Information Security

Assignment # 04

CSRF 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

CSRF Lab using SEED's Lab

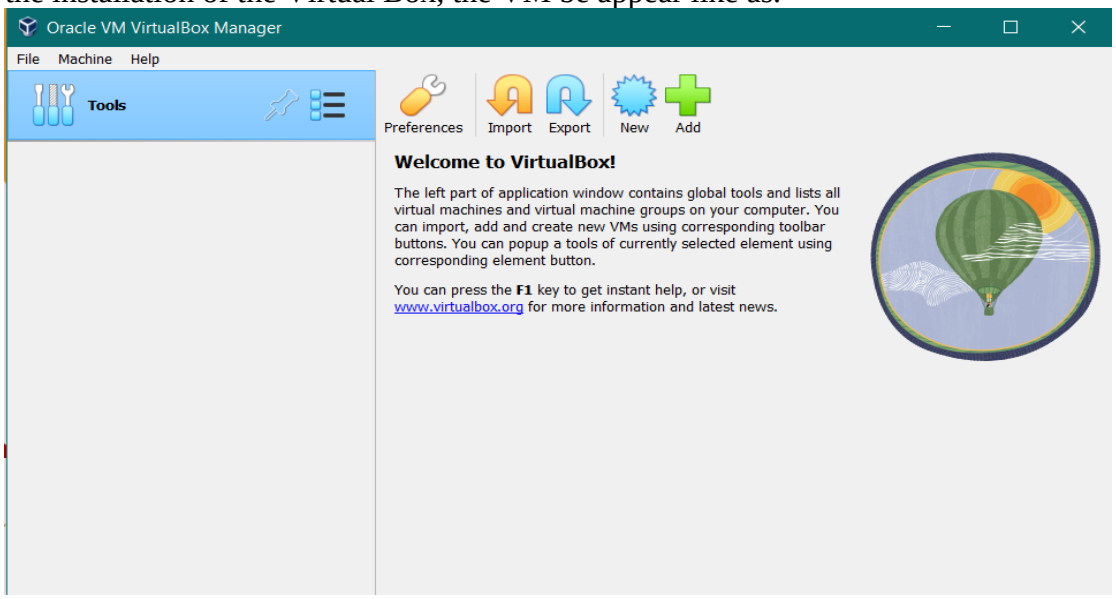
1- CSRF Lab:

Description:

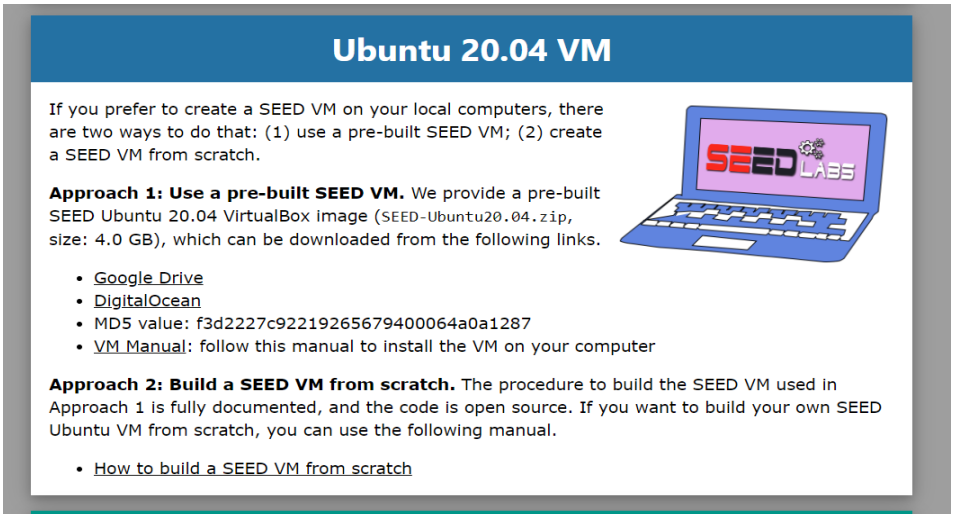
To starting, the Installation requirements are.

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

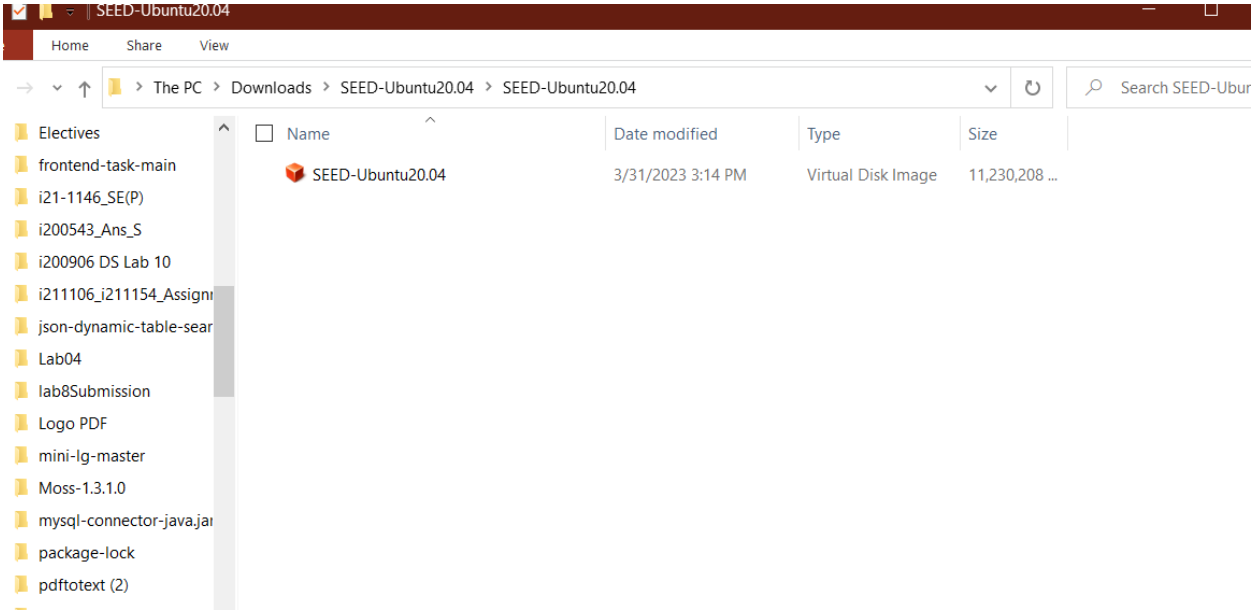
After the installation of the Virtual Box, the VM be appear like as.



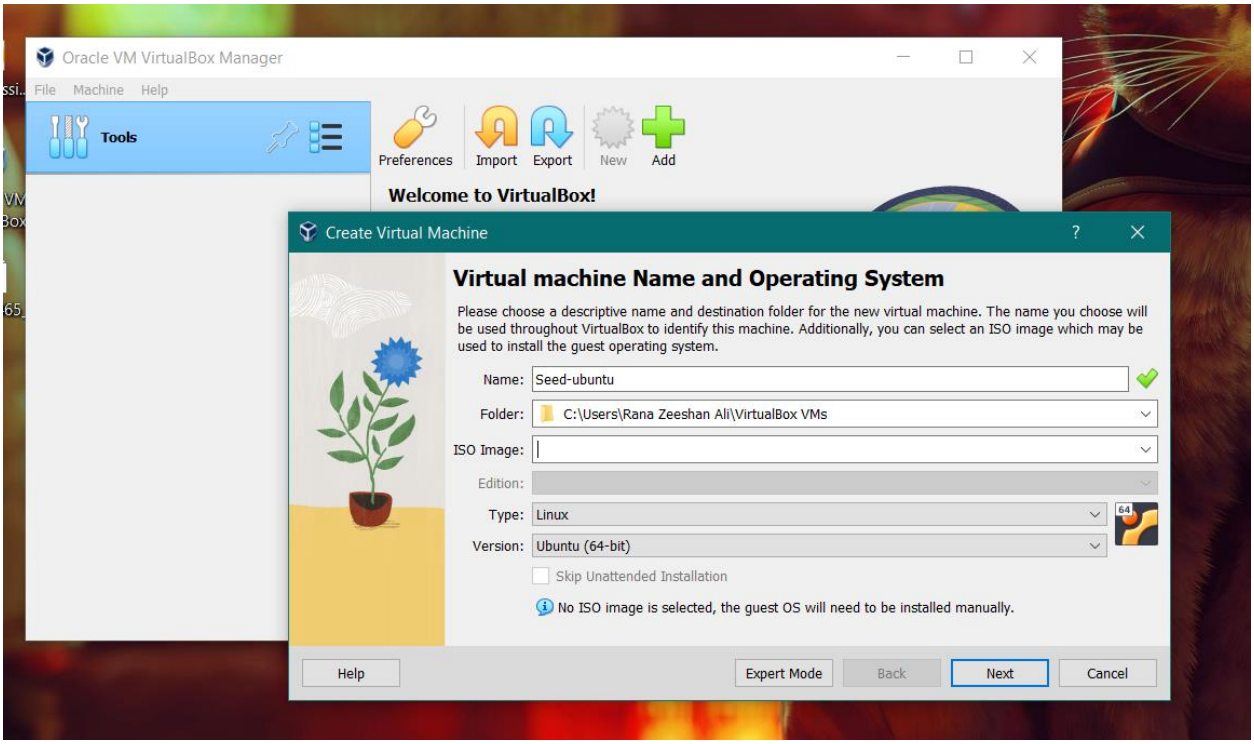
Now, Installing the Seed's Ubuntu, we have selected the version such as Ubuntu 20.04 VM as per requirements in the manual.



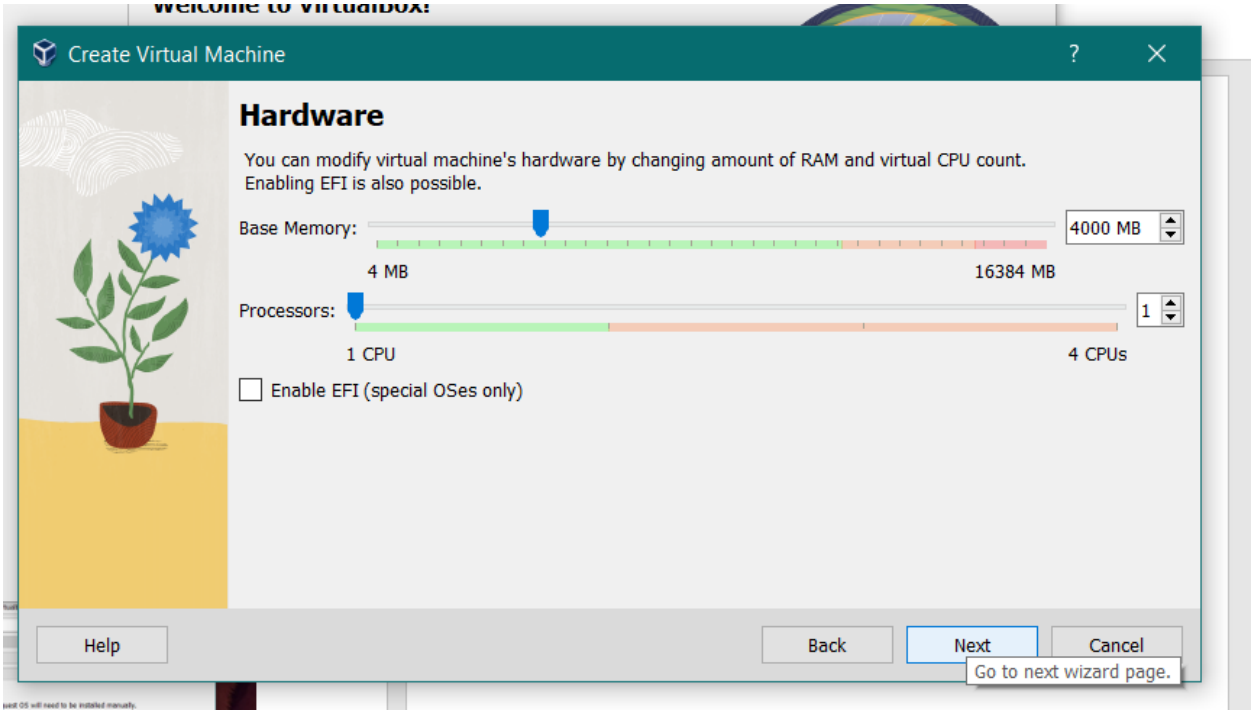
After Downloading and Extracting the zip file of the Ubuntu 20.04, it looks likes.



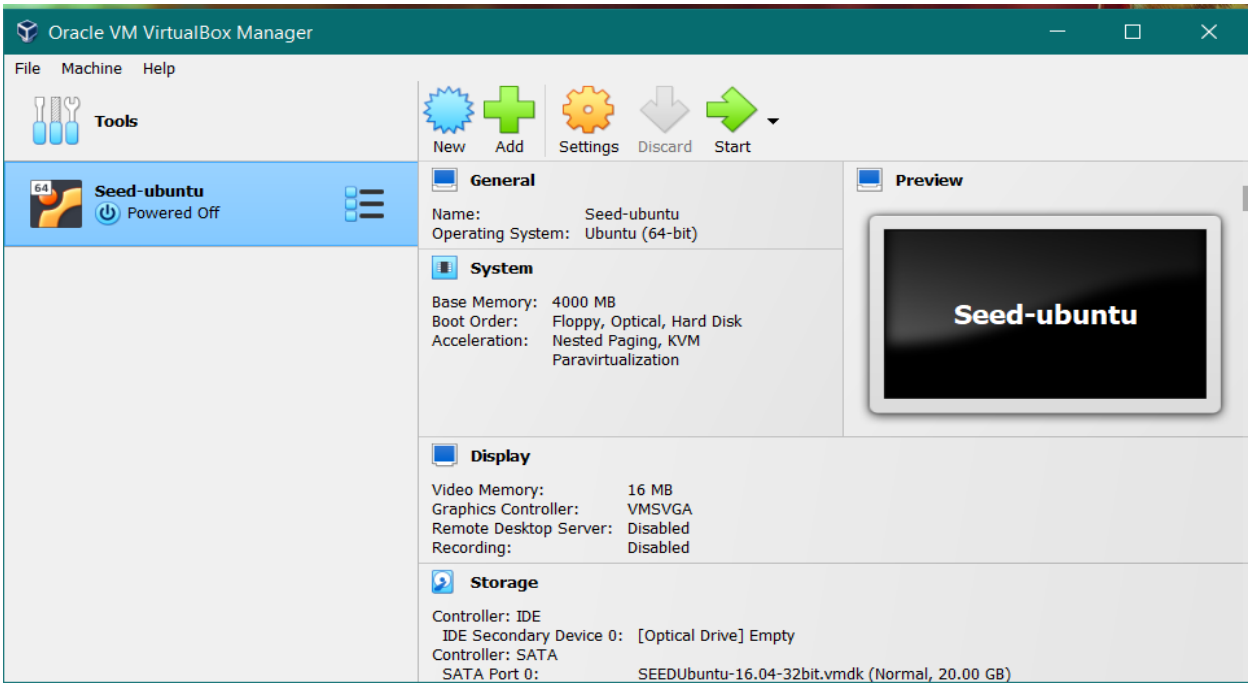
Now, to host the Ubuntu in VM box



Set the Memory Configurations

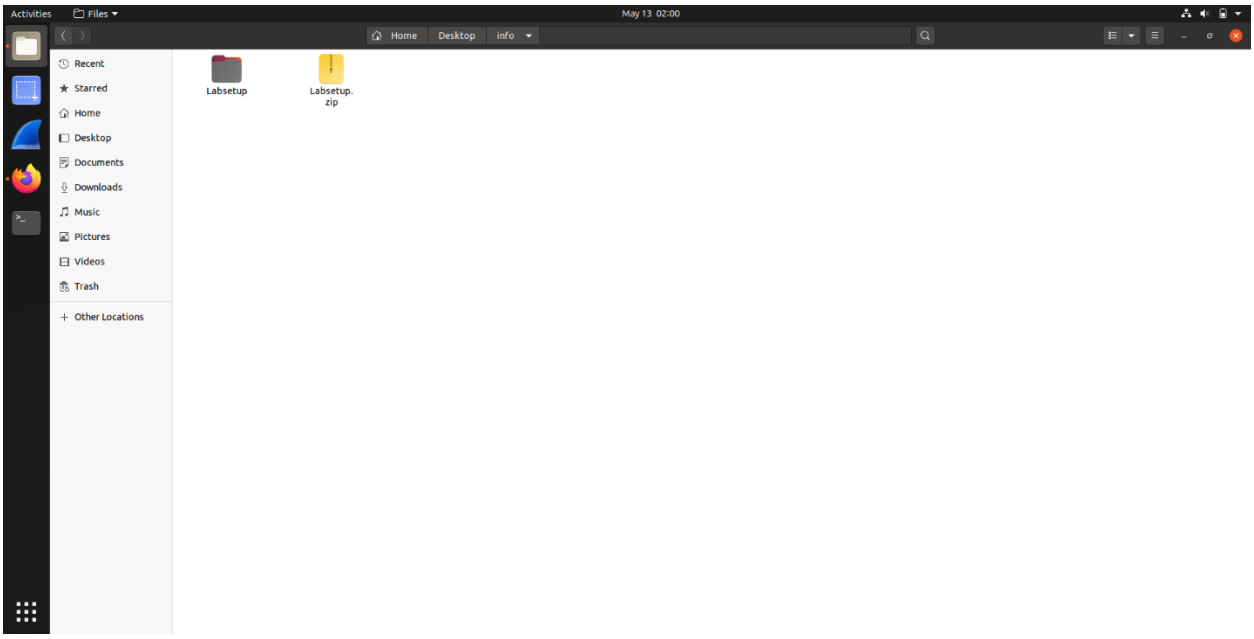


Now, the Ubuntu is successfully hosted.

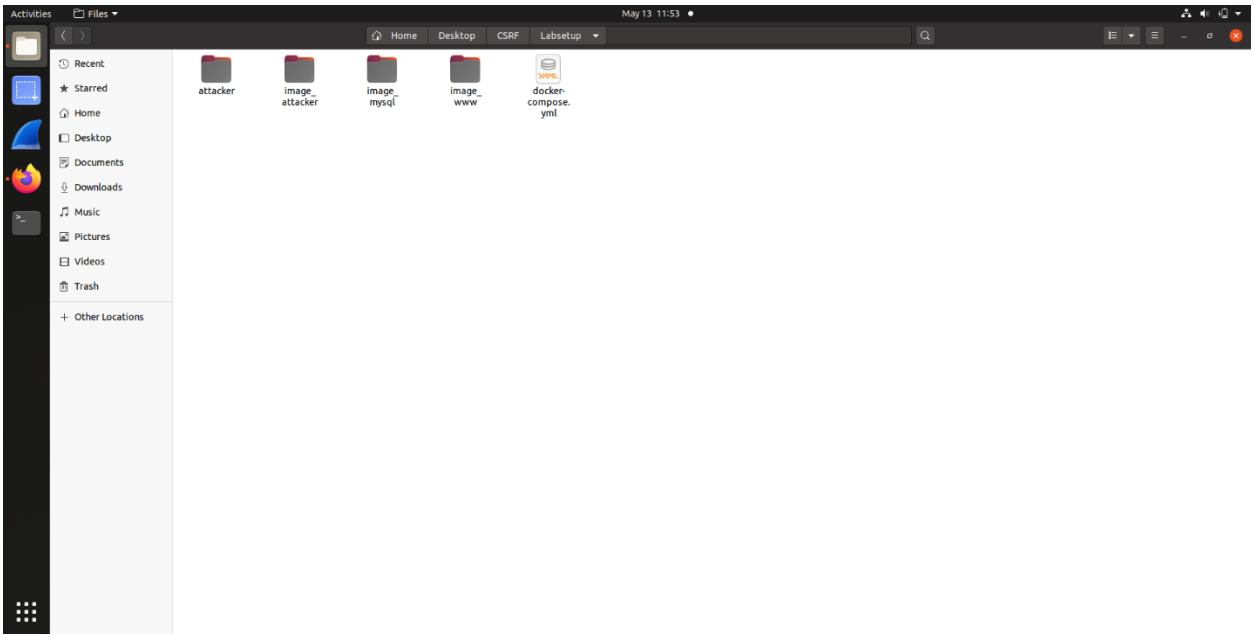


Lab Pre-Requisite Task:

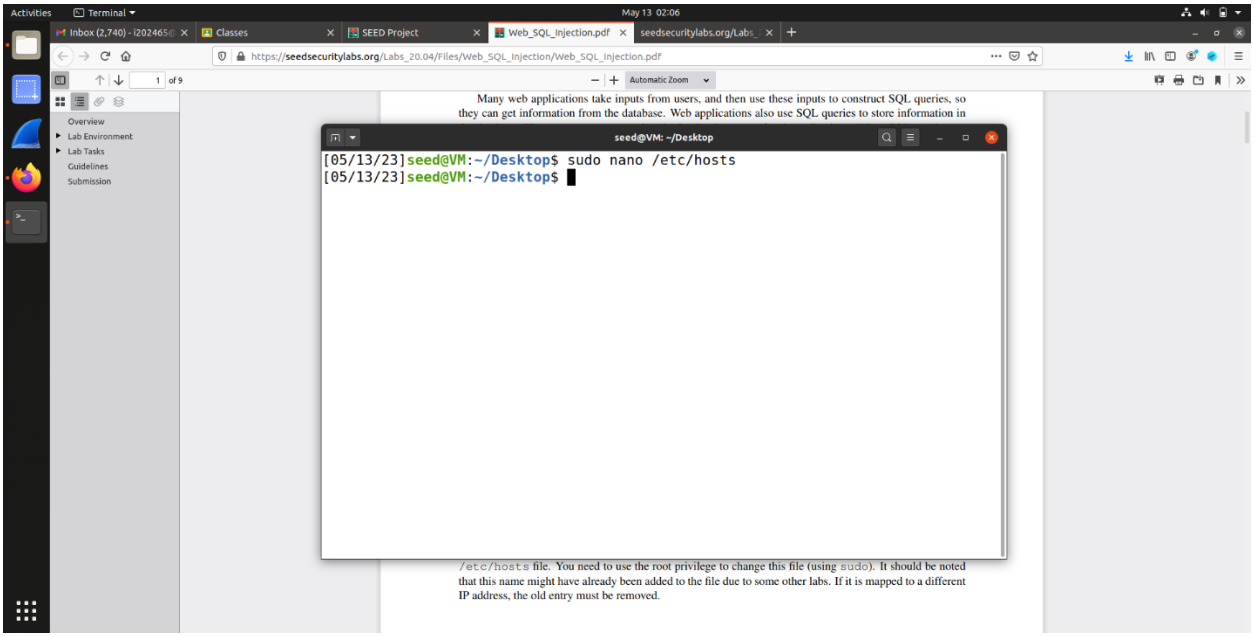
Download the Lab Setup file and extract it.



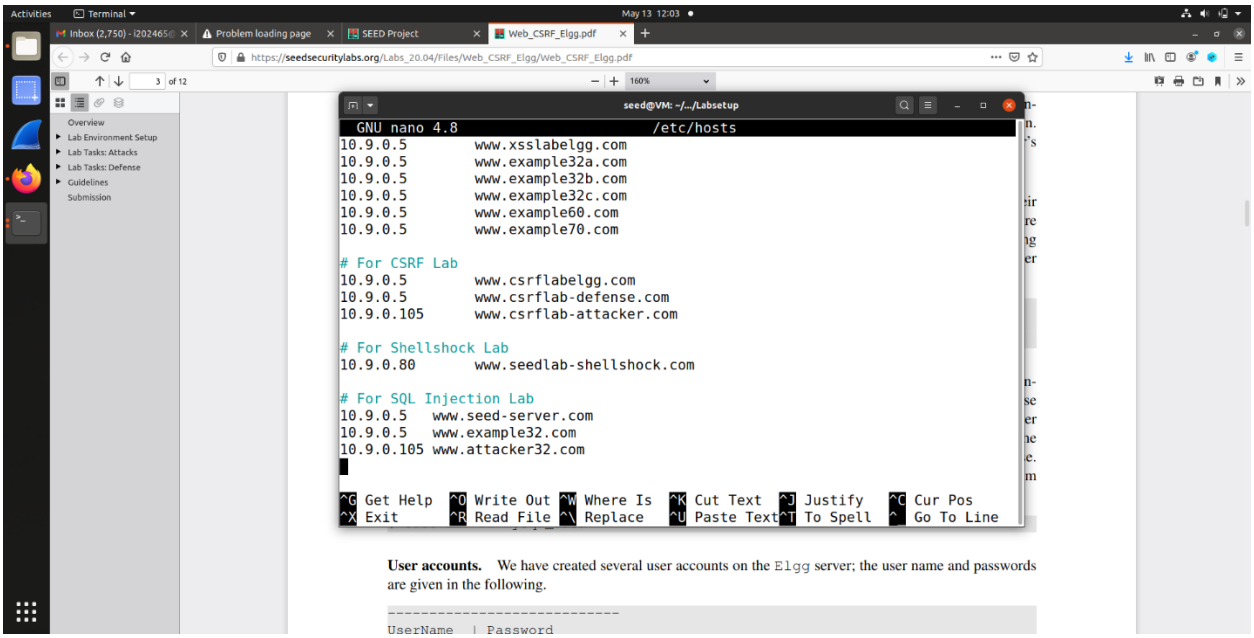
After Extracting, it shows all the file and folders in it.



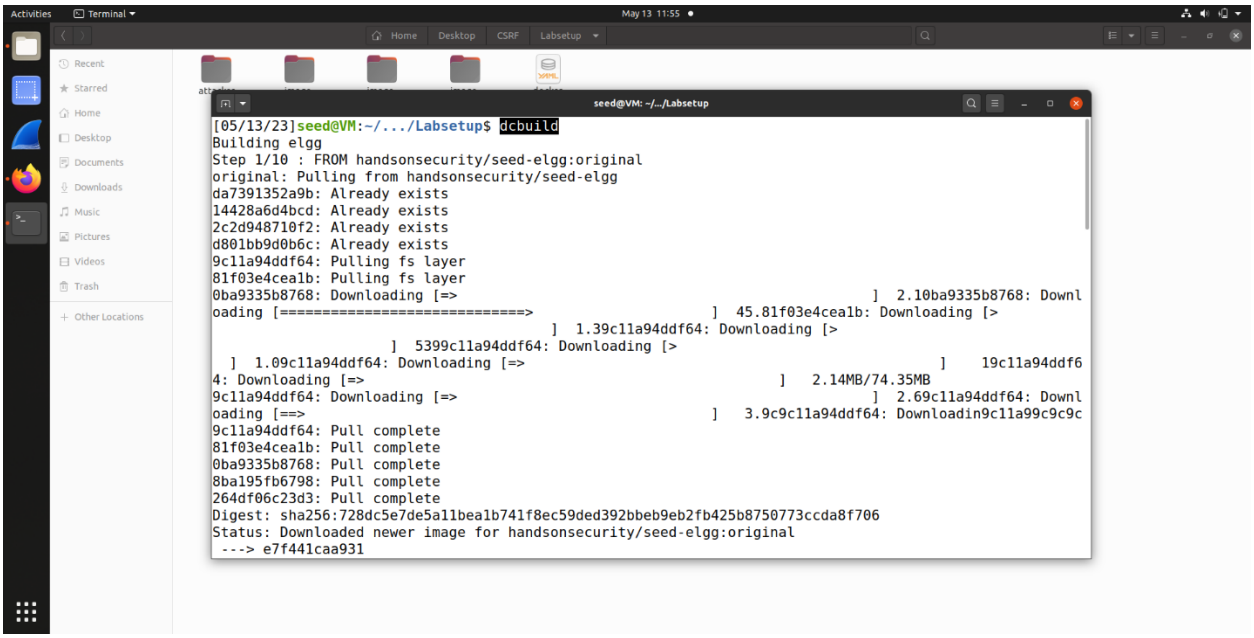
To Assign Ip of seed-server website to run on chrome easily.



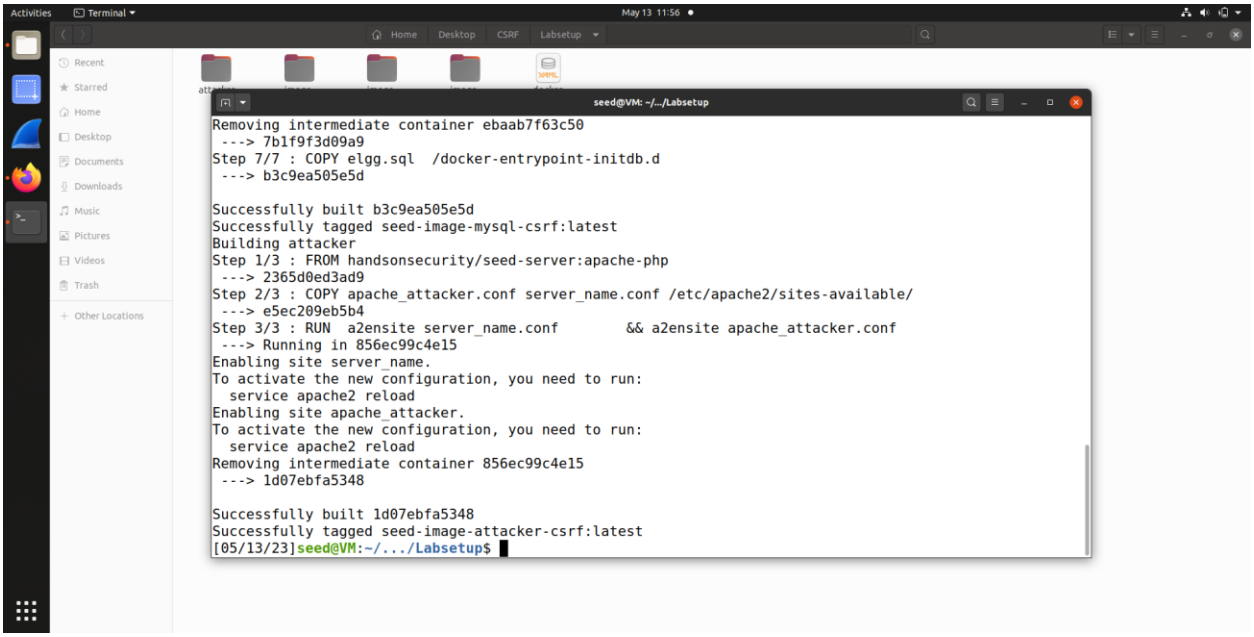
Add manually the website Ip in the file using the command line interface.



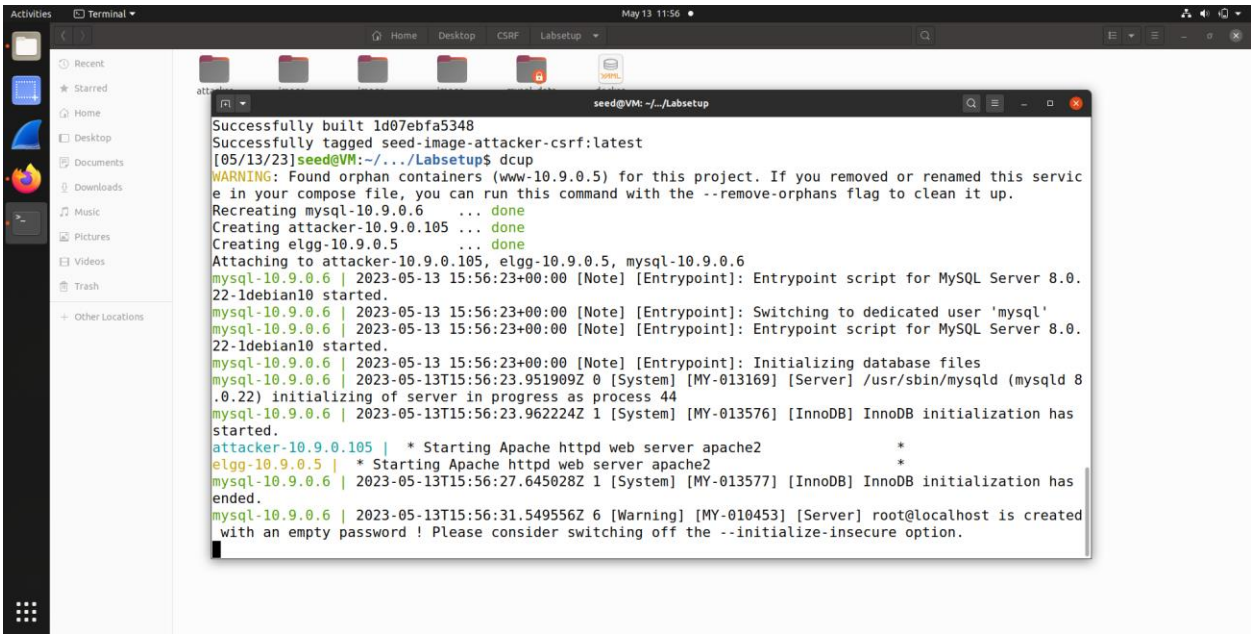
To Build the docker to make the containers of your website frontend and backend.



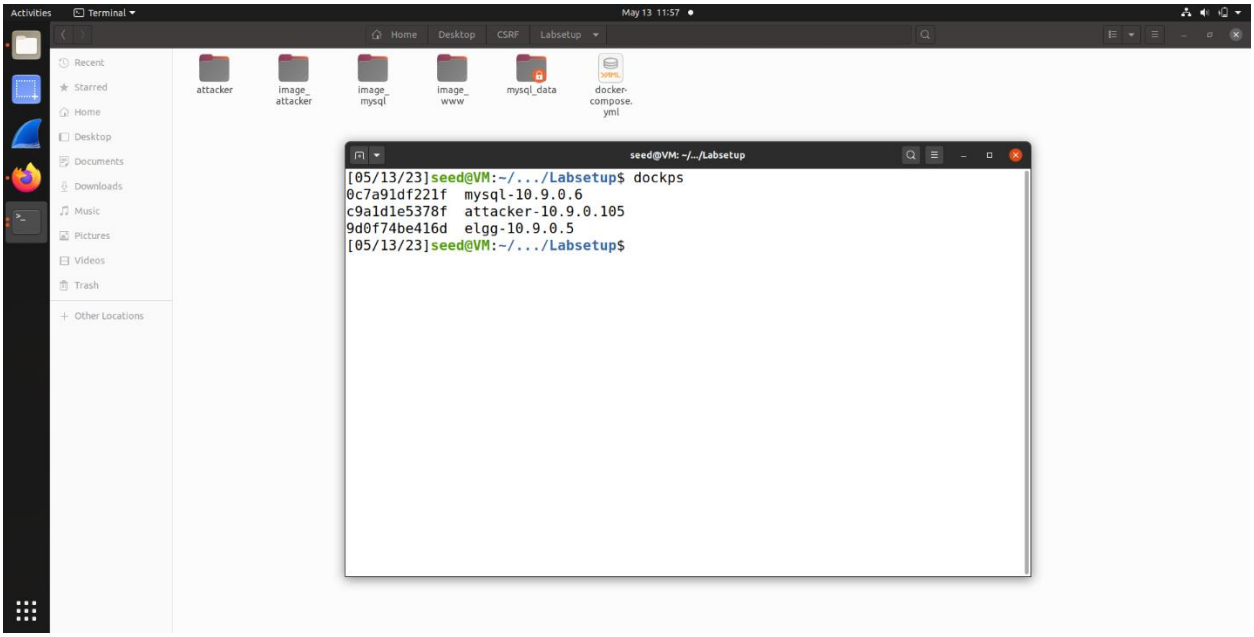
Now the docker build command is successful and docker containers are created.



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

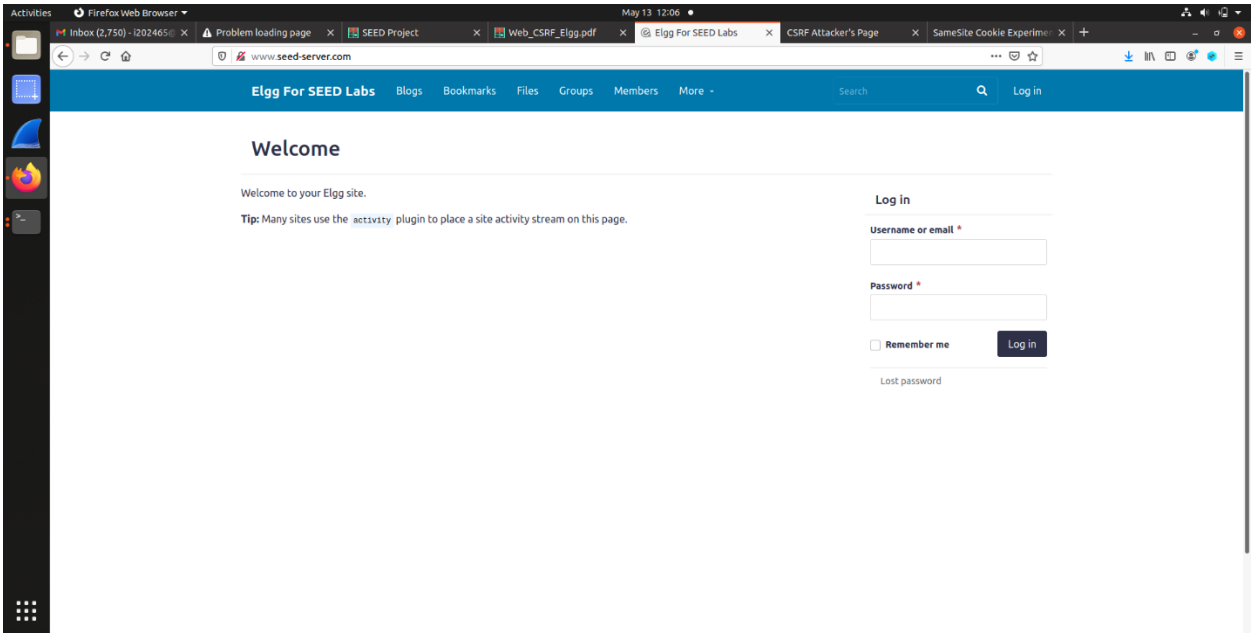


Now, to check which containers are created and how many containers are created.

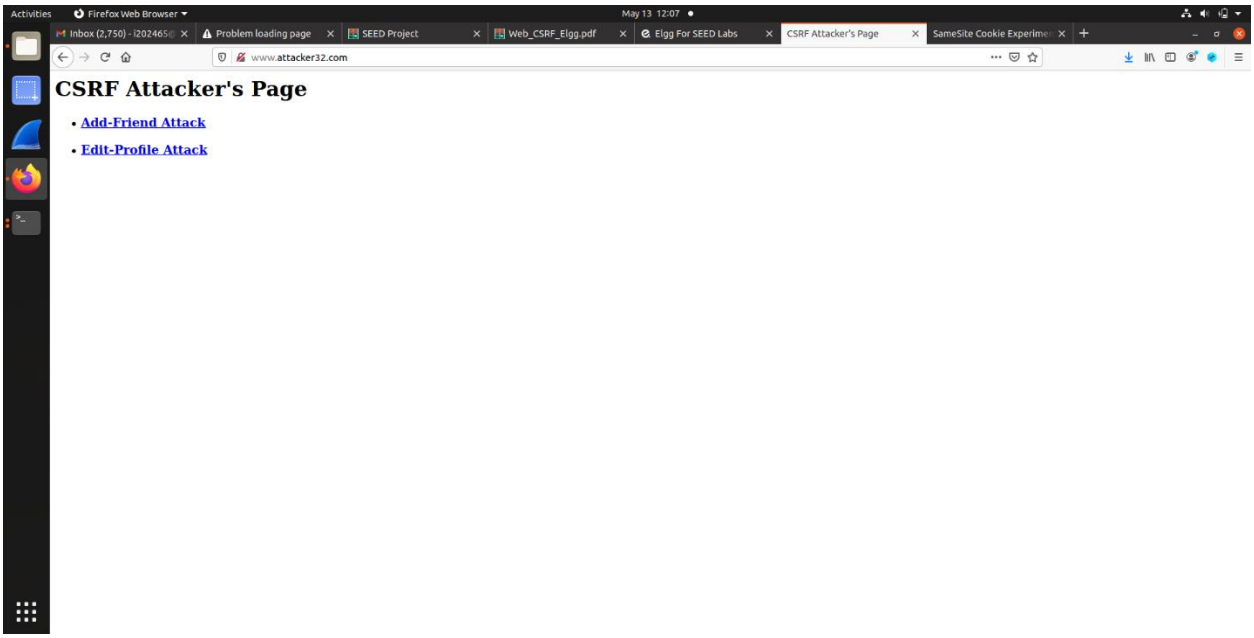


Now, check all the websites that are successfully hosting on chrome.

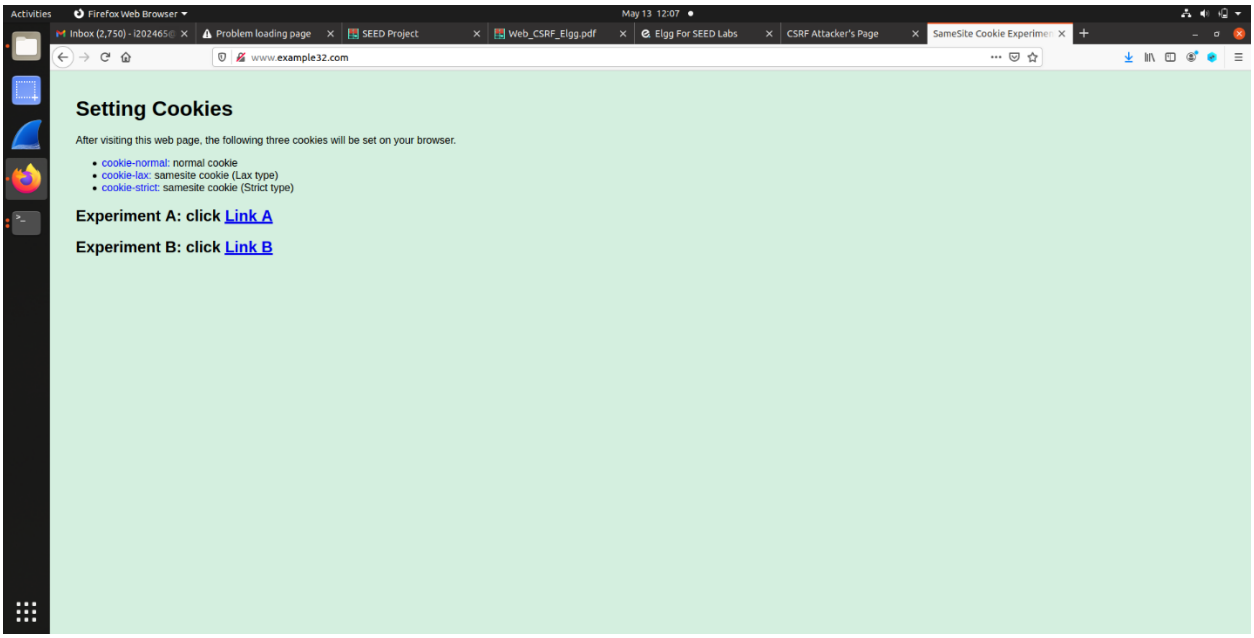
1st website.



2nd website

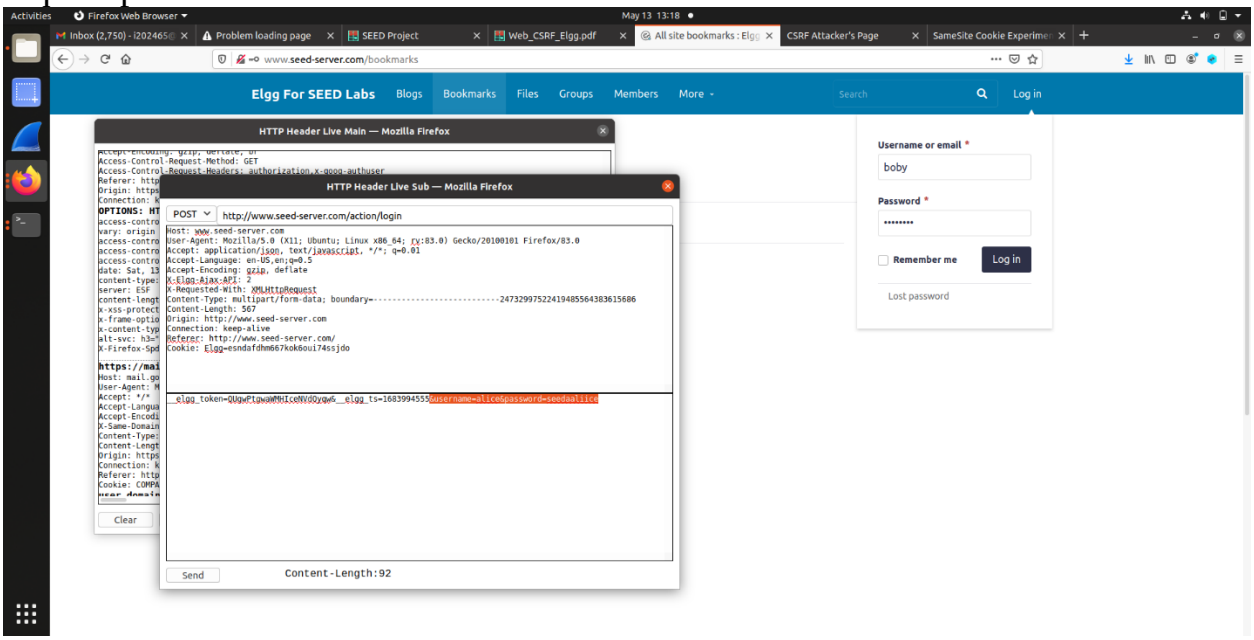


3rd website

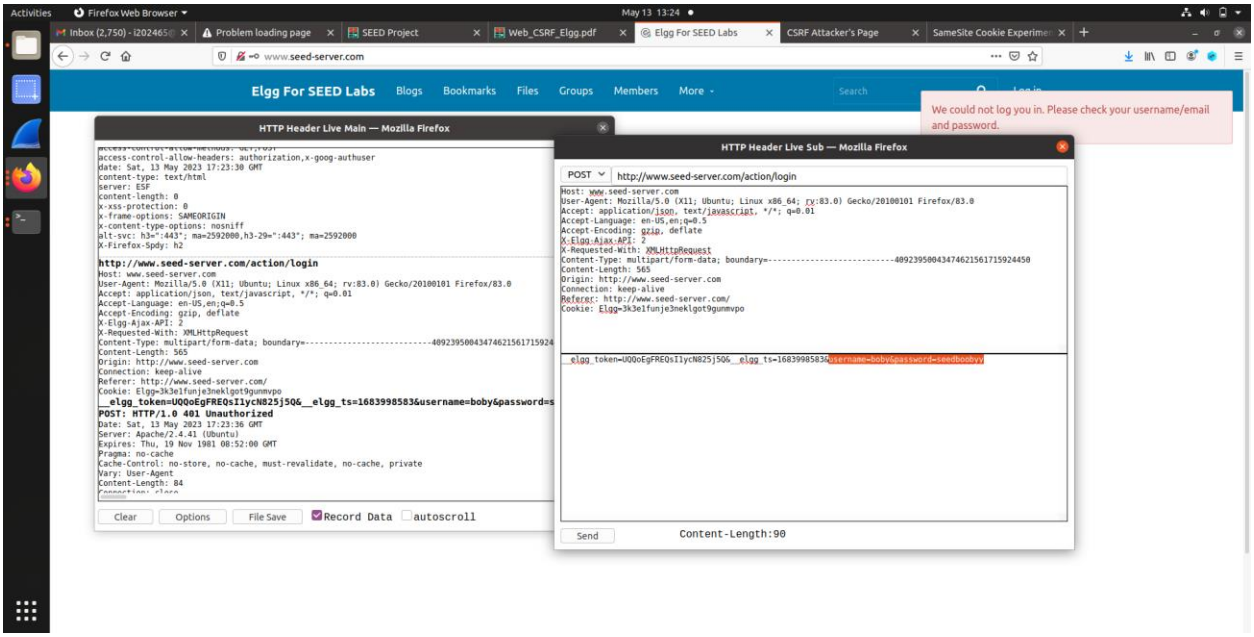


Task 1: observing HTTP request

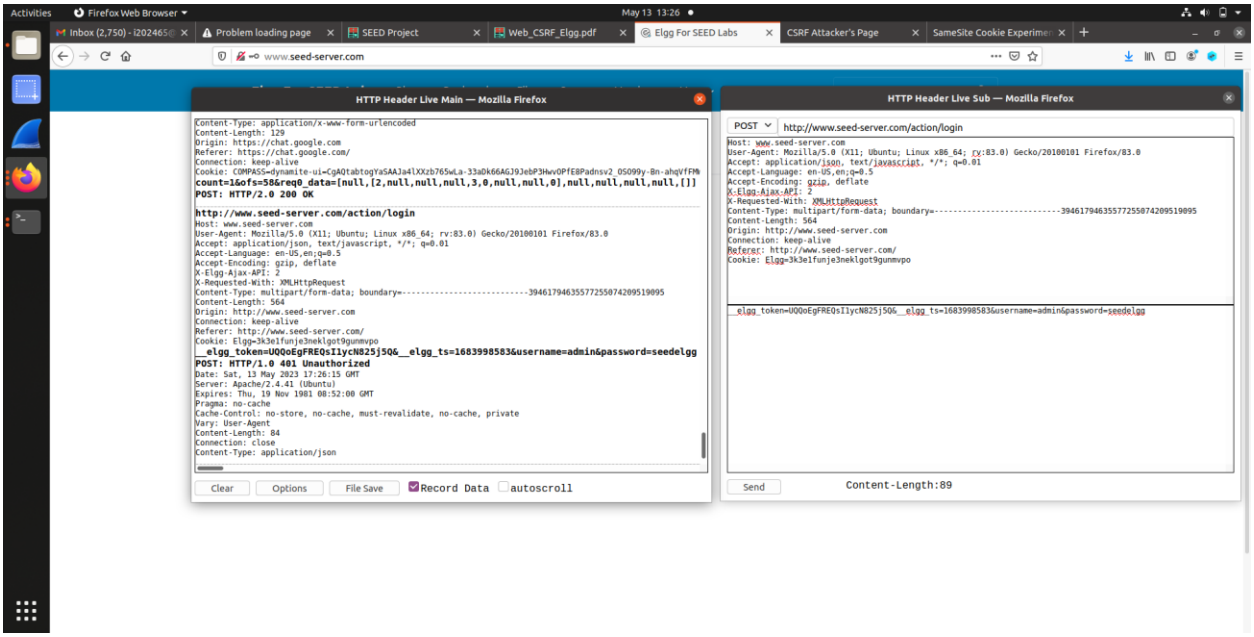
In this I am observing the request, when the user login to the website and I saw his request packet in the HTTP header live.



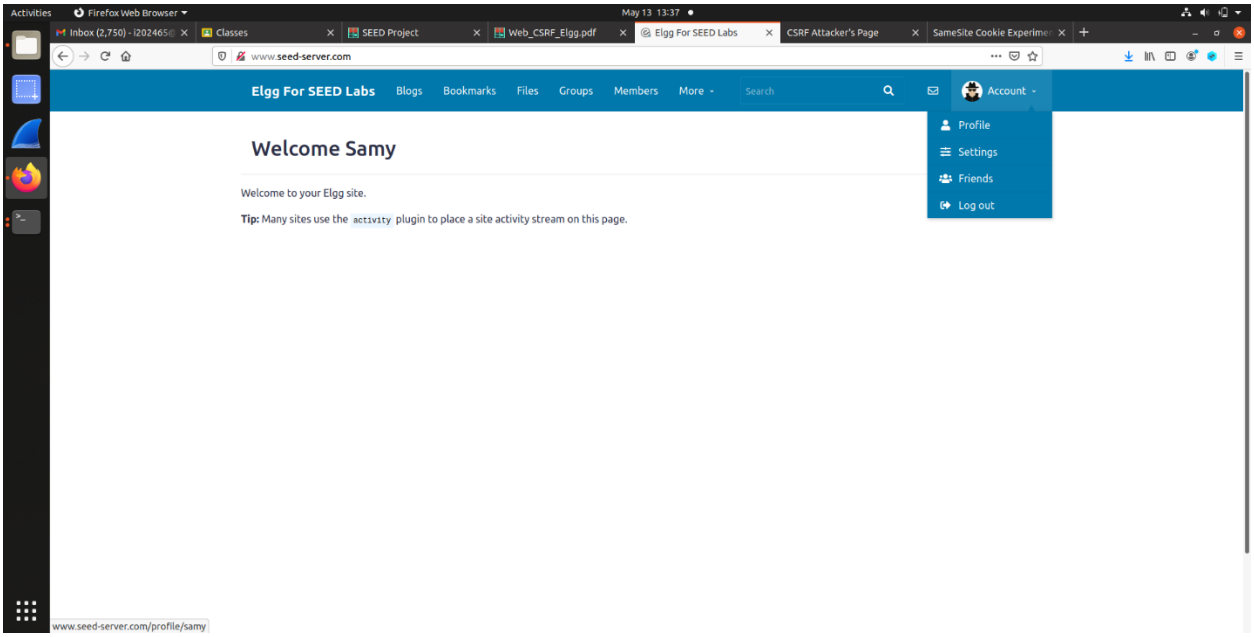
This is the request packet of boby, when he login in-to the website.



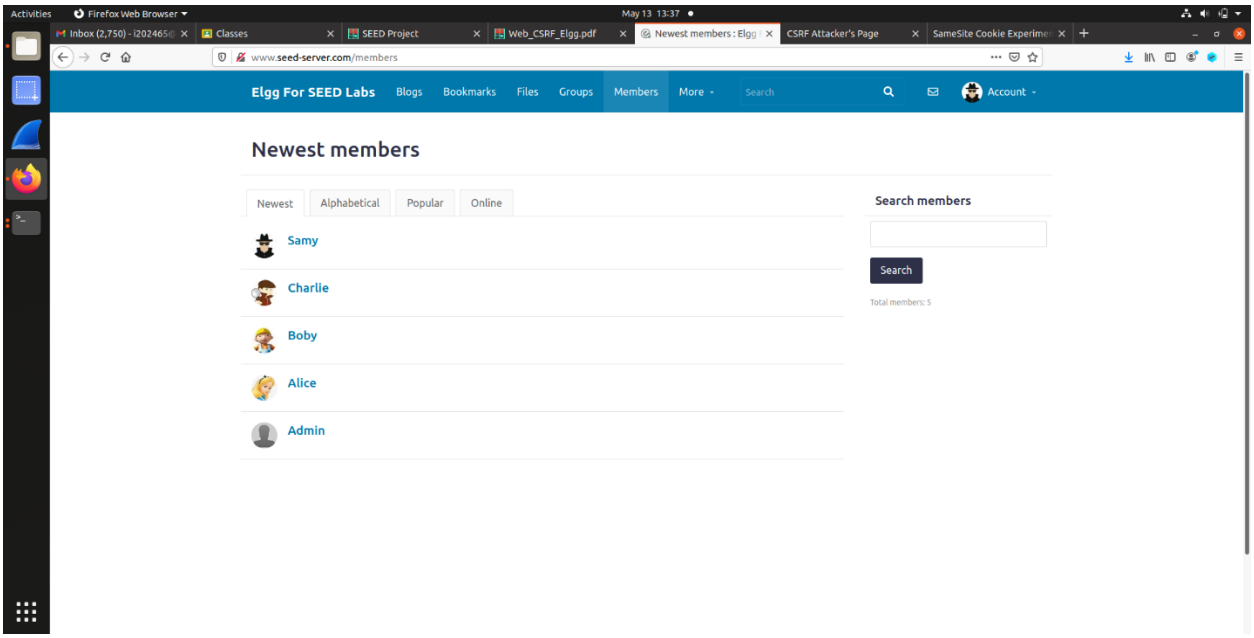
This is the request packet of admin, when he login onto the website.



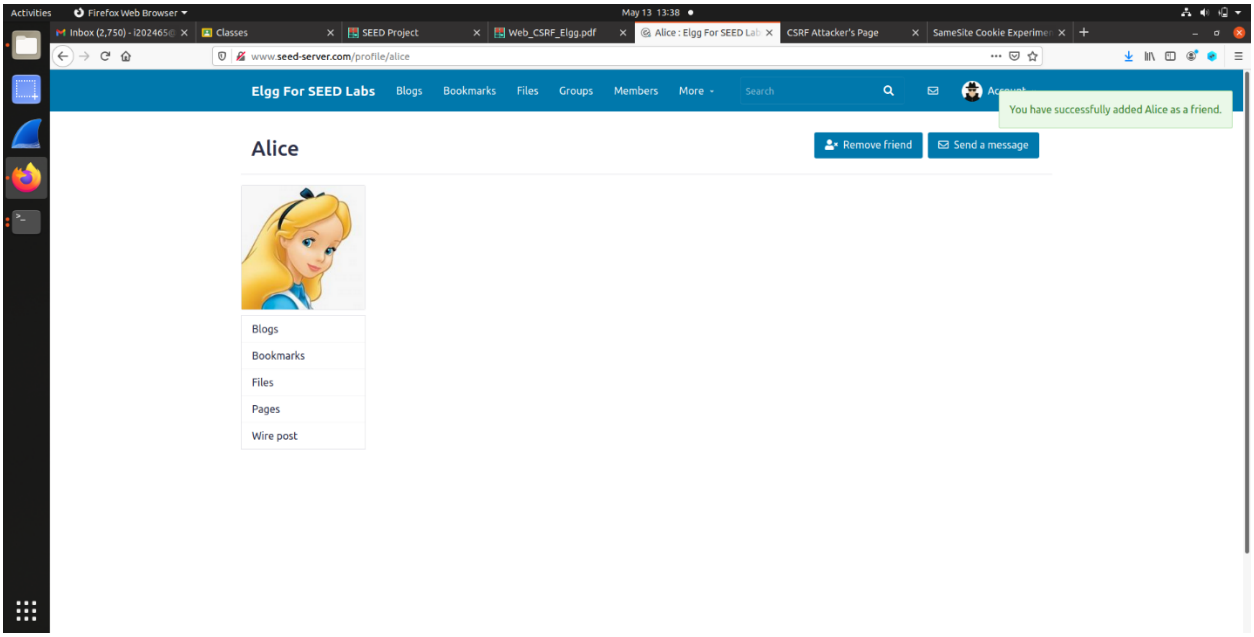
Task 2: Samy wants to be a friend of Alice, first he login into his account.



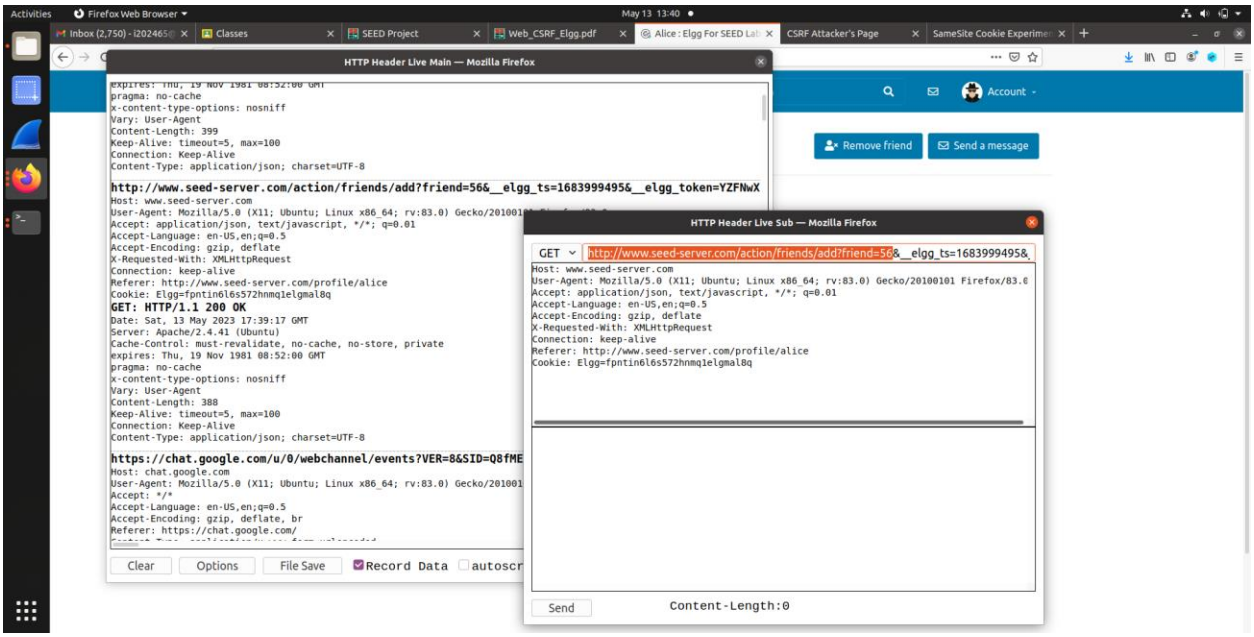
He saw his members, that have also been a user of this website.



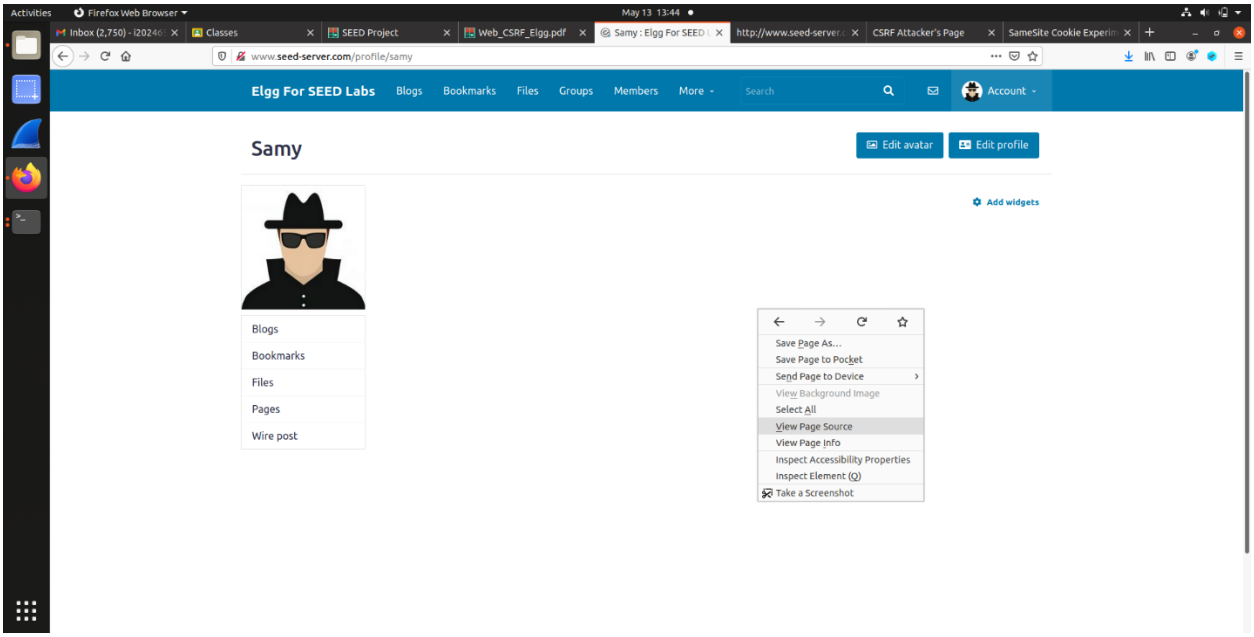
He clicks on the Alice Profile and sends the Friend Request.



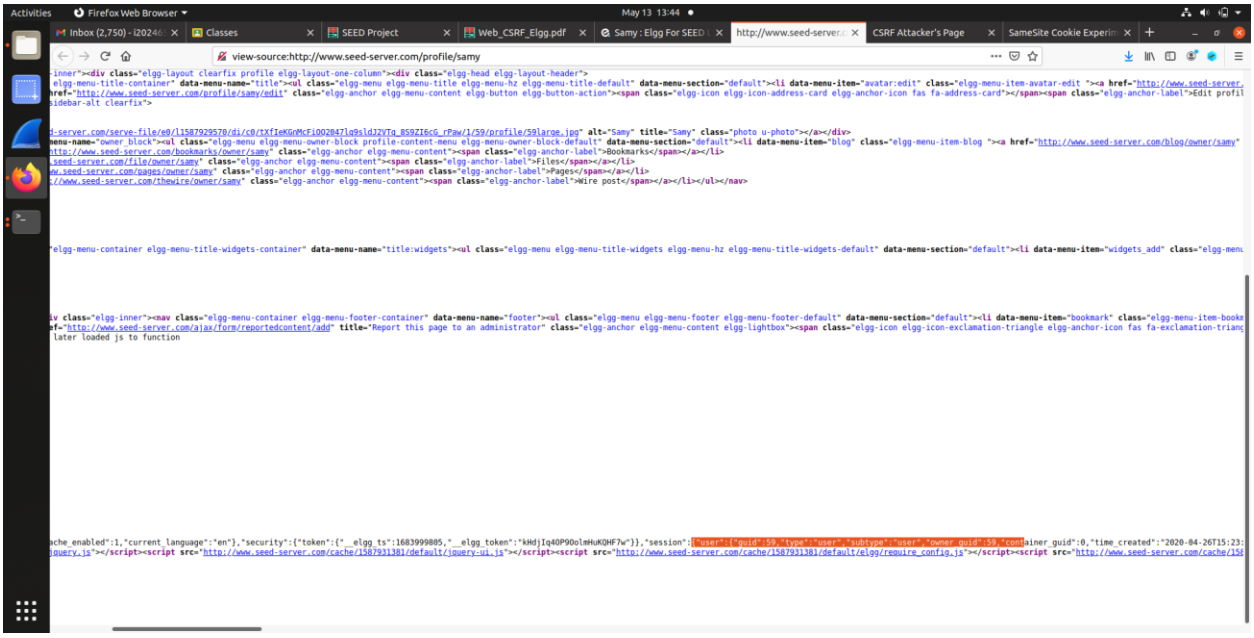
While, sending the samy also on the HTTP Header live to see and get his guid so that he can manipulates and do something with that. He gets the guid: 56 of Alice.



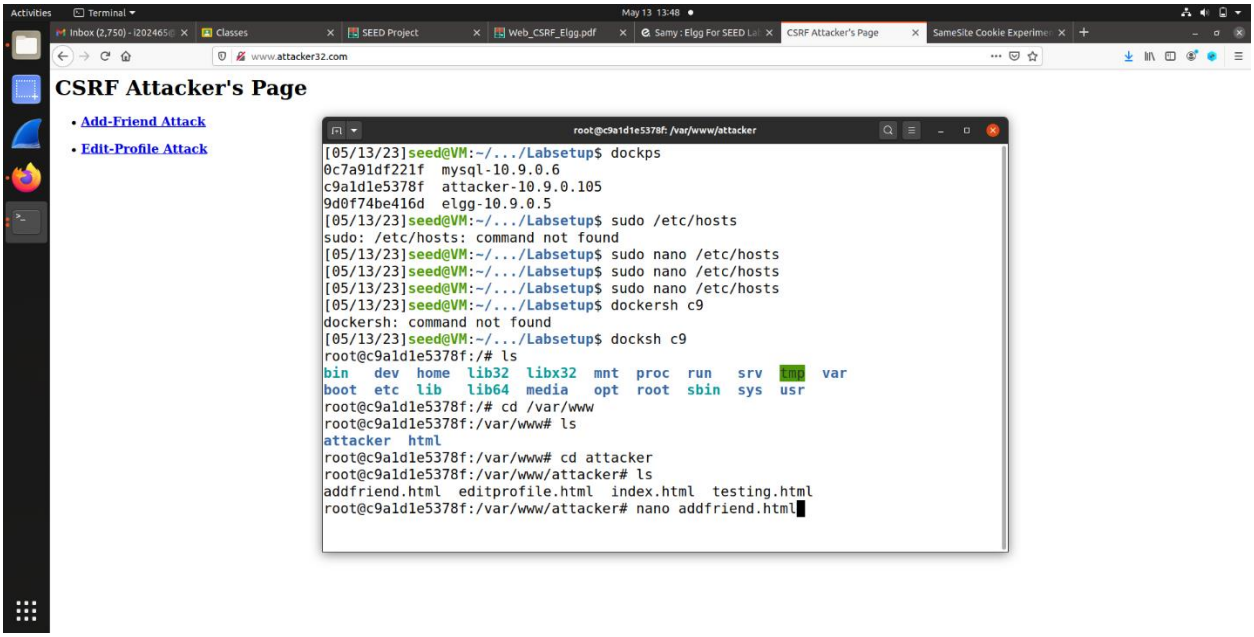
Now, samy also check his guid by inspecting or view the source page of the website.



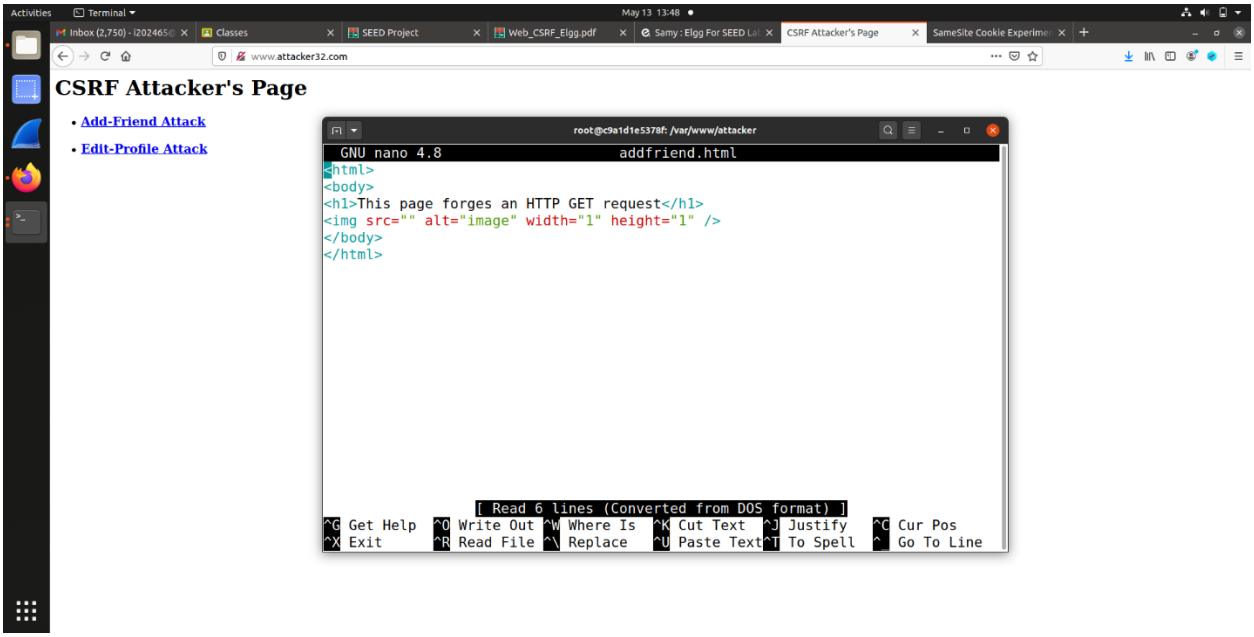
Now, here the samy got to know about his guid as 59.



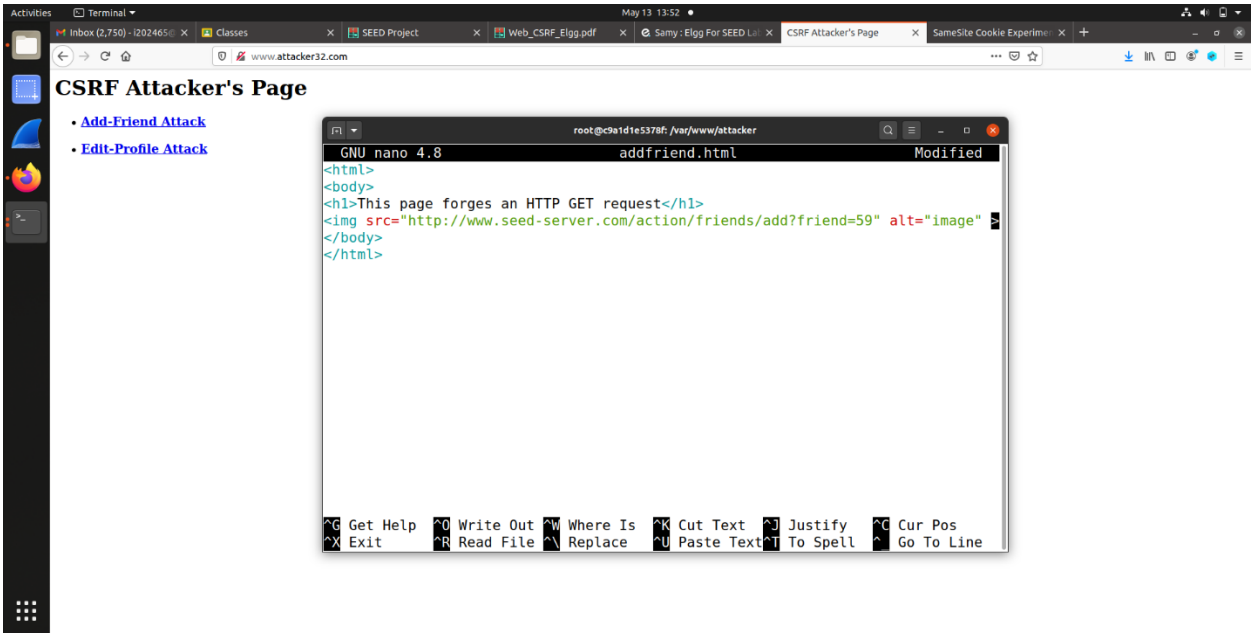
Now, login to the specific container



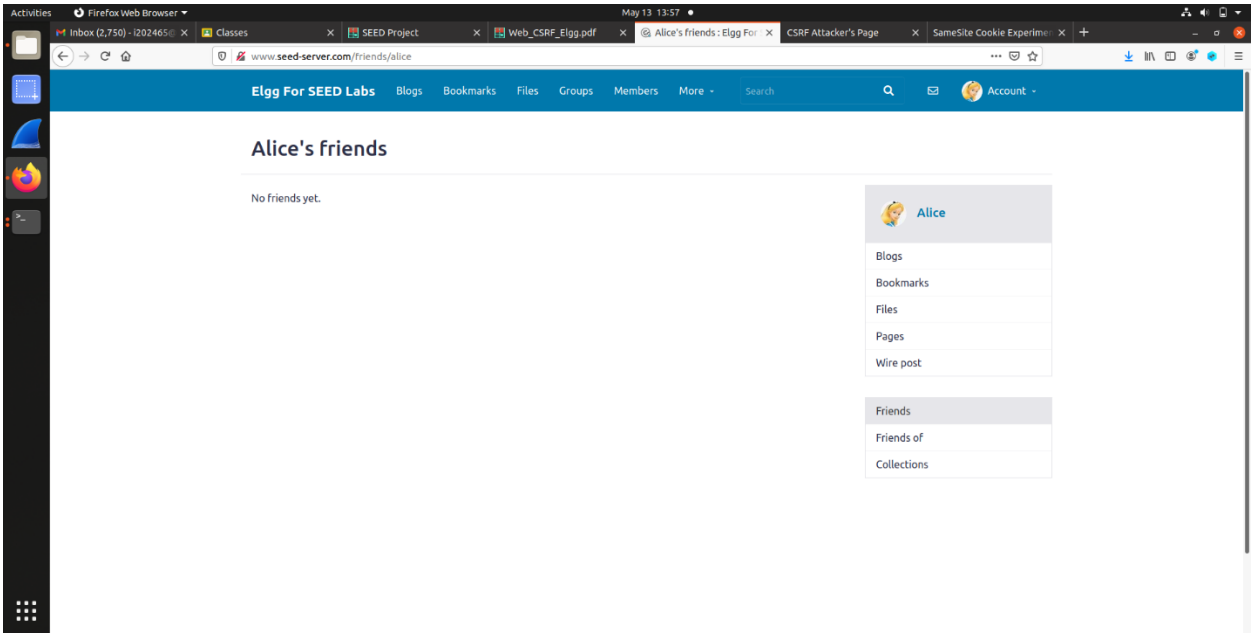
And edit the code so that it works properly according to the requirement.



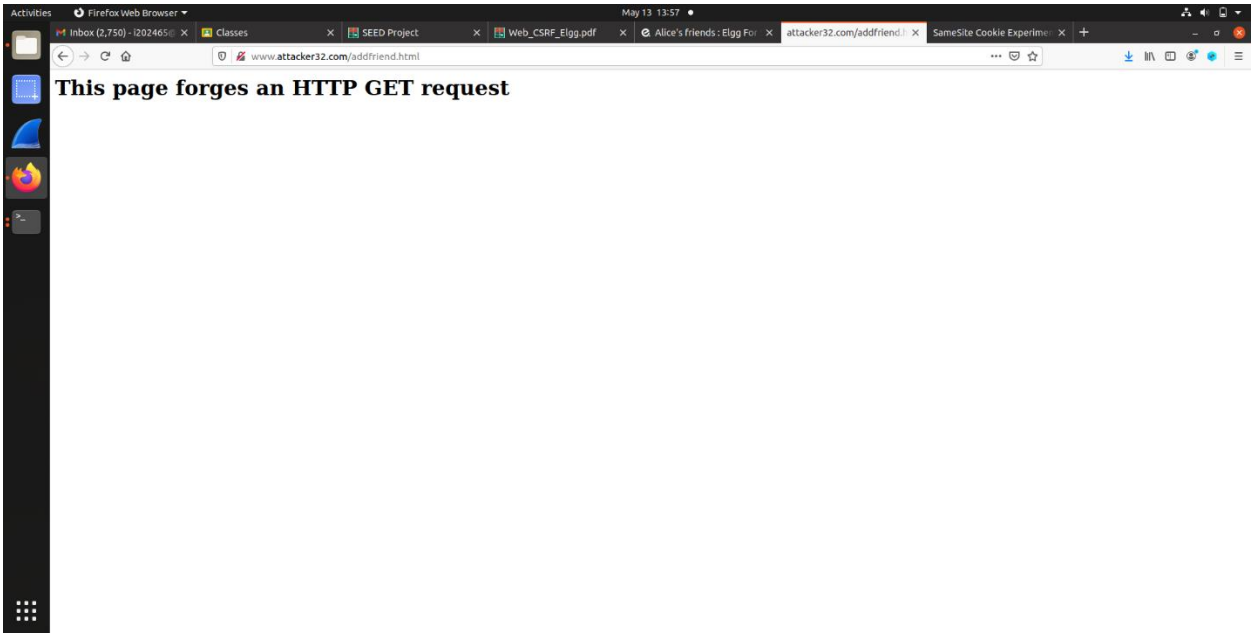
Here, the edited code in which the src link is added.



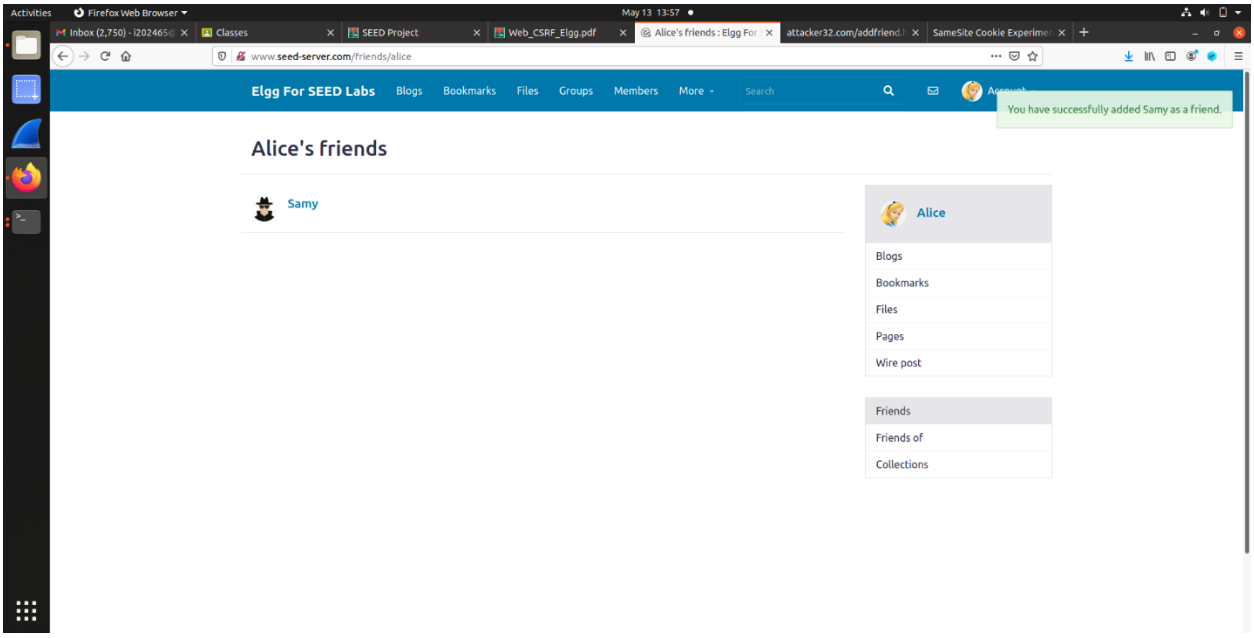
After saving the updated code, Firstly Alice have no friends in his list.



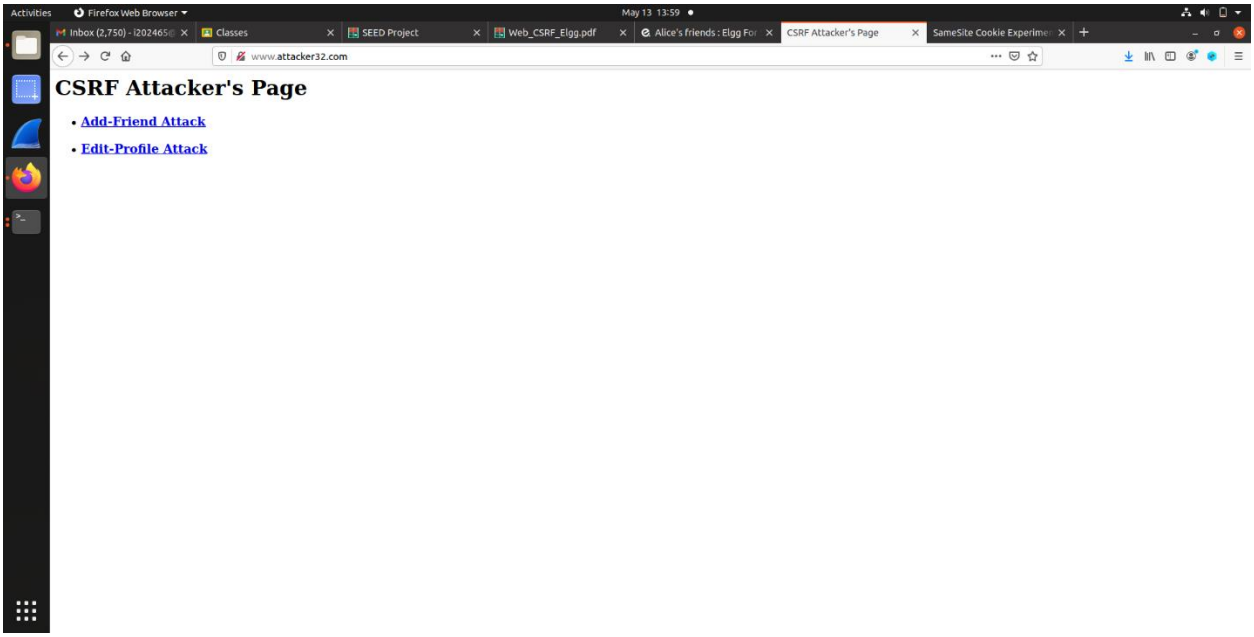
After the Add friend attack is launched and done successfully.



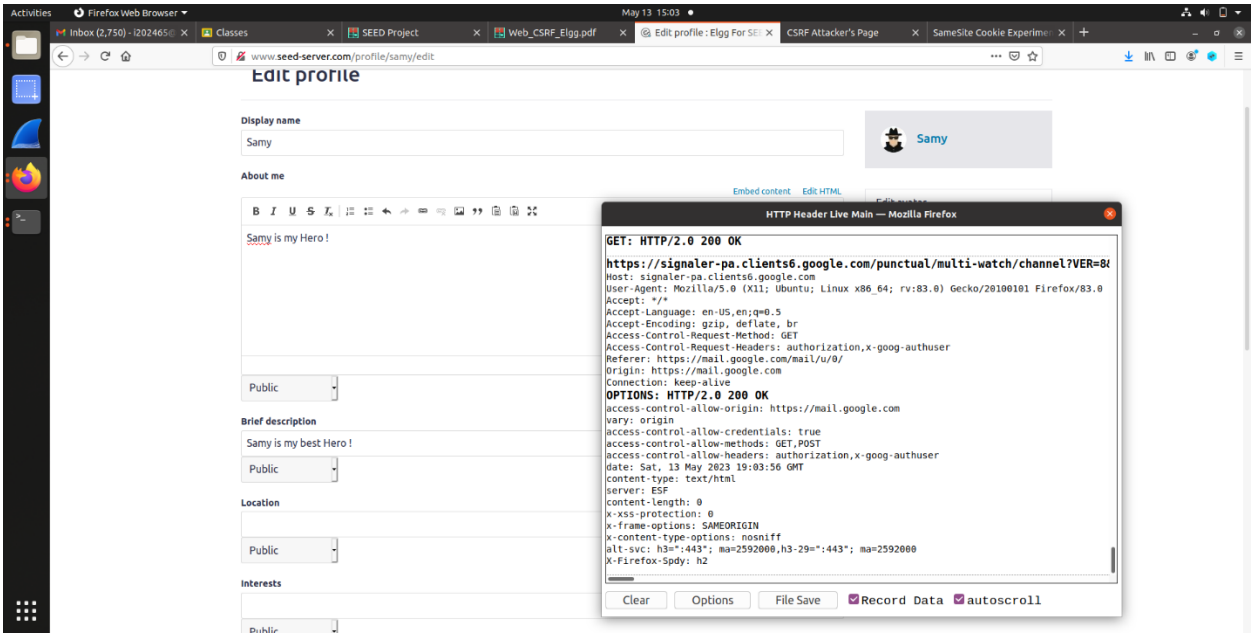
Now, the samy is in her friends list, and alice didn't accepted and samy didn't requested, so it means the attack is done successfully.



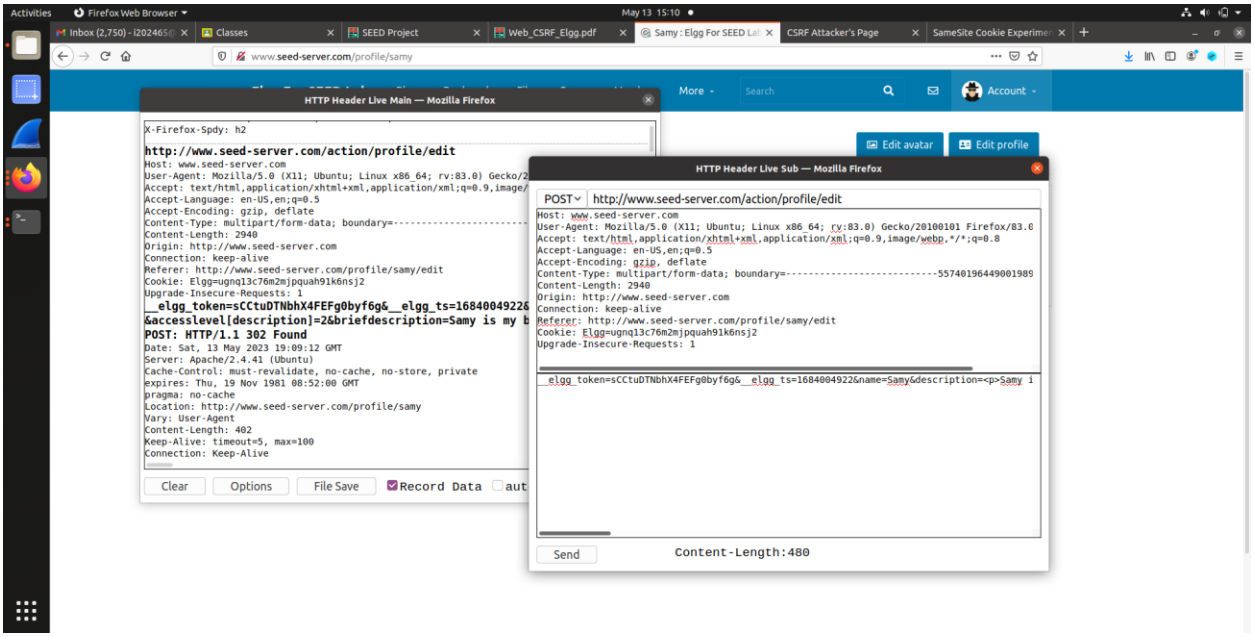
Now, this is the Attacker page, where he can send the malicious website to redirect to other websites.



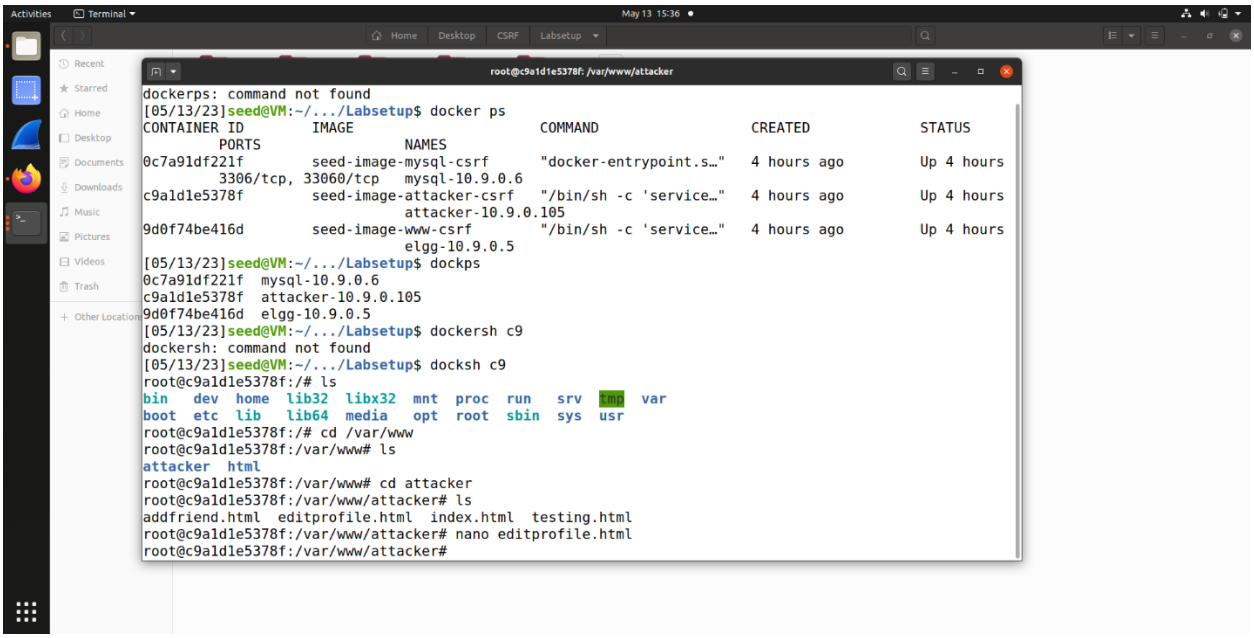
Task 3: Edit details Attack, now samy wants to see his name in the bio of Alice. First he edit his details.



Now, he captures the packets detail using the HTTP header live and takes the post command url as to use it in malicious purpose.



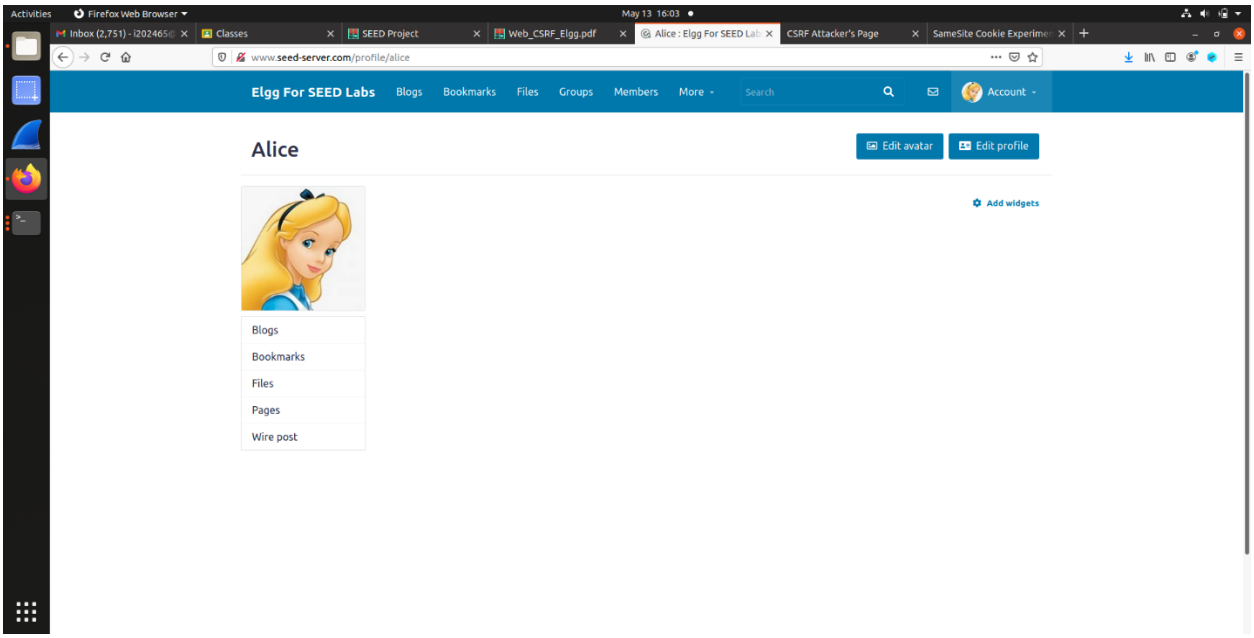
Now, login to the specific container and get into the directory where the file is placed.



Now, first check the code details, what are in the code, then change it accordingly.

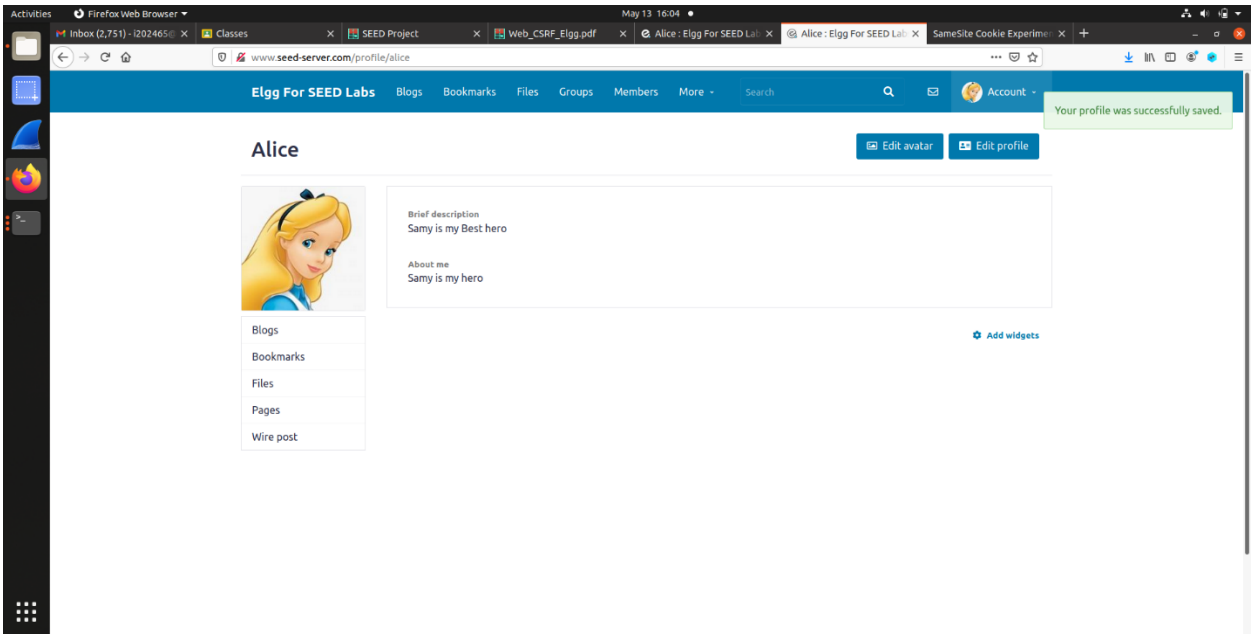
This is the updated code of file, in this file there are some changes that are required.

Now, this is picture before attack, Alice has no description in his bio.

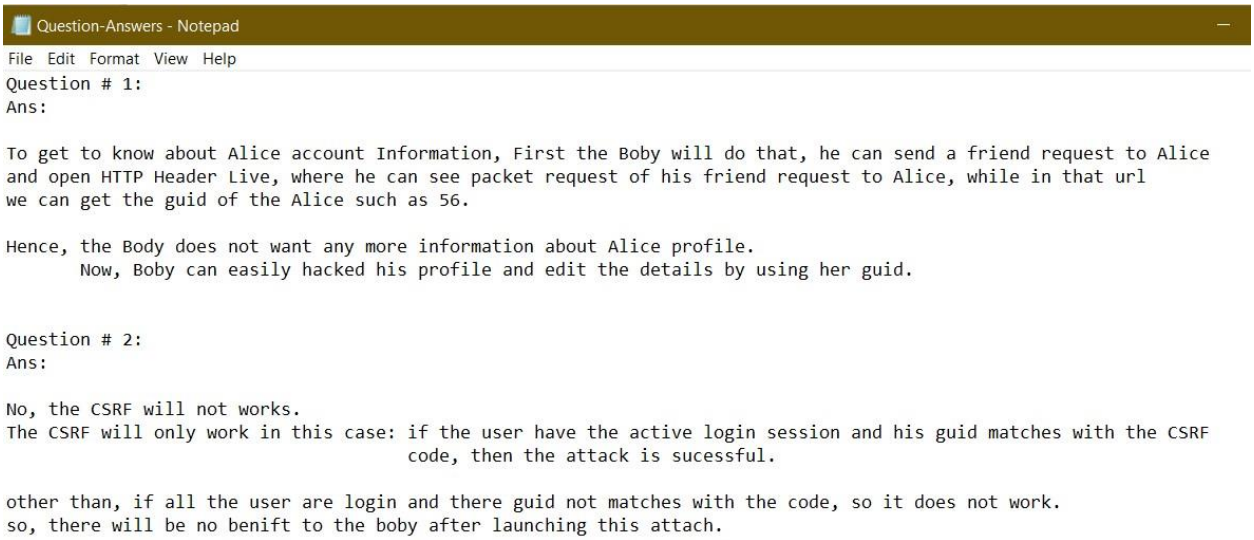


When the Attack launches, and the Alice profile would face many circumstances.

The attack is done successfully, the bio is updated by this attack.



Task 3.2: Answers the Questions

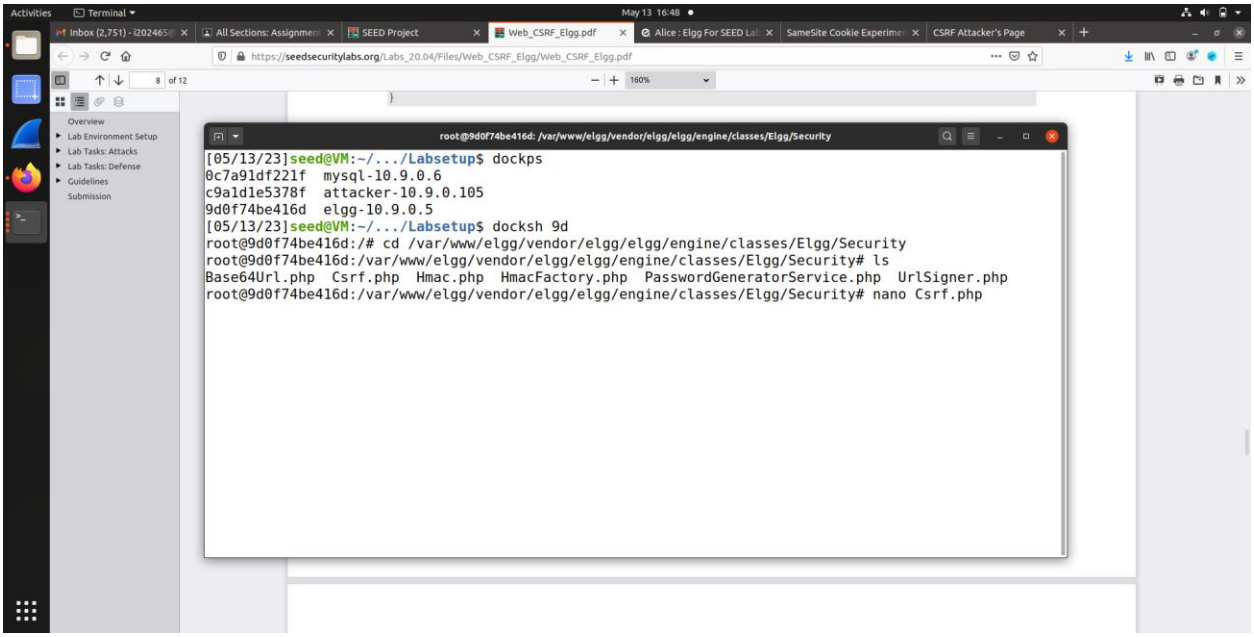


Question-Answers - Notepad

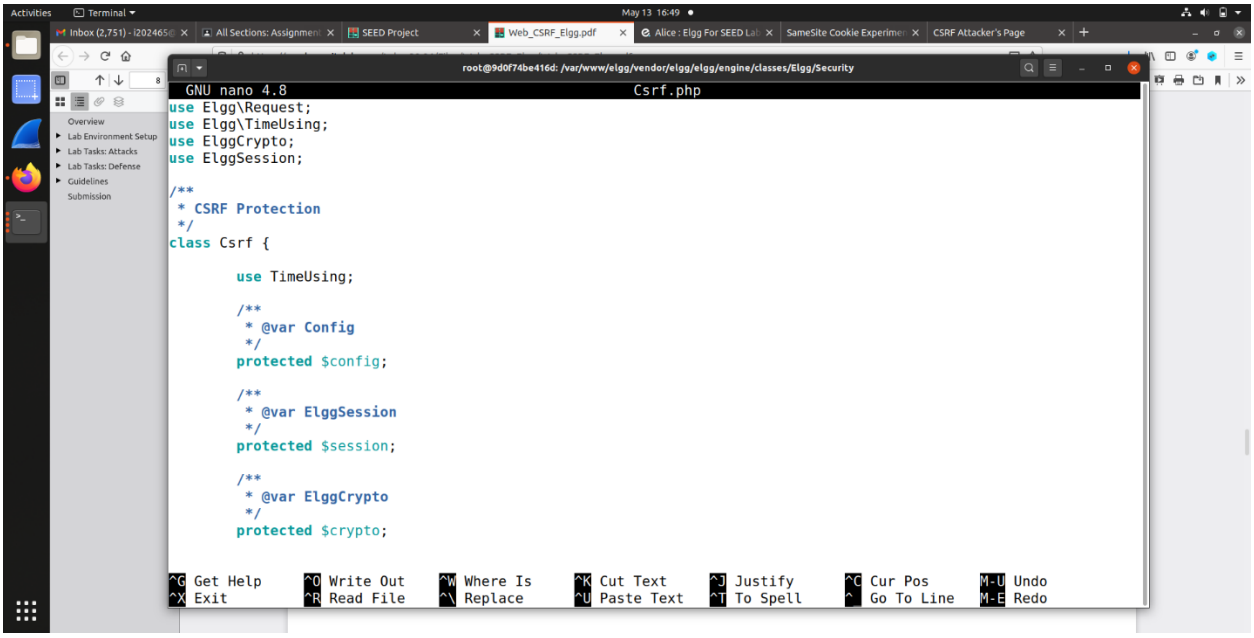
File Edit Format View Help

```
Question # 1:
Ans:

To get to know about Alice account Information, First the Boby will do that, he can send a friend request to Alice
and open HTTP Header Live, where he can see packet request of his friend request to Alice, while in that url
we can get the guid of the Alice such as 56.

Hence, the Body does not want any more information about Alice profile.
       Now, Boby can easily hacked his profile and edit the details by using her guid.


Question # 2:
Ans:

No, the CSRF will not works.
The CSRF will only work in this case: if the user have the active login session and his guid matches with the CSRF
                                      code, then the attack is sucessful.

other than, if all the user are login and there guid not matches with the code, so it does not work.
so, there will be no benift to the boby after launching this attach.
```

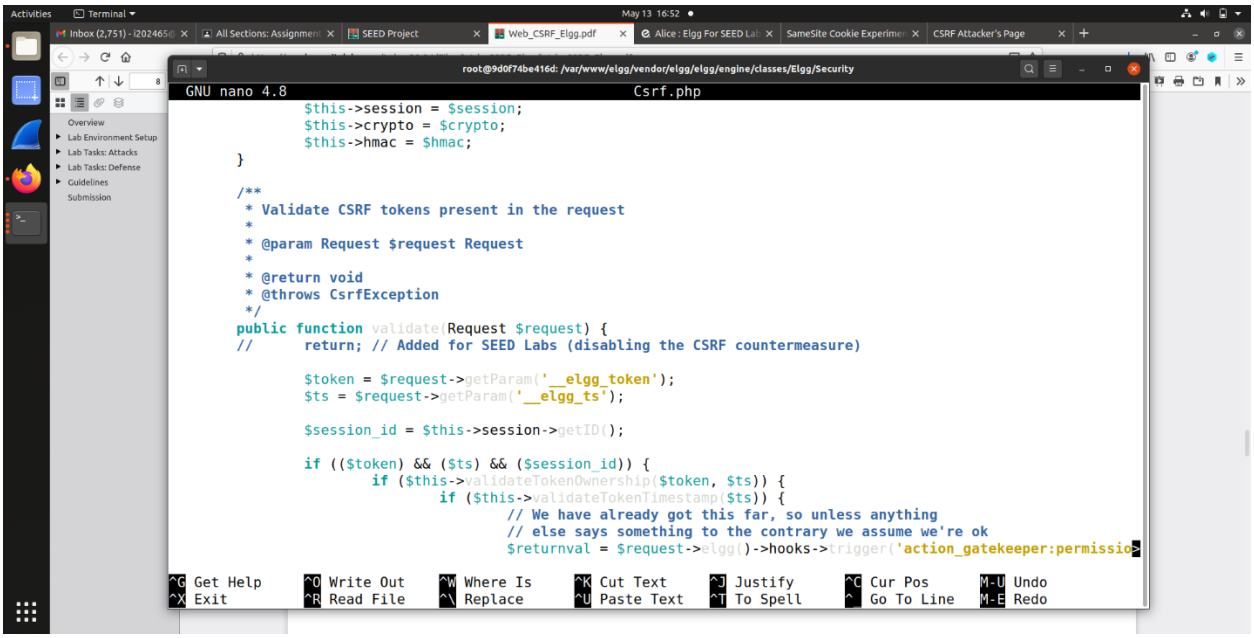
Task 4: 4.1: Enable Counter Measures.
Now, login to the specific container and get into the directory where the file is placed.



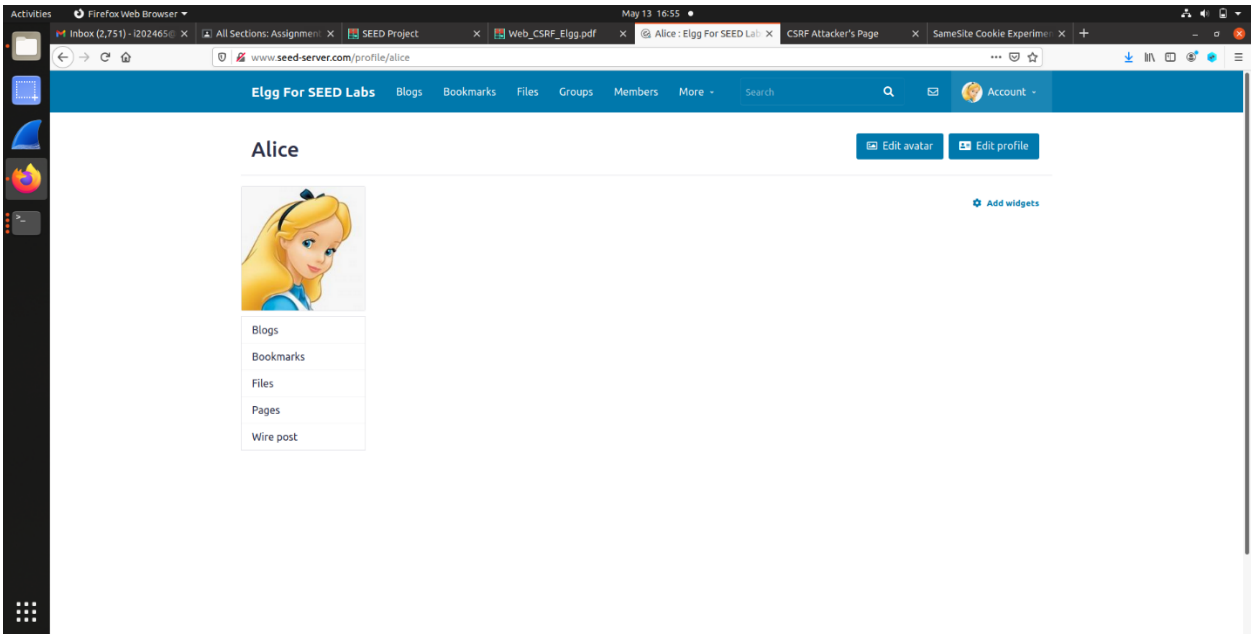
This is file without edited, Now makes the changes according to the requirement and security of the website.



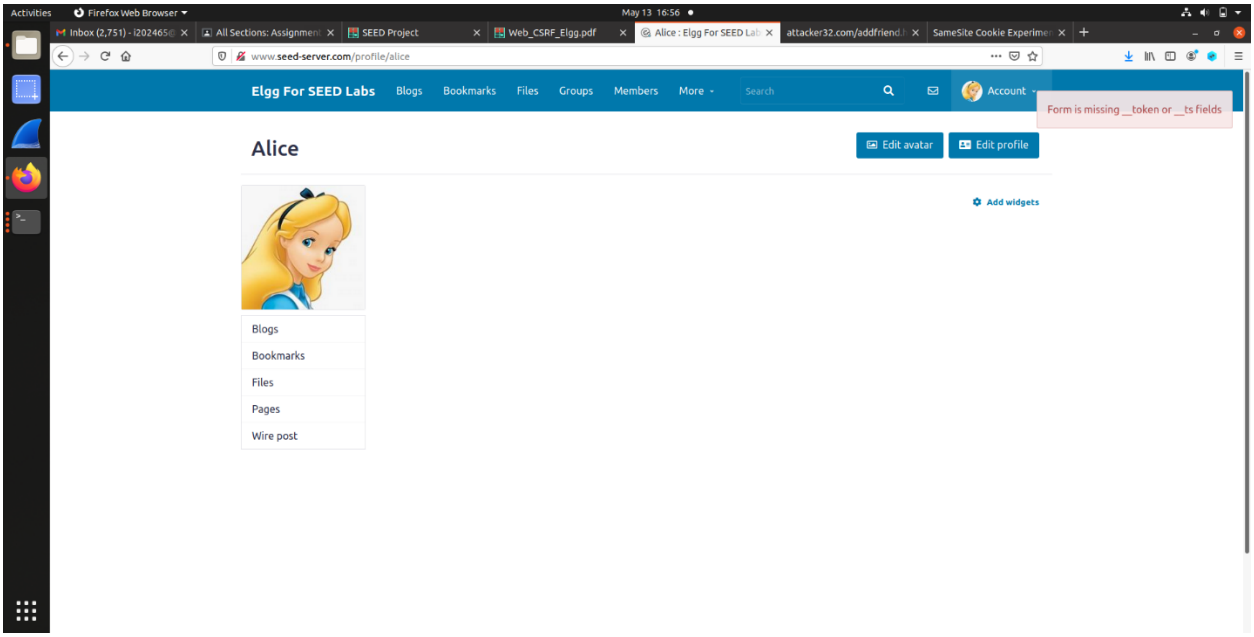
This is the updated code, where the return function is commented to make a secure connection.

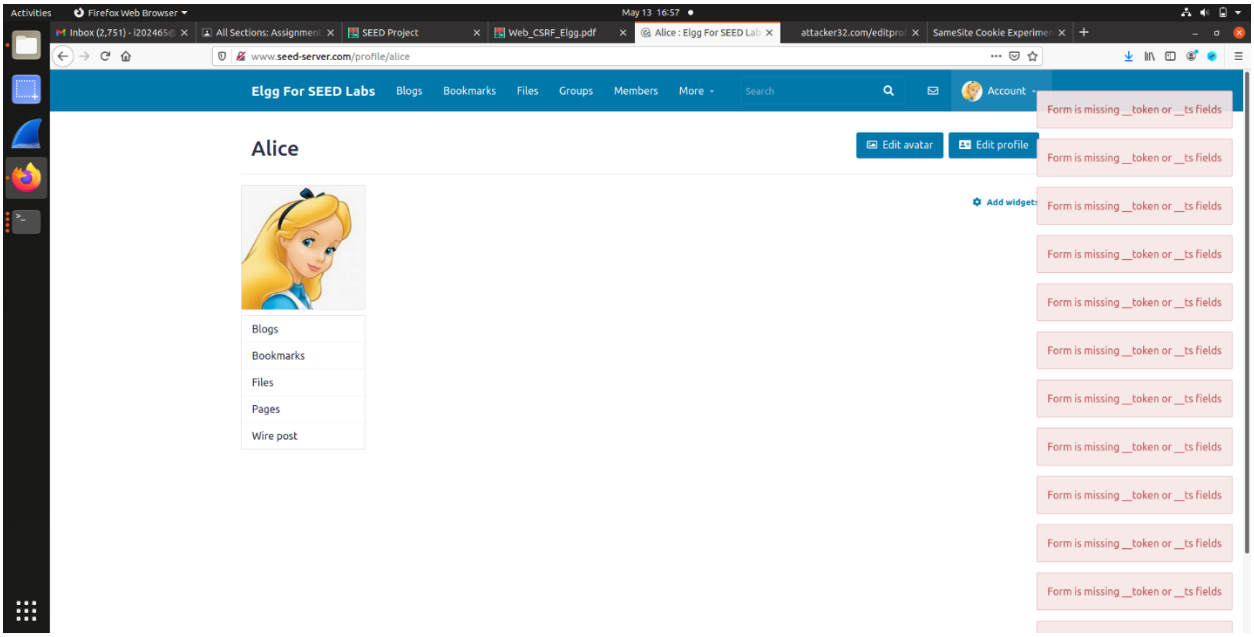


Now, you are already login as Alice profile and check that all tha CSFR attacks are now applicable or not.

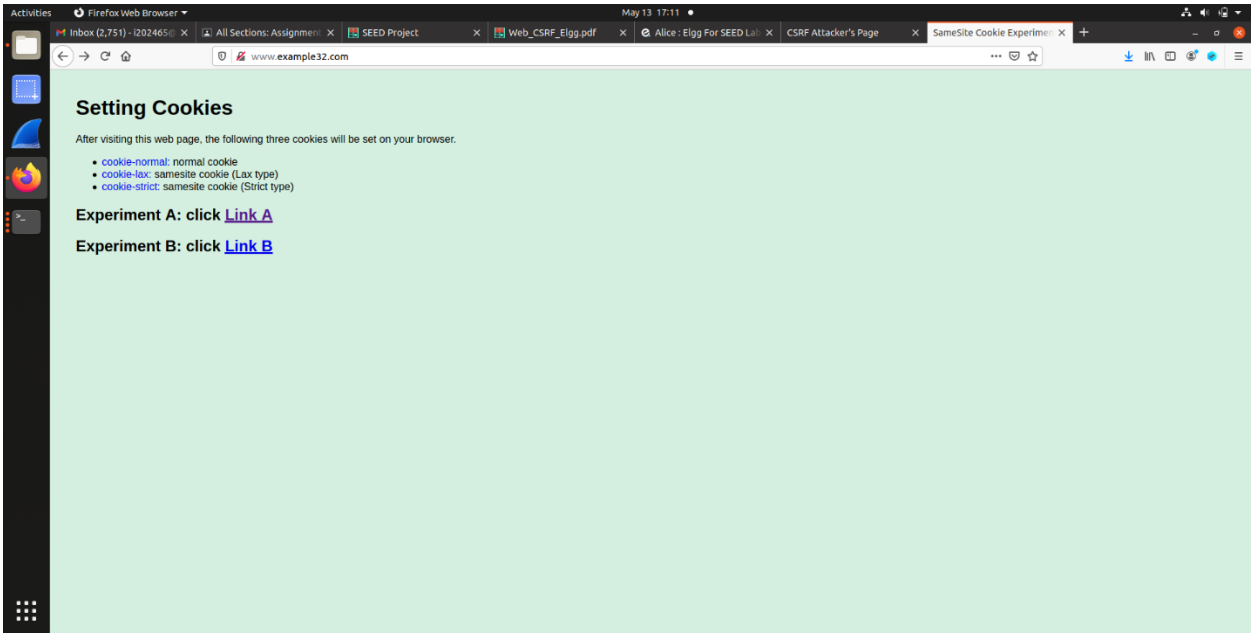


Now, as the CSRF attacks do not have access to do with that particular user. It displays error because of different tokens from the different session logs which are not fulfilling the authenticity of the website. Below two pictures show error result of both Attack as we did above with other users.

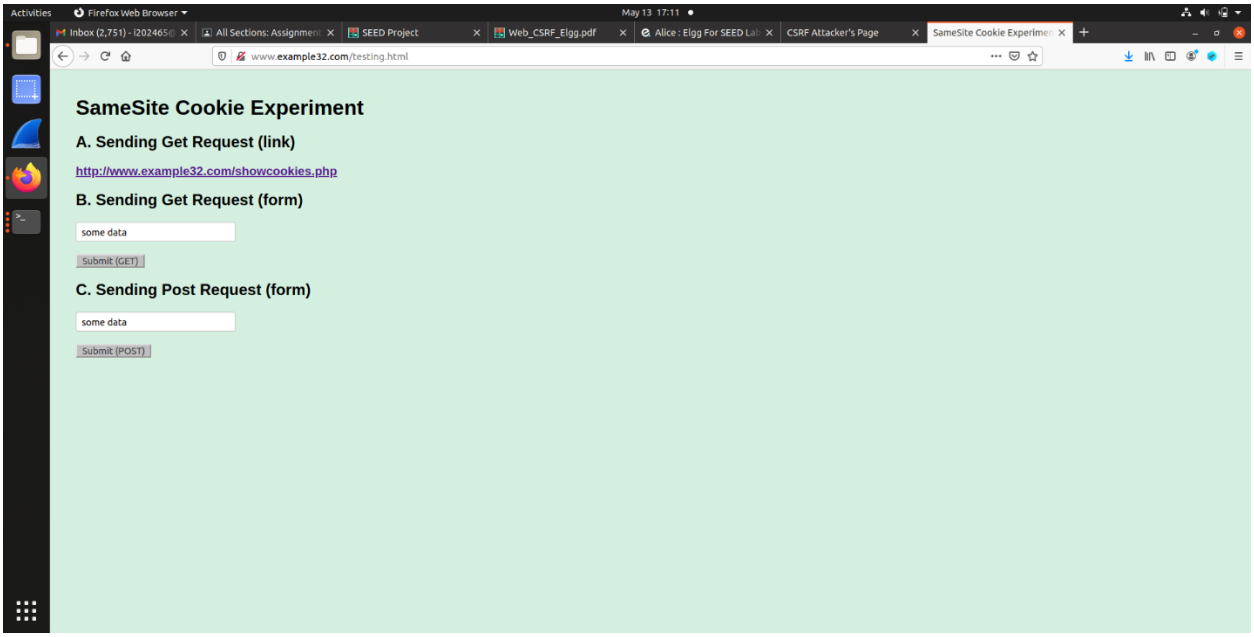




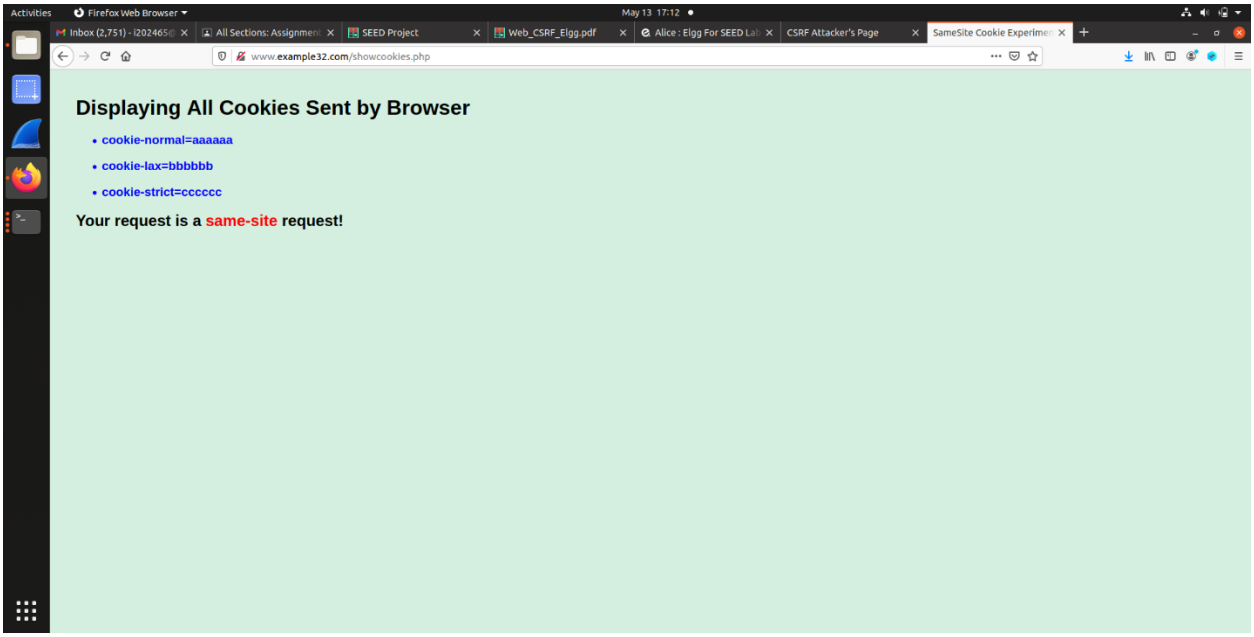
Task 4.2: Experimenting the same-site & cross-site cookies.
In Experiment A, it redirects to the same site and all the cookies would follow the cookies accordingly.



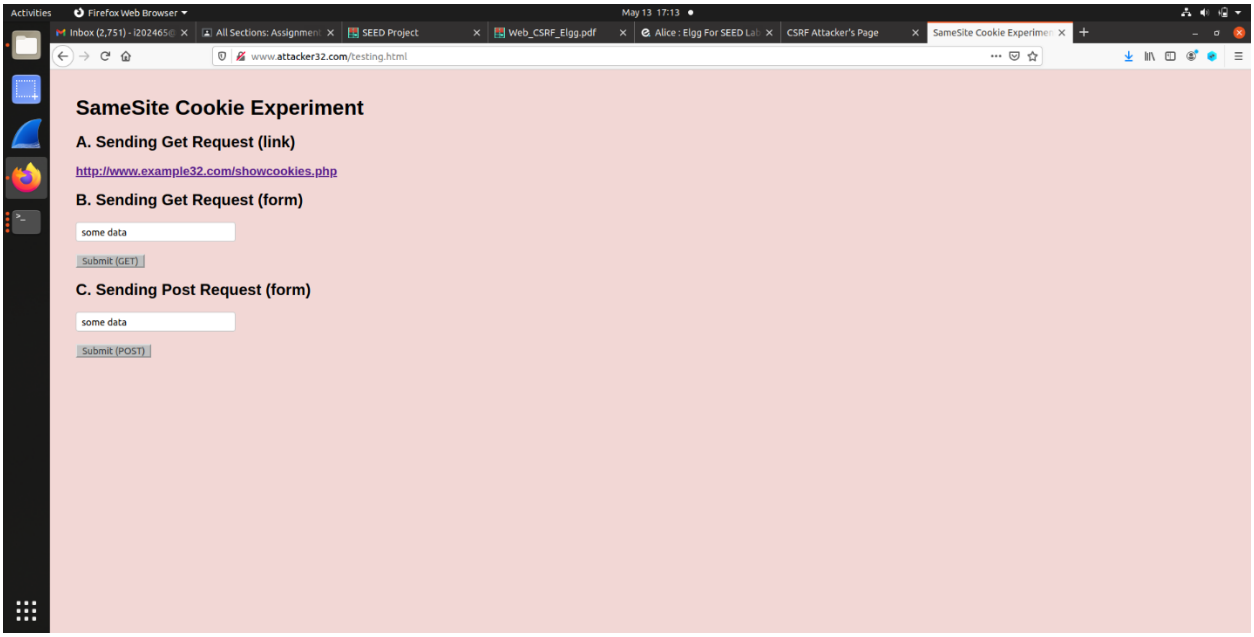
In this, either we send the post or get request to the same website, it have all those cookies that it already has.



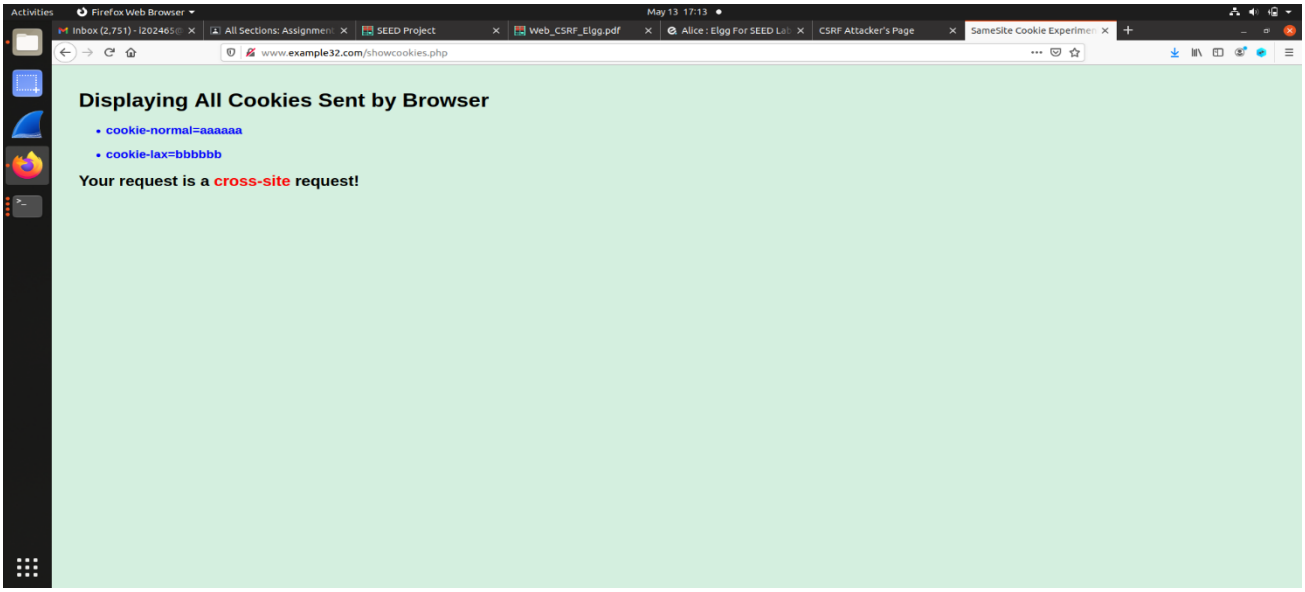
The output is the same for all the requests that would be placed from the same website.



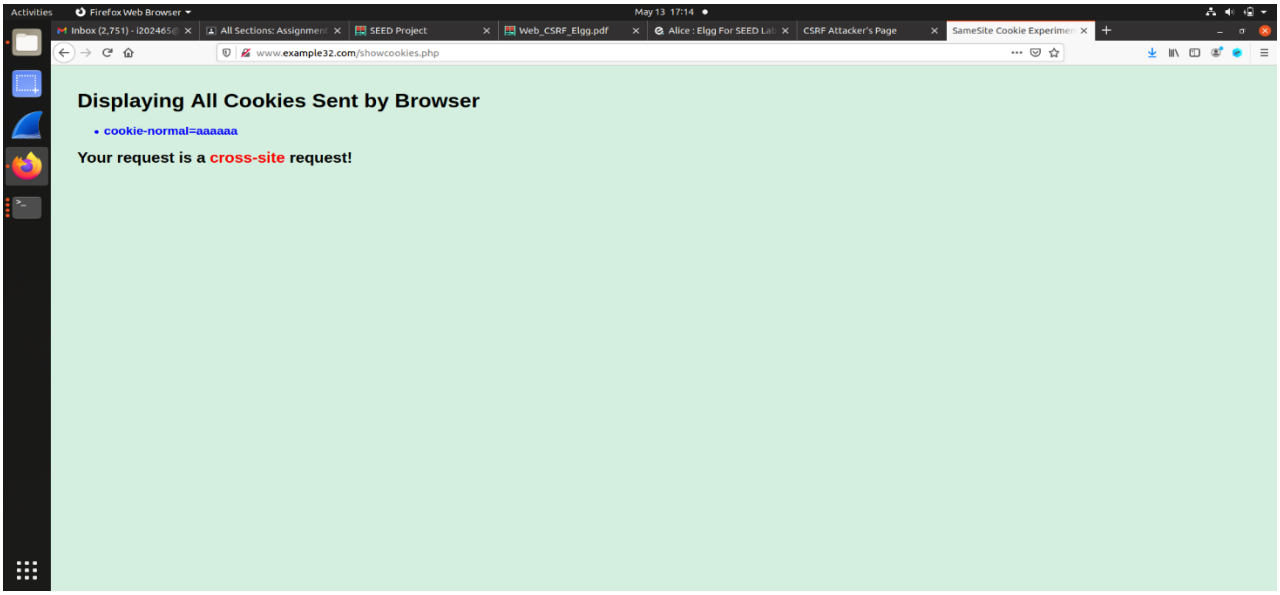
Now, if the request is redirected to other websites, the Experiment B is there.



It is output for get and link request that is placed in Experiment B.



It is output for the post request that is placed in Experiment B.



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	XXS, CSRF → pre-Setup & Task 1,2, 3,4,5,6