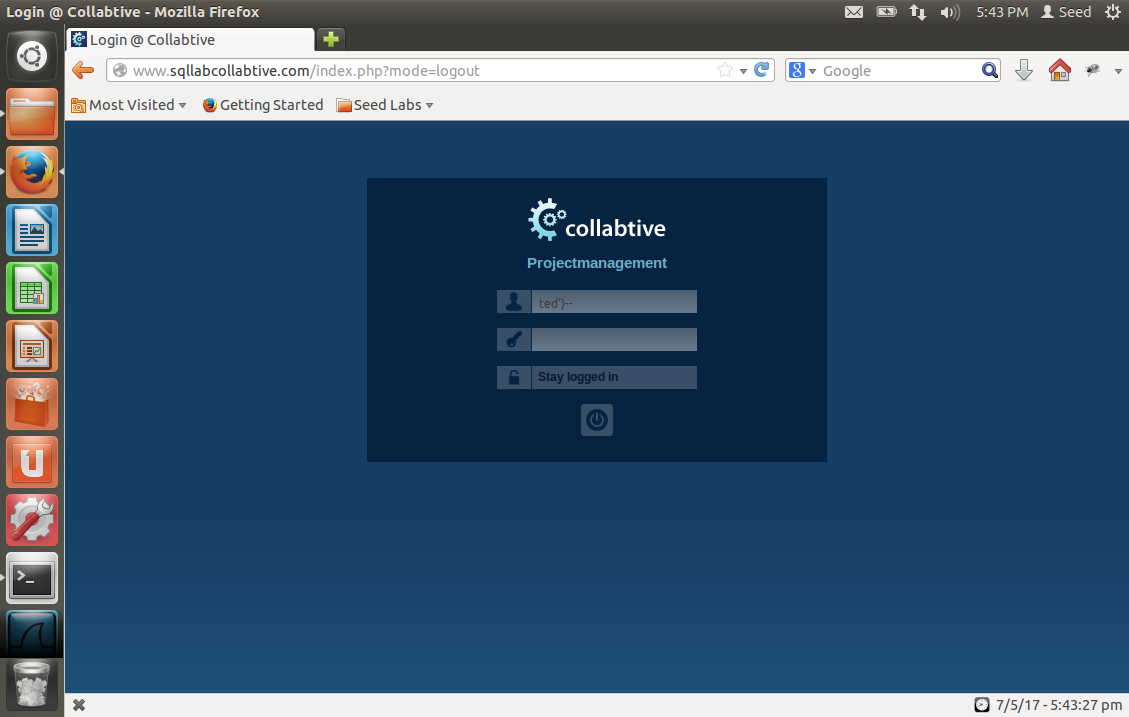
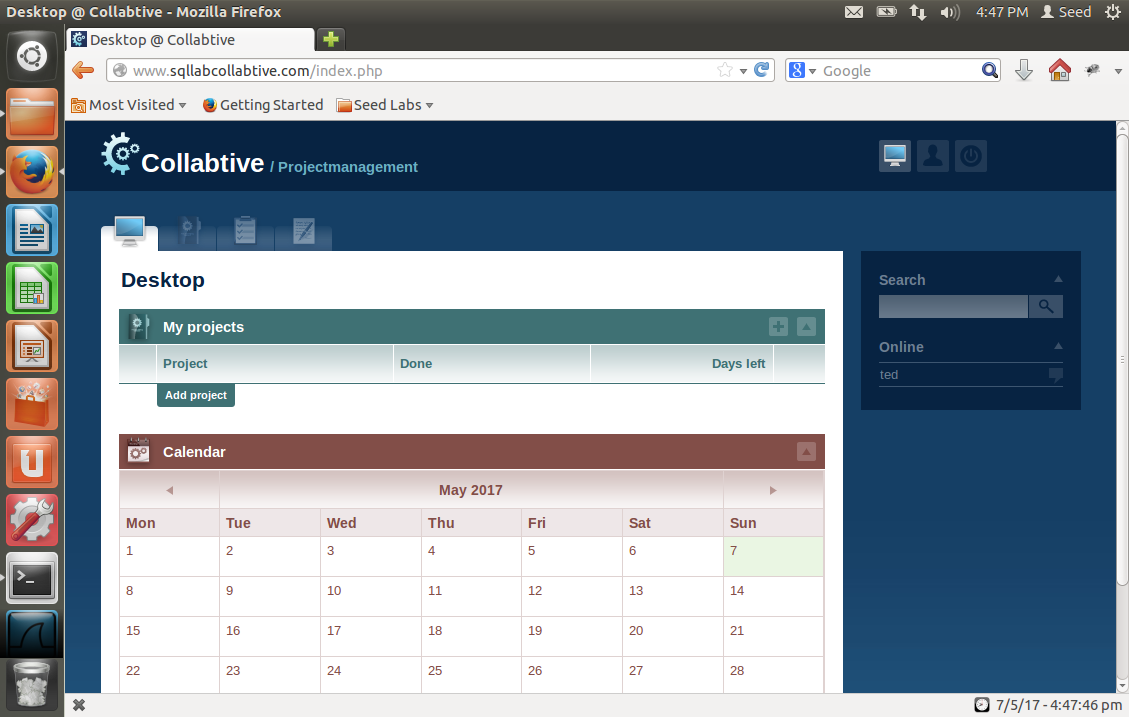
Michael Ly

EX6

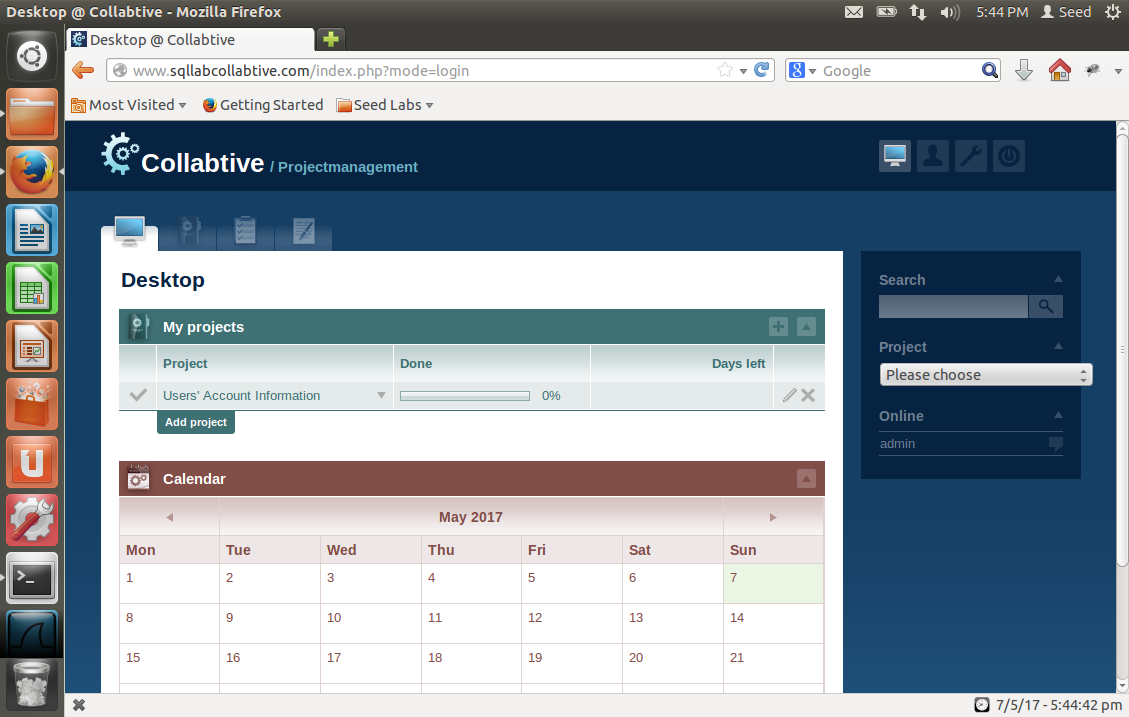
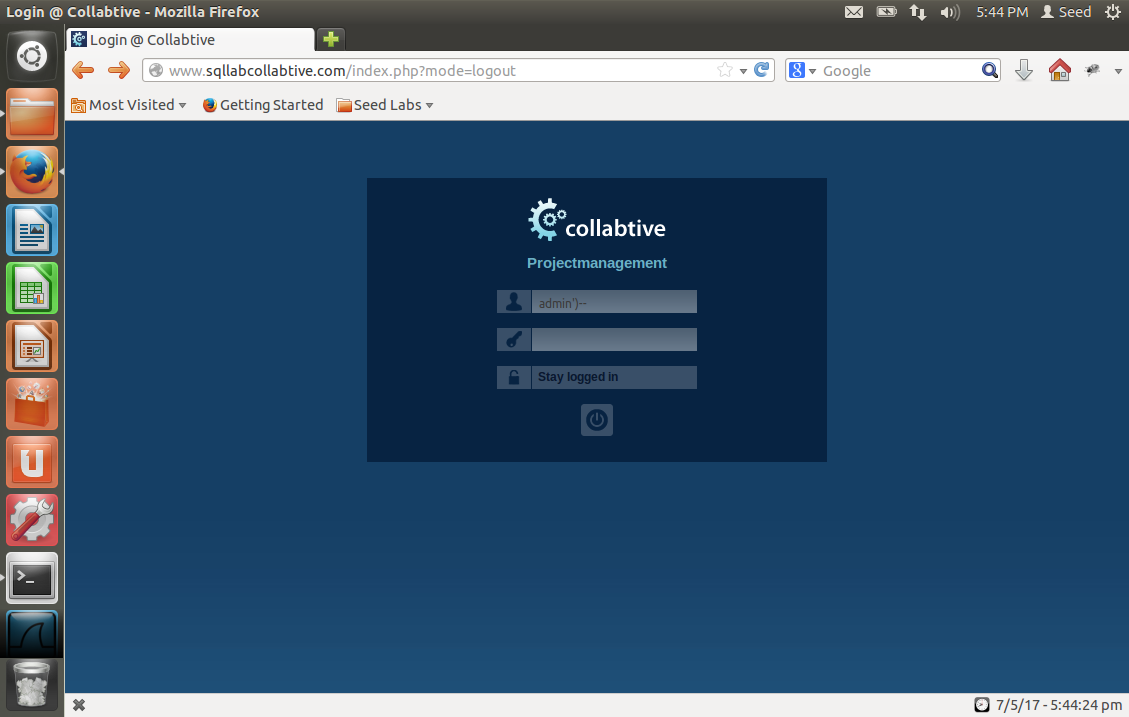
1.

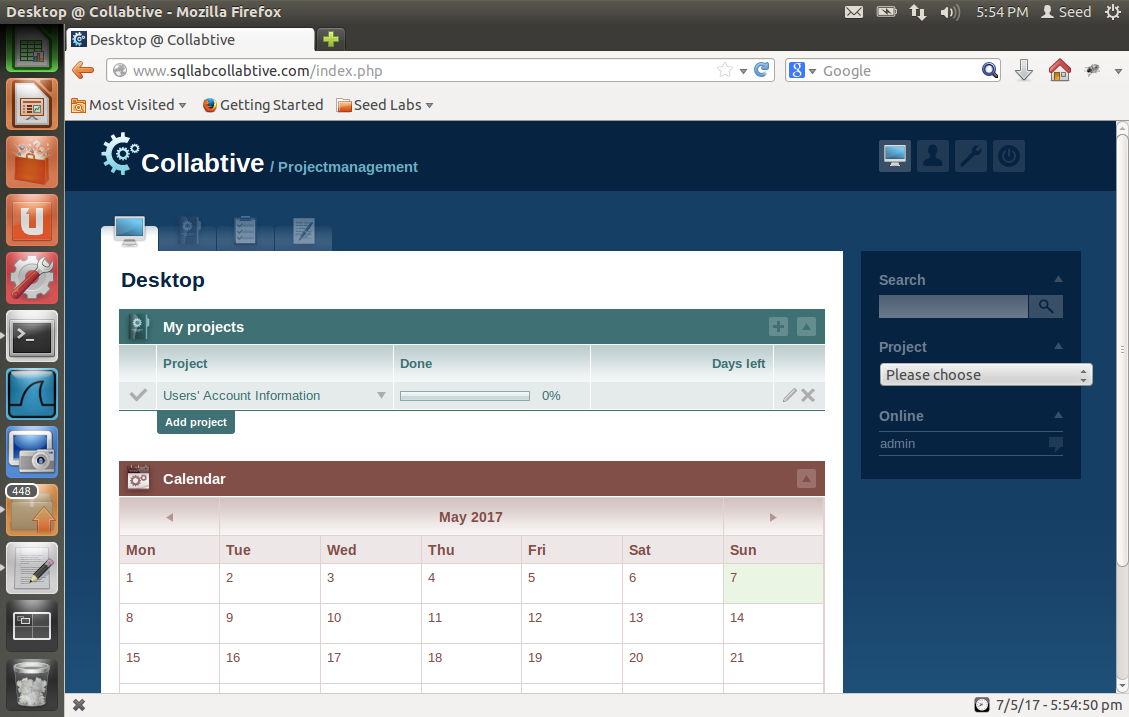
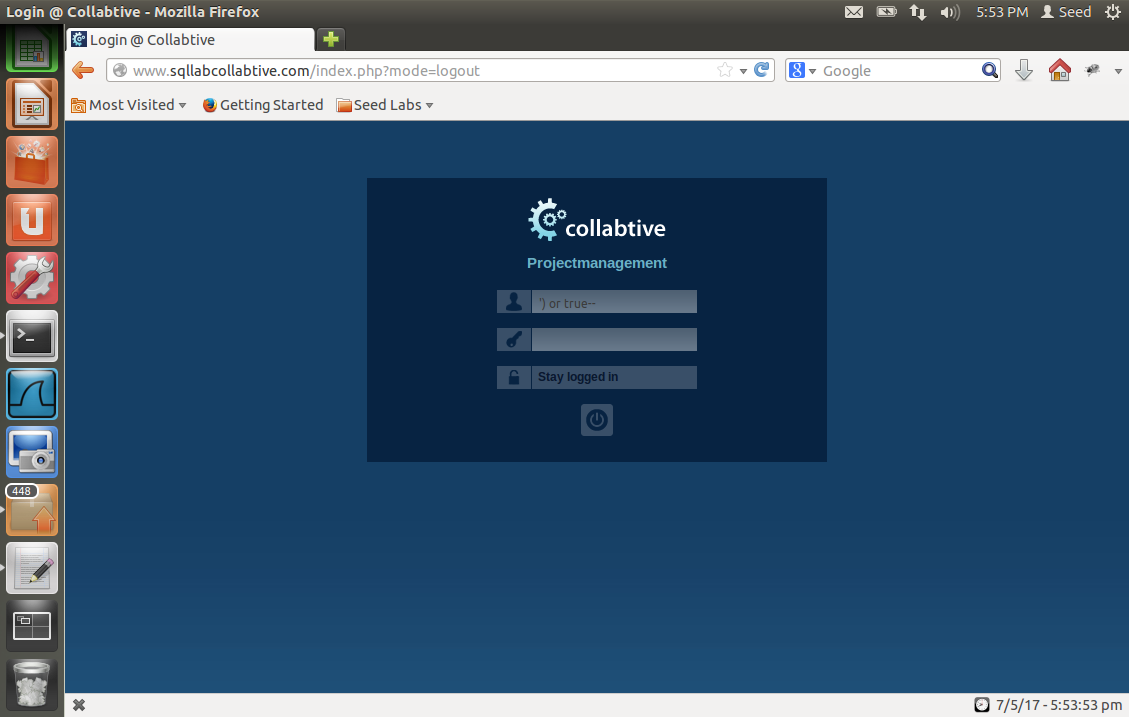
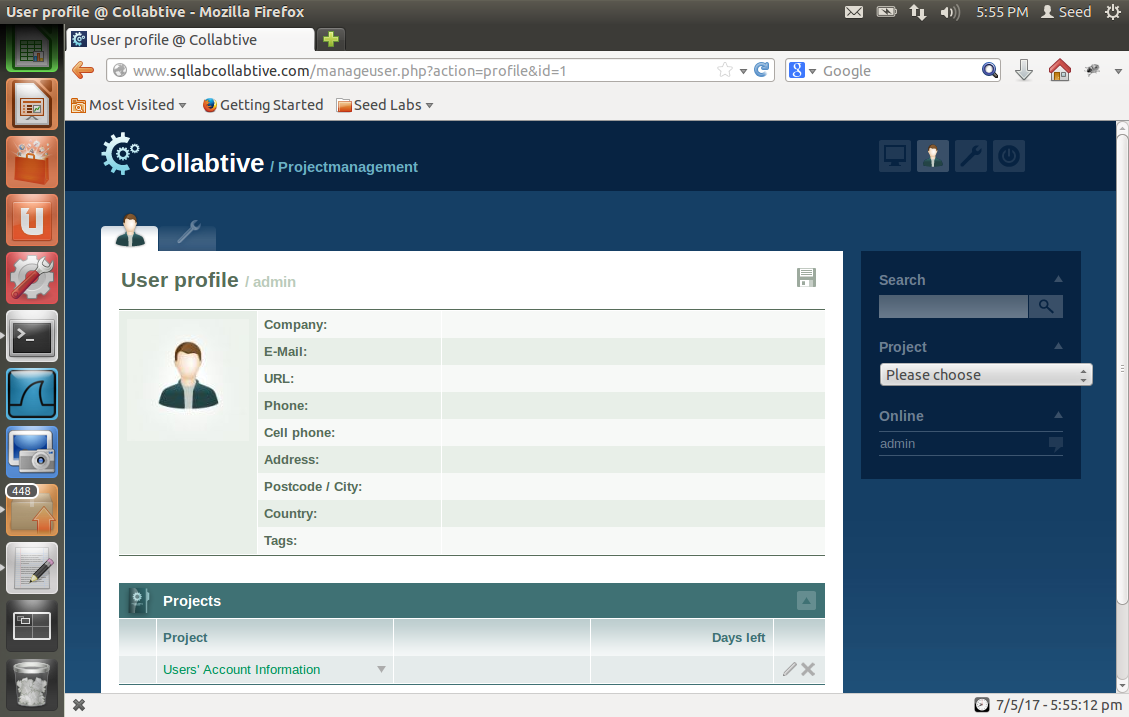
Ted



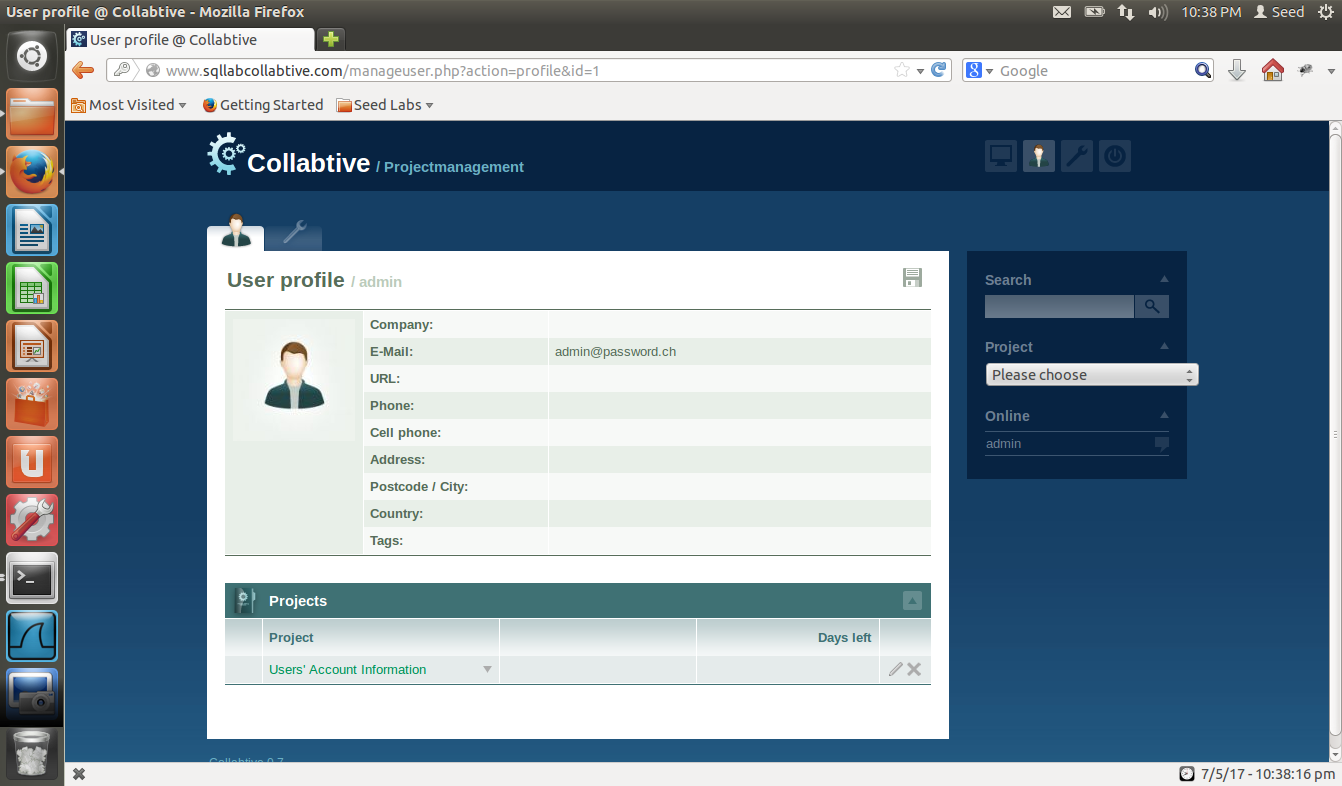
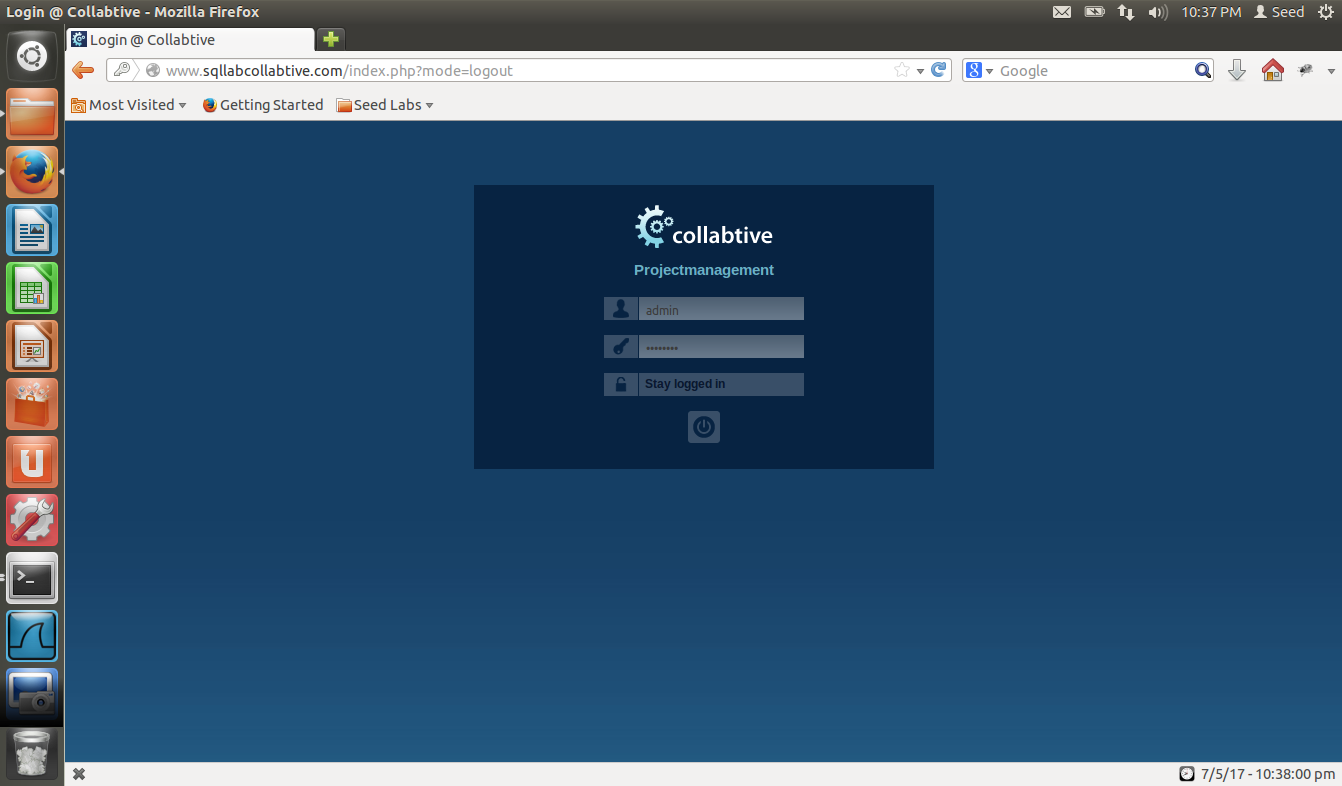
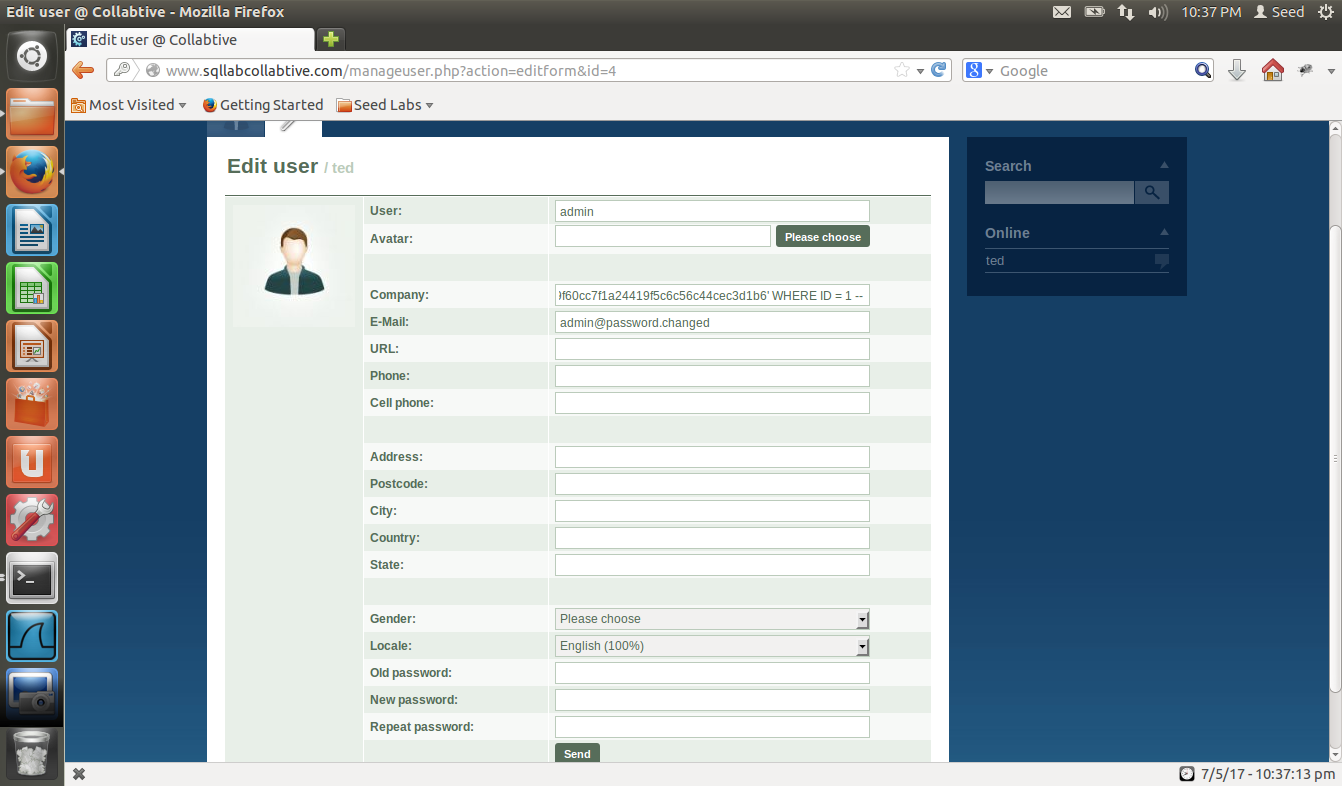
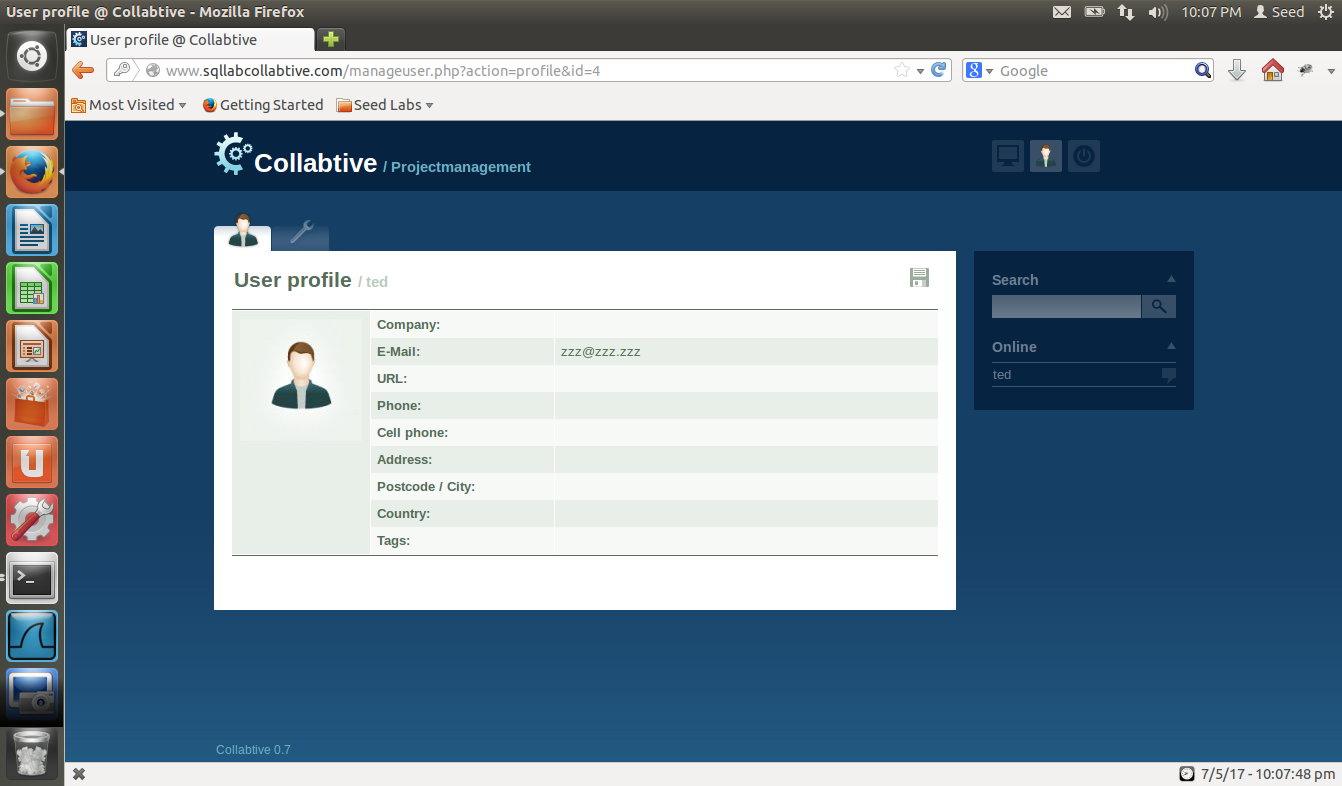
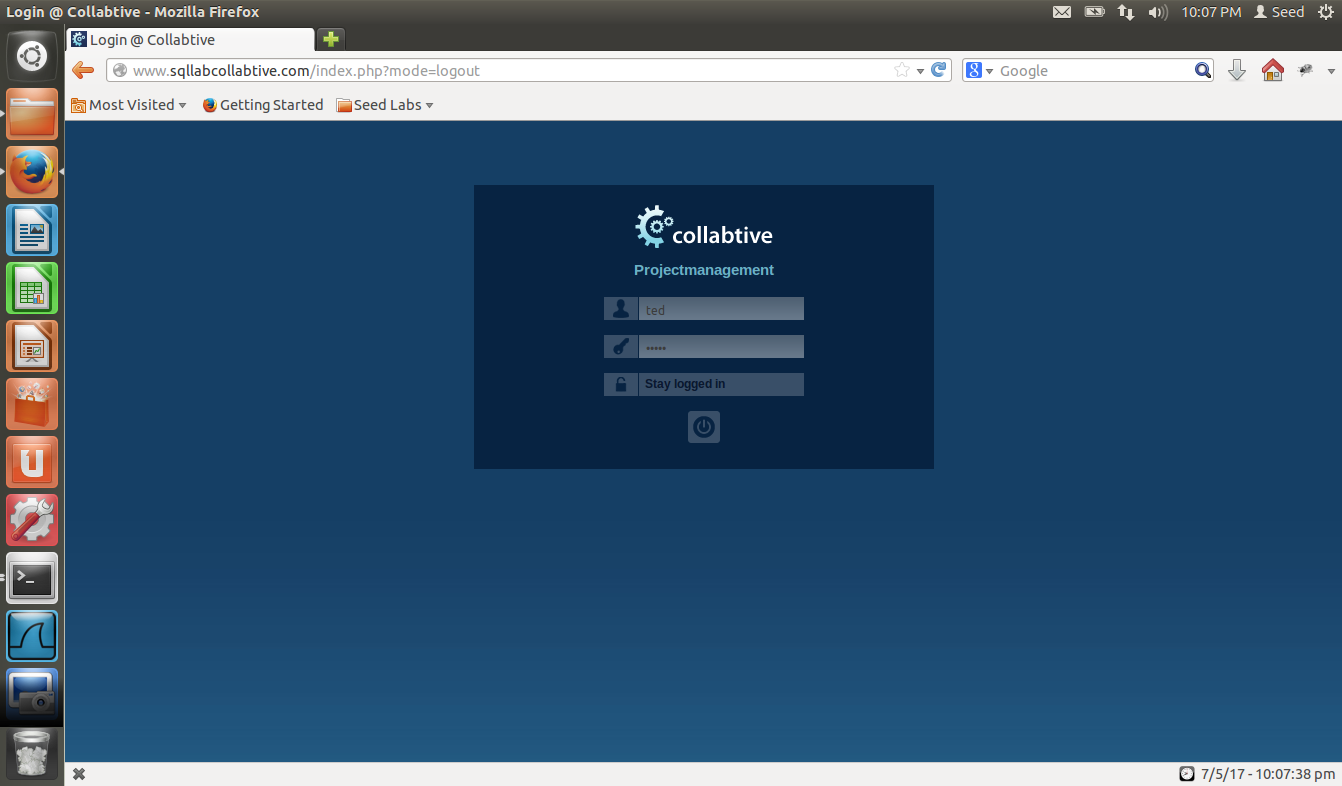
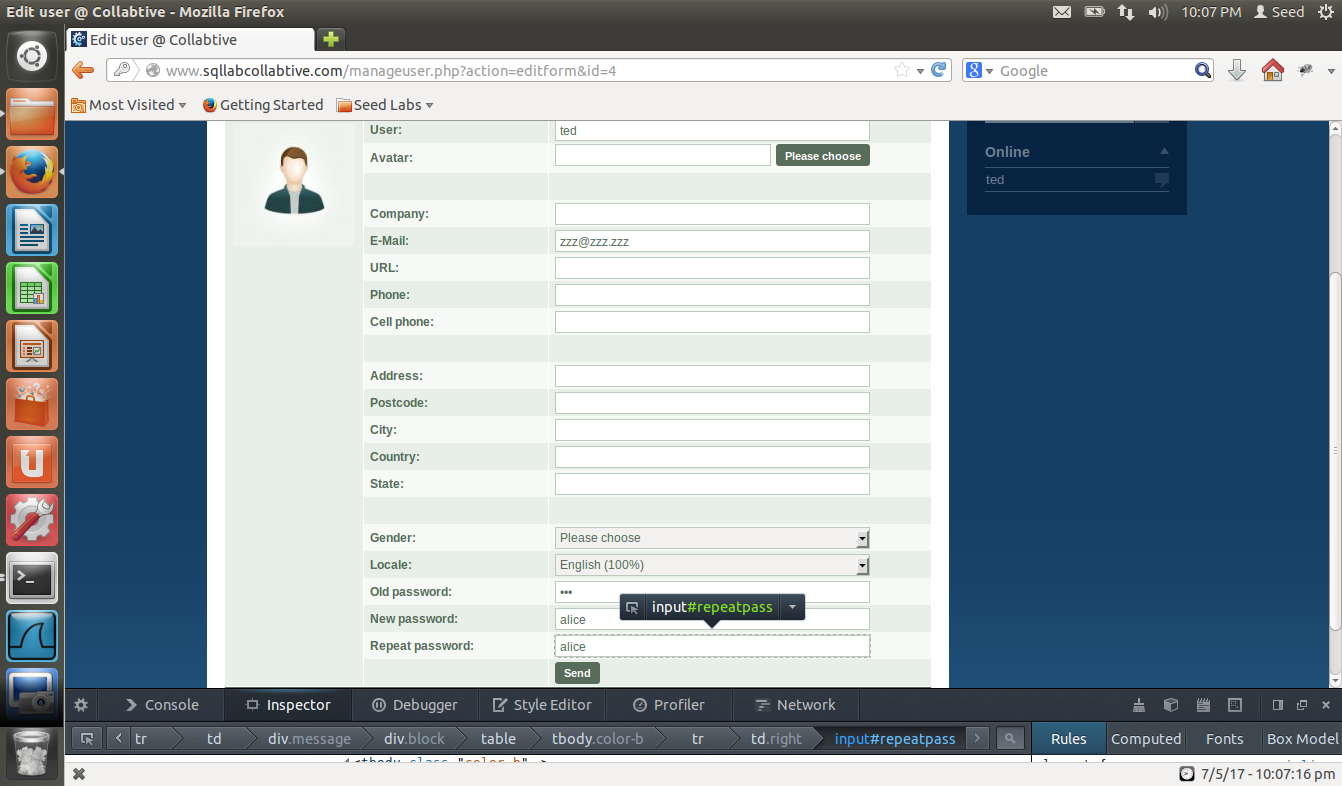


Admin



Blank userThe website thinks the user is “admin”

Extra:



Looking through the code that allows the editing of a user profile, we can see that the company variable is suspectible to an injection

//modified for SQL Lab

//$company = mysql\_real\_escape\_string($company);  
therefore, we can change the password of admin through this field. We pass in “ ', `pass` = 'b977b689f60cc7f1a24419f5c6c56c44cec3d1b6' WHERE ID = 1 -- “ (without the quotation marks) into the company field which changes the password of the admin account to “notadmin.” The pass passed in is the sha1 value of “notadmin” which was calculated using a online convertor. The ID is the id of the admin account which was manually obtained from logging in the admin account in the previous question.