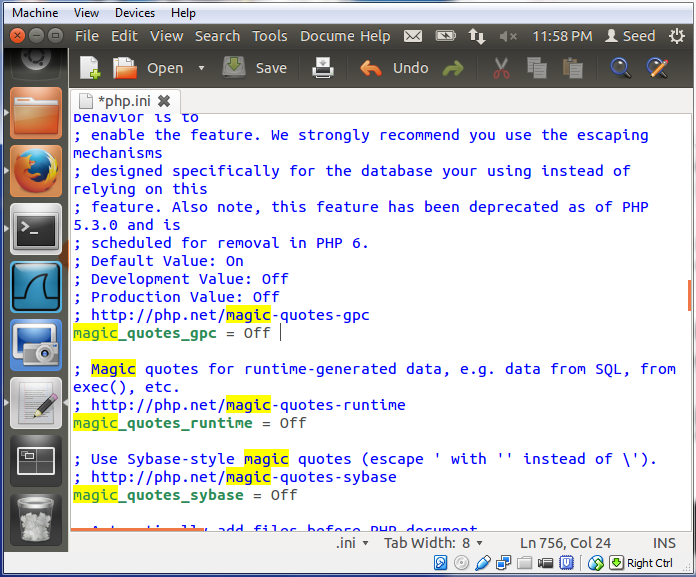
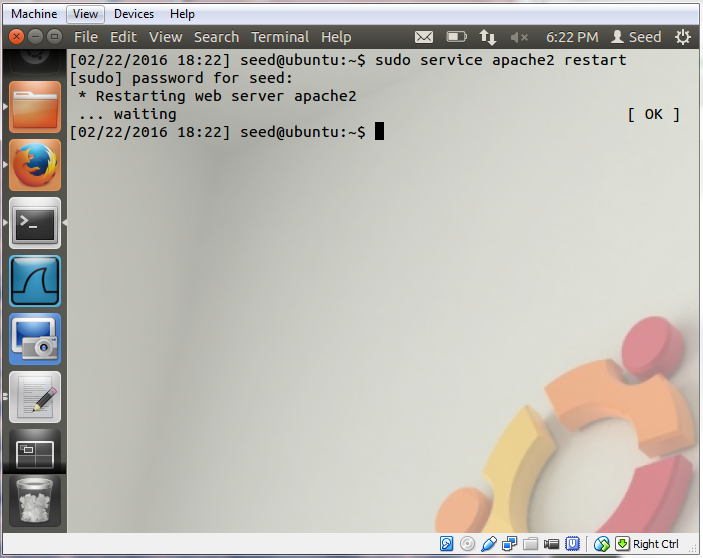
**CS380 Exercise 4 Kyle Turchik**

**Brent Reed**

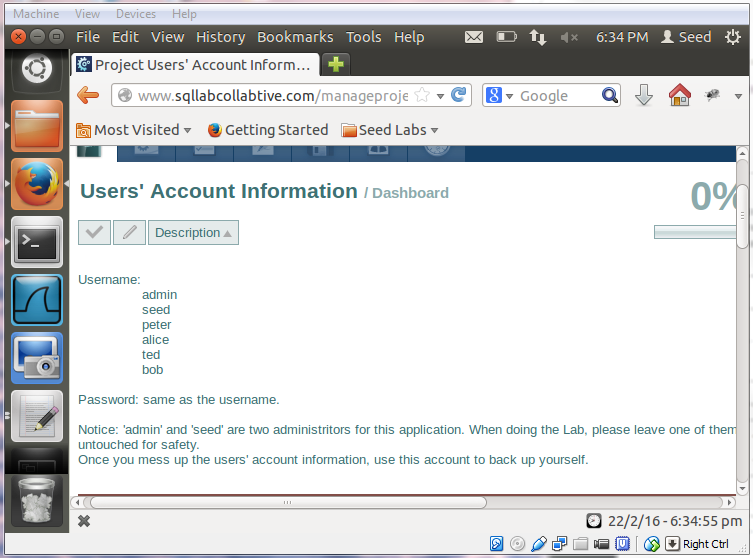
Turning off protection for SQL injection.



Restarting the apache web server.



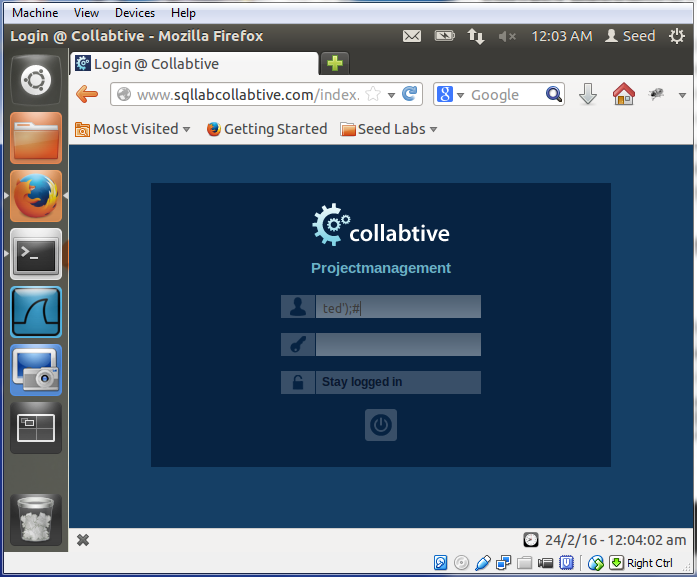
Users’ Account Information visible in admin account.



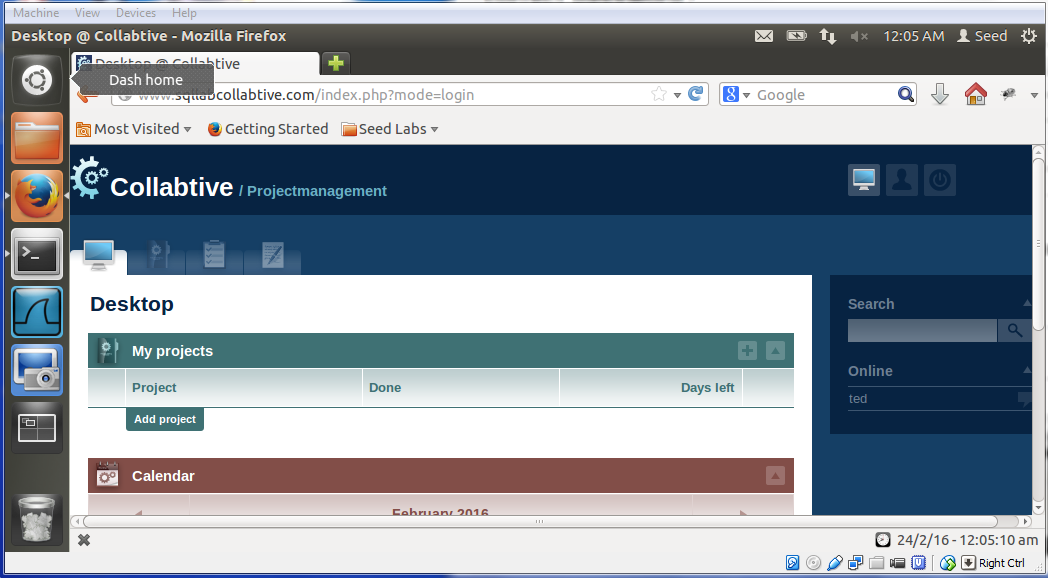
***1.) Can you login as the administrator without providing their password?***

Enter any username followed by **‘);#** to bypass the password check when logging in.

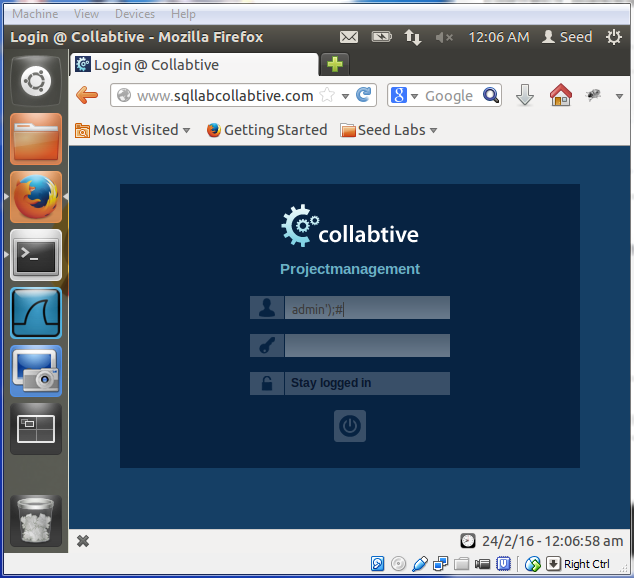
The **'​** and **)**, match the **​'​**and **(** before them in the query, then the **;** completes the query, and finally a **#** comments out the rest of the query.



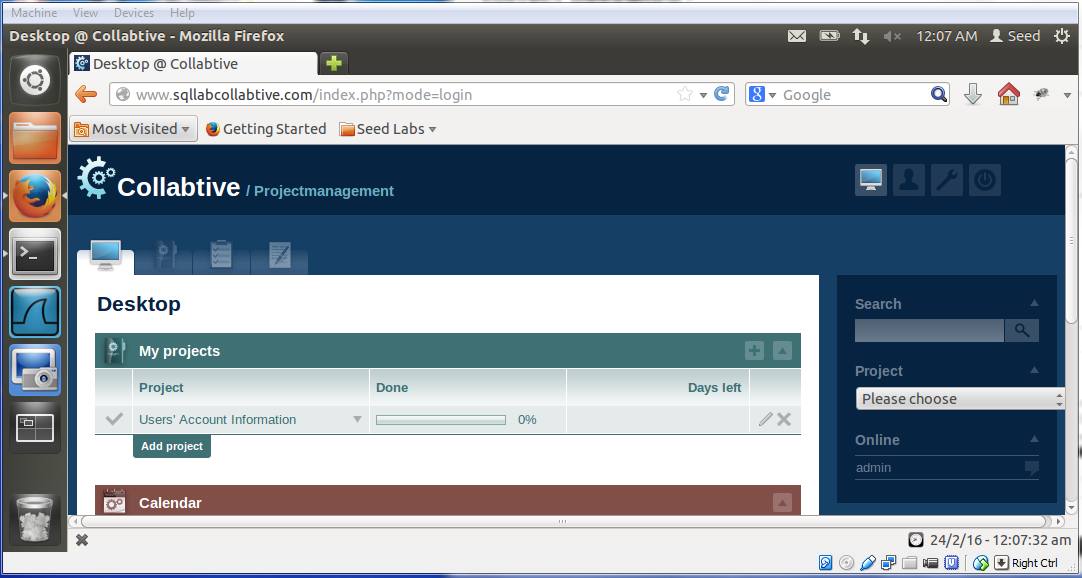
Successfully logged in as ted.



Logging into admin’s account with the same technique.

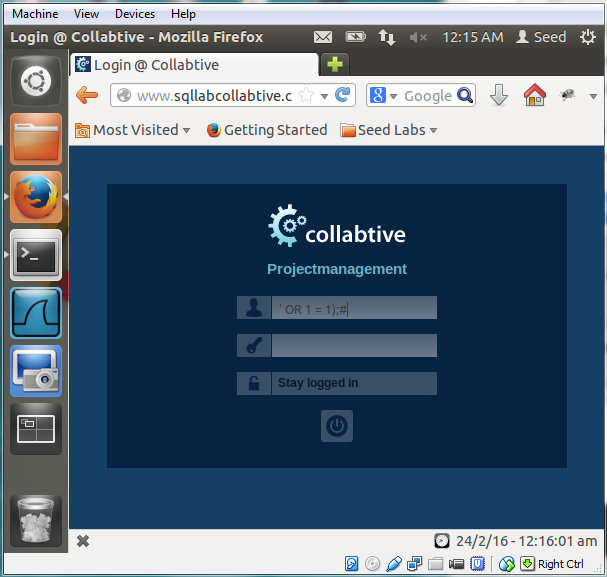


Successfully logged in as admin.

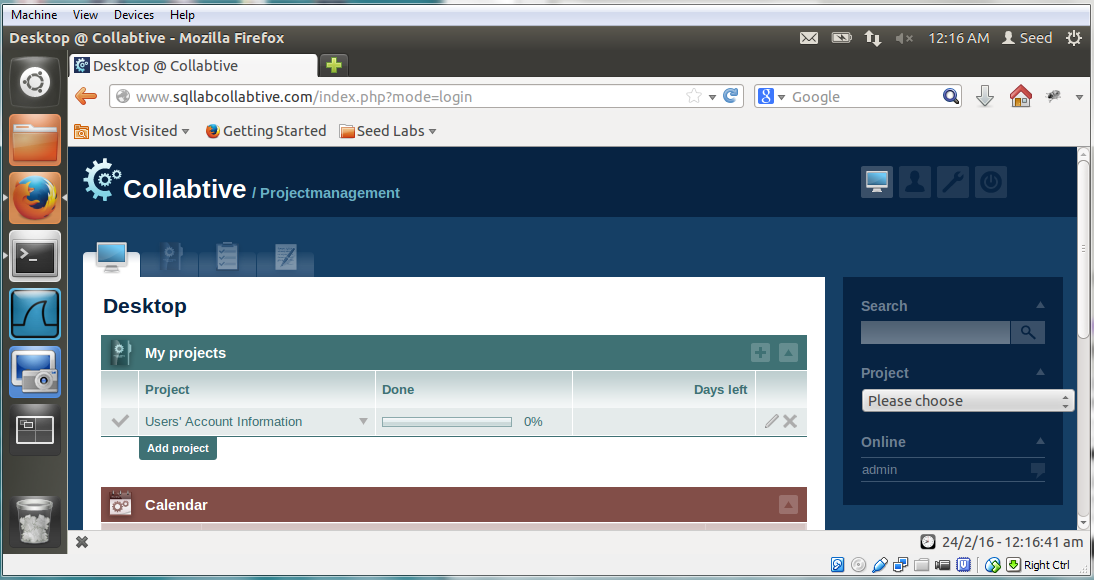


***2.) Can you login with a blank username?***

Enter **‘ OR 1=1);#** into the user field.



The website thinks you are the admin.



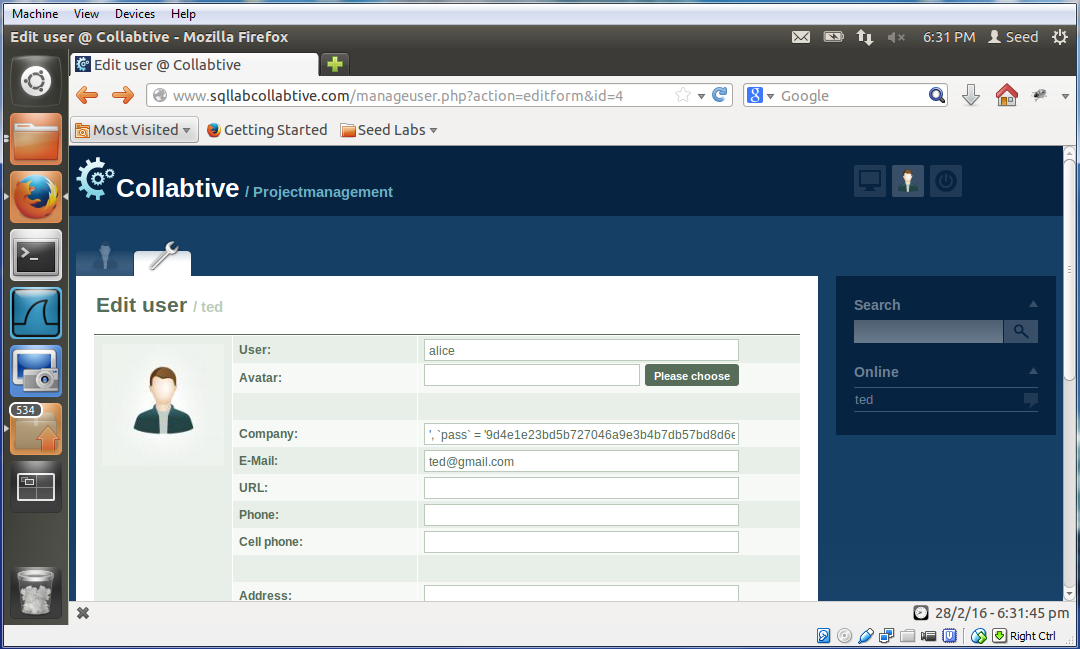
**BONUS**

***1.) Log in as ted and change the password of alice.***

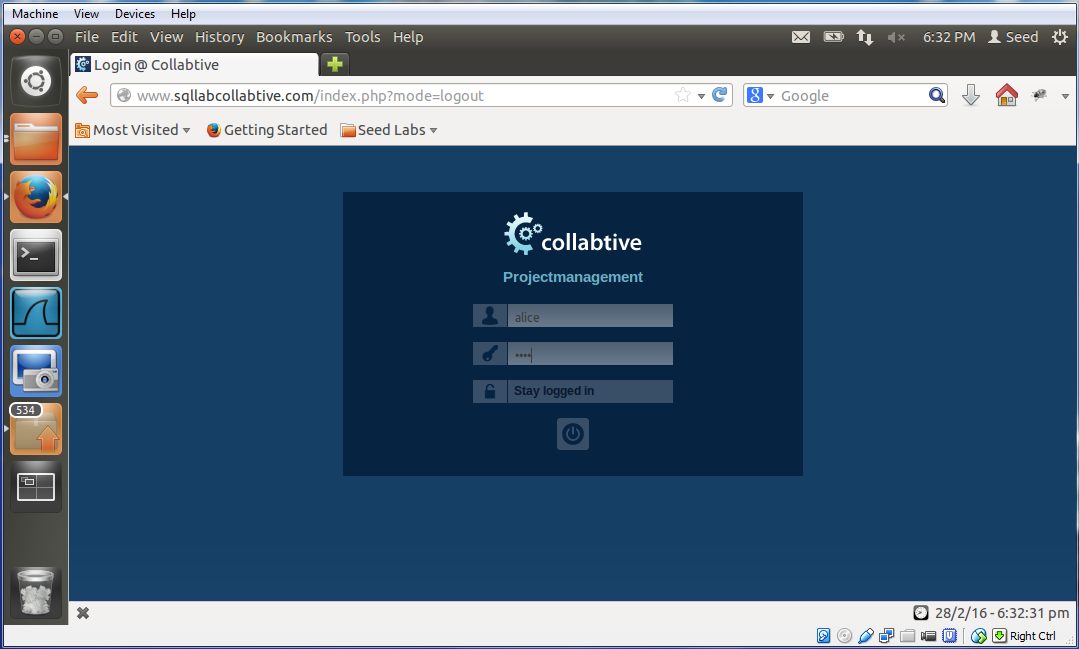
The “company” field is susceptible to injection.

Determine alice’s ID number (“6”) and the SHA1 hash for the new password. Then enter “alice” as the username, any email account, and in the company field add

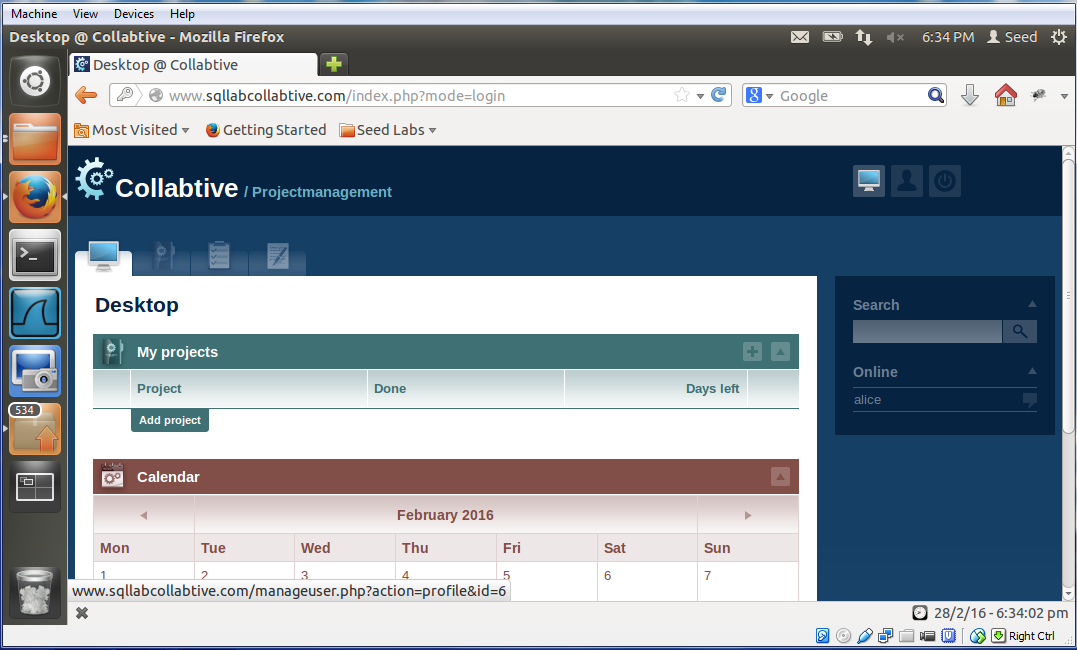
**', `pass` = '9d4e1e23bd5b727046a9e3b4b7db57bd8d6ee684' WHERE ID = 6 #**



Logging in as alice using the new password, “pass.”



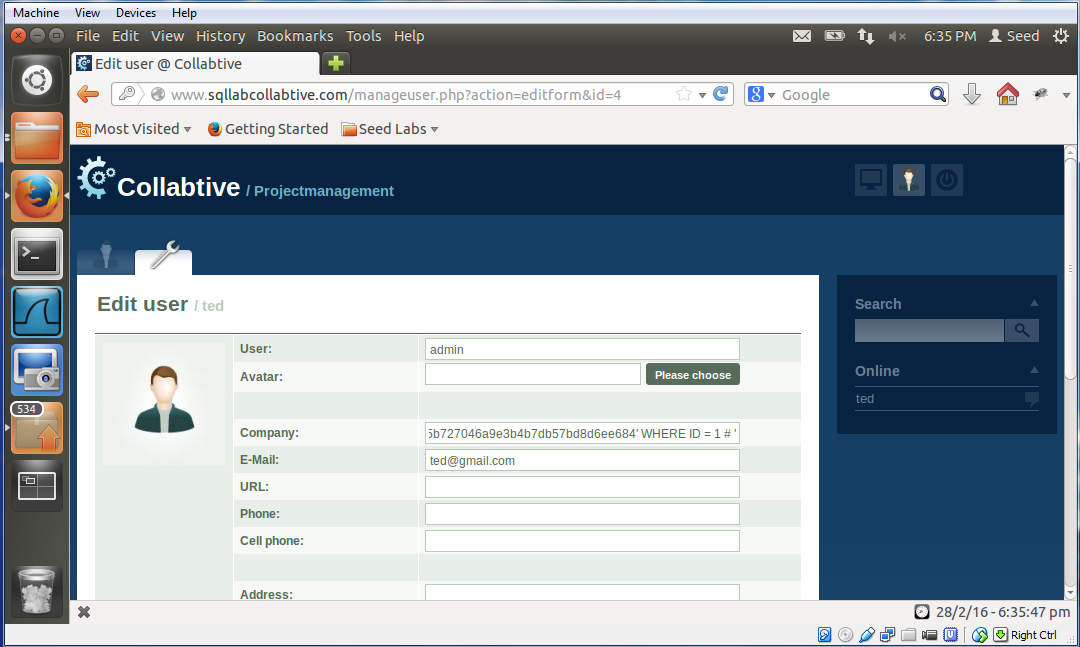
Successfully logged in as alice.

NOTE: By mousing over “My account” we can see the link (displayed at the bottom left corner) contains alice’s ID number, which we determined was 6 by testing. 

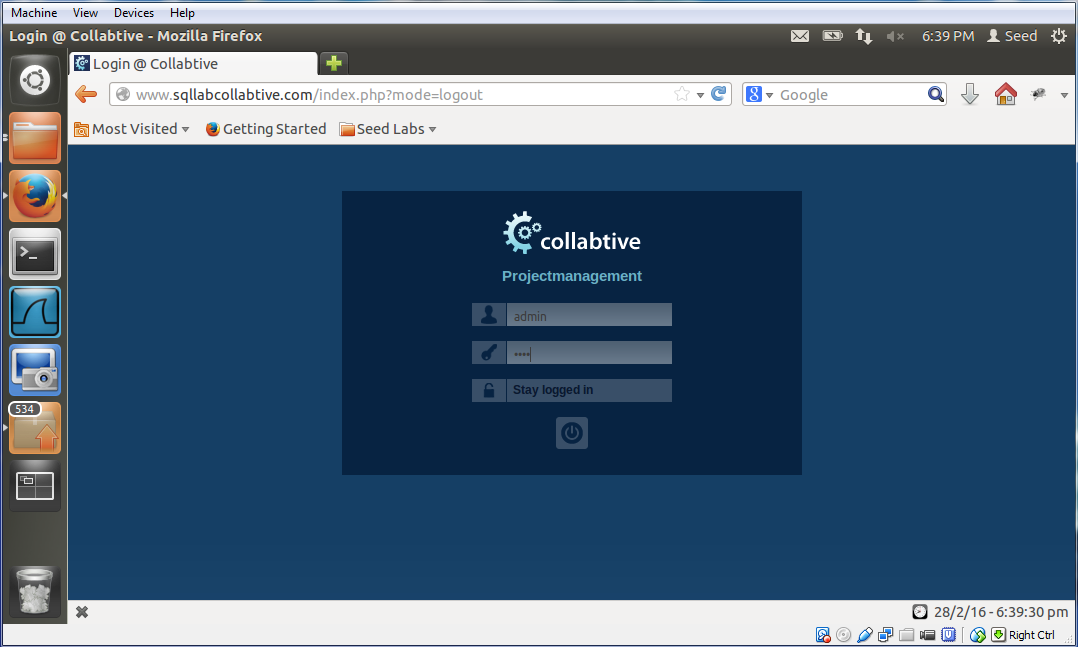
***2.) Log in as ted and change the password of admin?***

Determine admin’s ID number (“1”) and the SHA1 hash for the new password. Then enter “admin” as the username, any email account, and in the company field add

**', `pass` = '9d4e1e23bd5b727046a9e3b4b7db57bd8d6ee684' WHERE ID = 1 #**



Logging in as admin using the new password, “pass.”



Successfully logged in as admin.

NOTE: By mousing over “My account” we can see the link (displayed at the bottom left corner) contains admin’s ID number, which we determined was 1 by testing.

