Information Security

Assignment # 04

SQL Injection 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

SQL Injection Lab using SEED's Lab

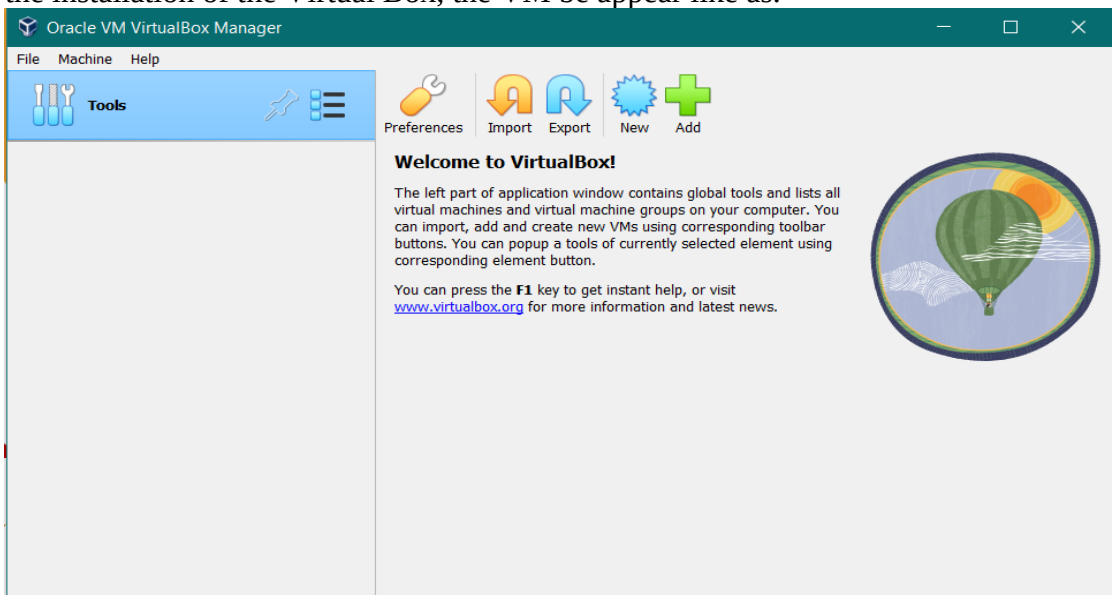
1-SQL Injection Lab:

Description:

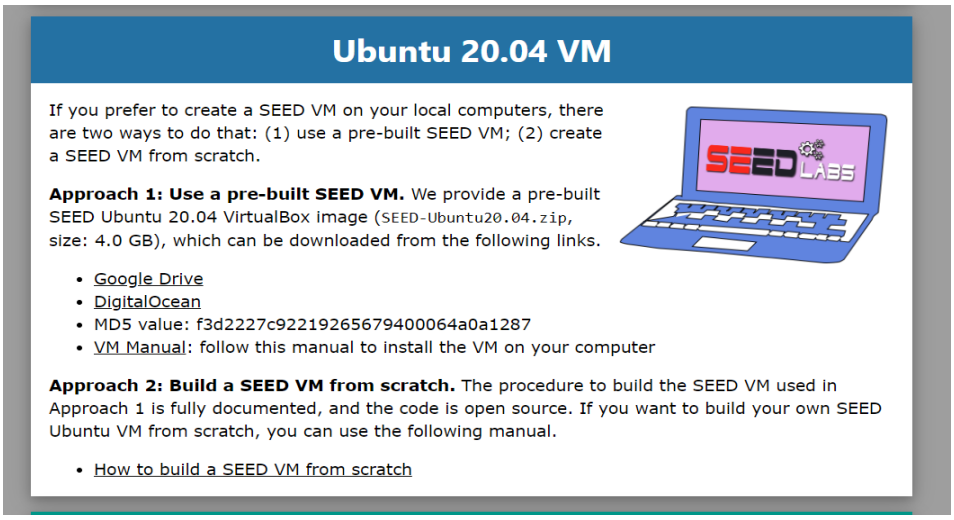
To starting, the Installation requirements are.

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

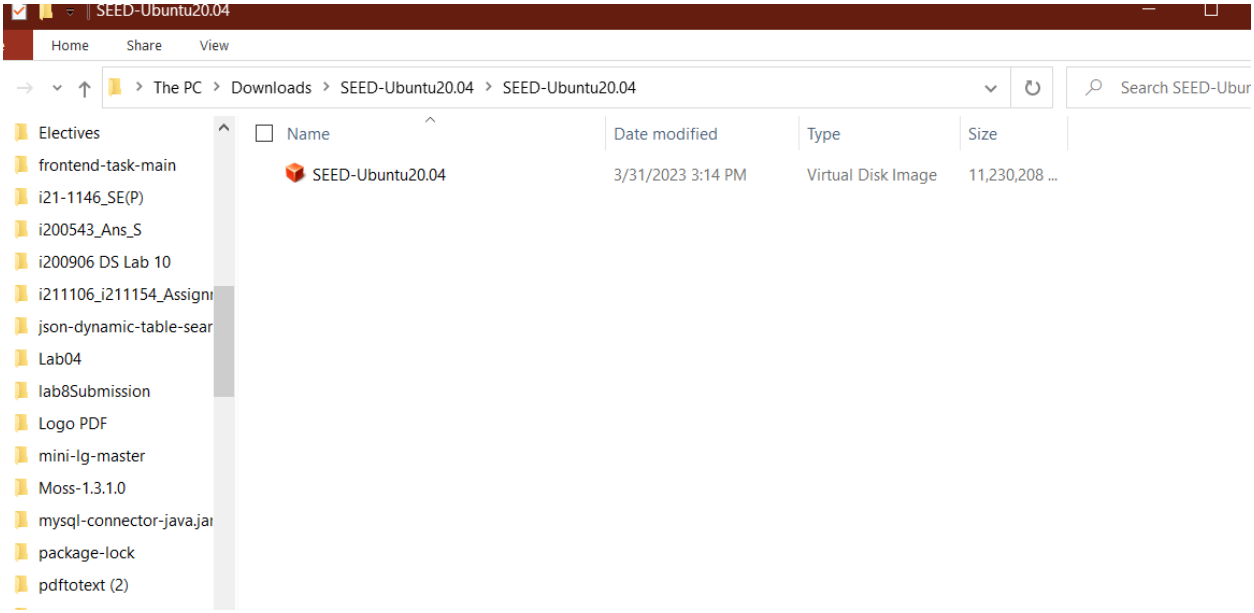
After the installation of the Virtual Box, the VM be appear like as.



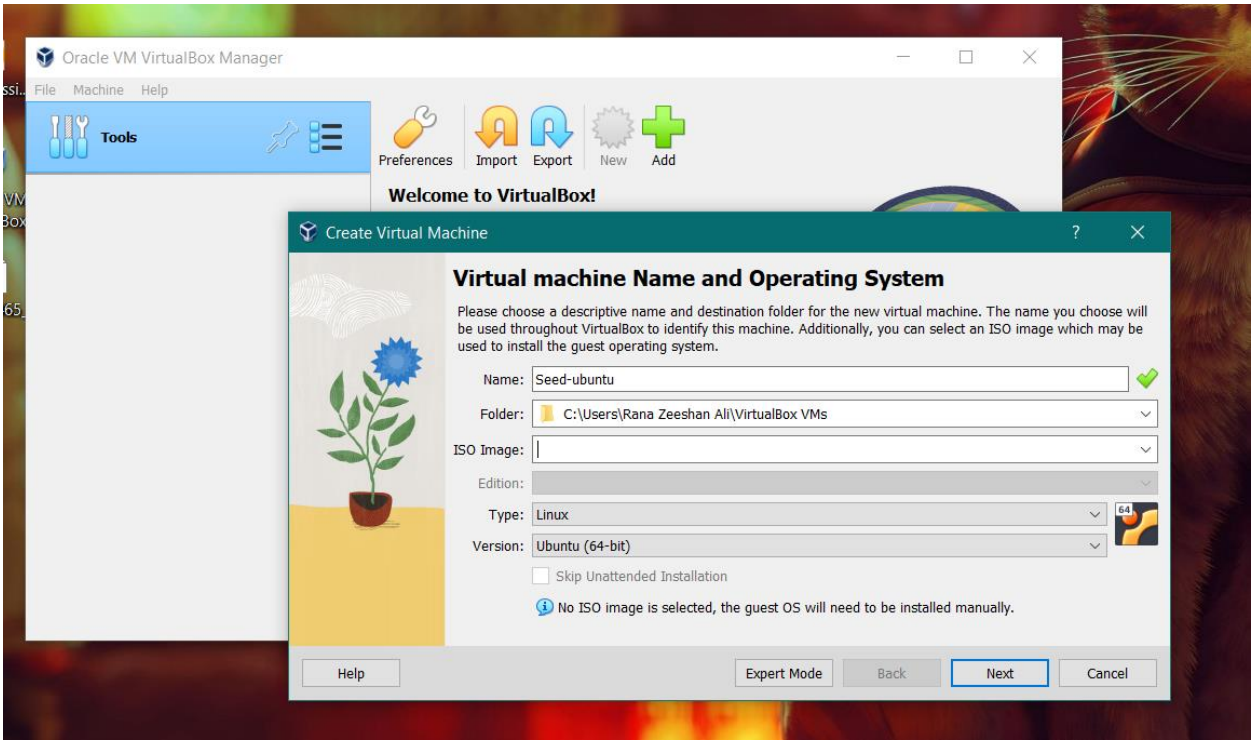
Now, Installing the Seed's Ubuntu, we have selected the version such as Ubuntu 20.04 VM as per requirements in the manual.



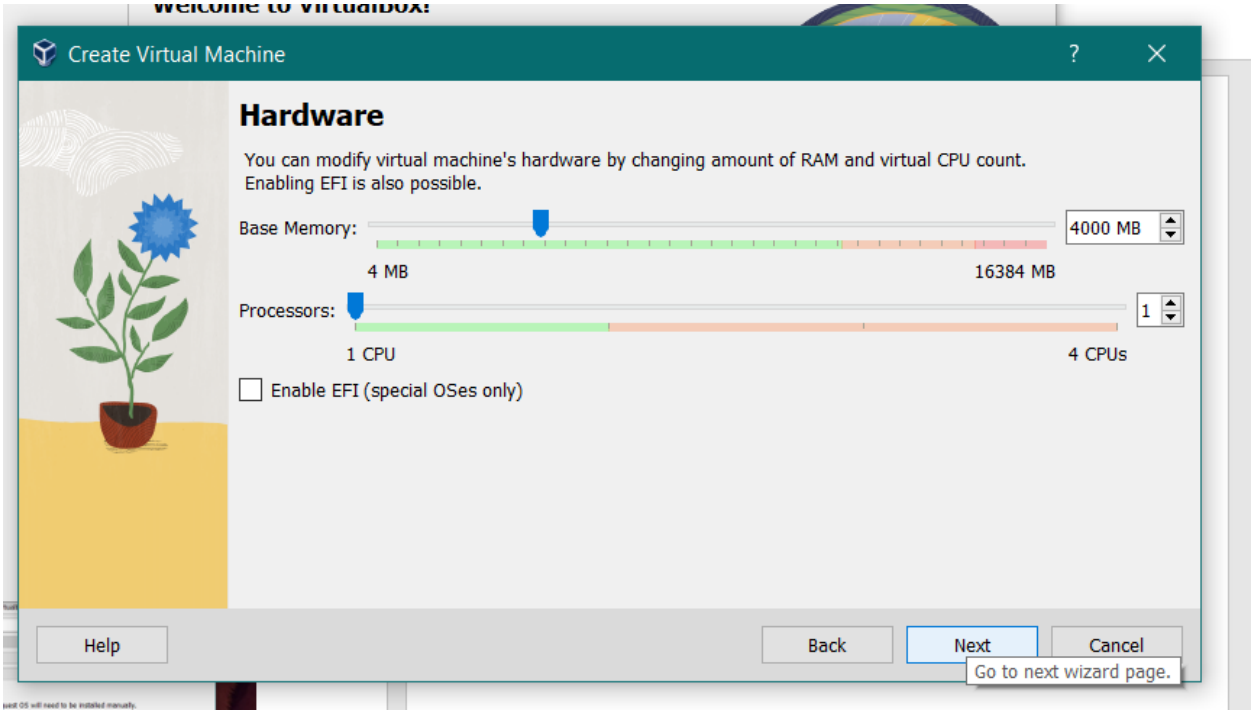
After Downloading and Extracting the zip file of the Ubuntu 20.04, it looks likes.



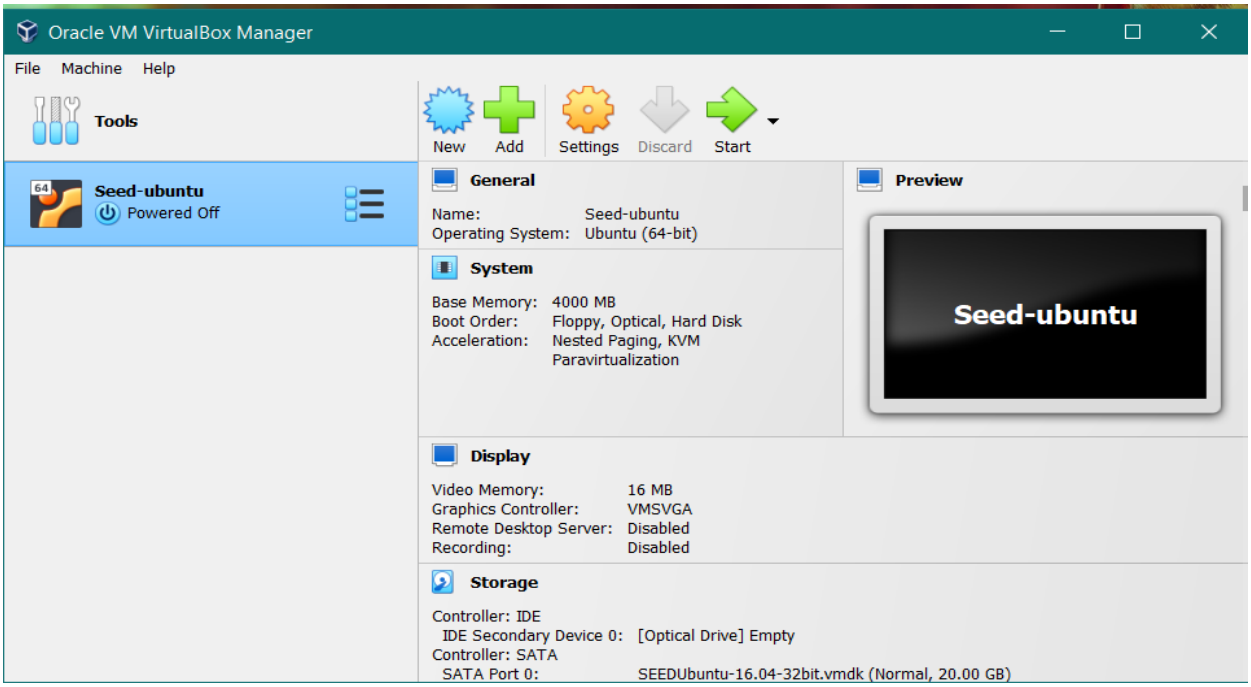
Now, to host the Ubuntu in VM box



Set the Memory Configurations

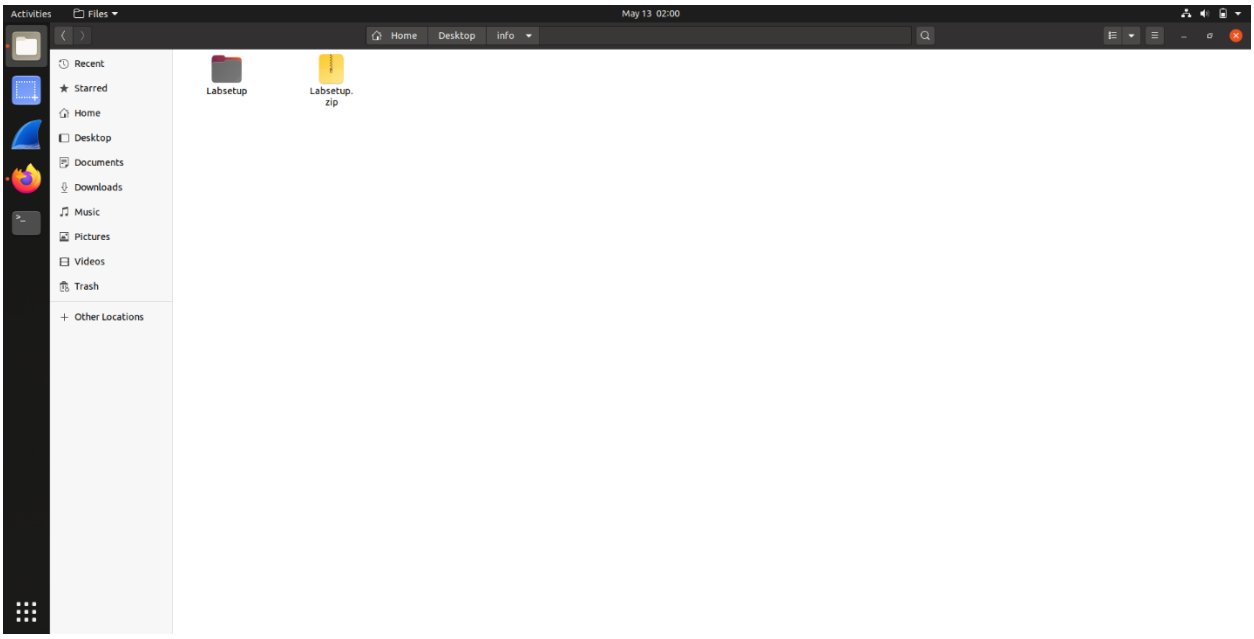


Now, the Ubuntu is successfully hosted.

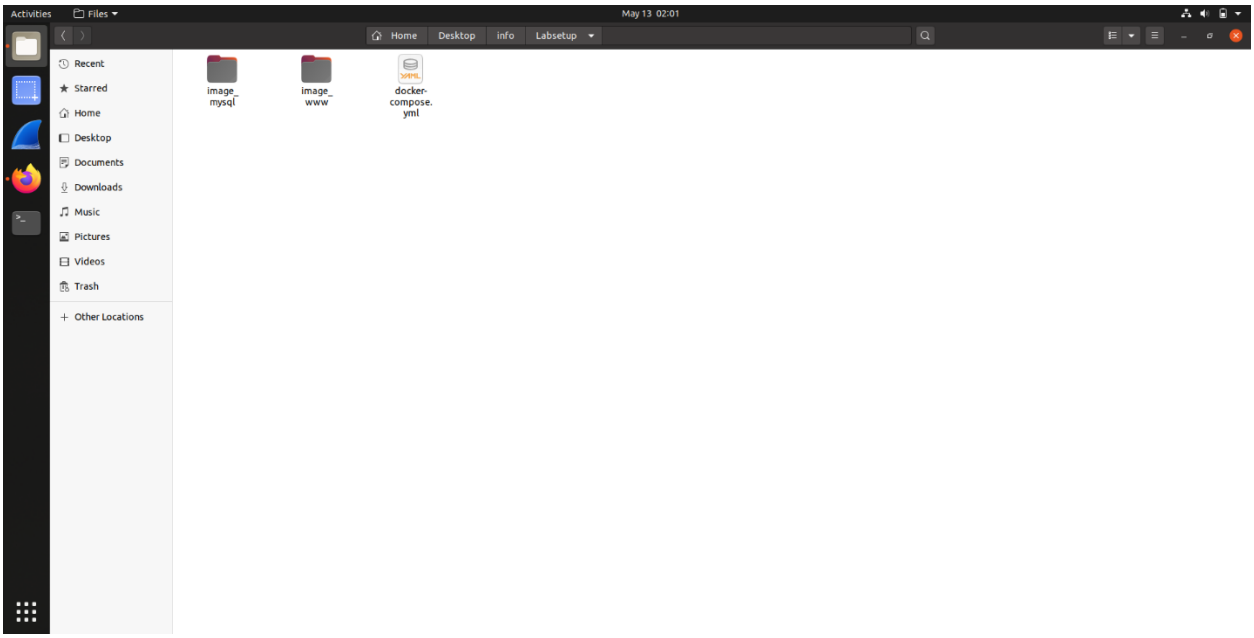


Lab Pre-Requisite Task:

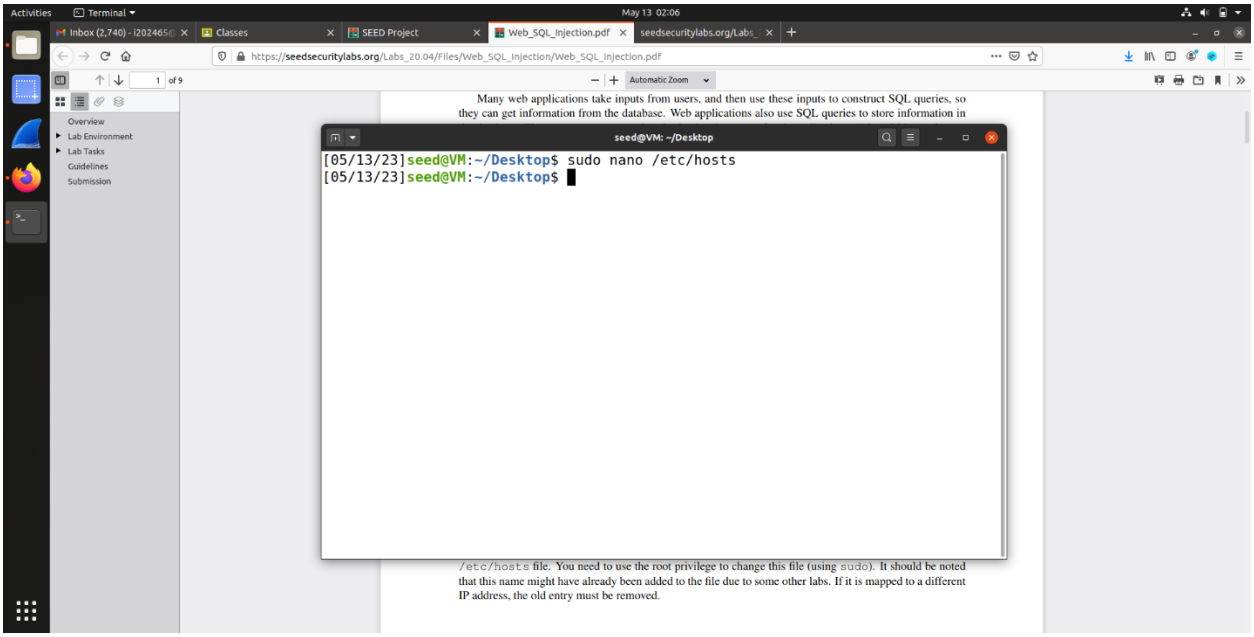
Download the Lab Setup file and extract it.



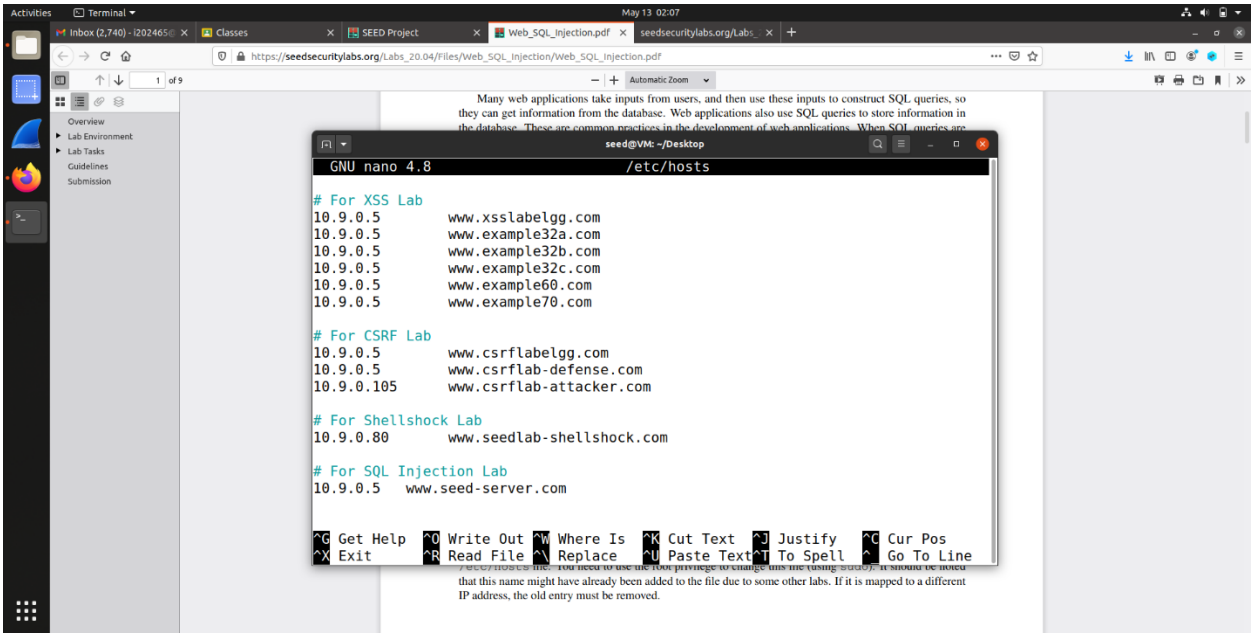
After Extracting, it show all the file and folders in it.



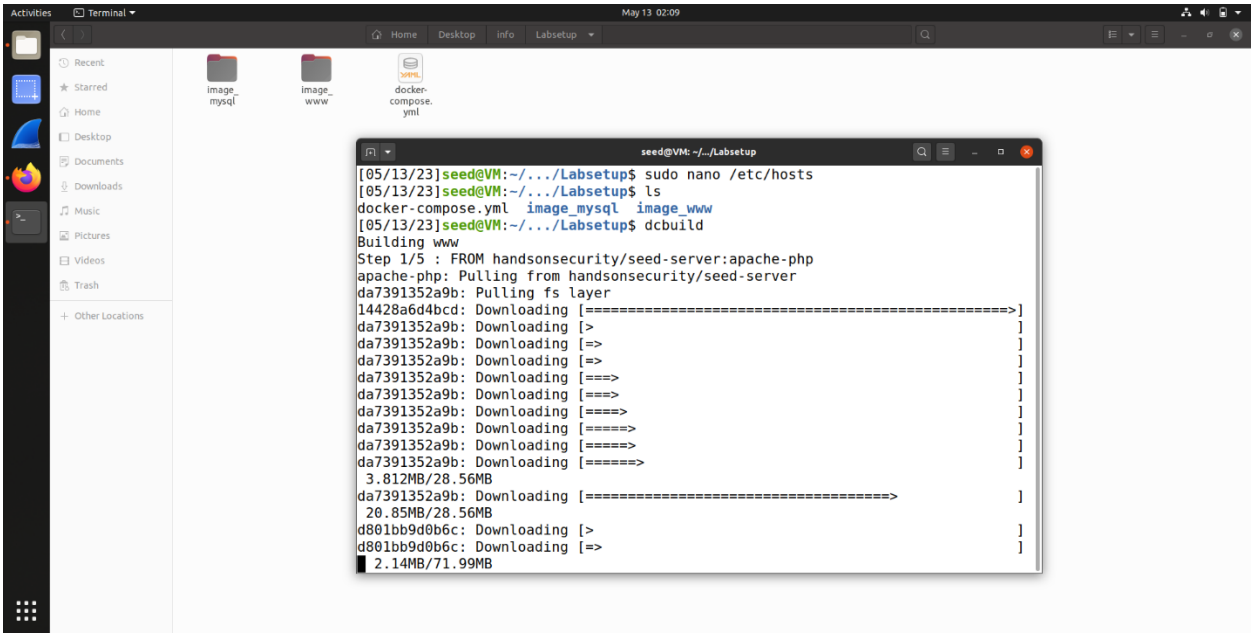
To Assign Ip of seed-server website to run on chrome easily.



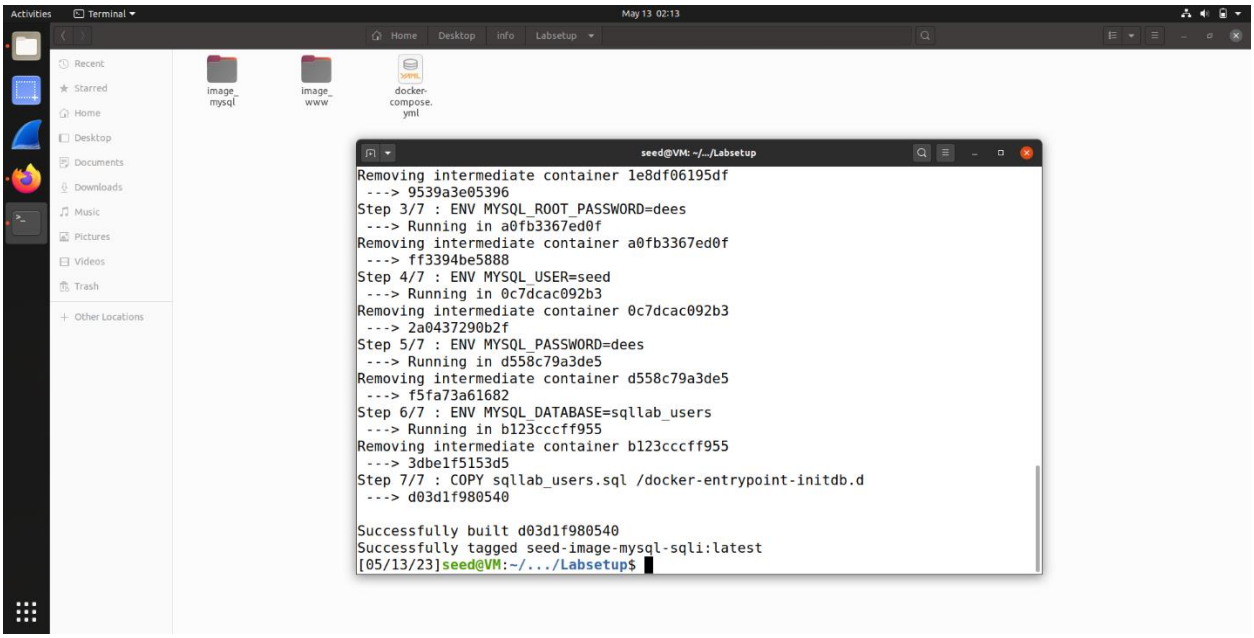
Add manually 10.9.0.5 www.seed-server.com in the file using the command line interface.



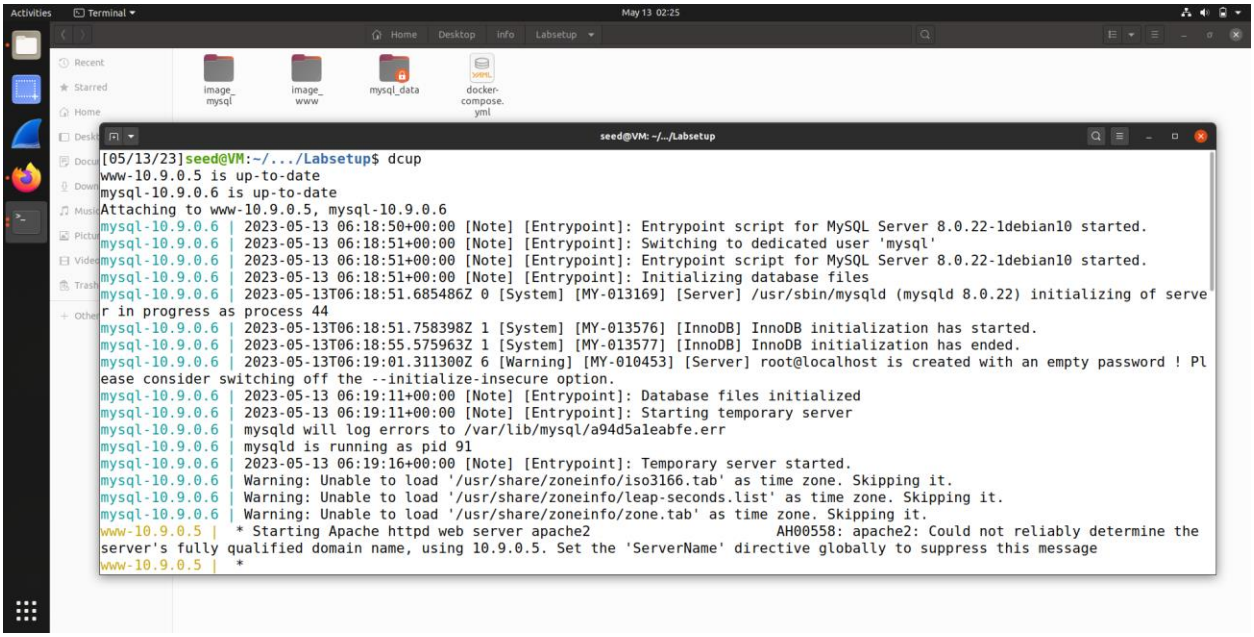
To Build the docker to make the containers of your website frontend and backend.



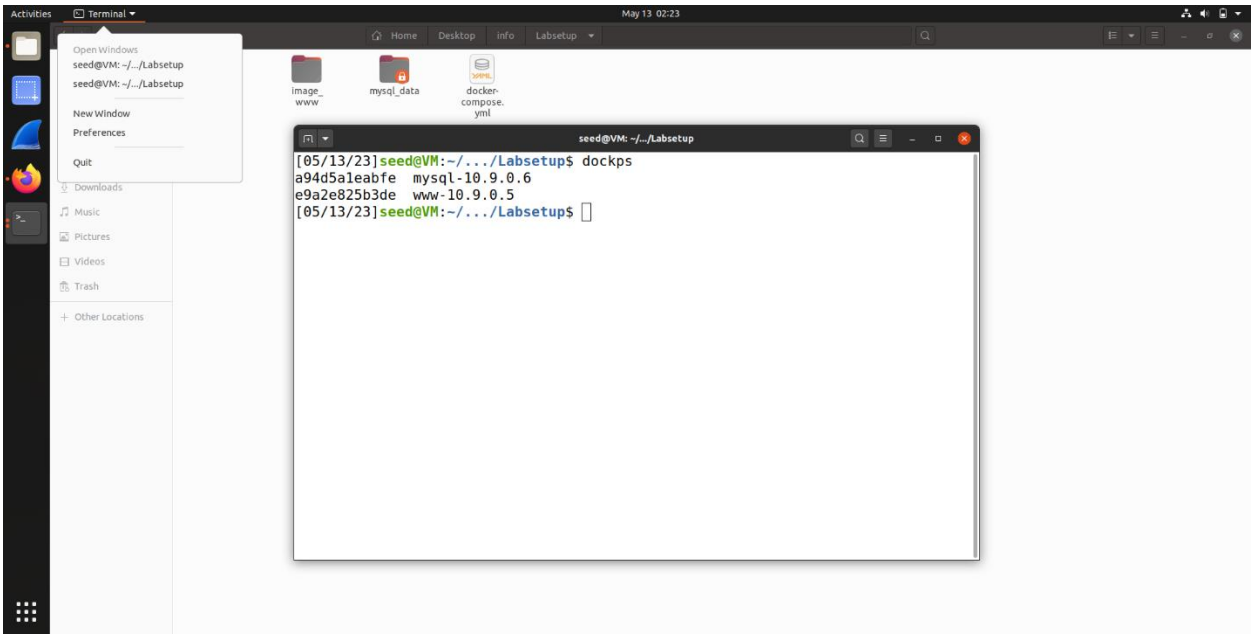
Now the docker build command is successful and docker containers are created.



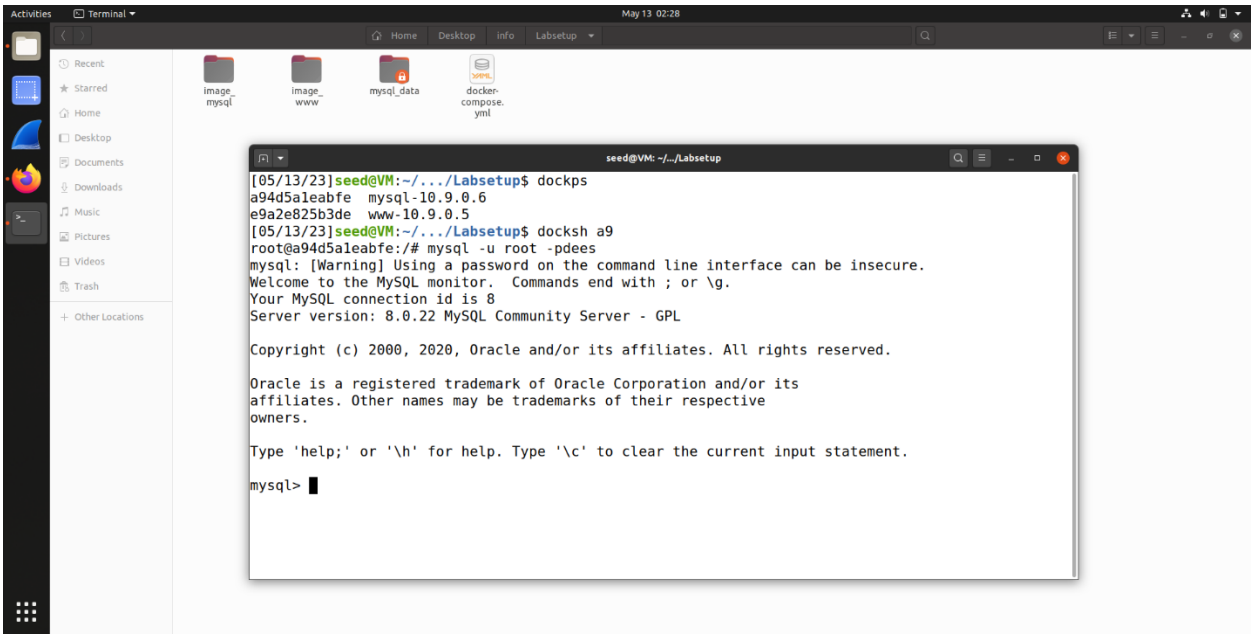
To run the containers, we use docker up comands to make them in running state.



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

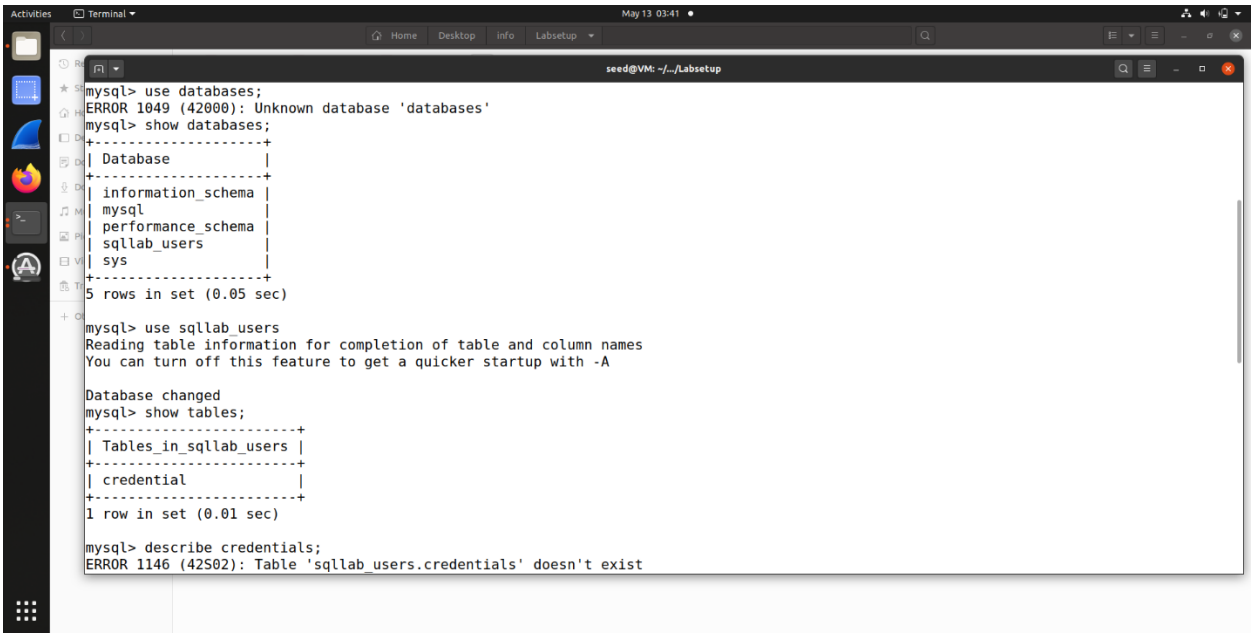


Now, to login into specific container use docksh container id.

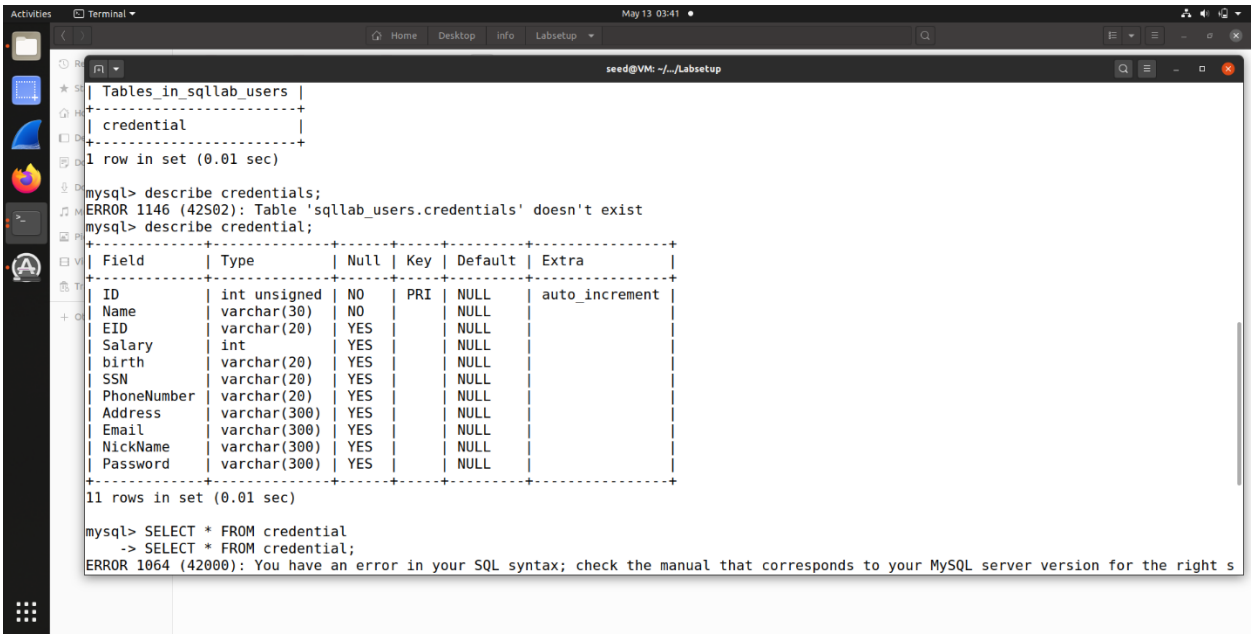


Task-1: Get Familiar with Sql Commands

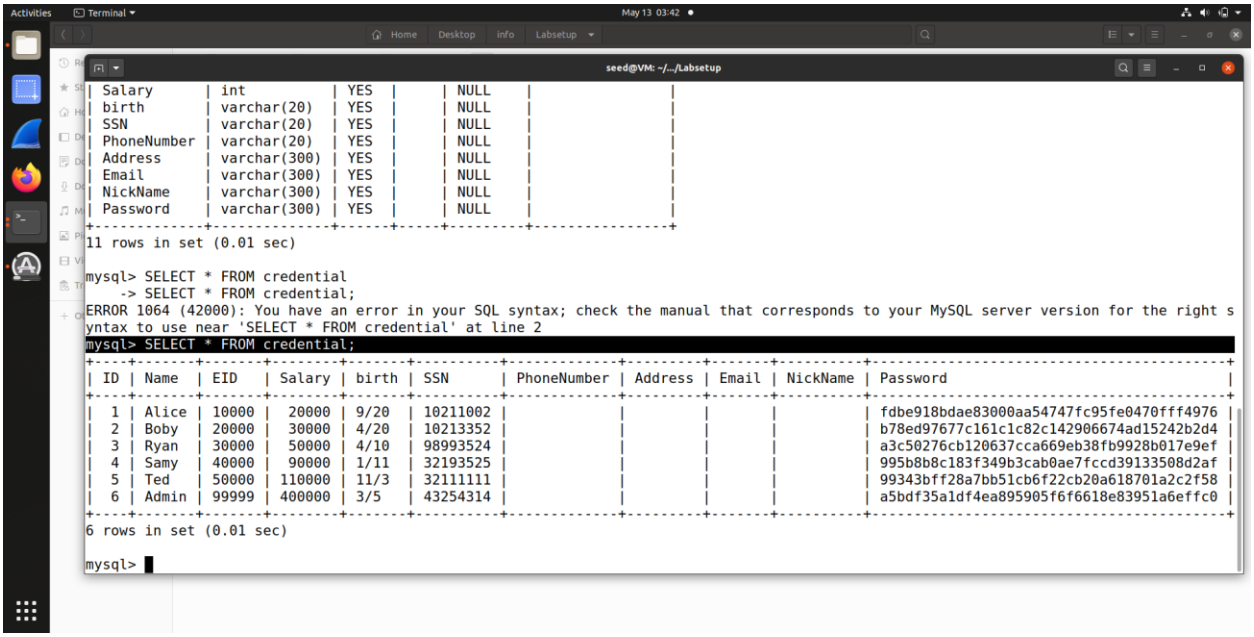
Now, to check the database and tables into the sql folder, these are following commands.



Now, to check what are the fields in that tables.

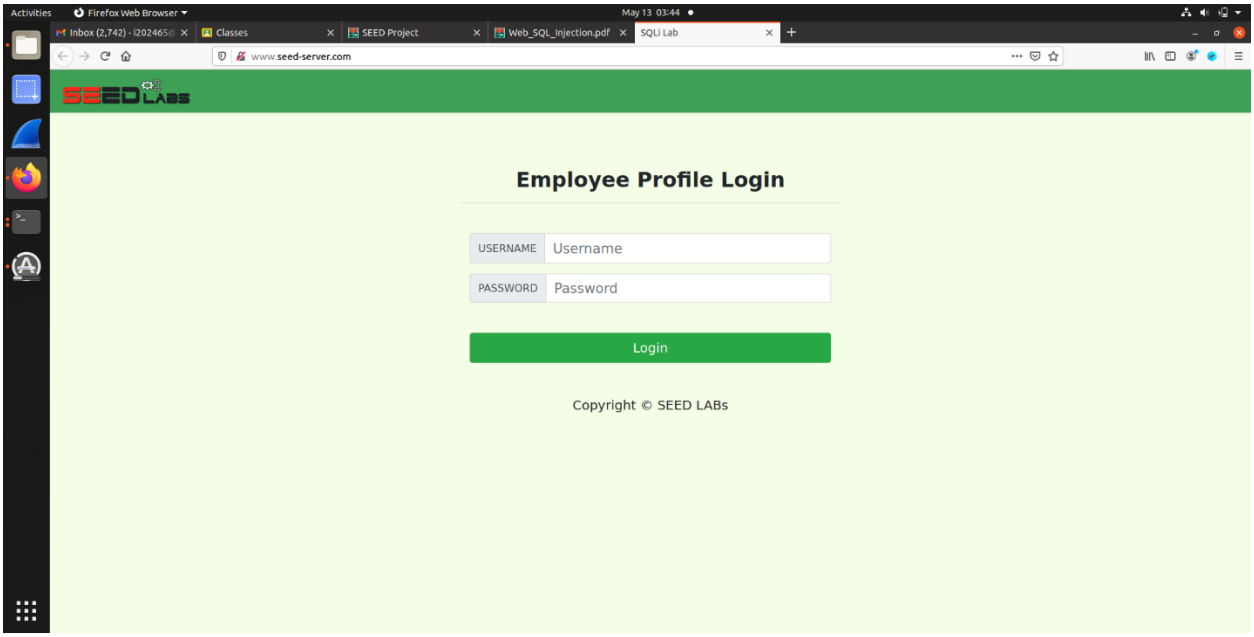


Now, to check what are the data in the credentials table. Displaying the data in the table.

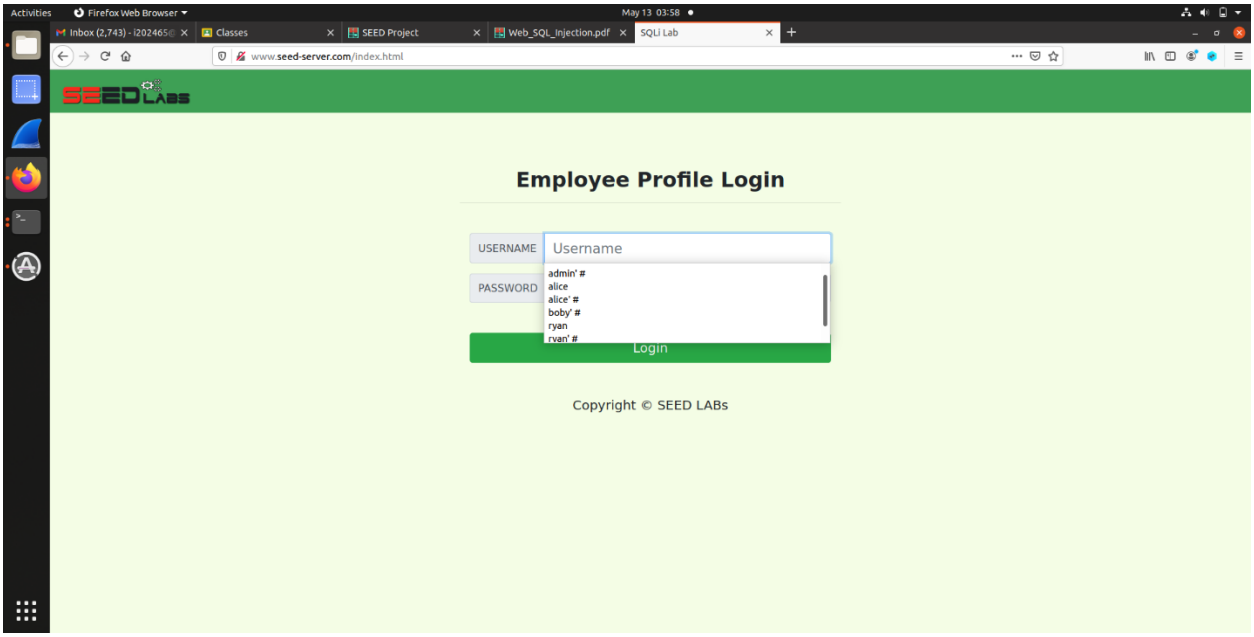


Task2:

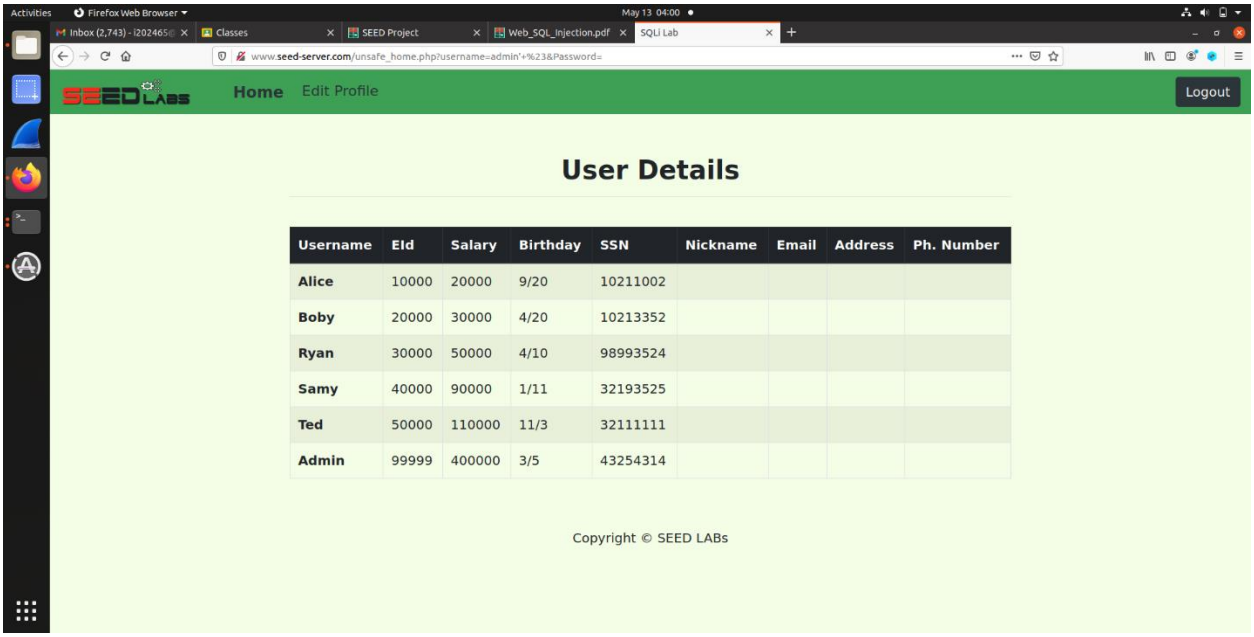
First run the website into the chrome browser.



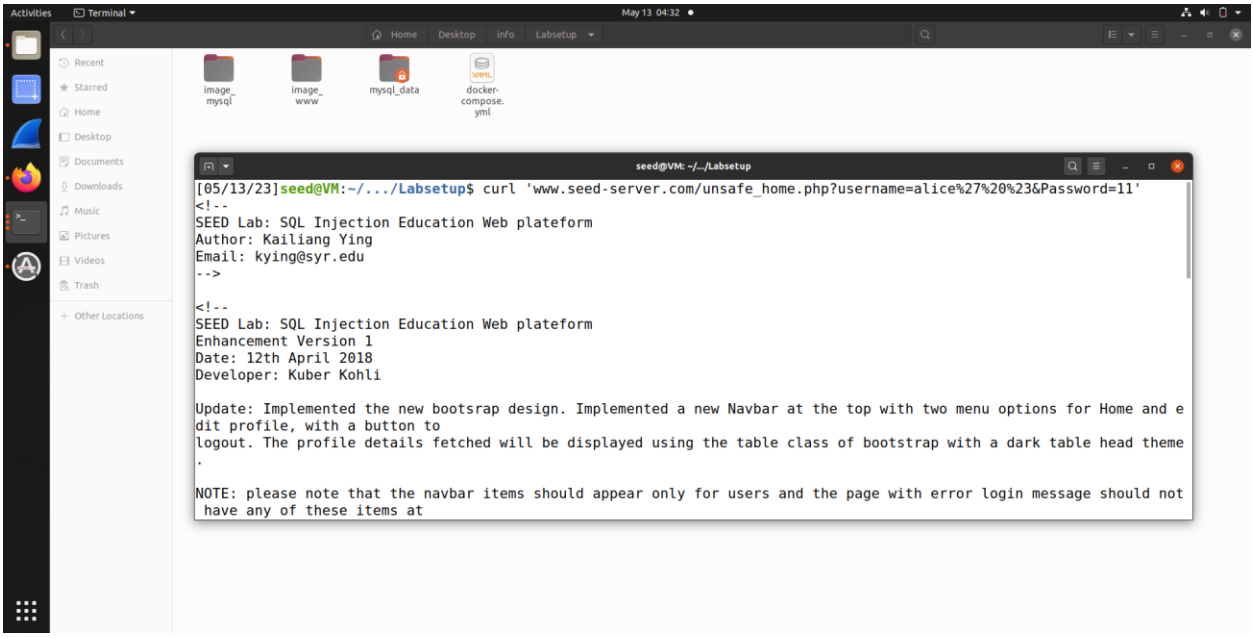
Task: 2.1: Firstly, login into the website by real login and login by Sql injection commands and the commands are admin' #.



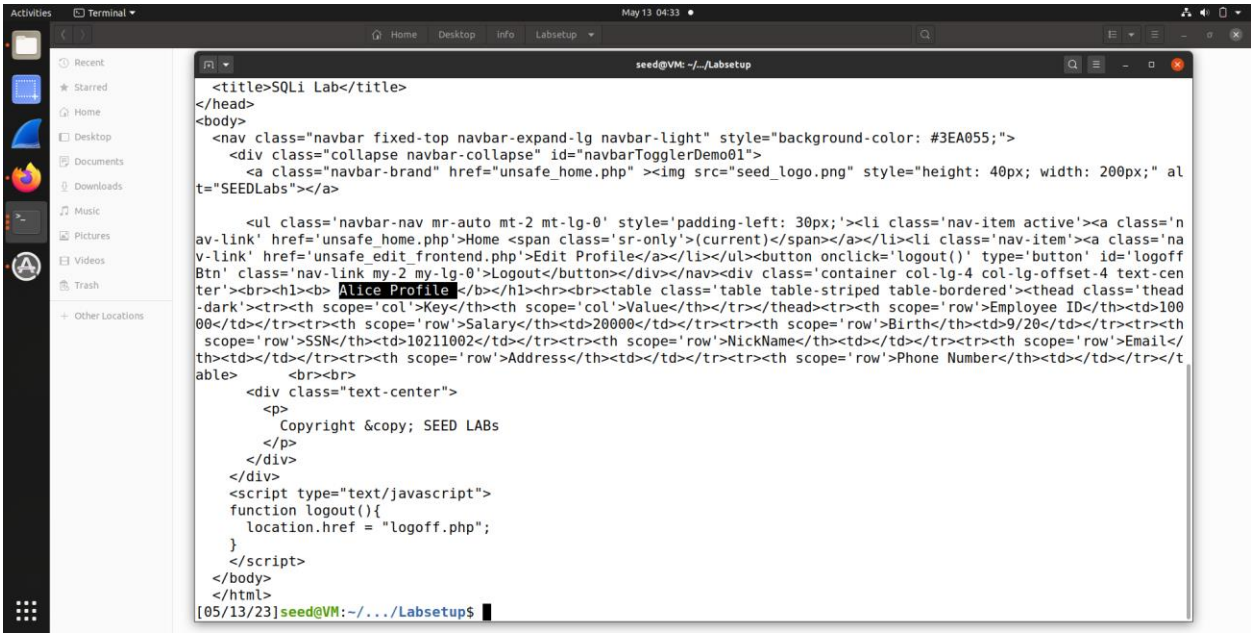
After sql injection command on admin account, it displays all the details about the user that are registered on our website.



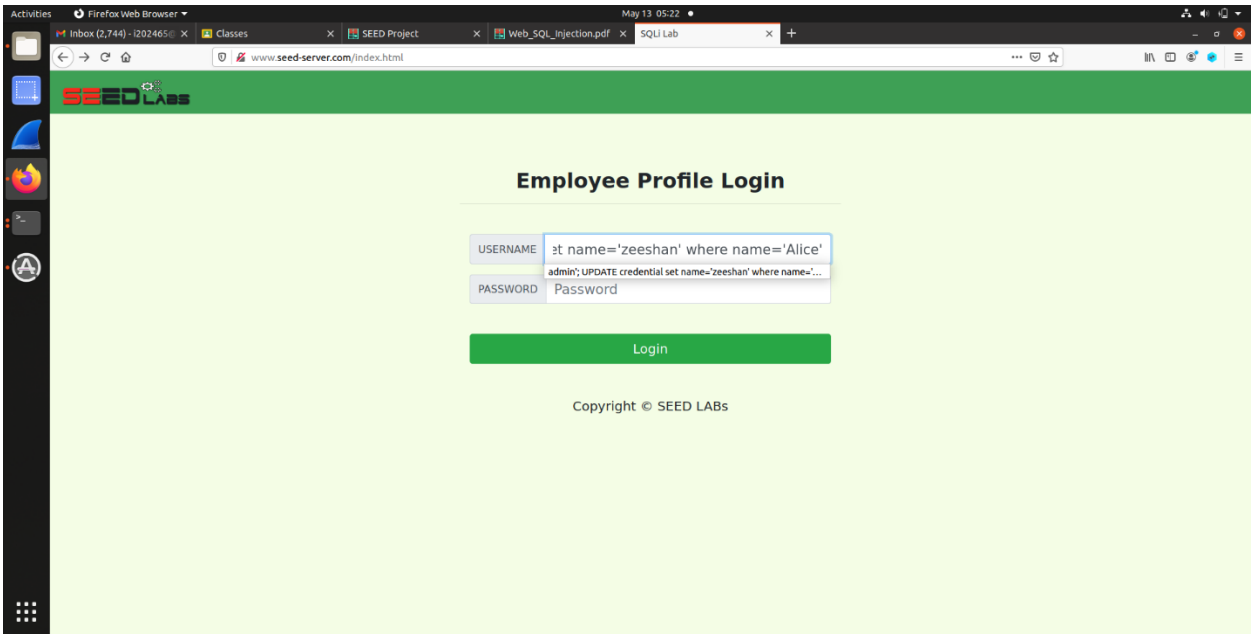
Task 2.2: Now, doing sql injection by command line by adding %27%20%23 for space and comma or hash value.



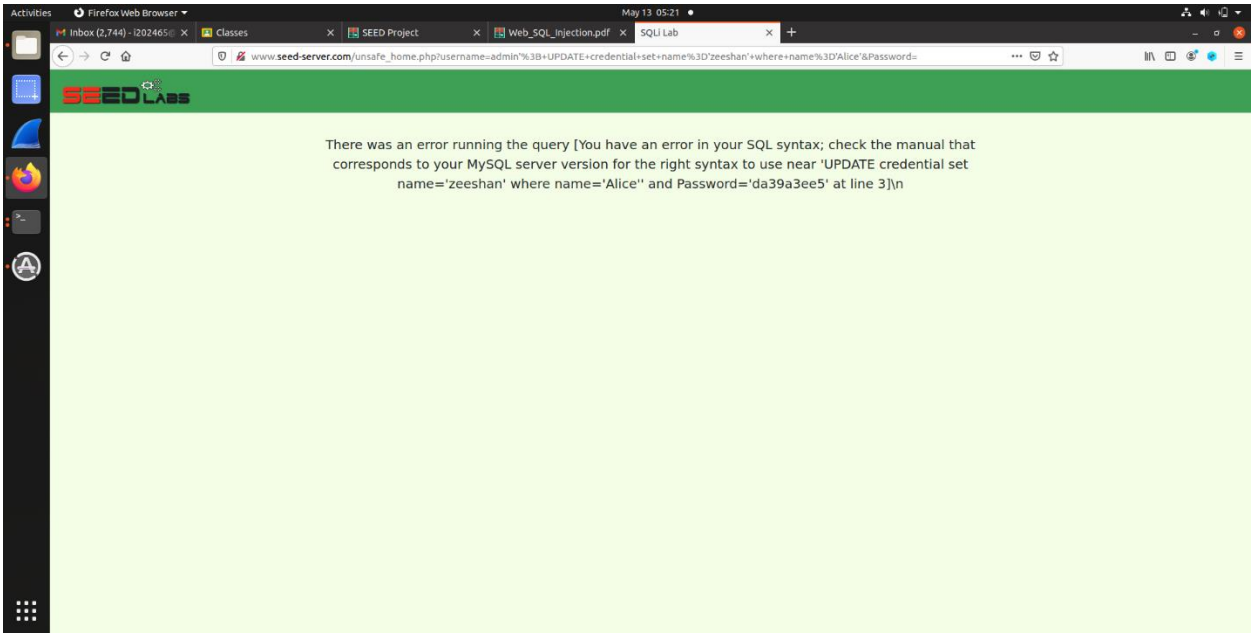
Now, I have done the Sql injection successfully and login into the Alice profile and the picture demonstrates all the details of the Alice profile.



Task 2.3: Now, append the new sql statement and check what does it behaves.

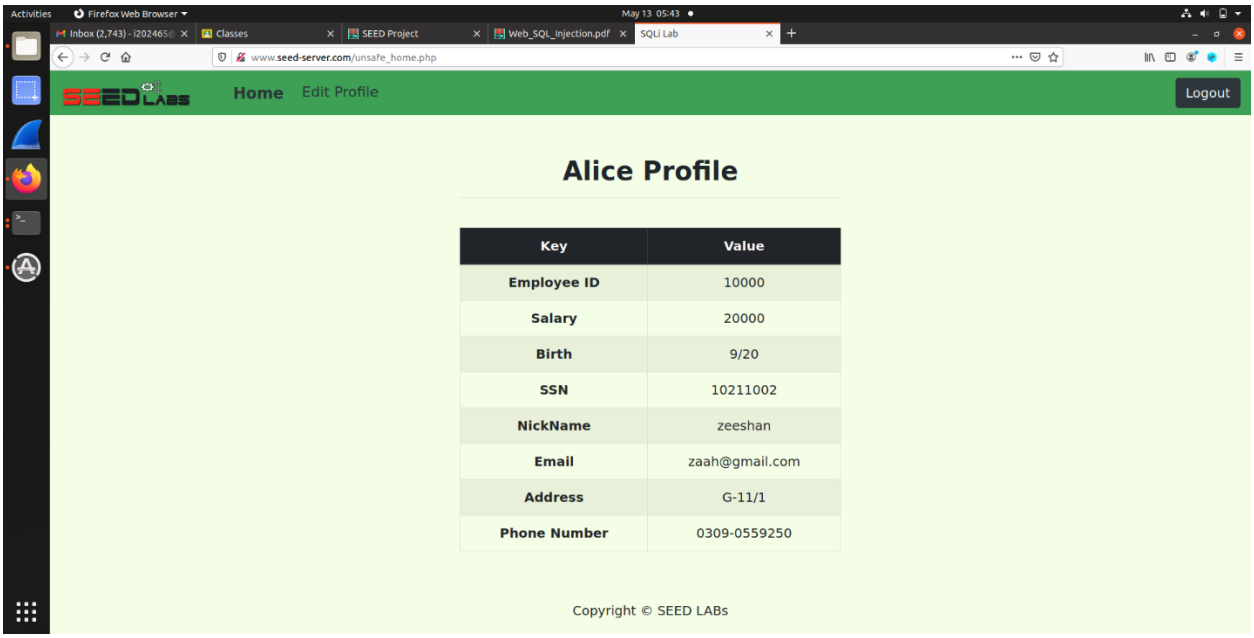


It does not entertain the multiple Query in the login field, so it gives such error.

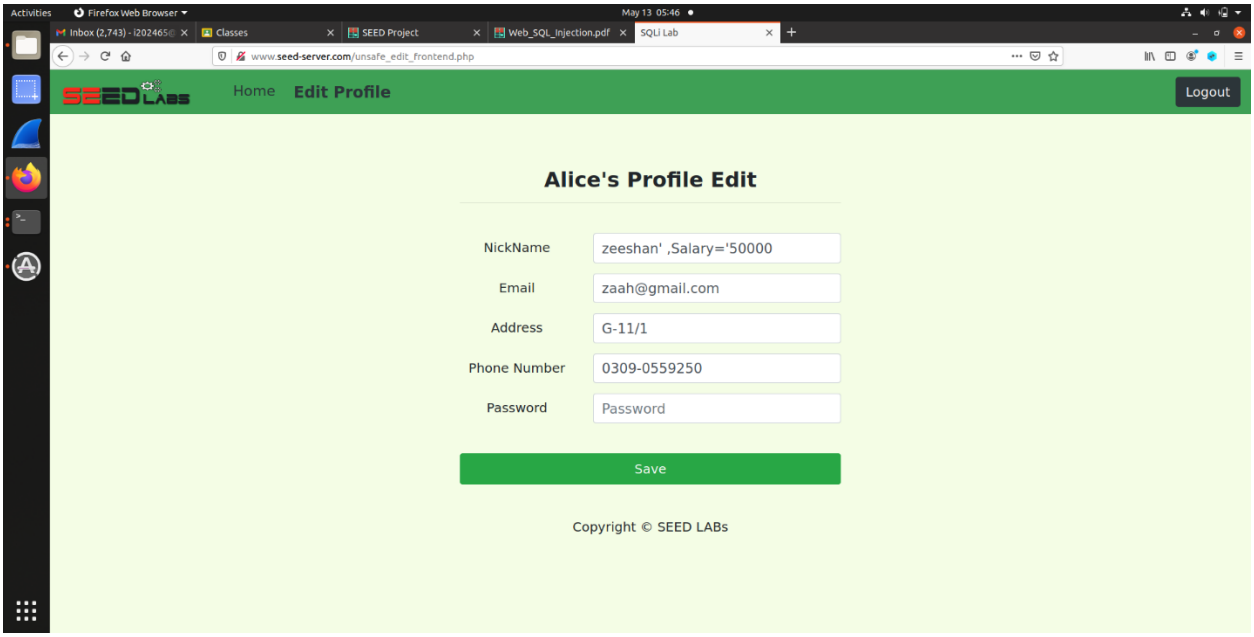


Task 3:

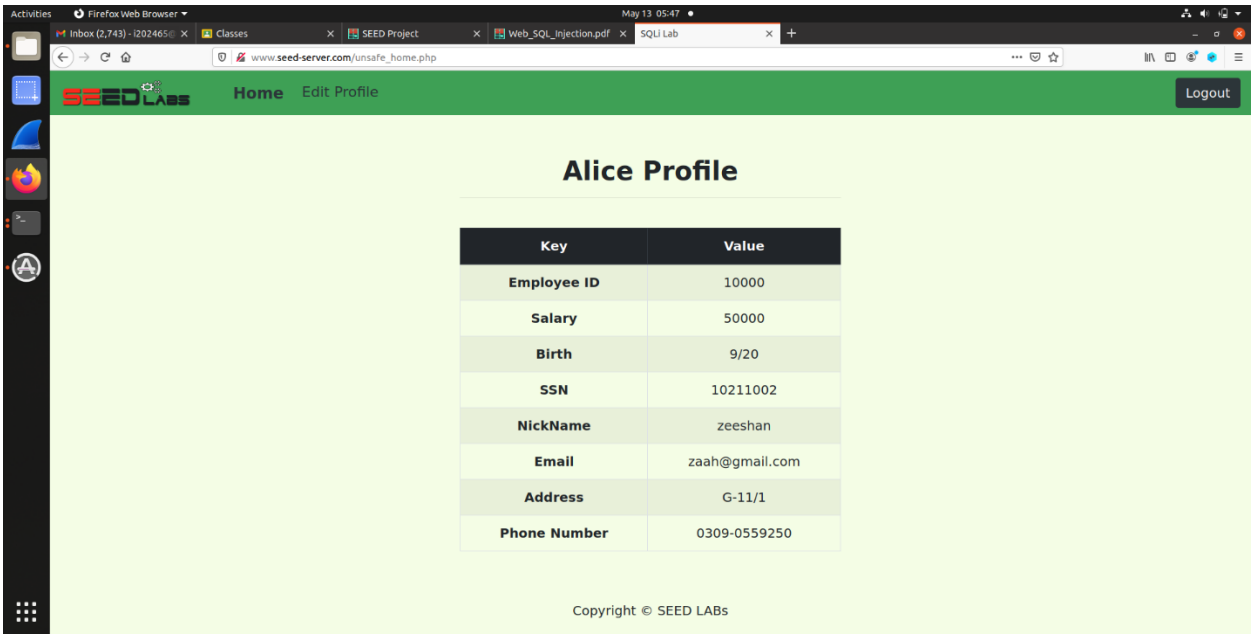
Firstly, these are the Alice Profile details that perform all the tasks.



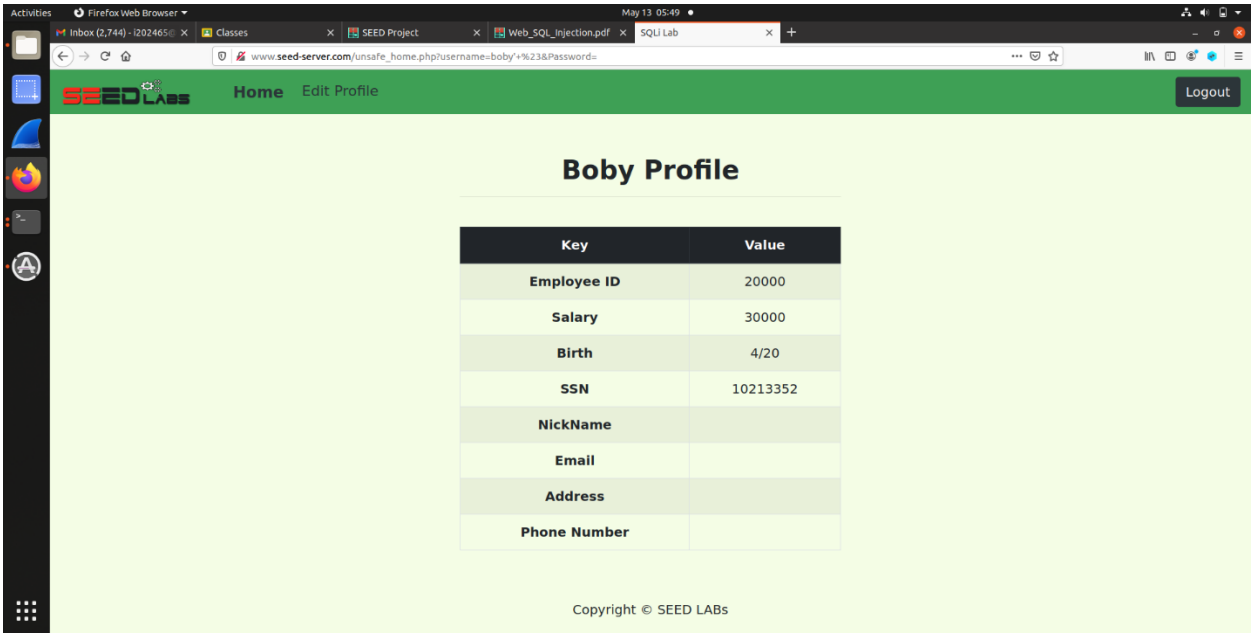
Task 3.1: Alice would change his salary by doing sql injection and the command is written in the Nickname field area.



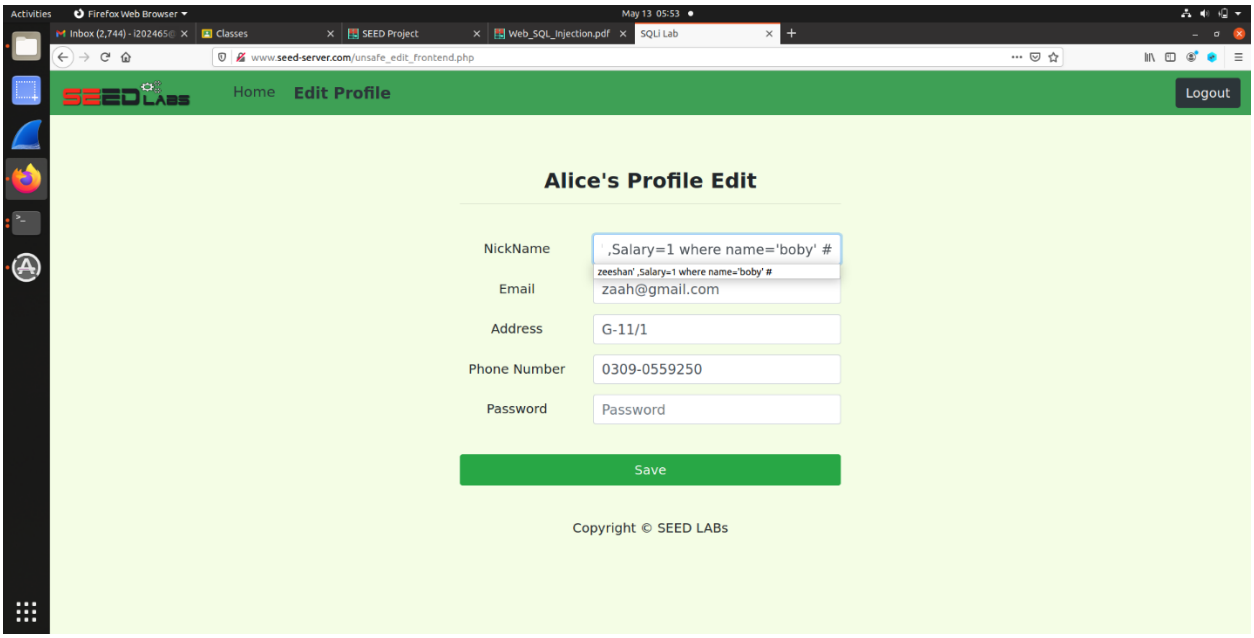
Now you can check, the salary of Alice is updated when SQL injection is successful.



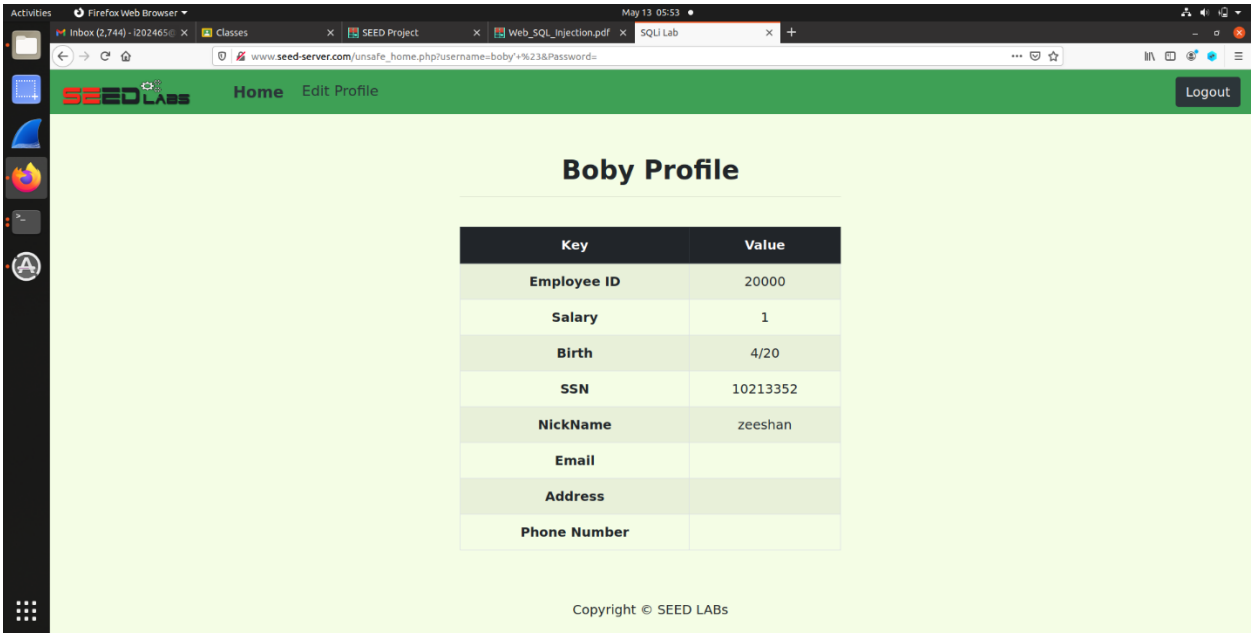
Task 3.2: This is Boby profile picture; the task is to reduce his salary to 1$.



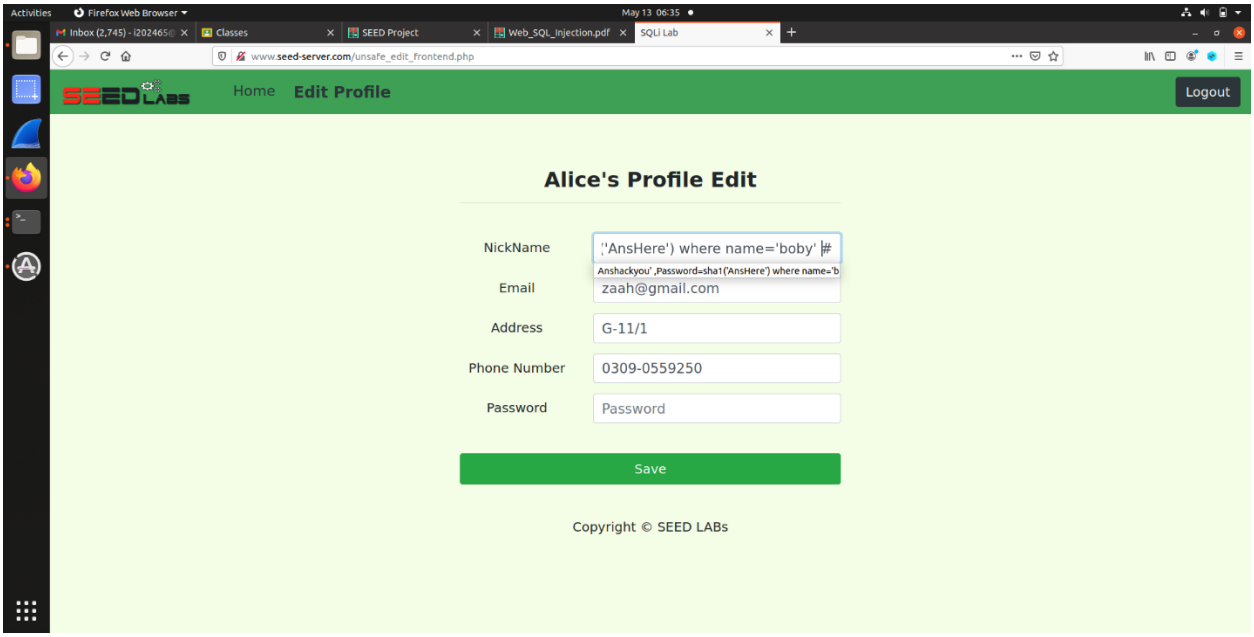
Now there is the command to the SQL Injection, Alice would do with boby profile.



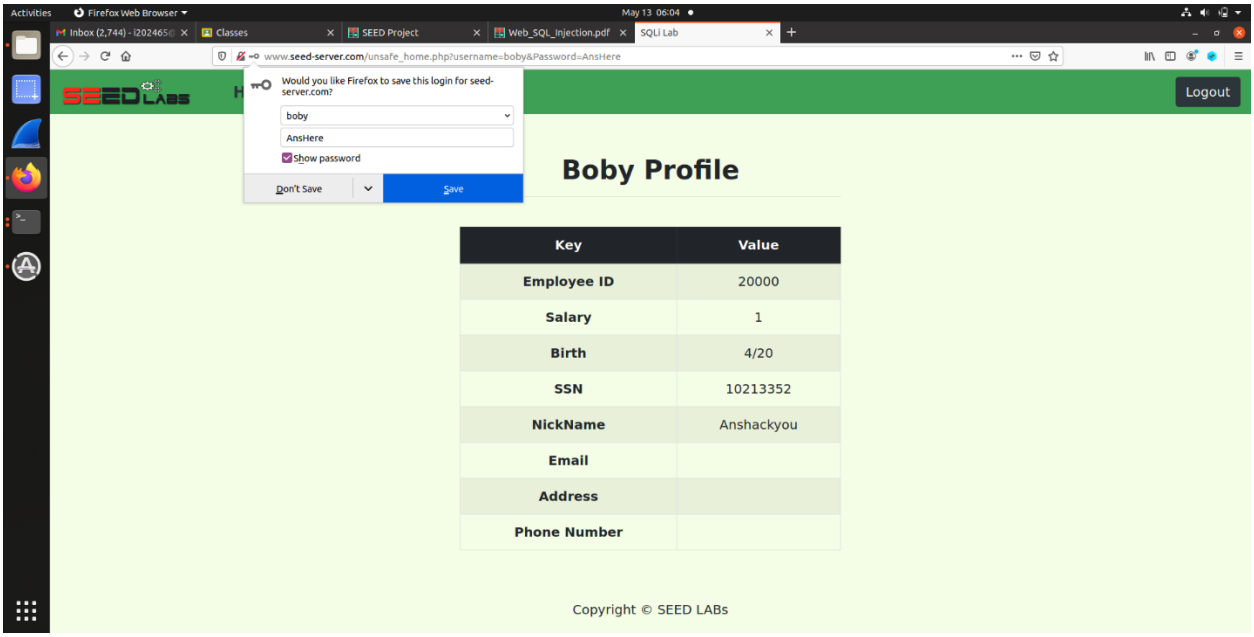
Now, here is the boby profile, it will change when the SQL injection is successful.



Task3.3: To change the password of the boby profile, Alice would write this command that will change the password.

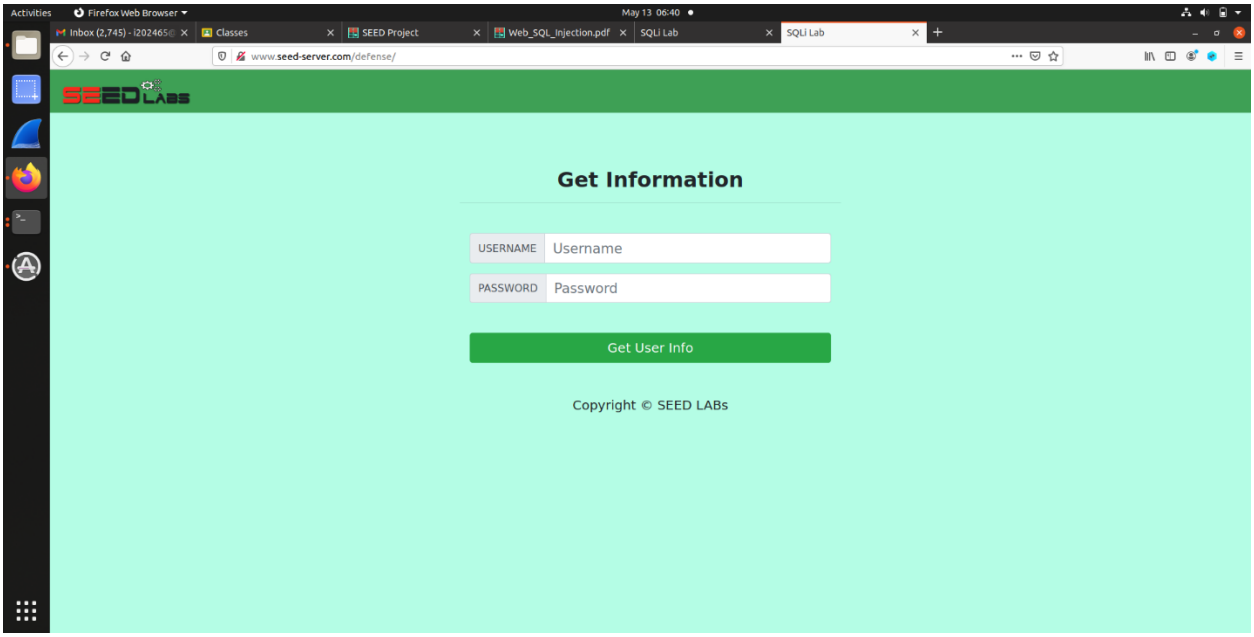


Now, in this picture the update password is displayed and I login with the new password and successfully access the boby profile.

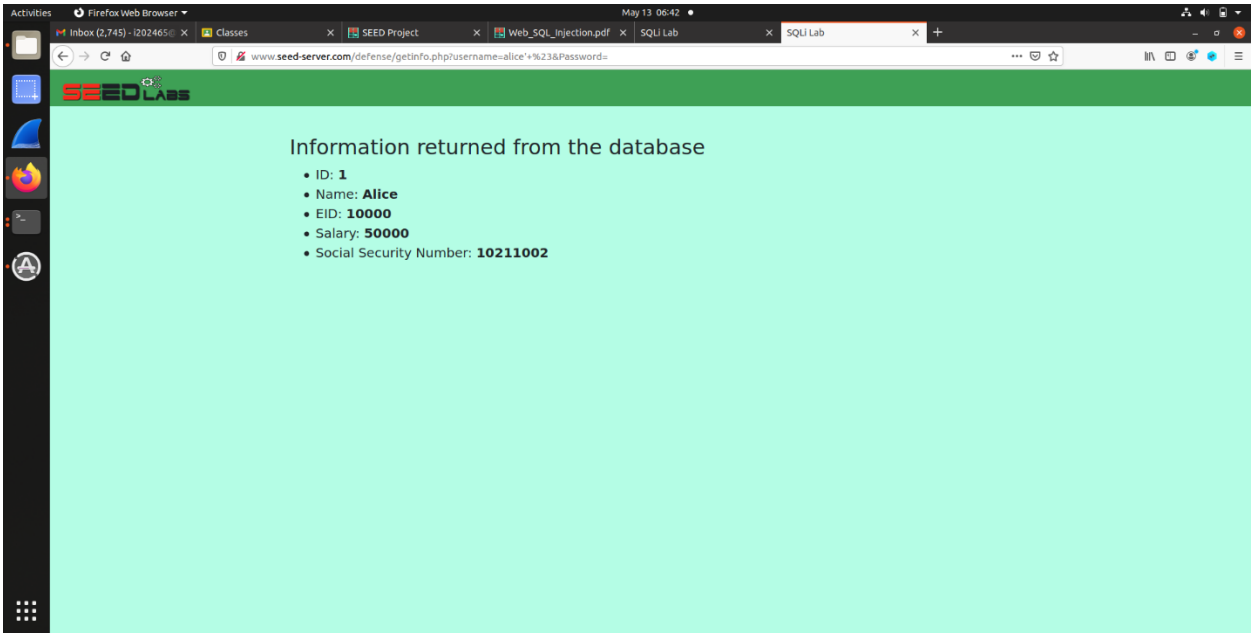


Task-4:

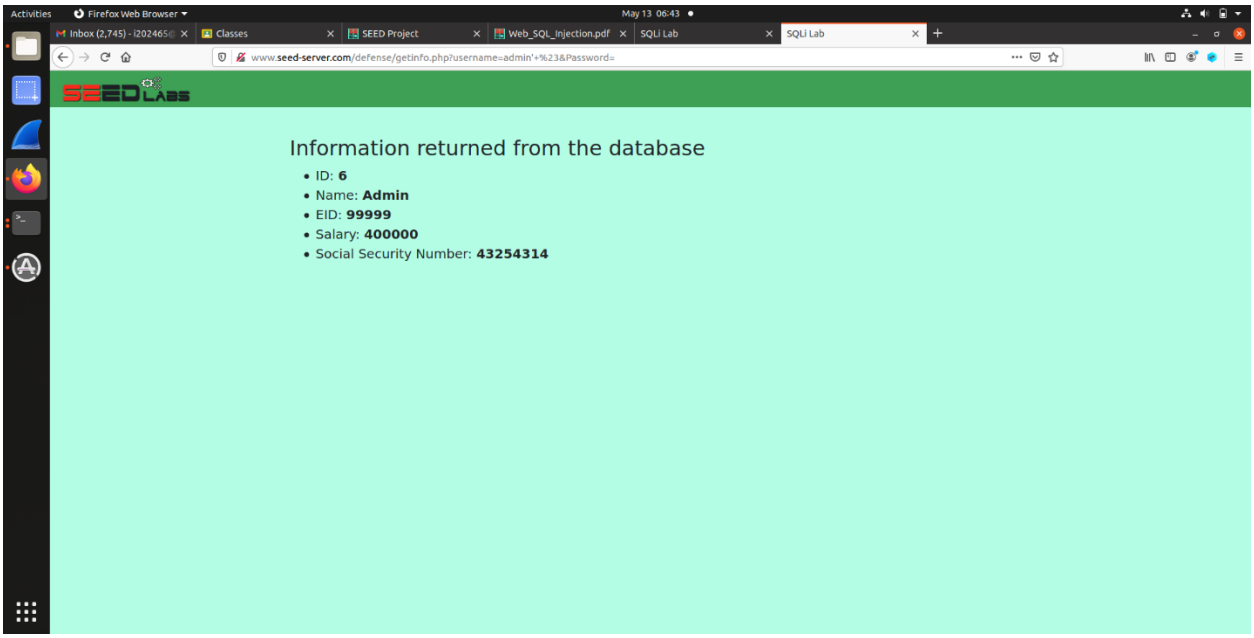
Counter Measures: use this website in the defense version. It interface looks like.



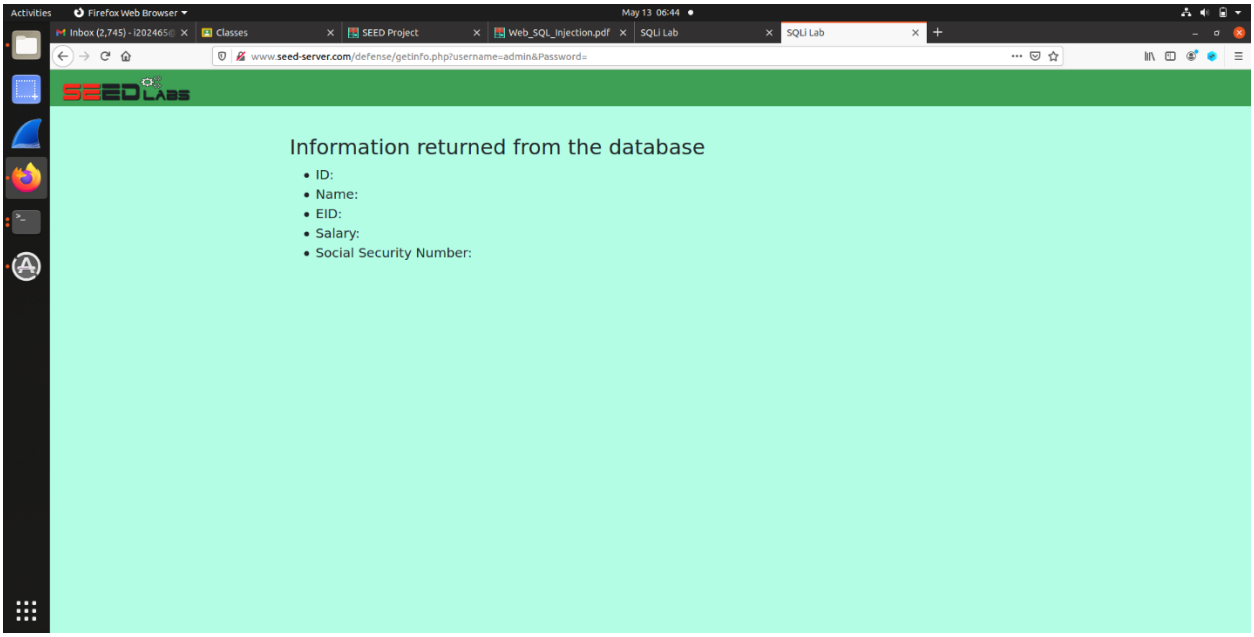
When I login to Alice profile, it displays its information looks like.



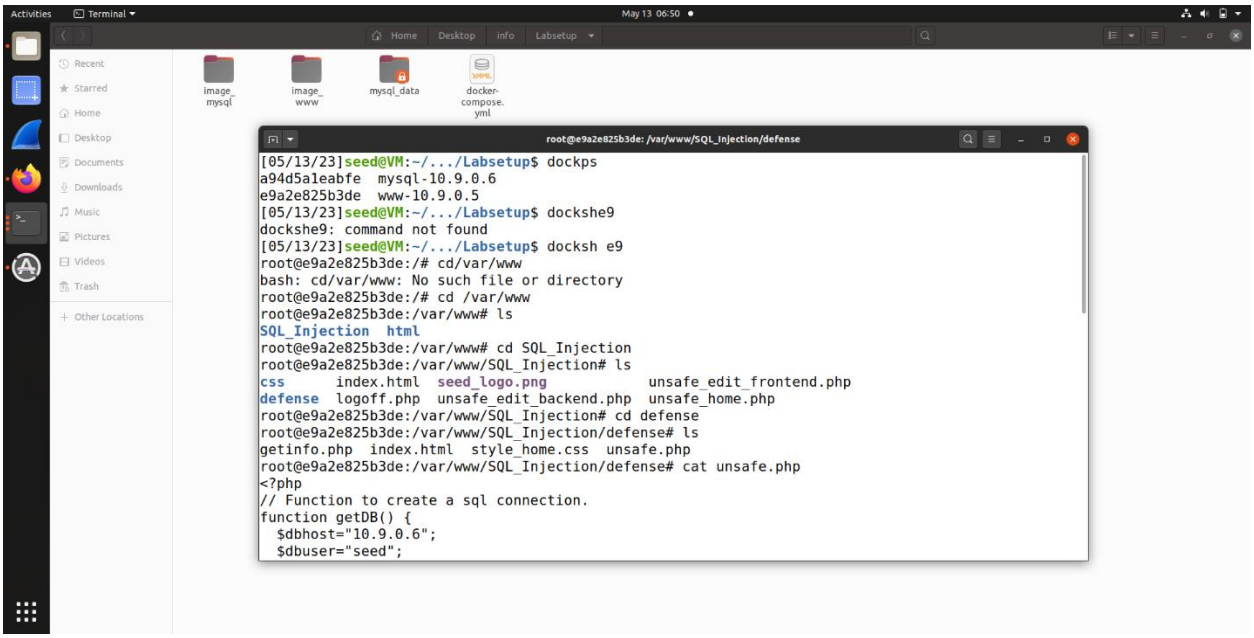
When I login to Alice profile, it displays its information looks like.



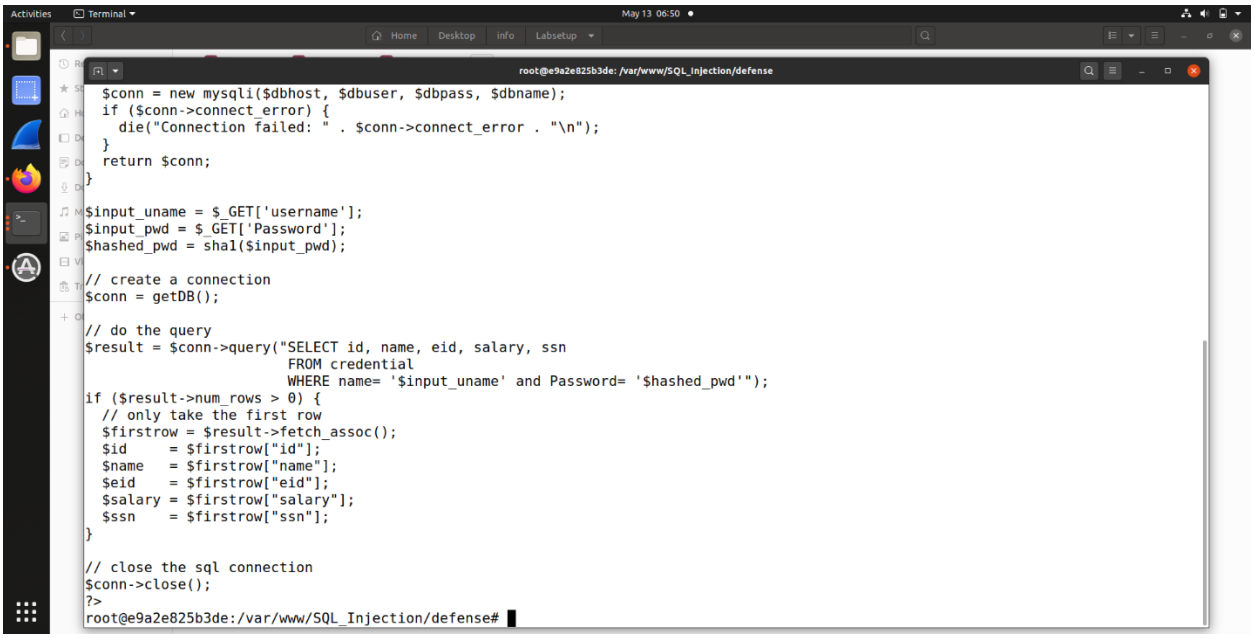
When the user didn’t fill in full info, it displays info look like.



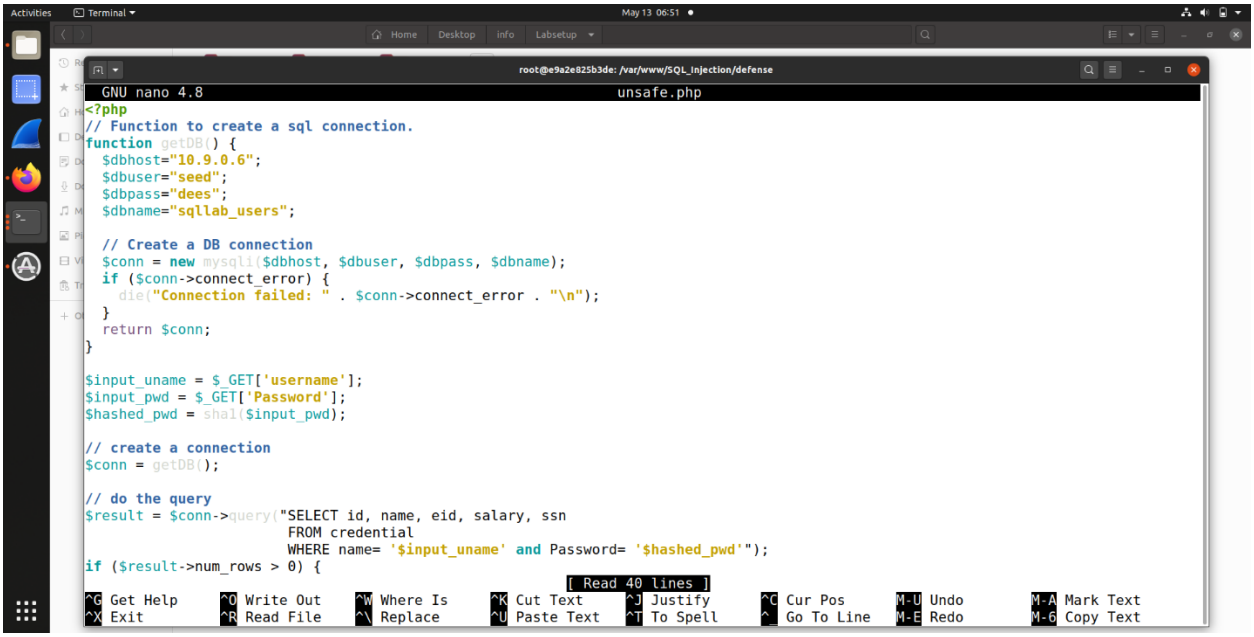
Now login to the website container, get into the code to change the vulnerabilities.



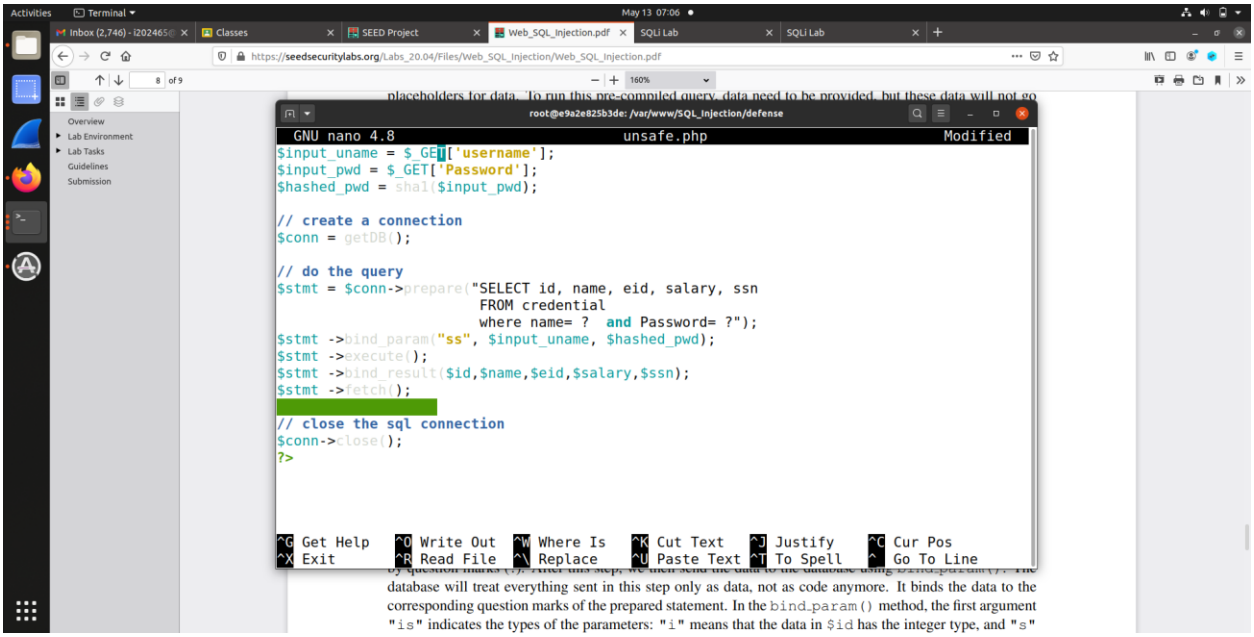
This is the code that has input to all SQL injection.



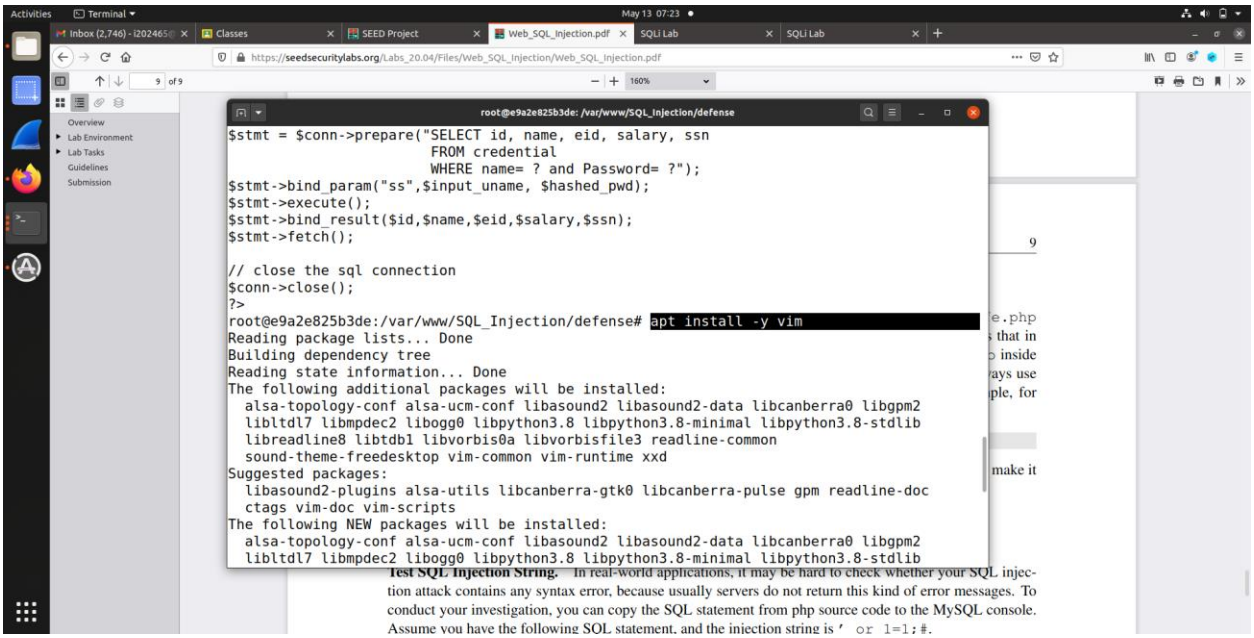
Now, change this code to reduce all the vulnerabilities.



This is the update code that caters to all the vulnerabilities about the SQL injection and stop all wrong input values in the input field.

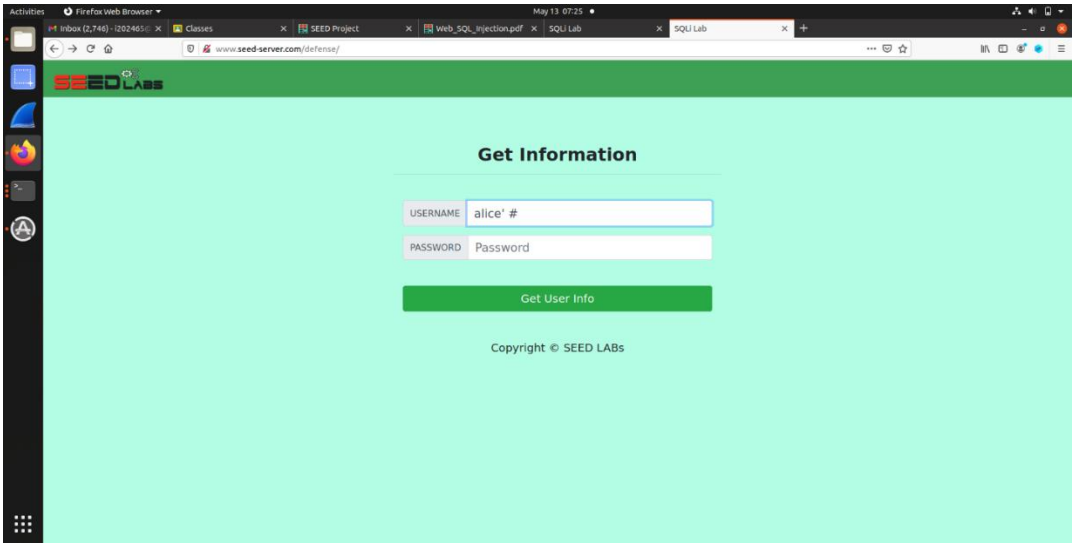


Now, to store all updated permanently in container of that website, I run the highlighted command.

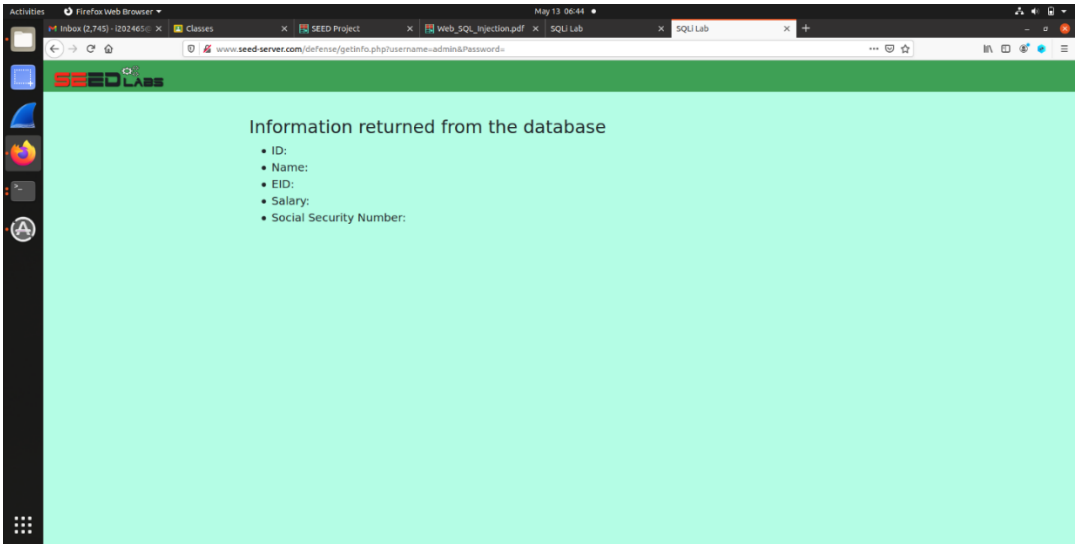


Now, again test the SQL injection command to check the vulnerability of the login page in the updated version.

Now, I am logging into the Alice profile.



The SQL Injection command does not work, and it only displays the empty information.



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