MAIN TASKS
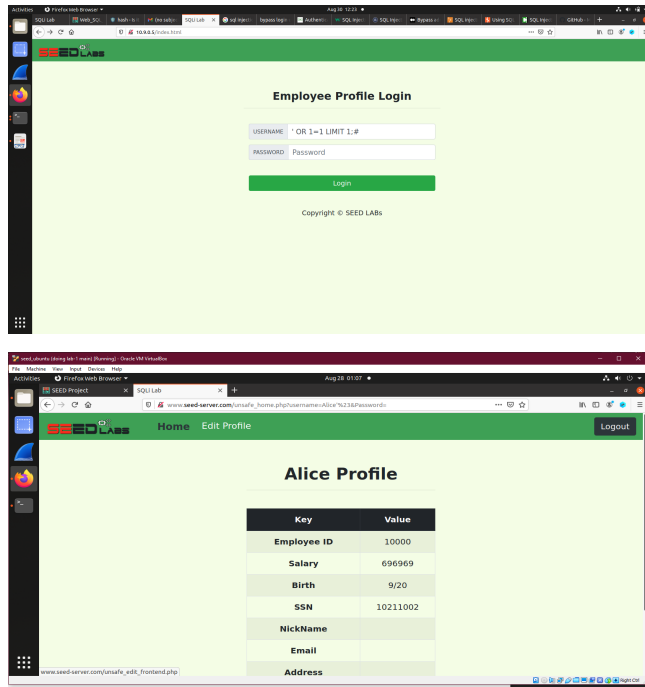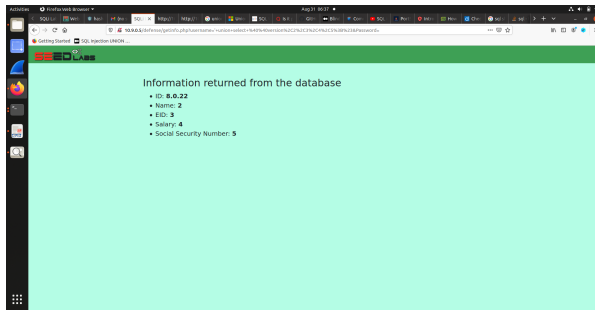
TASK-1:


So to do the first task I have to write <' OR 1=1 LIMIT 1;#> to enter into Alice's profile. For this command we don't need to know the password because the mysql is executed in such a way that the password part is commented out.

TASK-2:

As we can't run more than two sql commands at the same time, what I did here is I union with another select command that made it one sql command and kept on trying different numbers of table columns to make both the number of columns similar. And after choosing 5 columns it gave me the anticipated result.

TASK-3:
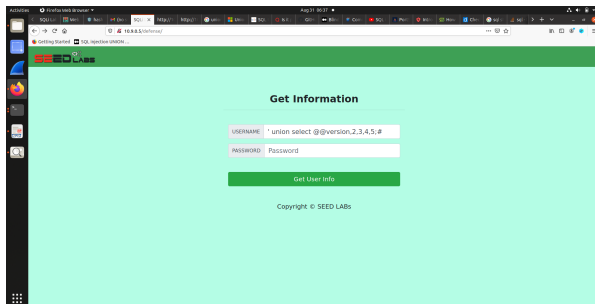
And just to know the version of mysql I have to just replace the first column name with @@version to get the ans.

TASk-4:

——–

——–

TASK-5:

Yes, obviously it will make the website less vulnerable. As we won't have any way of passing sql commands to inject sql. So yes it will definitely decrease the vulnerability.

TASK-6:

The values of eid and passwd will be the user that we want to sign in as and then use commenting technique to avoid giving the password.
So, the whole command will look something like this;

Username: User_name'#
Password: we don't need the password

TASK-7:

To change the salary of Raddington, I just used the same code along with the name of Raddington and then comment out the rest of the code. The command is ',Salary='22' WHERE name='Raddington';#