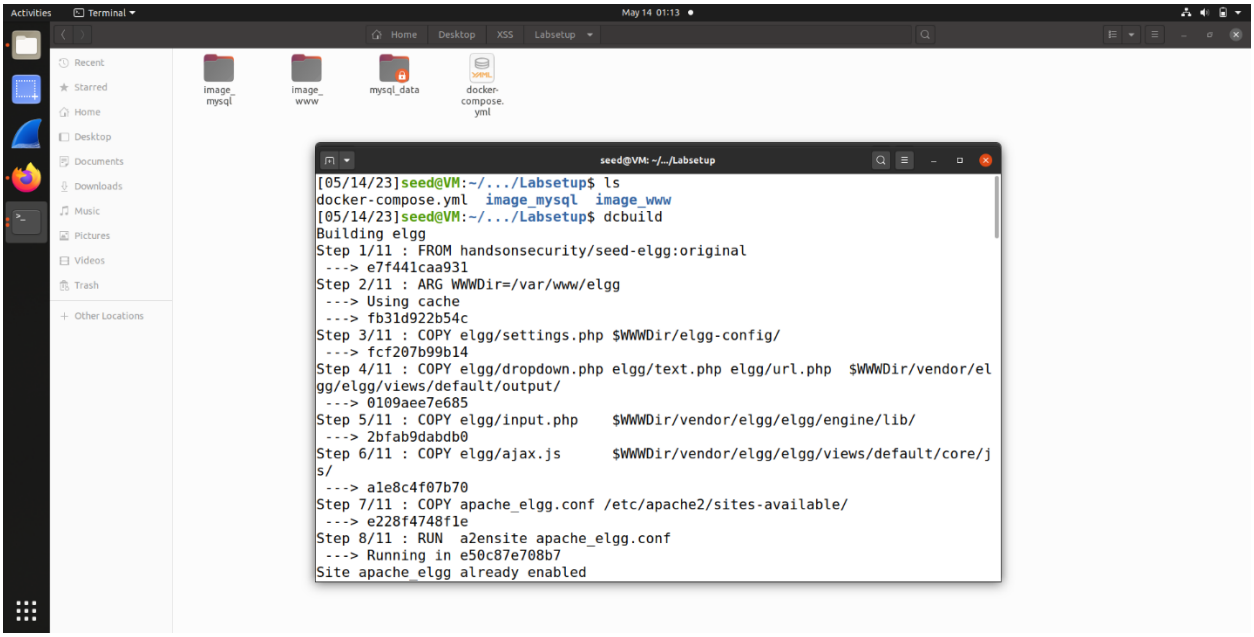
To Build the docker to make the containers of your website frontend and backend.



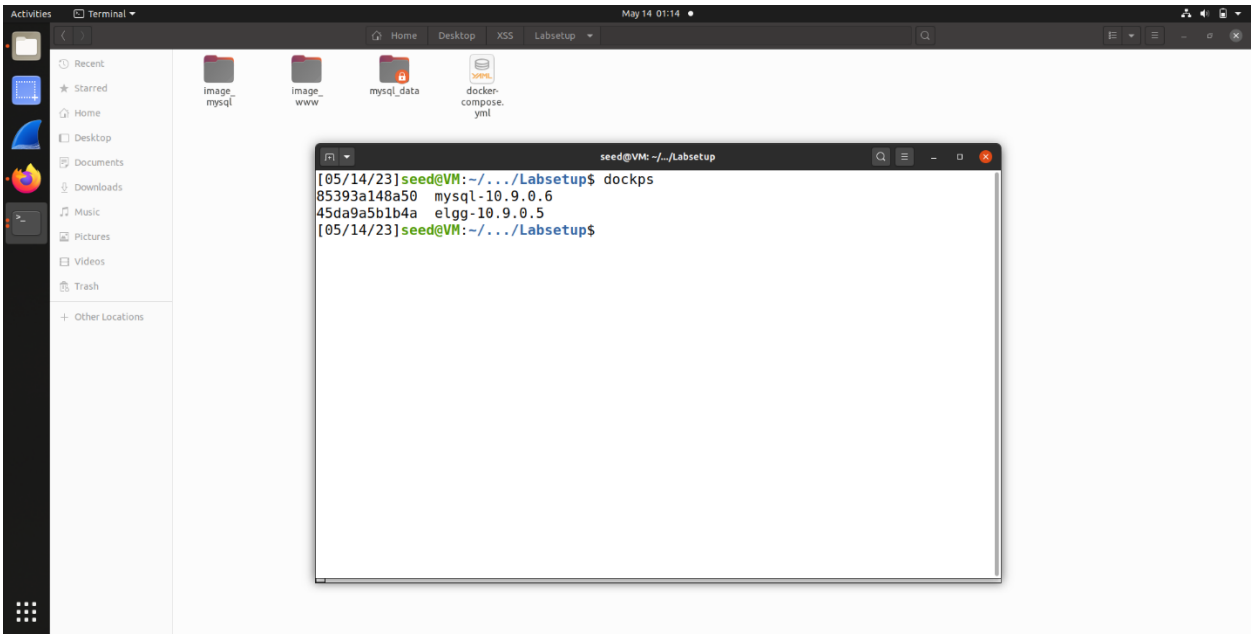
Now the docker build command is successful and docker containers are created.



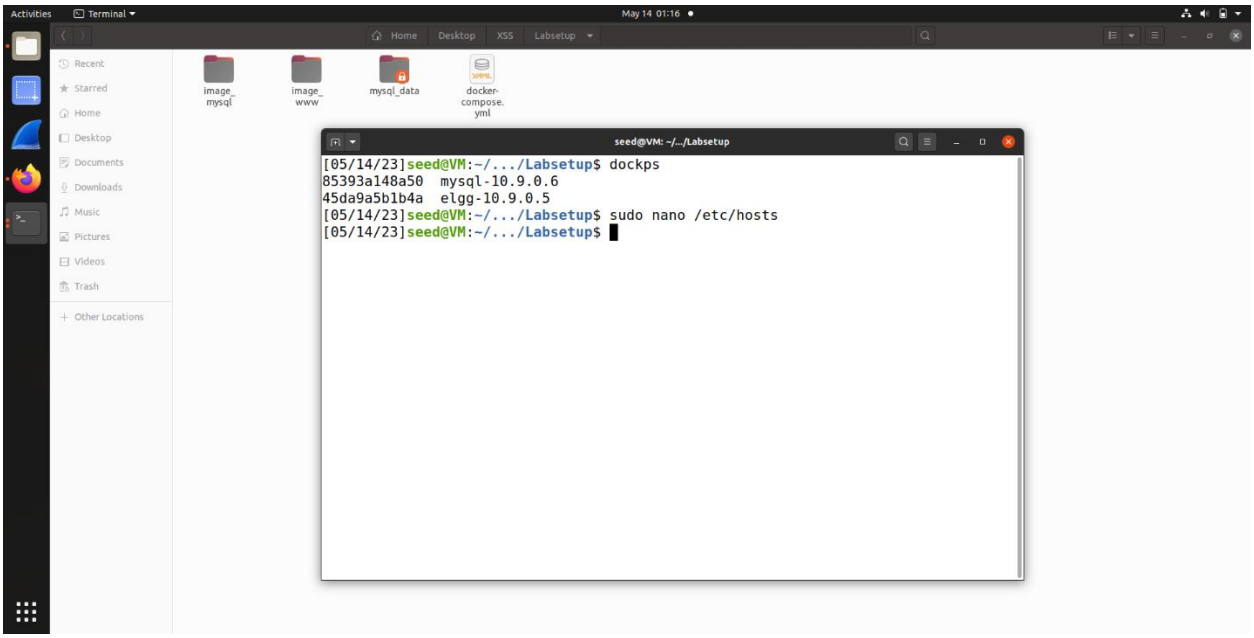
To run the containers, we use docker up comands to make them in running state.



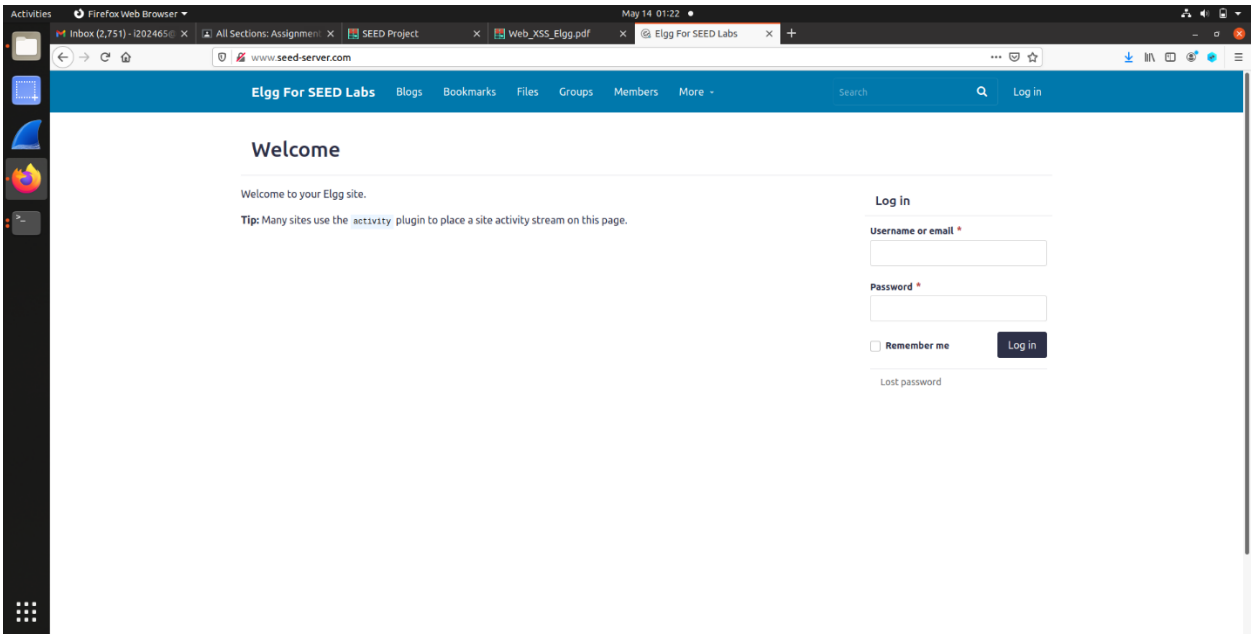
Now, to check which containers are created and how many containers are created.



Now, to login into specific container use docksh container id.

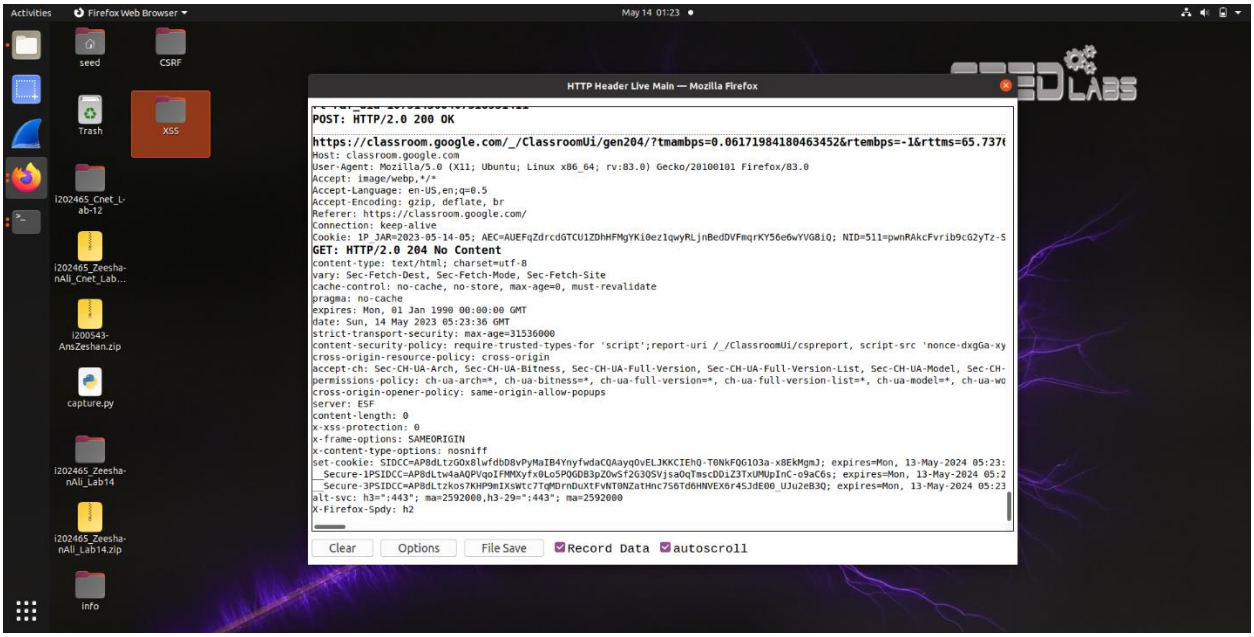


Now, to check the website is running or not, these are the following address.

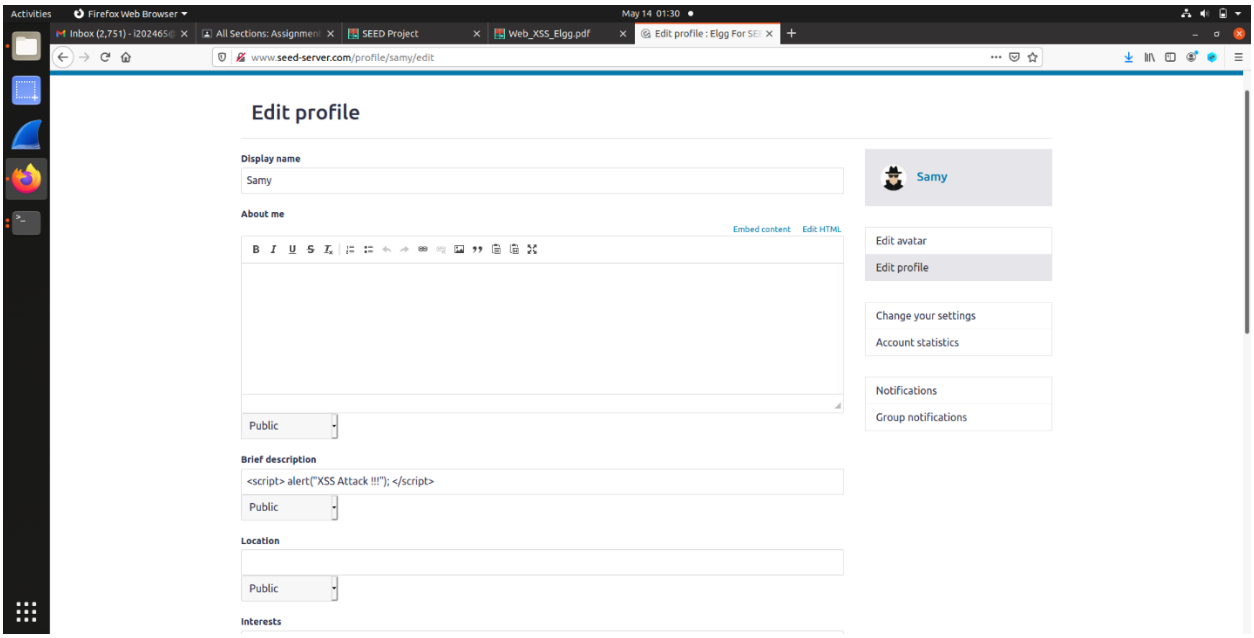


Task-1:

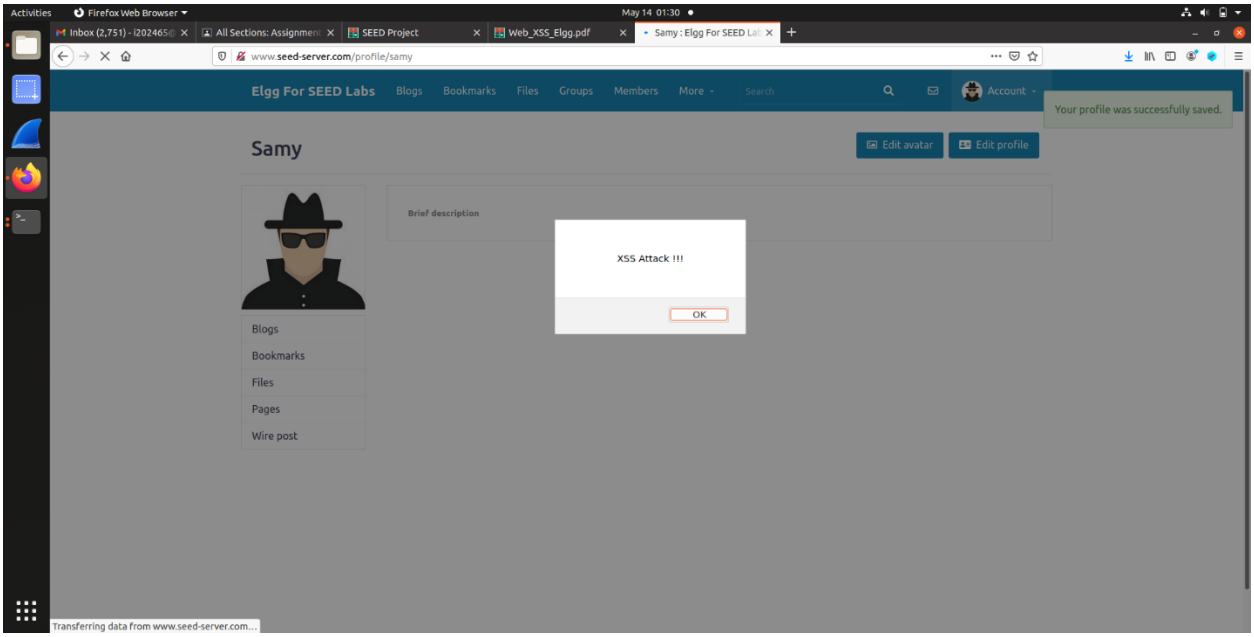
Now, to capture the packets, the HTTP header live works here.



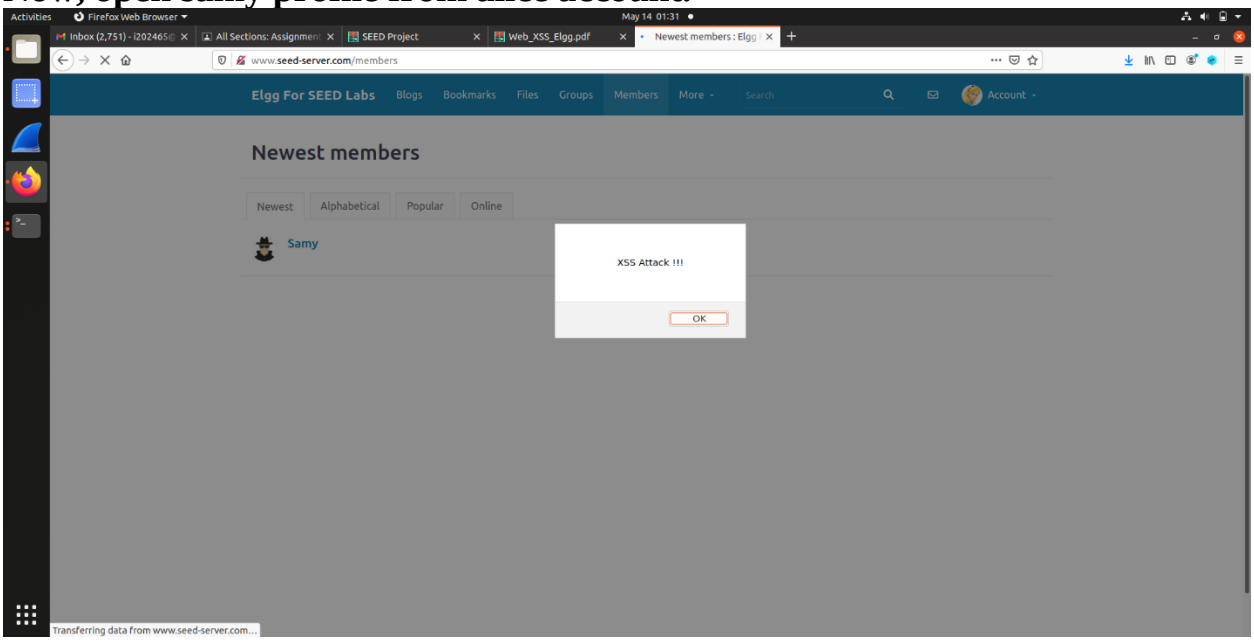
Task2: do ASS Attack and prompt on screen.



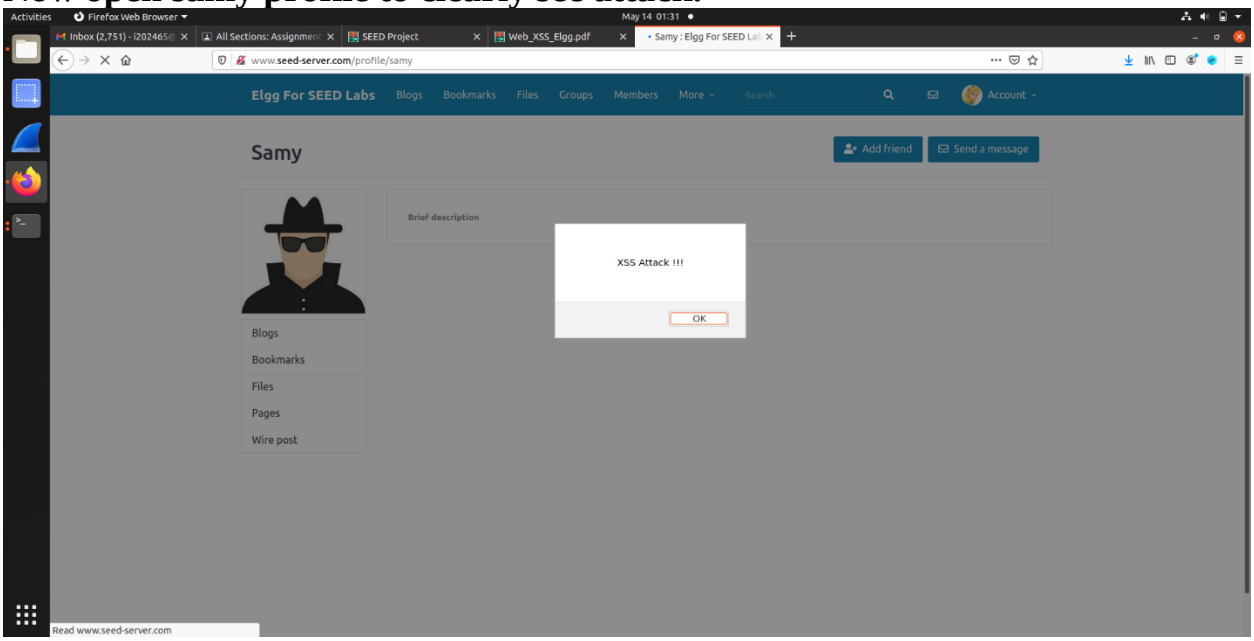
First open its own profile.



Now, open samy profile from alice account.

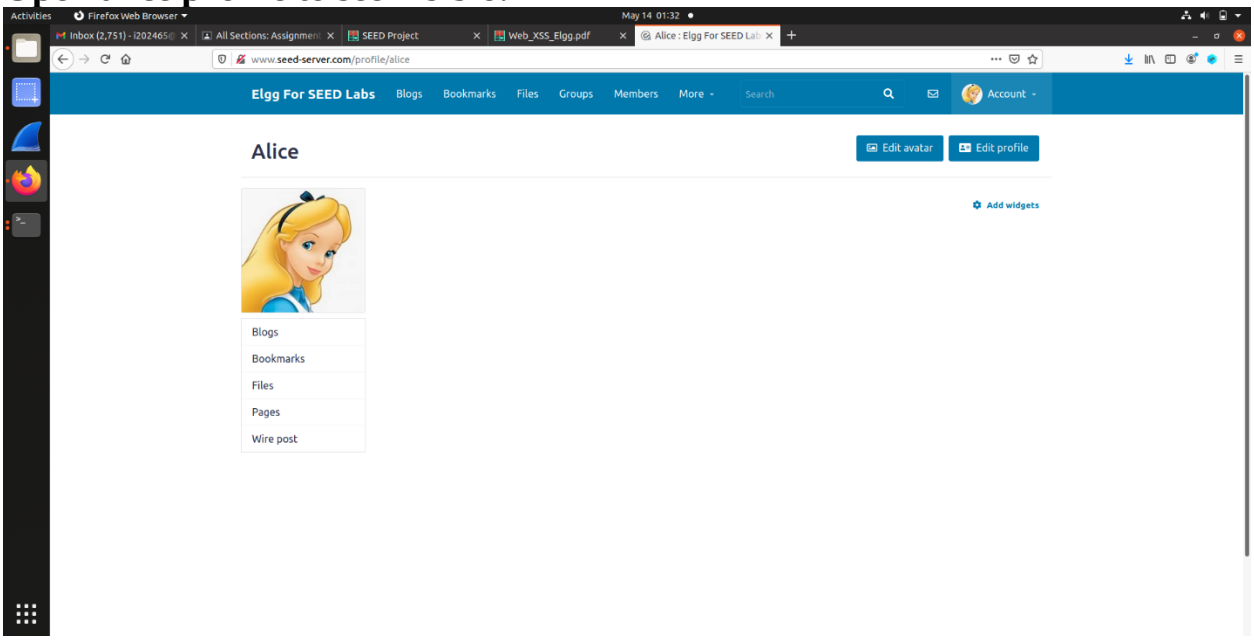


Now open samy profile to clearly see attack.

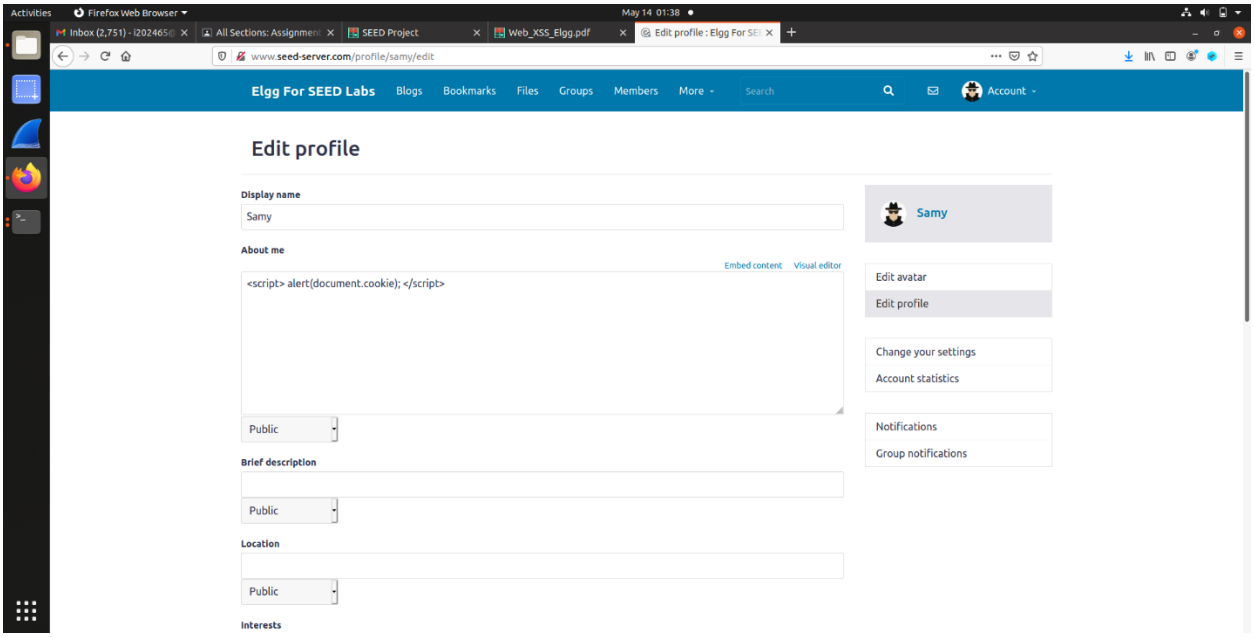


Task 3:

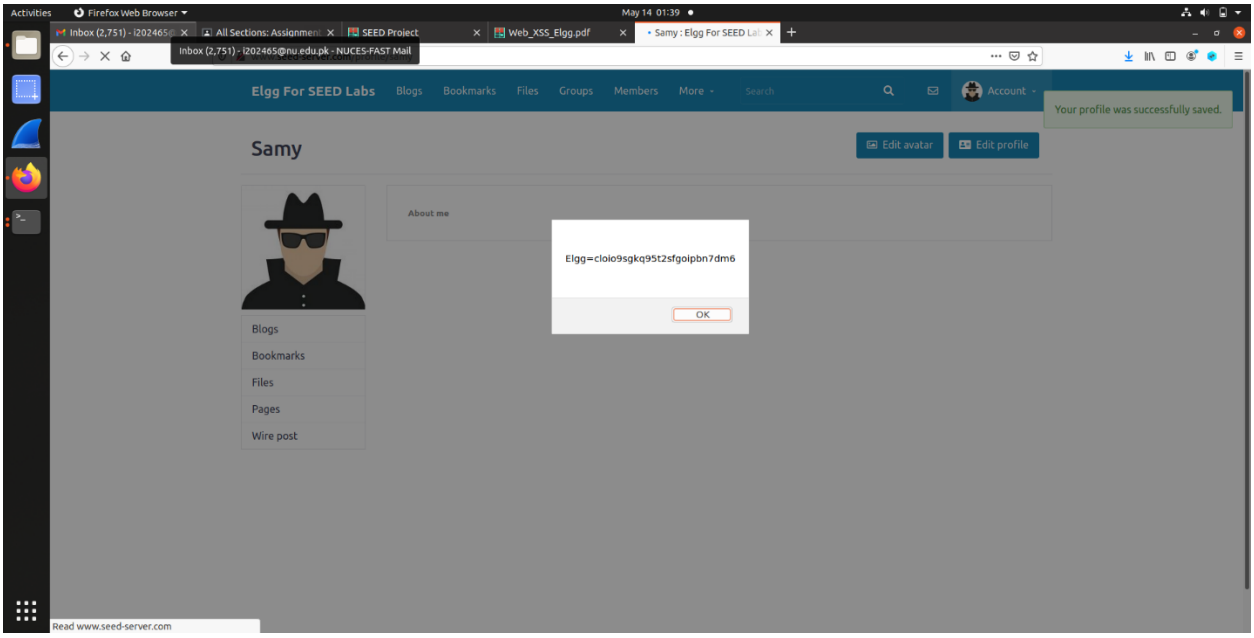
Open alice profile to see his bio.



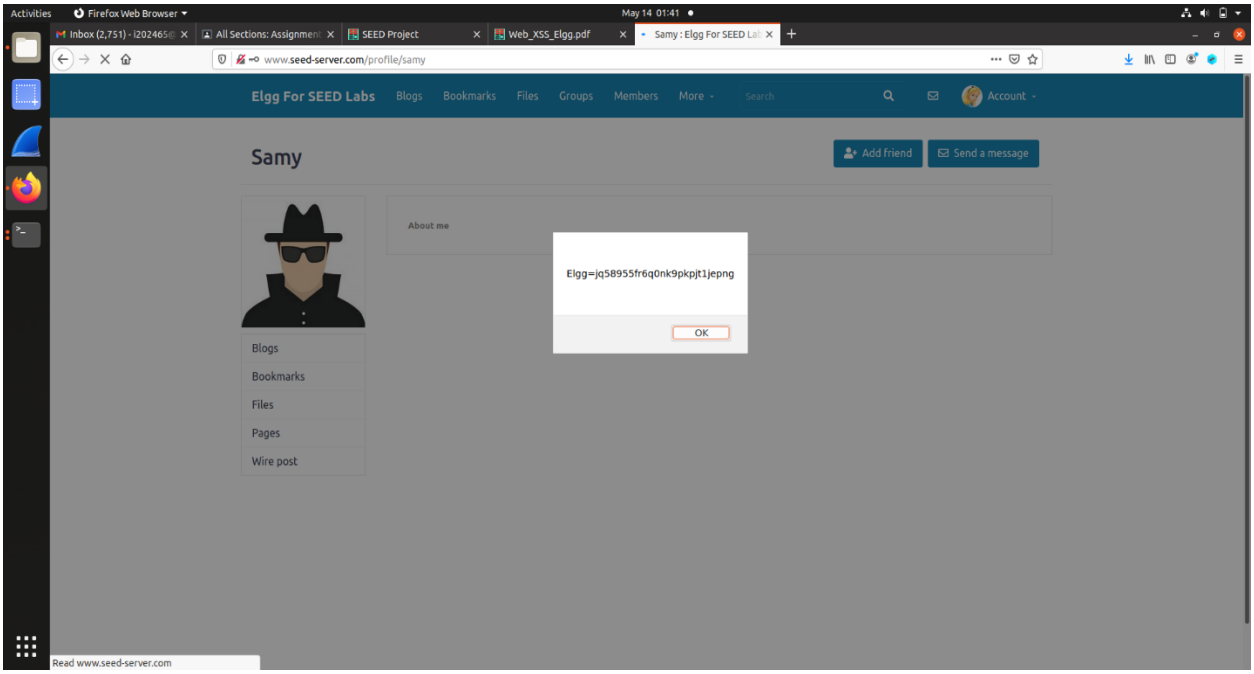
Samy edited his about me to do attack.



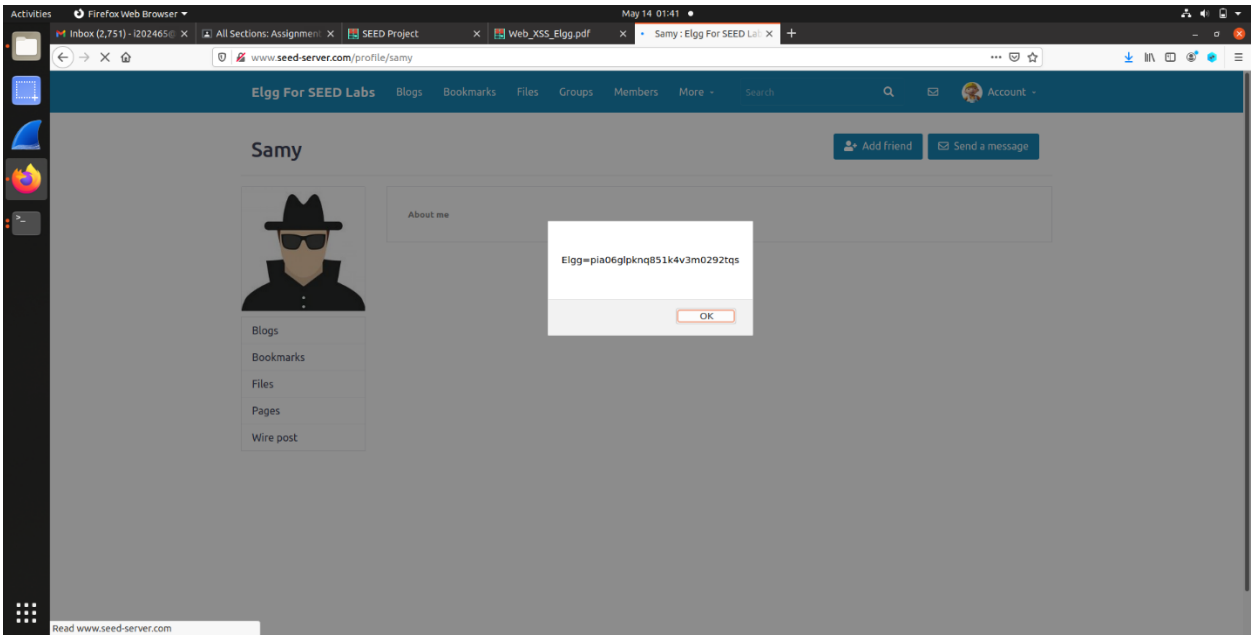
Now, Samy displays his cookies after attacking on his account.



Now, Alice displays his cookies after attacking by his account.

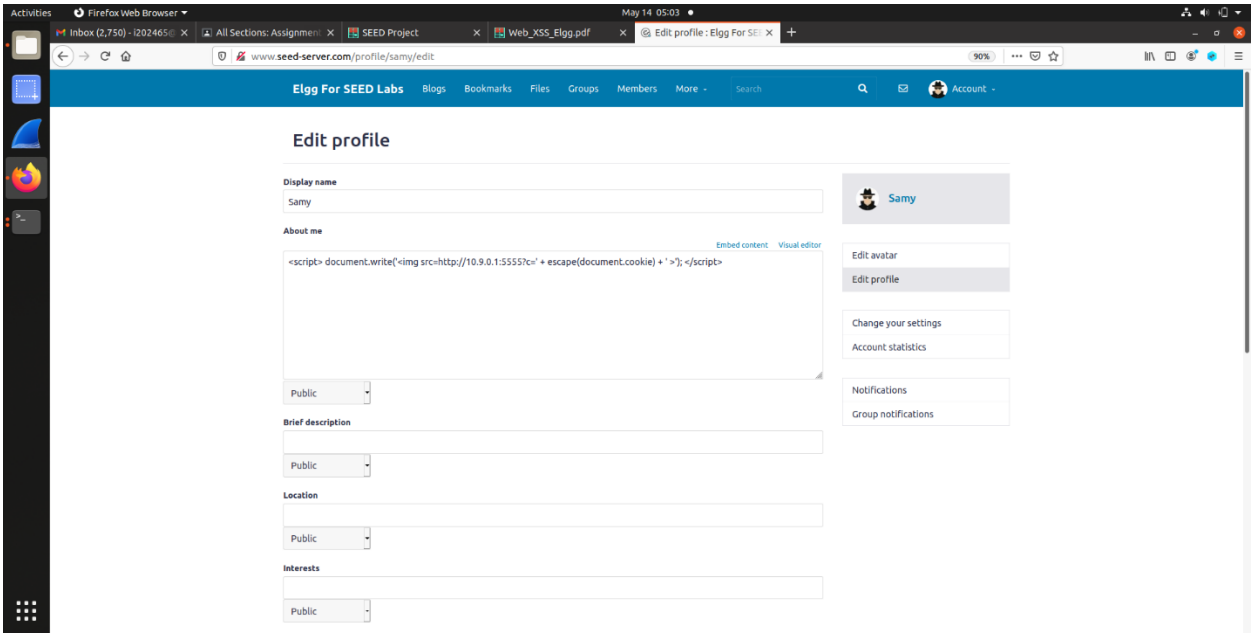


Now, Charlie displays his cookies after attacking his account.

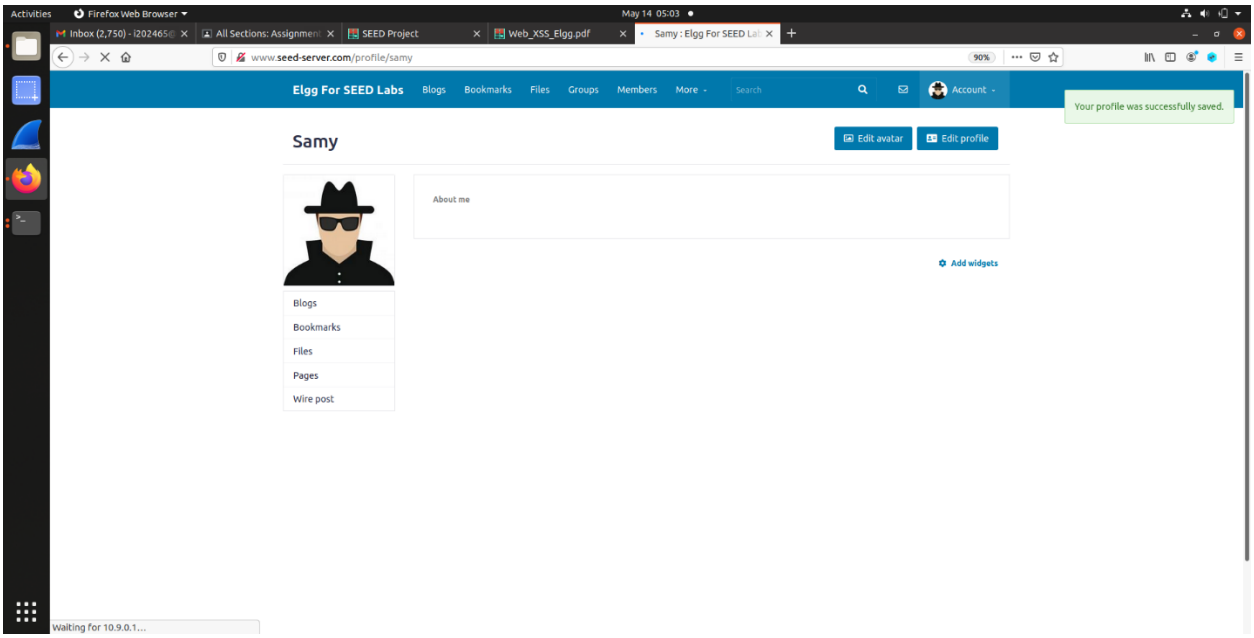


Task 3:

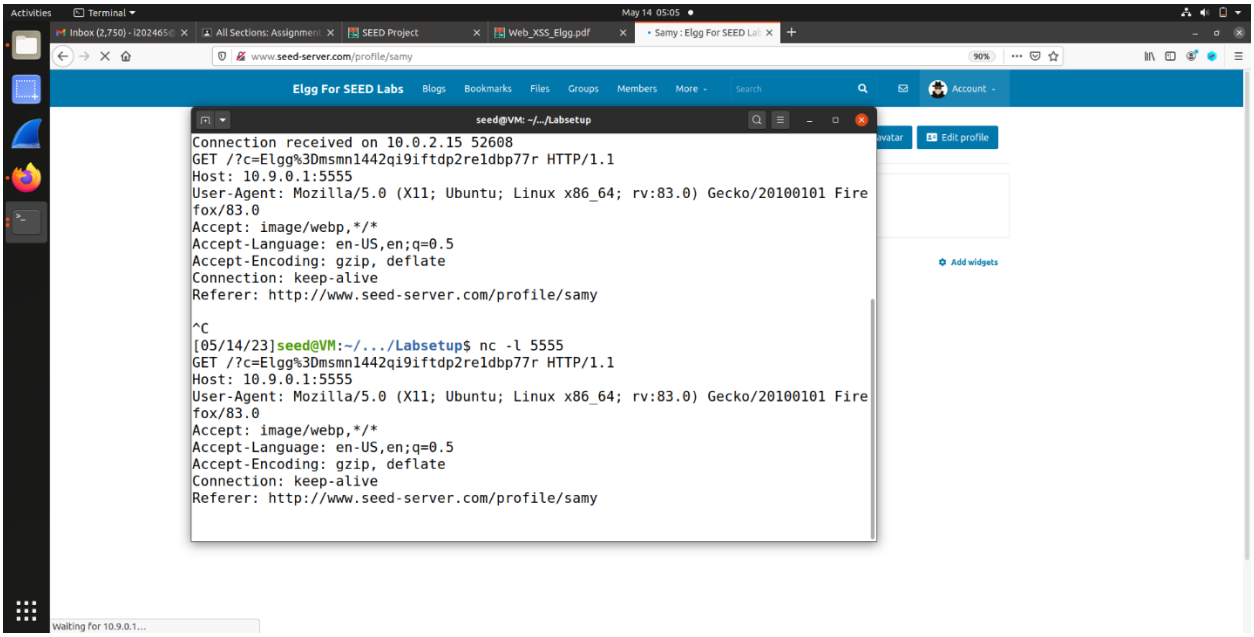
Firstly, these are the Samy Profile details and print details by command line.



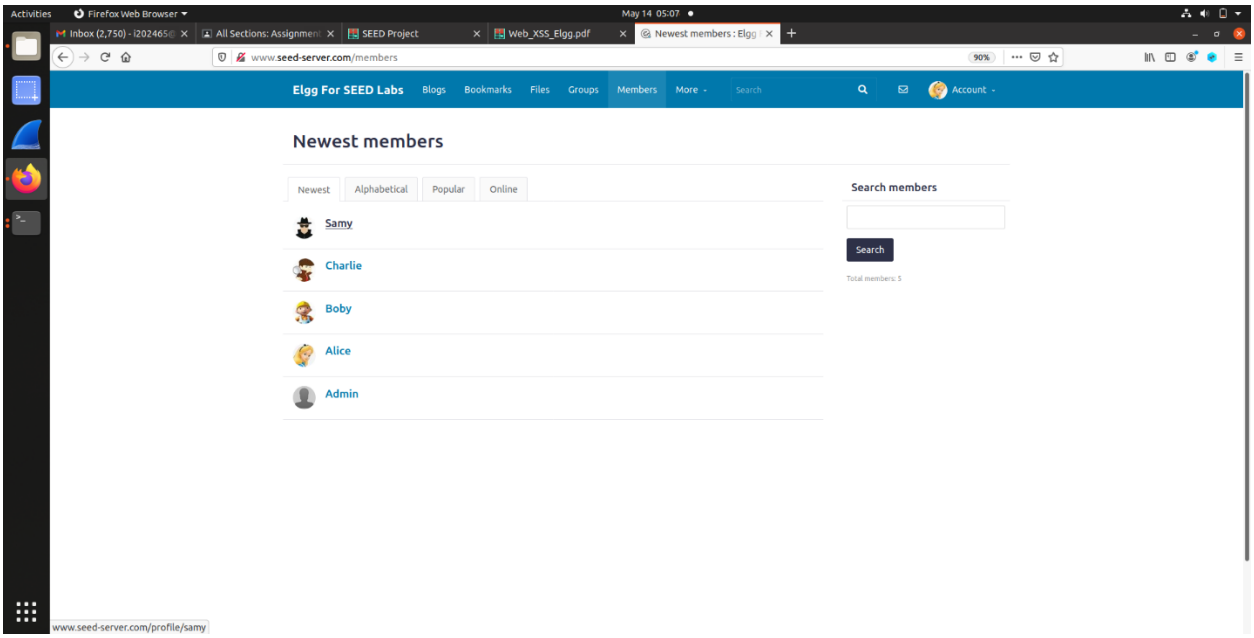
All the files are saved and attack is launch.



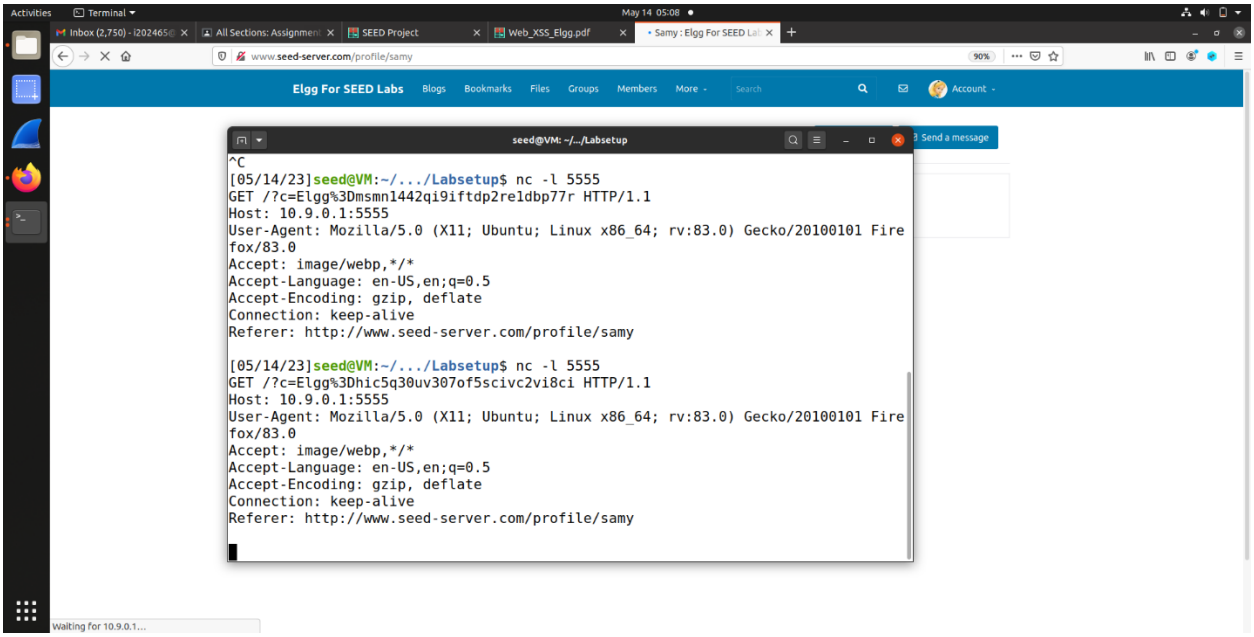
Now you can check, the packets are captur and details are here.



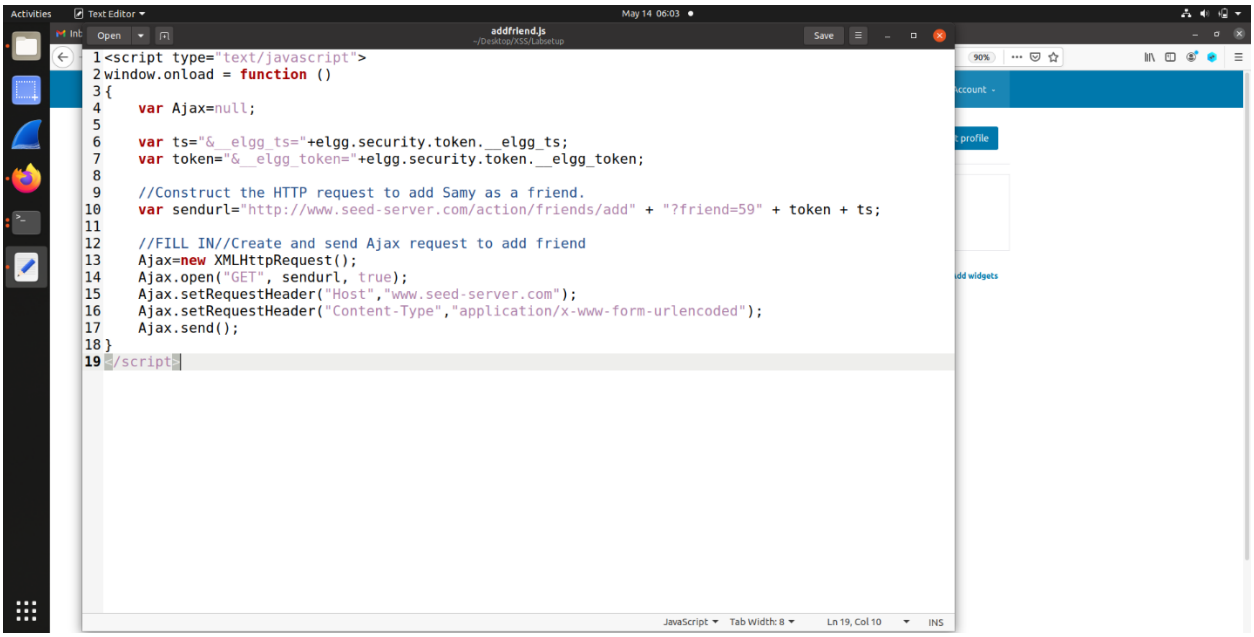
Now open the samy profile from the alice account.



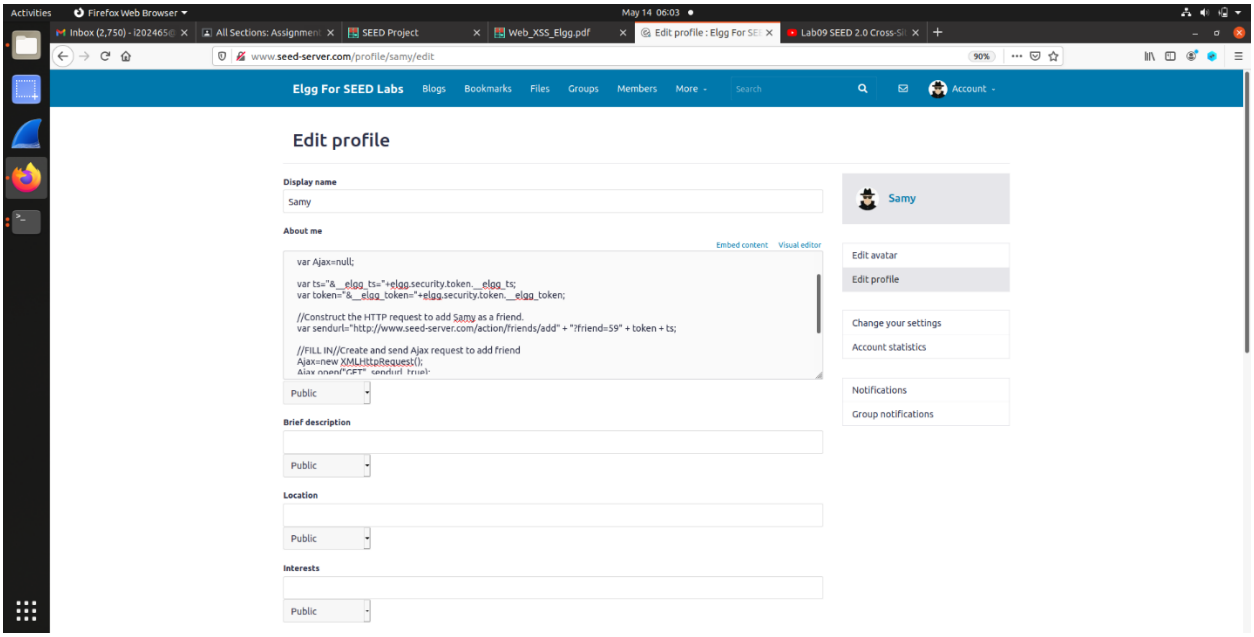
This is the packets details in the alice profile.



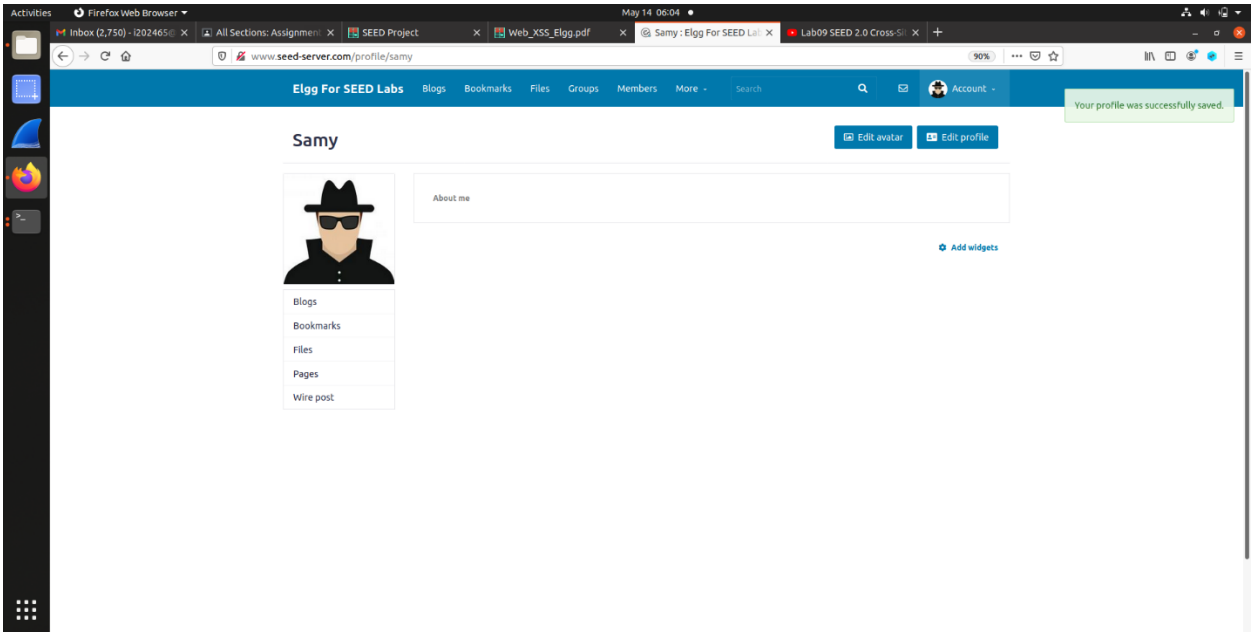
Task-4: Now add the samy by just clicking on alice account members list.



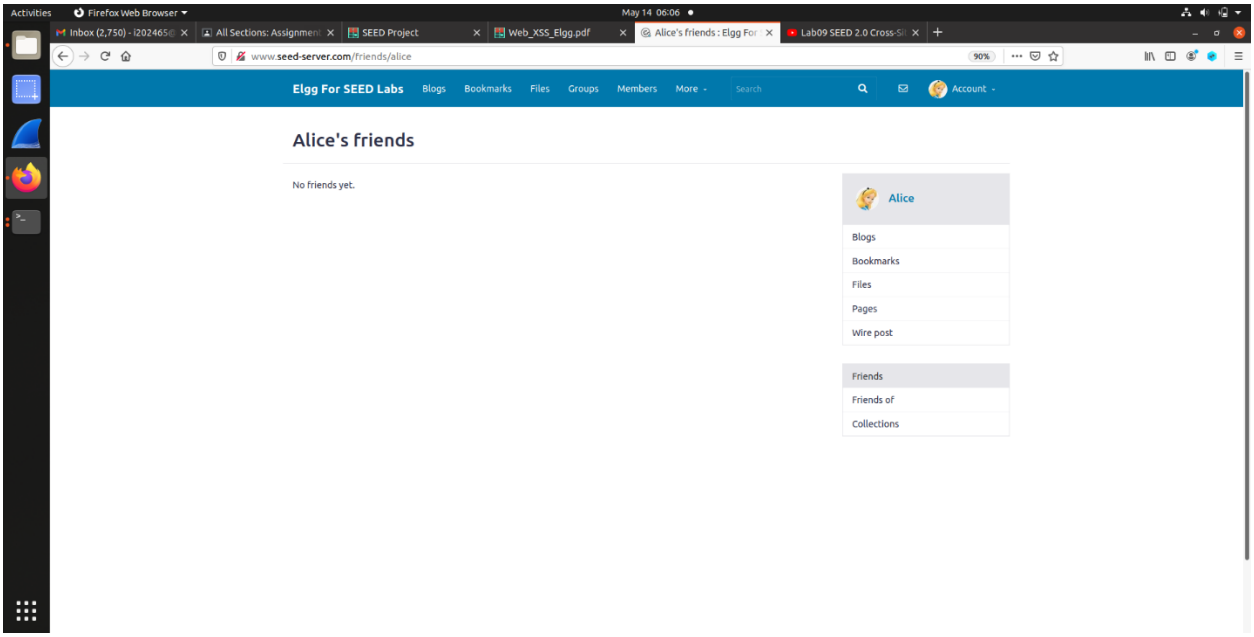
To add the code in the about me of samy account that is shown above.



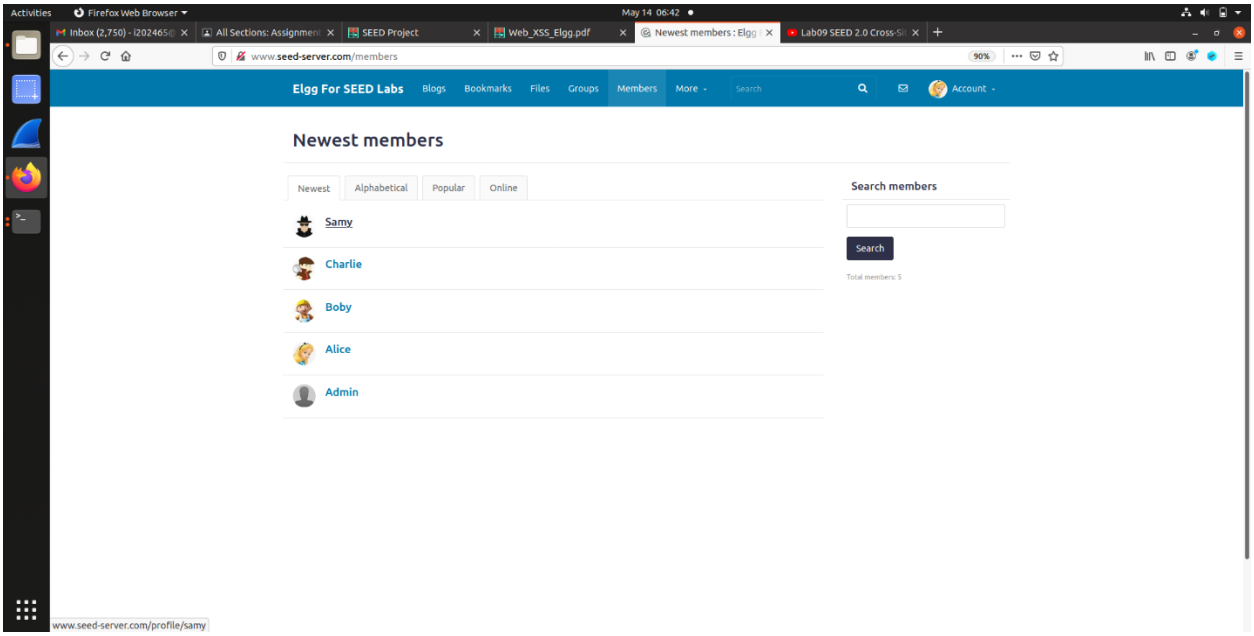
Now, save the changes launches the attack.



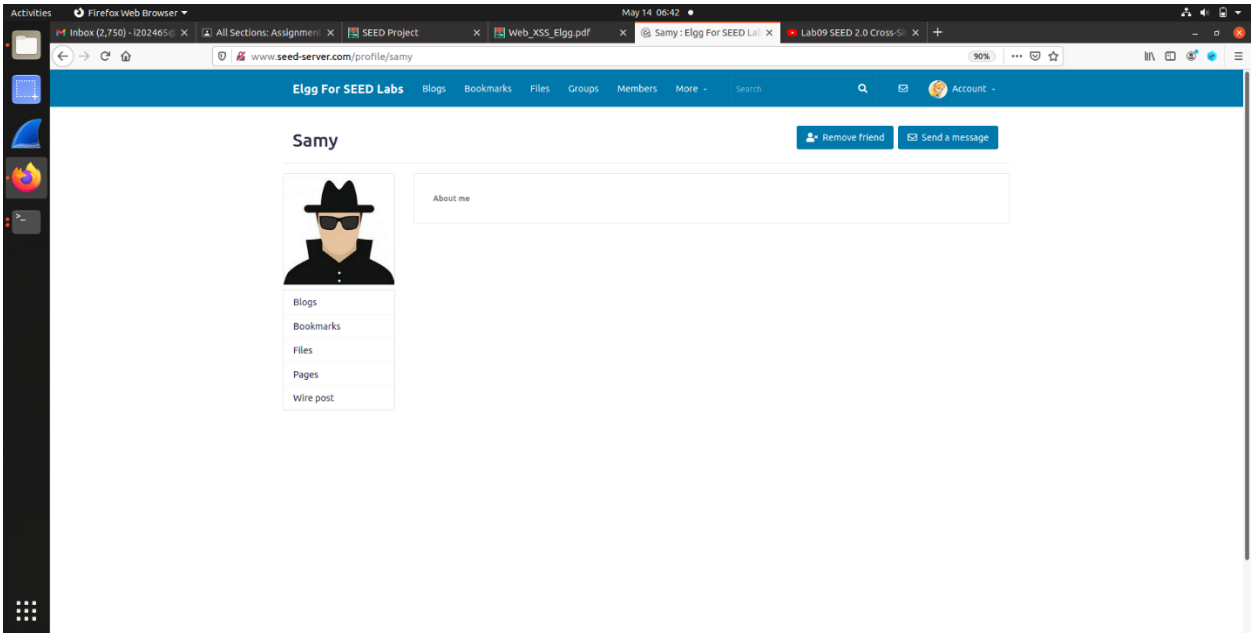
This is the Alice profile there is nothing here.



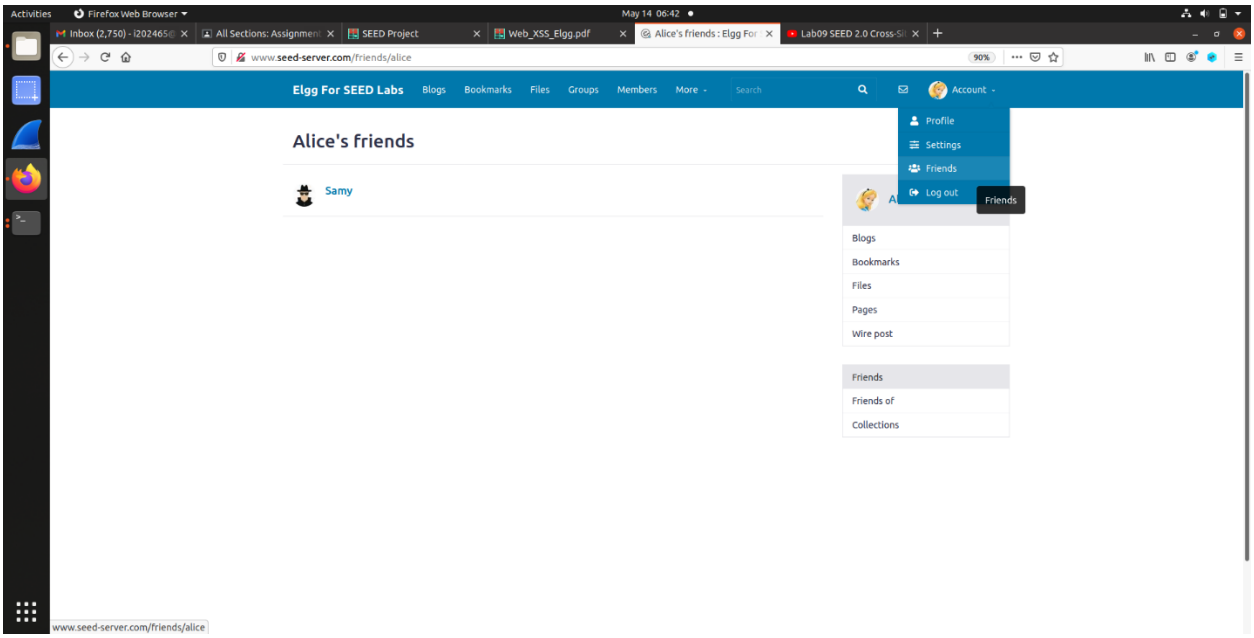
Open the members in the Alice account.



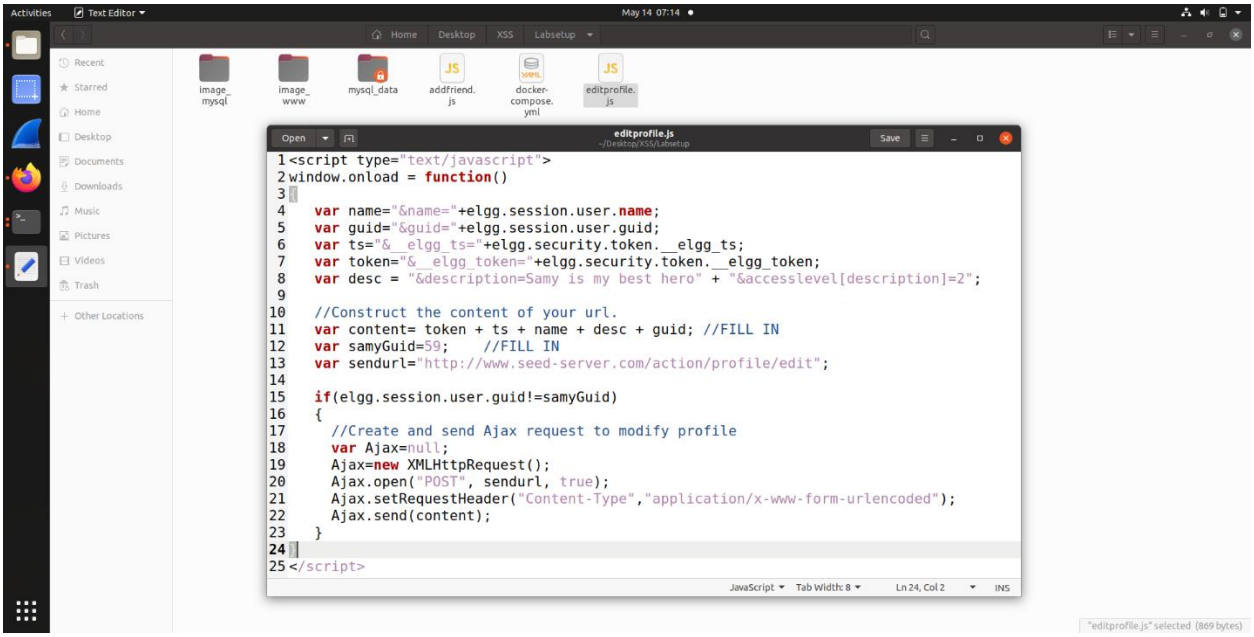
Click on the samy profile.



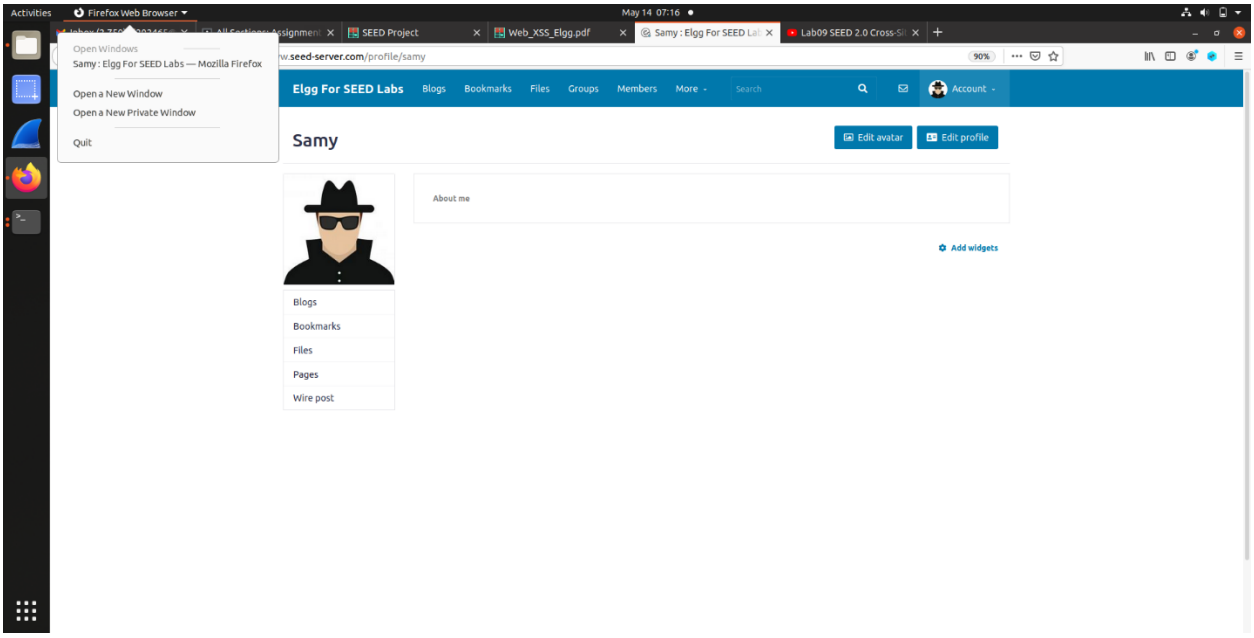
When click on the friends, it shows the samy as friend of alice.



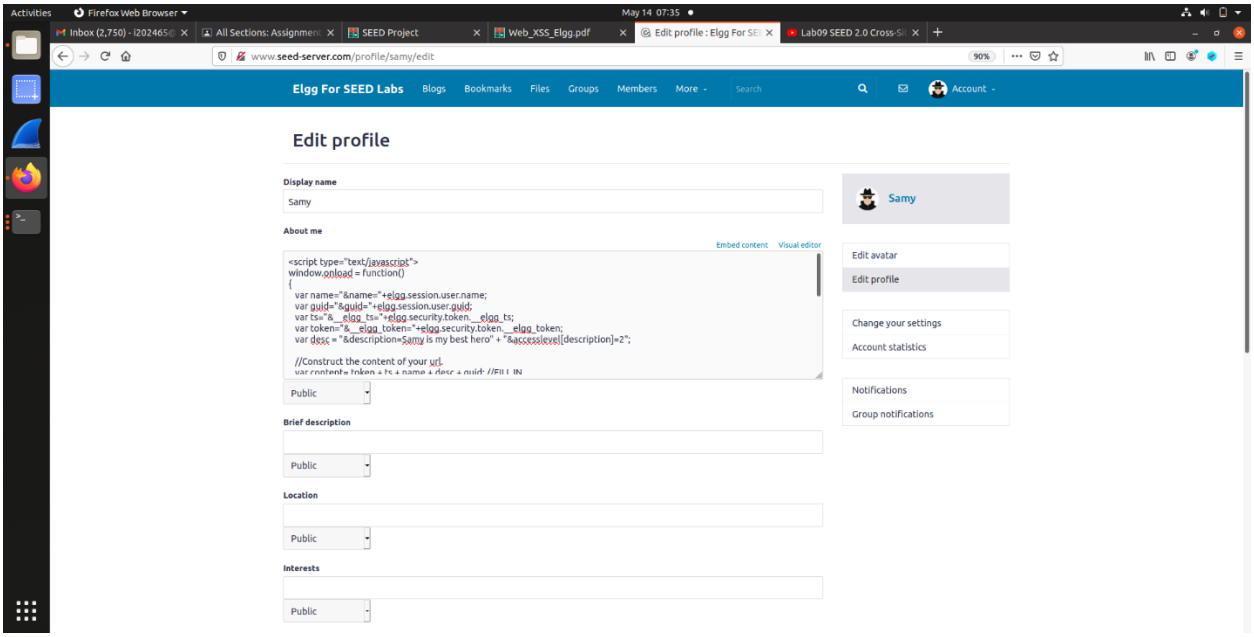
Task 5: check the victim of the attacker.



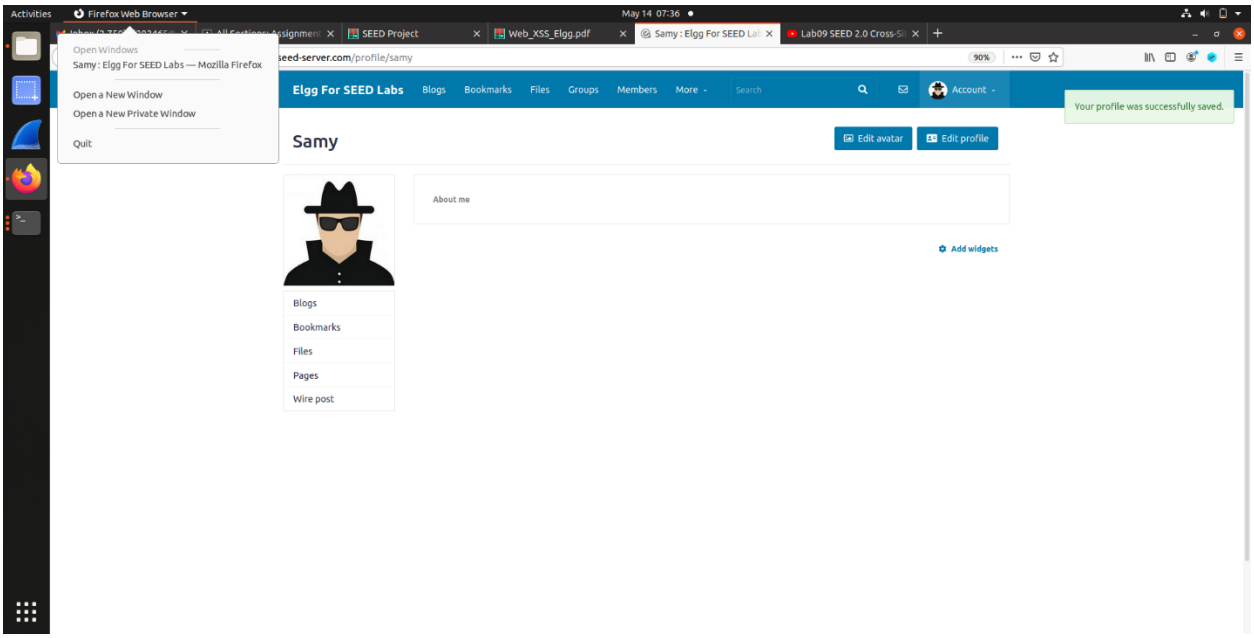
This is the samy profile.



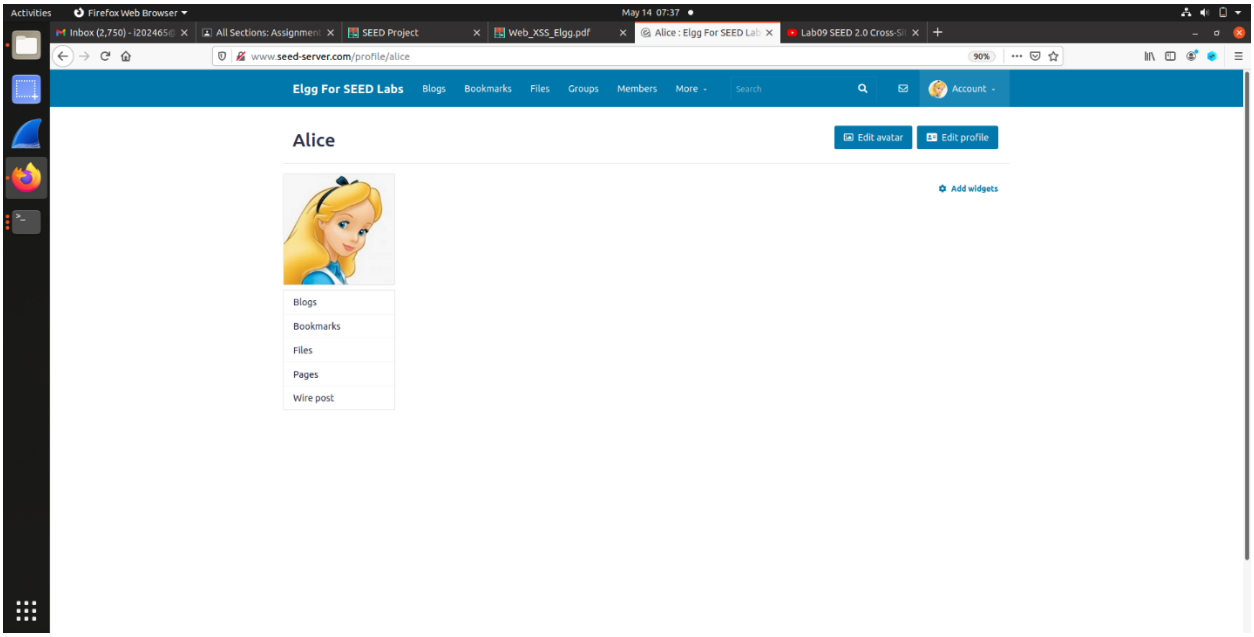
Now, add the code to the bio of the samy.



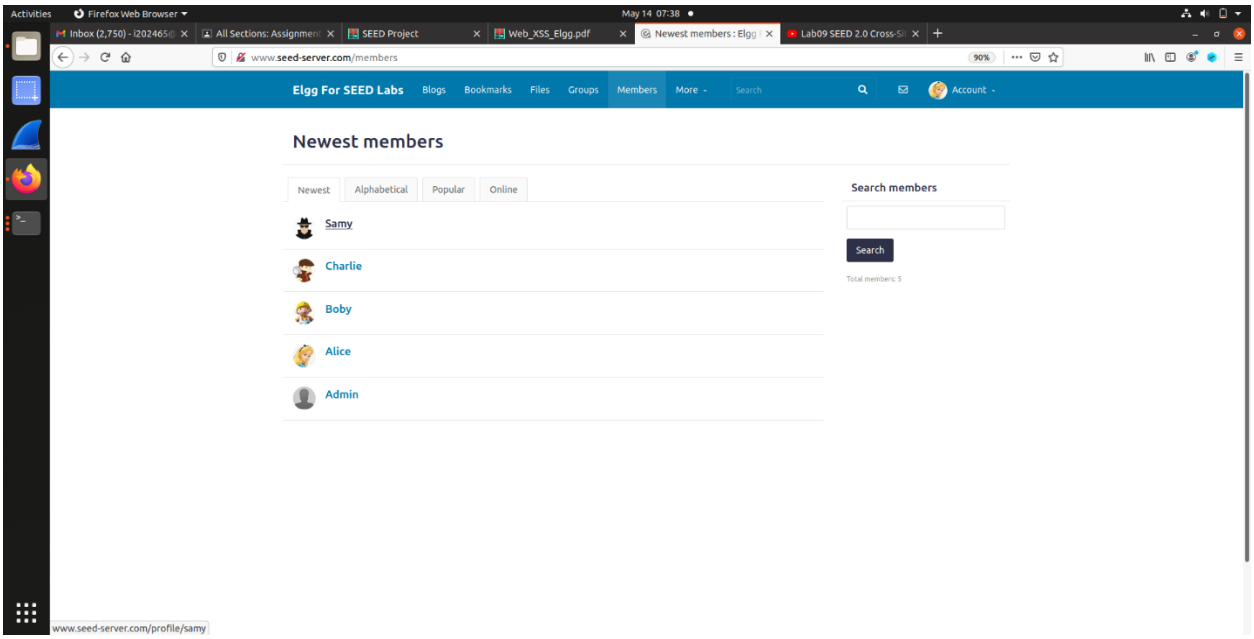
Now, changes are saved.



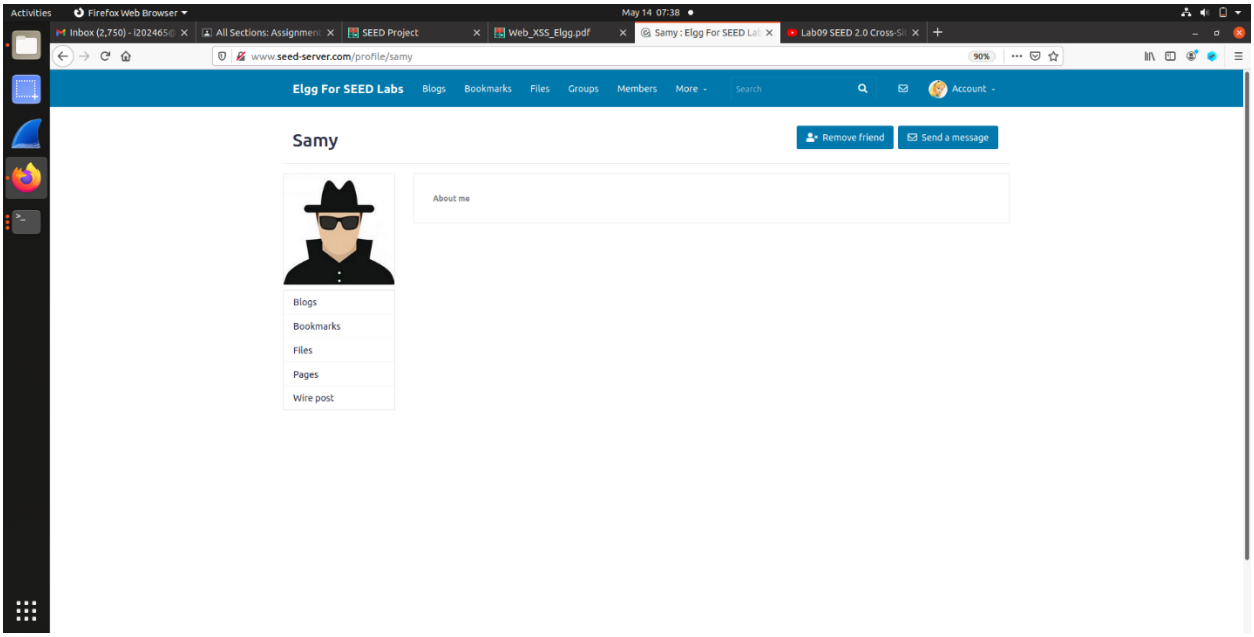
Now, open the Alice account.



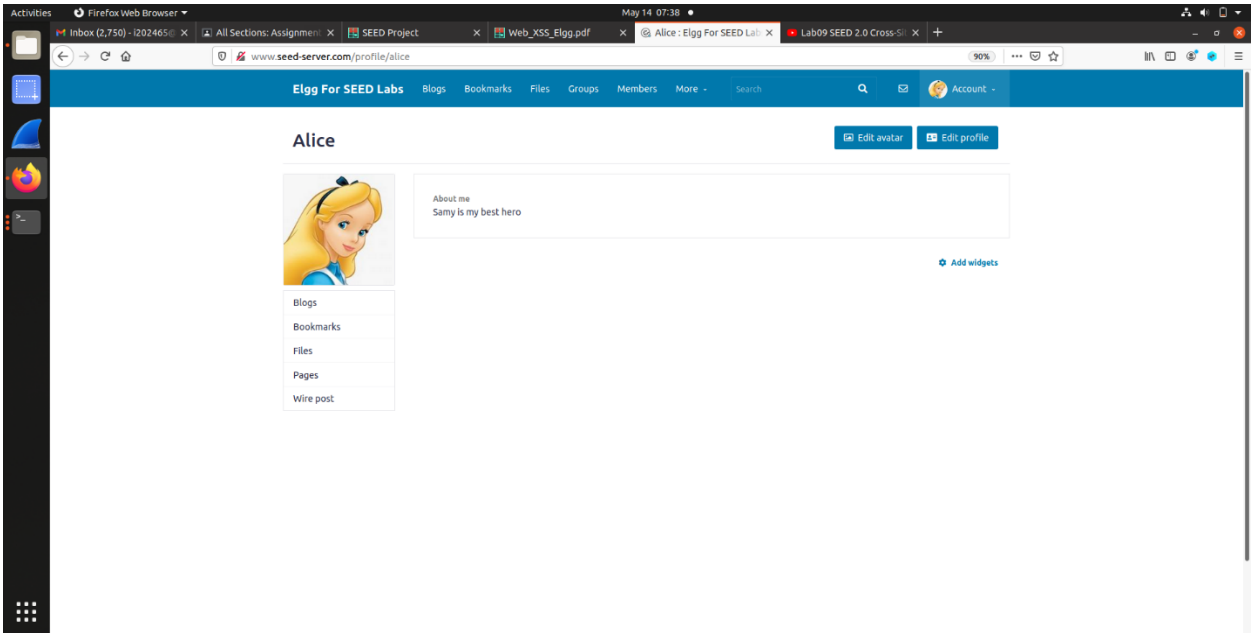
Now, check the members list of the alice.



Click on the samy profile.

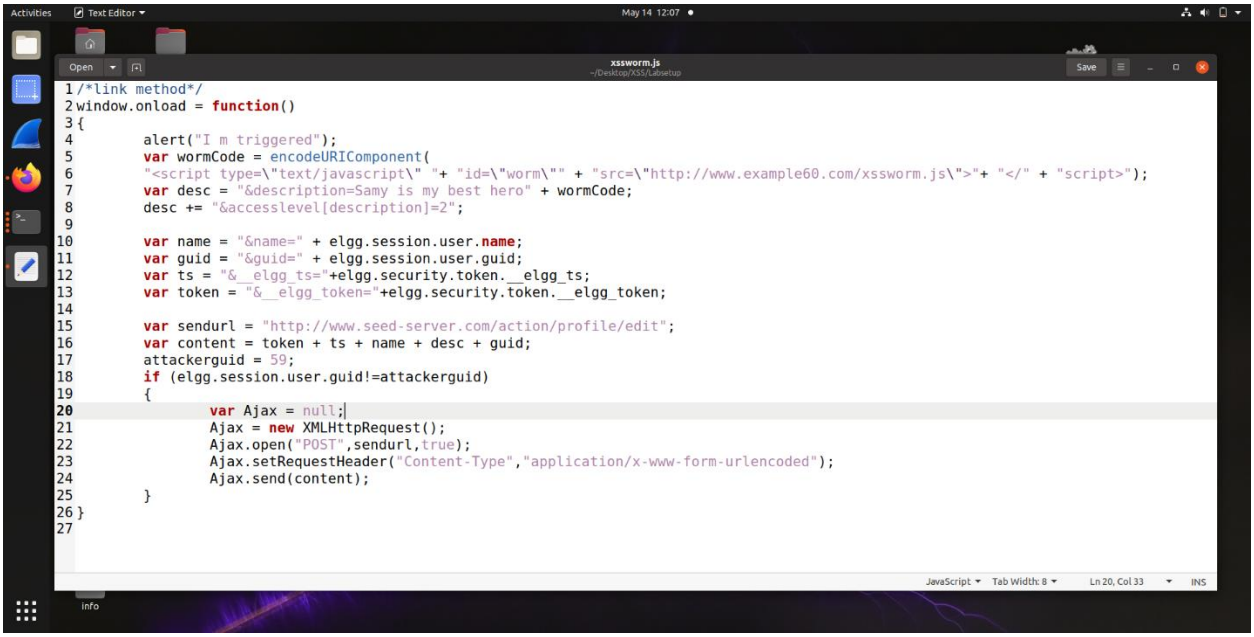


Attack is successfully done, and profile is updated.

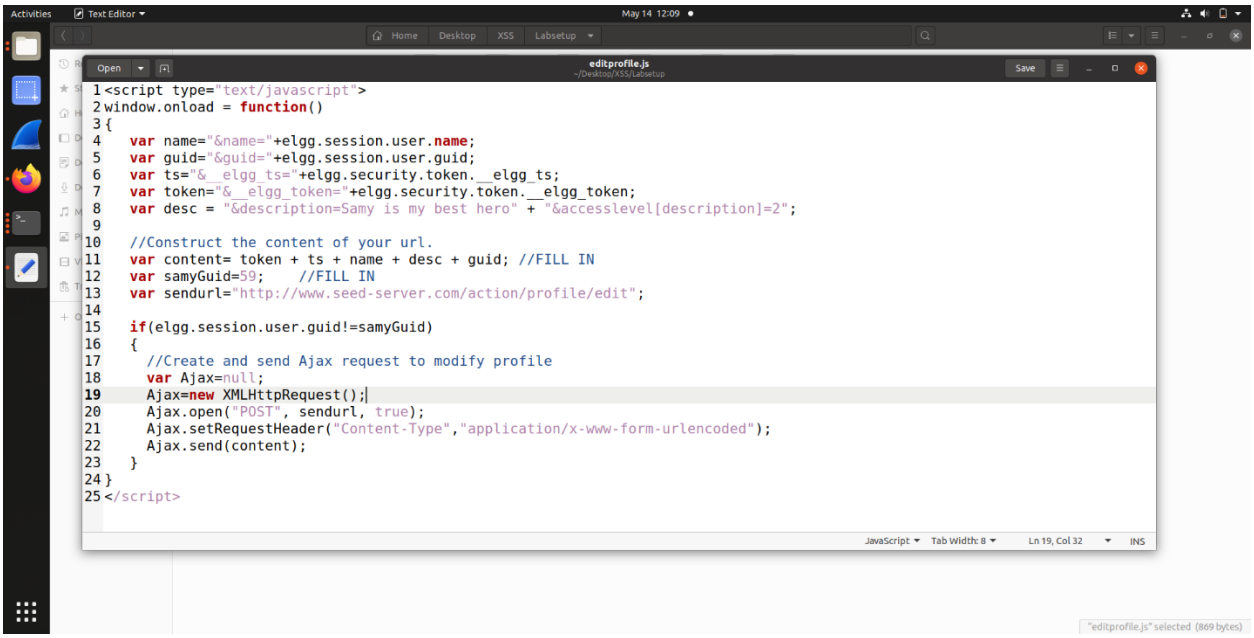


Task-6:

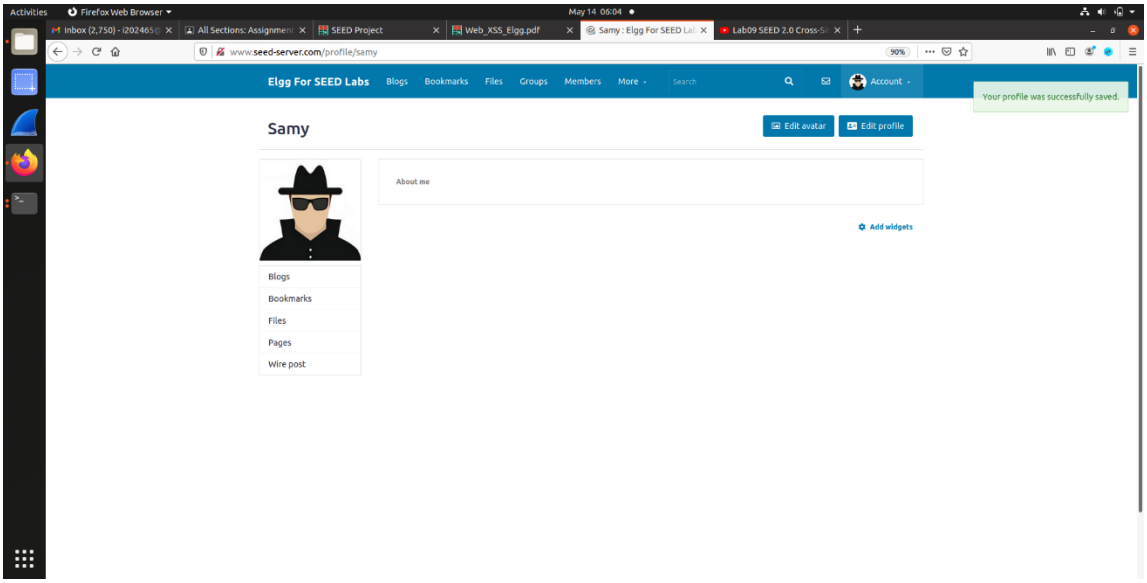
Malicious Codes are written in the JavaScript, and both are shown below.



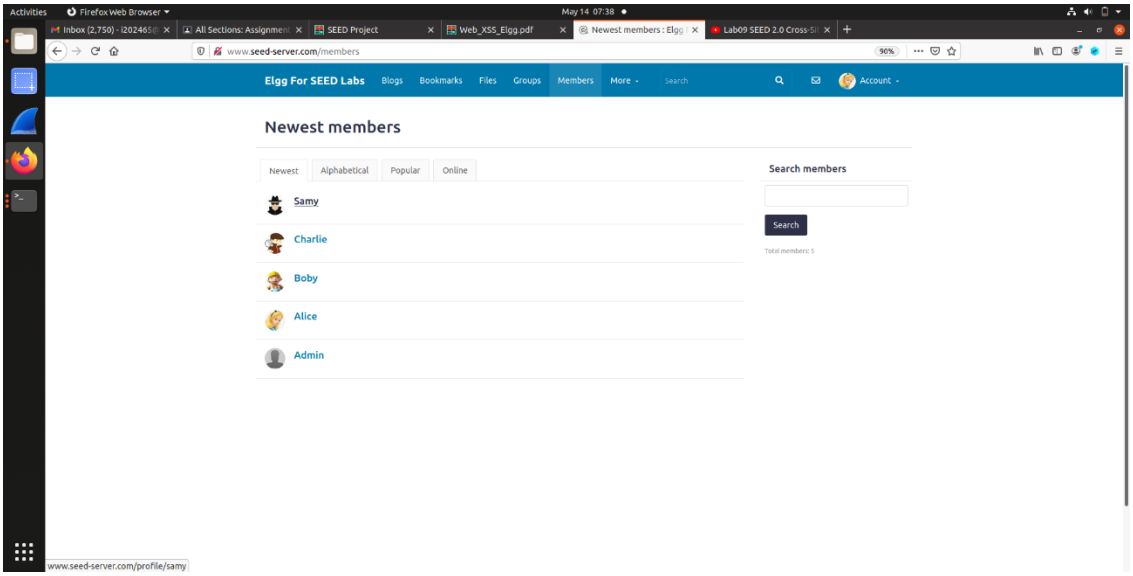
This is the worm and edited profile of the code.



All the changes are saved.



Now, open the Alice Account and



Work Division:

Name	Roll No	Work Division
Zeeshan Ali	20i-2465	SQL, CSRF → pre-Task & Task 1,2, 3,4,5,6
Ans Zeeshan	20i-0543	XSS, CSRF → pre-Setup & Task 1,2, 3,4,5,6