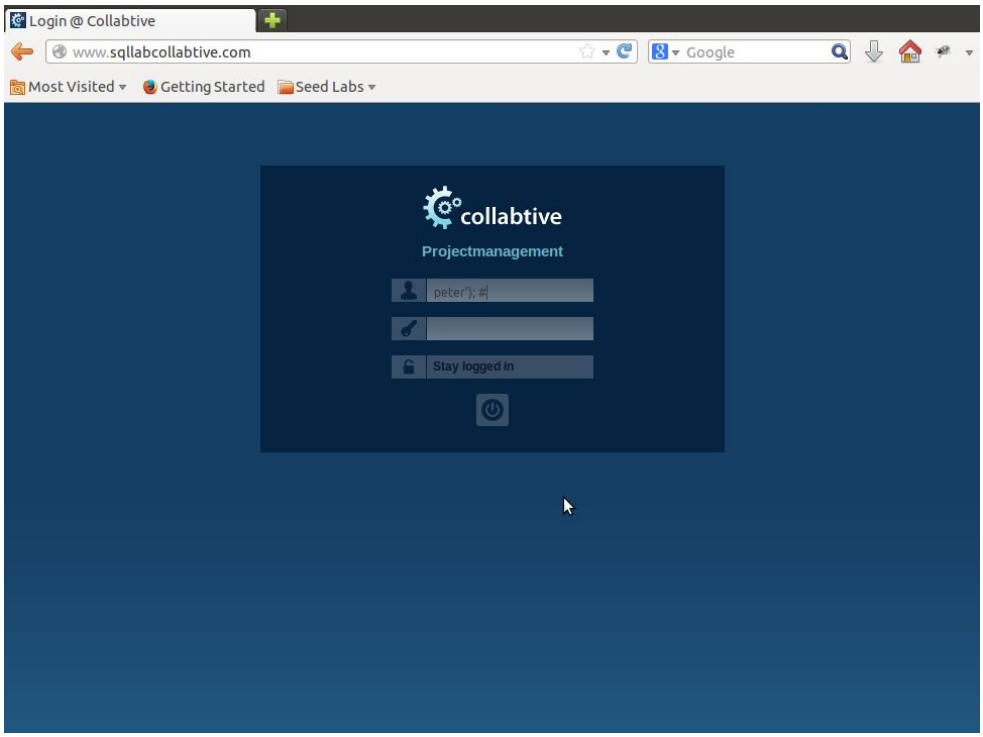
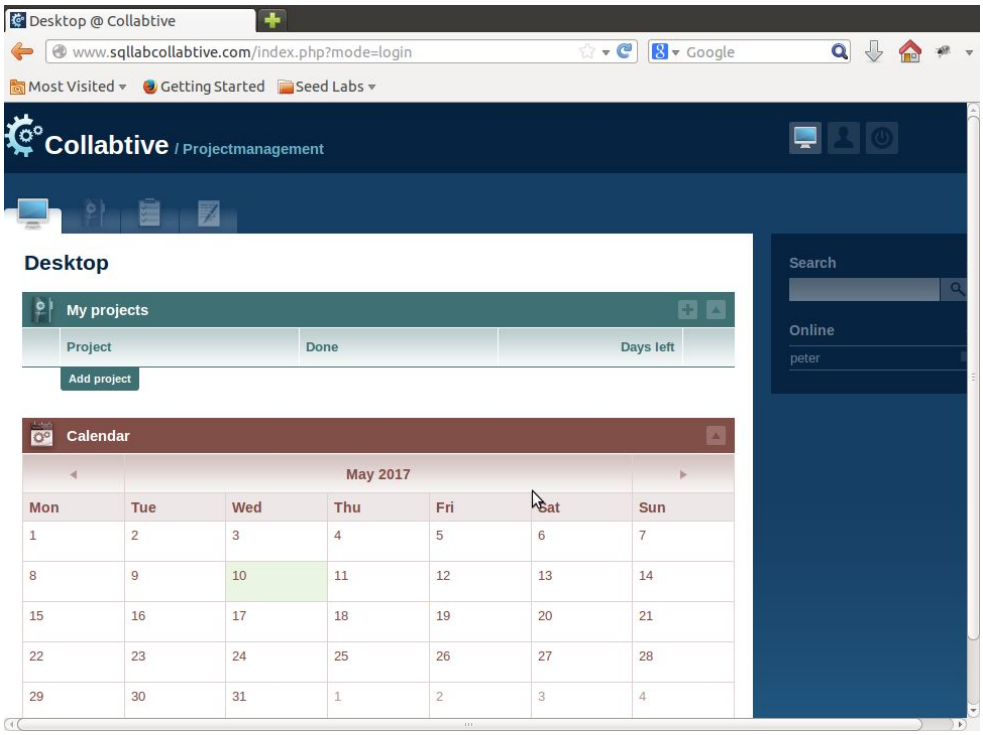
CS380 - EX5

Jhuo Wei Ku

(GitHub Repo: https://github.com/Narwow/CS380-EX6)

Task 1: To login to any non admin user without providing the password.



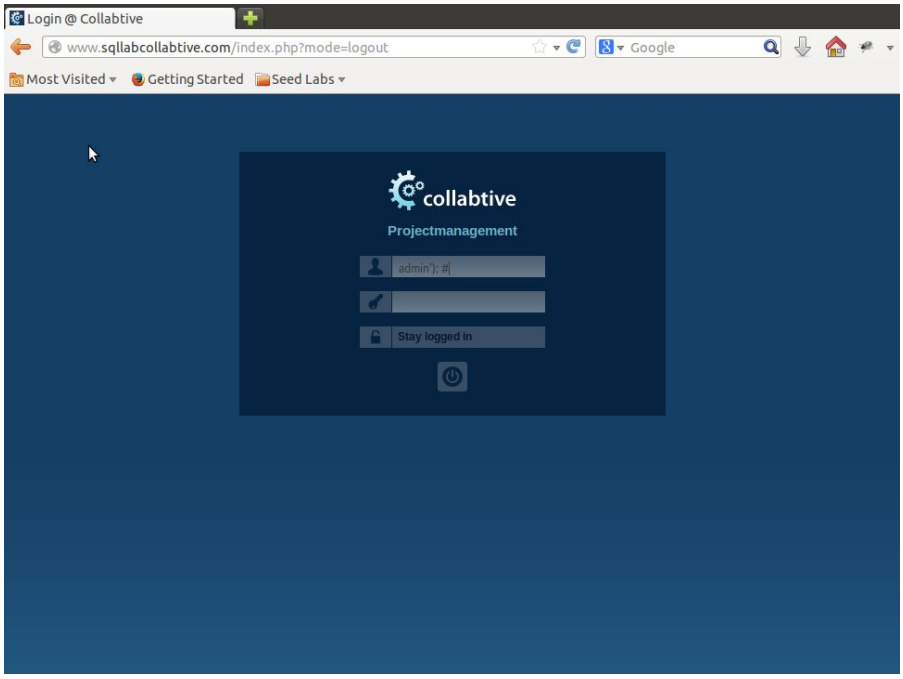


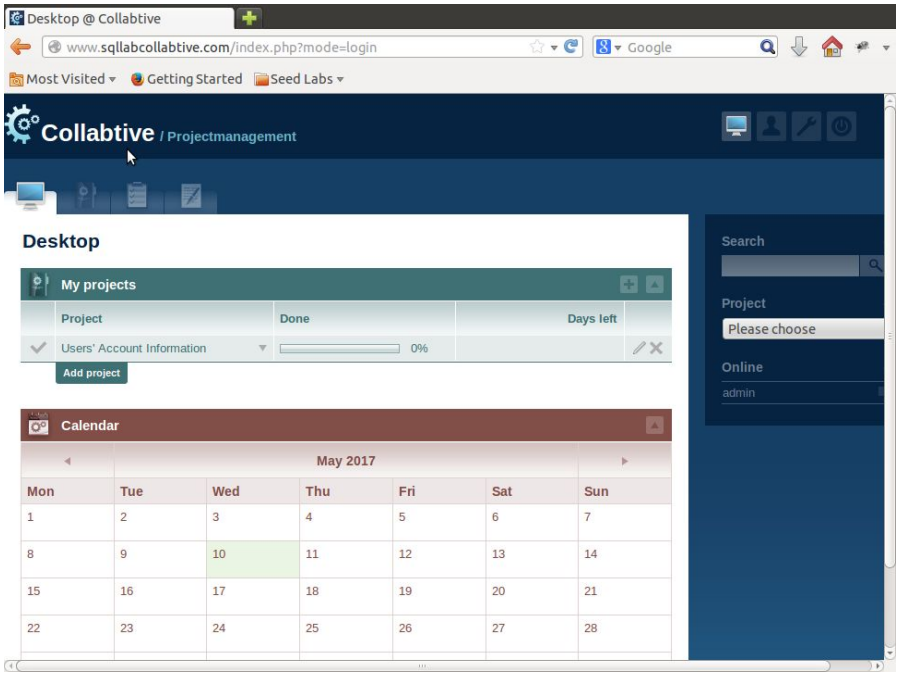
I used peter as an example for me to try to log in without his password “peter.” The SQL code,

WHERE (name = ’$user’ OR email = ’$user’) AND pass = ’$pass’");

is used to let you through when this statement becomes true. Therefore, I just have to try to inject a statement after $user and make this line of code true. I used peter’ to close out the name = ‘$users’ and a); to close the WHERE statement. After that, I used a # to comment the rest of the line so they don’t get executed as code.

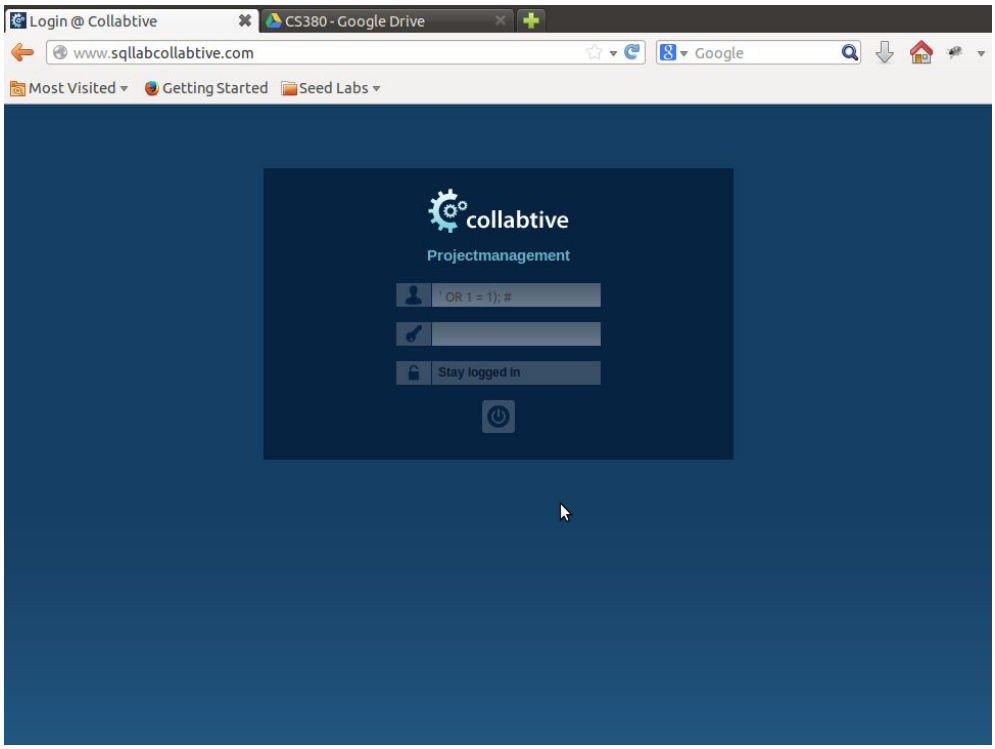
Task 2: To login to admin without providing the password.

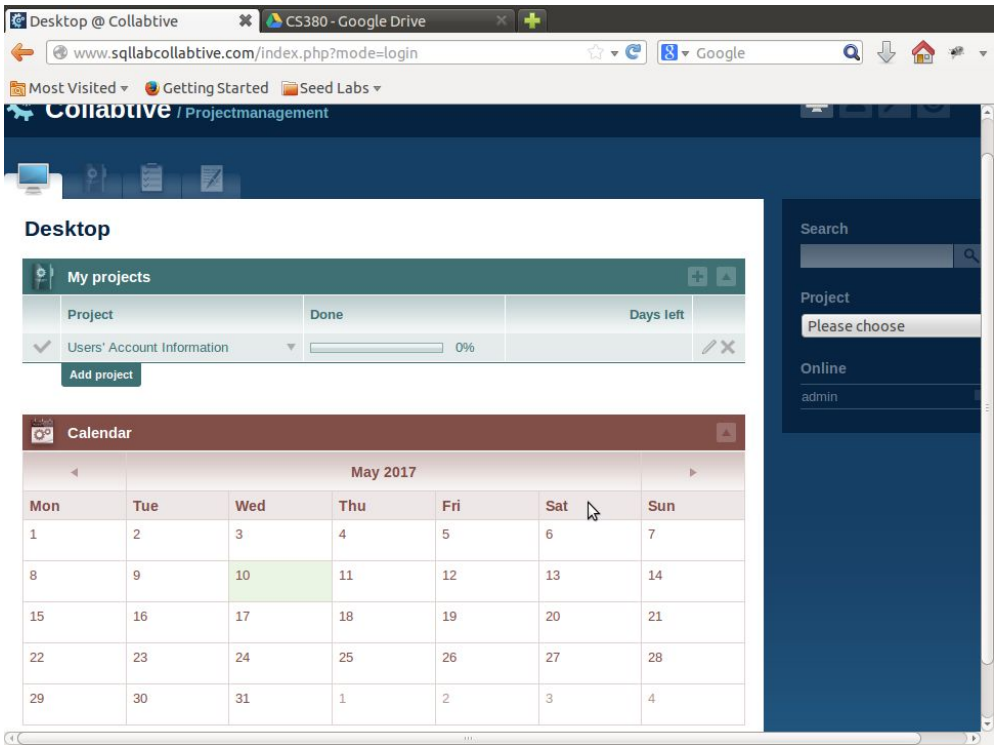




This situation is just like the one in task one. Therefore I used the same method admin'); # to inject the code and successfully enter the account.

Task 3: To login to any user without providing the password and the username.





In this case, I still have to make the statement true to login to the account. I still can't ignore the name = '$user'. Therefore I added a OR at the end and I used 1 = 1, which is always true. This way, I was able to login as admin.