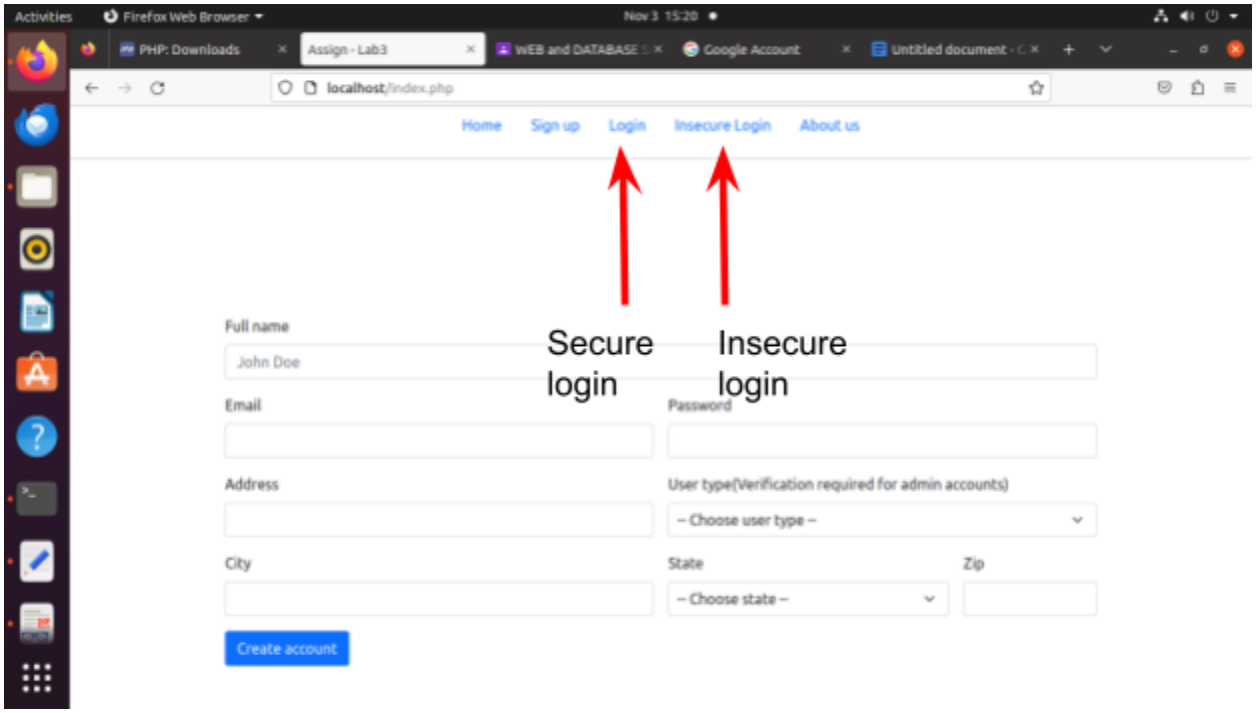
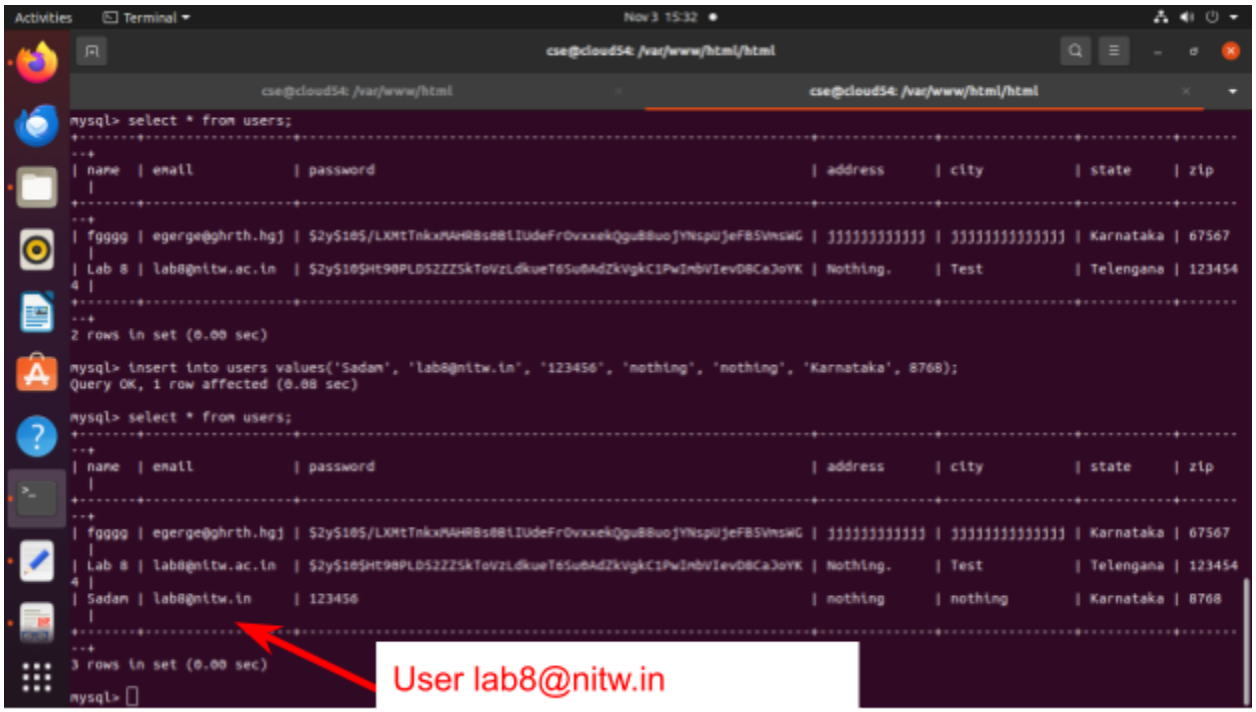
Roll No: 23CSM2R20 ***Name: Sadam Hussain Ganie***

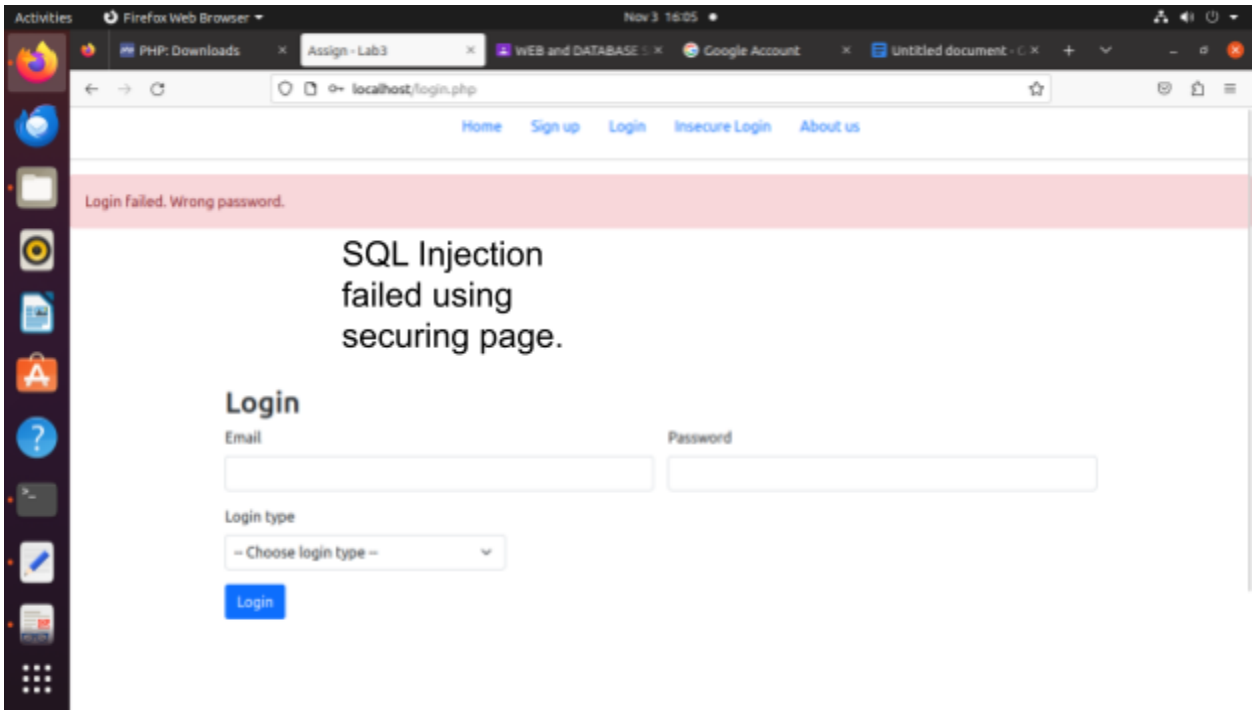
Assignment 8 - SQL Injection ***Subject: WDS Lab***

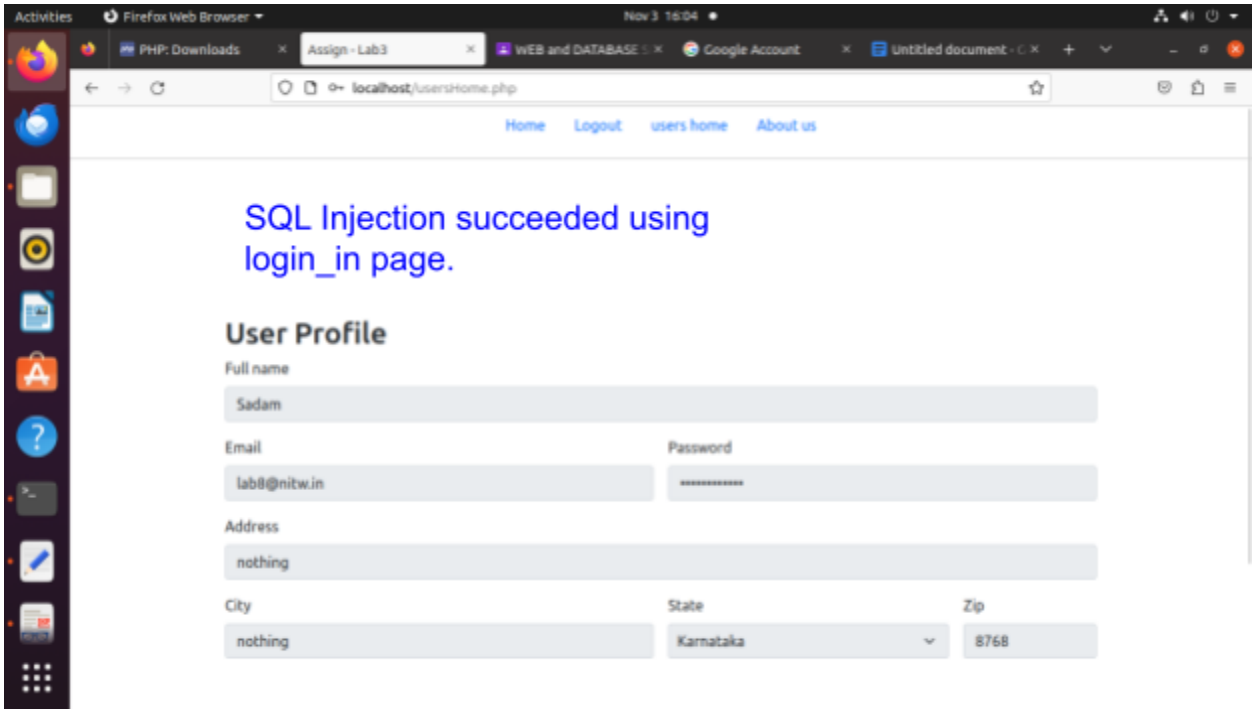


Now user with email "lab8@nitw.in" exists in database as shown below:



Now let's try to login using the “**login.php**” page and “**login_in.php**”. (Here login.php is a secure page where SQL injection won’t work, whereas login_in.php is an insecure page which can be easily attacked by sql injection.
Let us say we know the user email that is “lab8@nitw.in” but we don’t know the password. Let us prepare a password(Injection query).
Let us try with email = lab8@nitw.ac.in and password = **abcd’ or ‘1’=’1**
Following is the output:





Why?
Insecure login page does not validate user input and executes sql query directly. In above example **abcd' or '1'='1** means: **'Select * from users where email=lab8@nitw.in && password=abcd' or '1'='1'** which will always be true irrespective of password supplied.

Incase of a secure login page, I have used prepared queries which verify the user input. This can be prevented from frontend as well using Javascript(input validation).