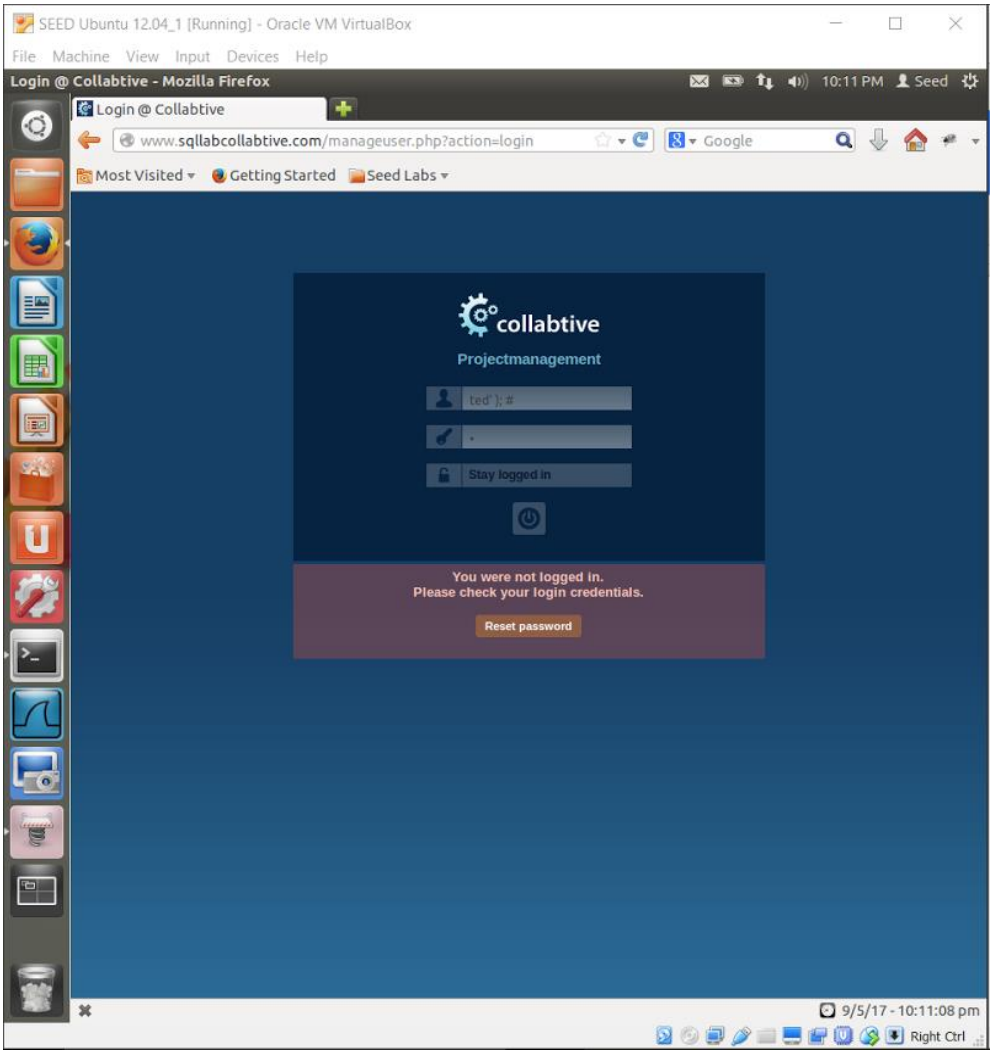
Pedro Ruelas
https://github.com/pruelas/Exercise_6

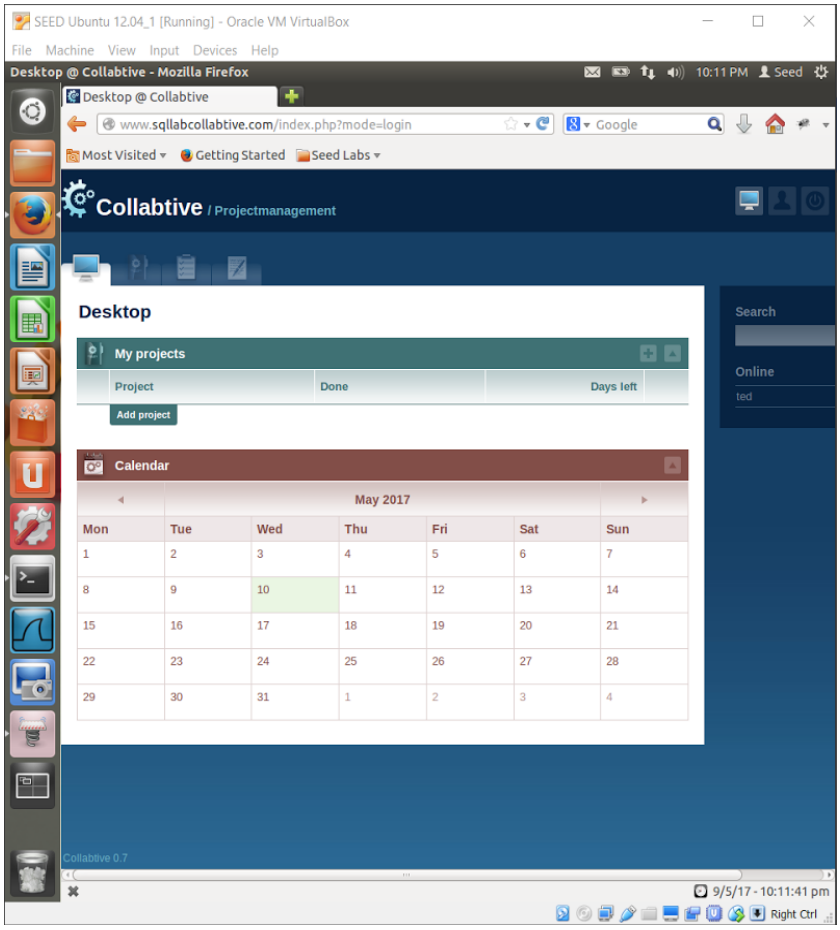
Exercise 6
SQL Injection in User Authentication

To be able to login as ted without providing the user's password, one must modify the WHERE statement so that it only selects a user from the user table with only the user's name. To be able to do that, one must enter to following characters:
ted'); #
The characters above modify the WHERE statement in the php file, so that it only checks the table for a user with the name 'ted' and doesn't check for a password.

Screenshot with input

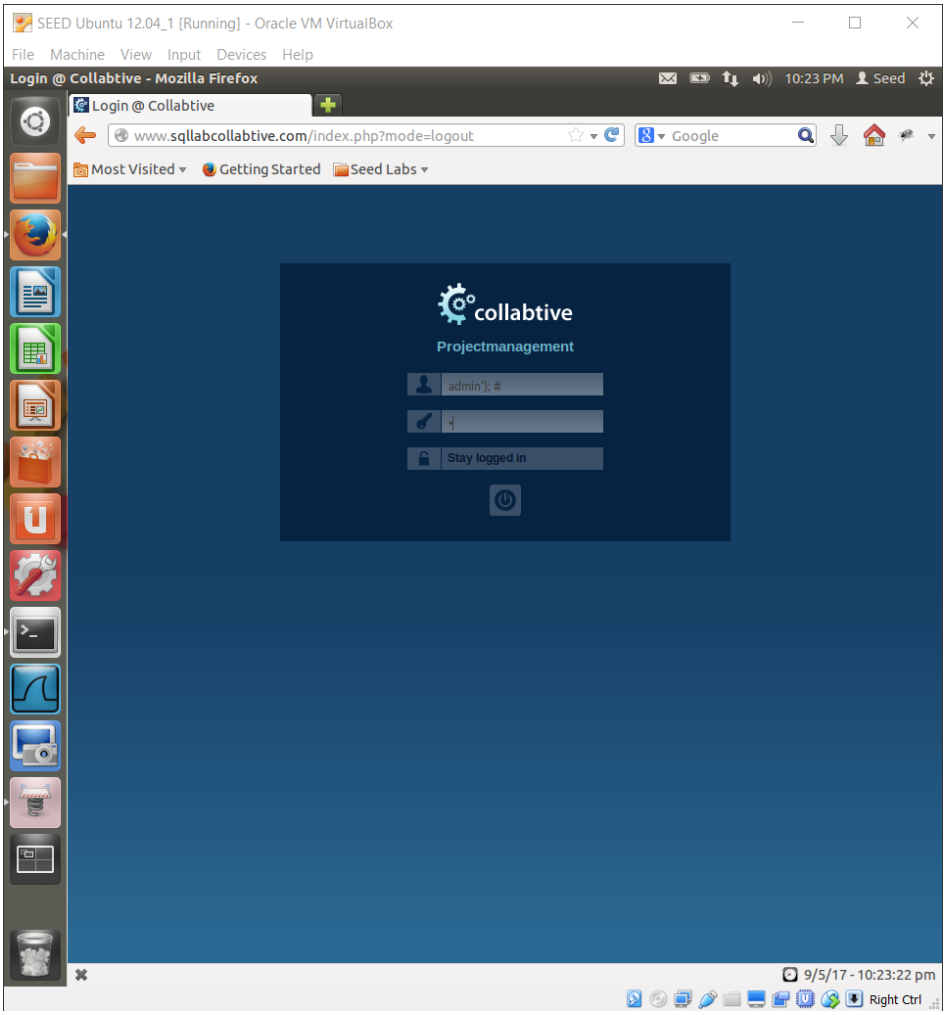


Screenshot after logging in

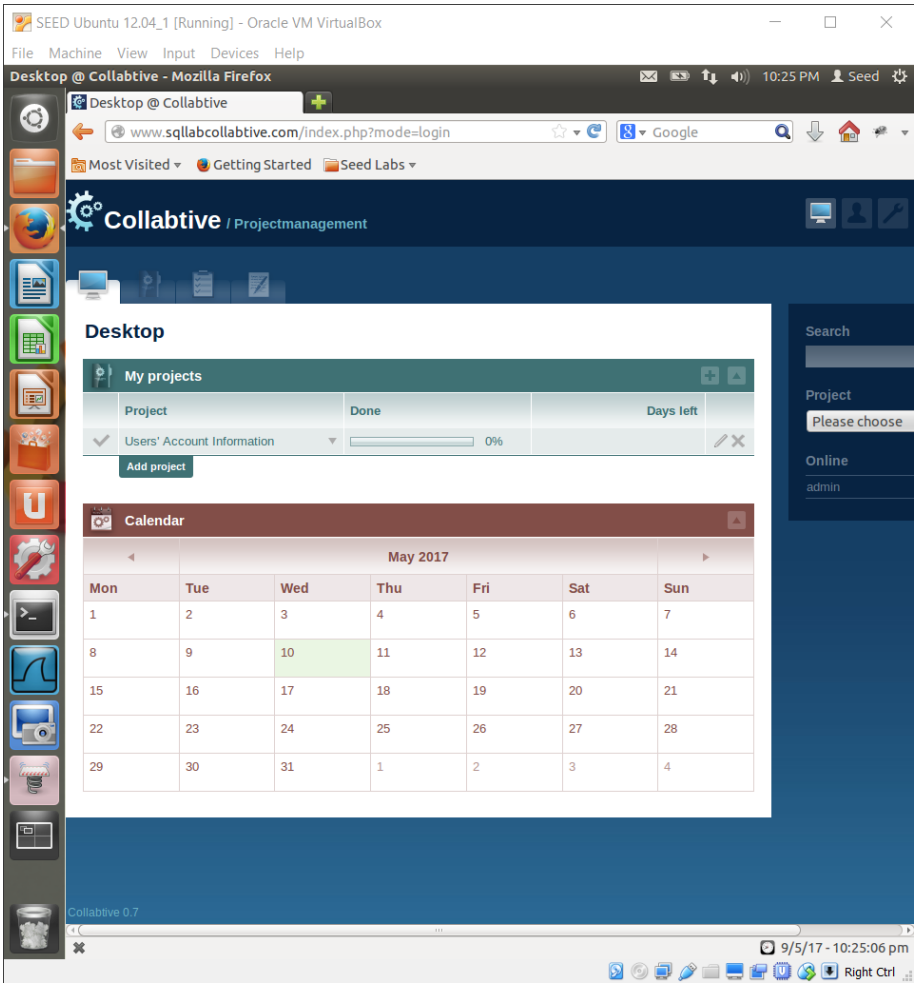


One can log in as the admin by using the same characters mentioned above, but replacing the name ted with admin. The characters used to log in as the admin without providing the password are the following:
admin');#

Screenshot of input



Screenshot after logging in

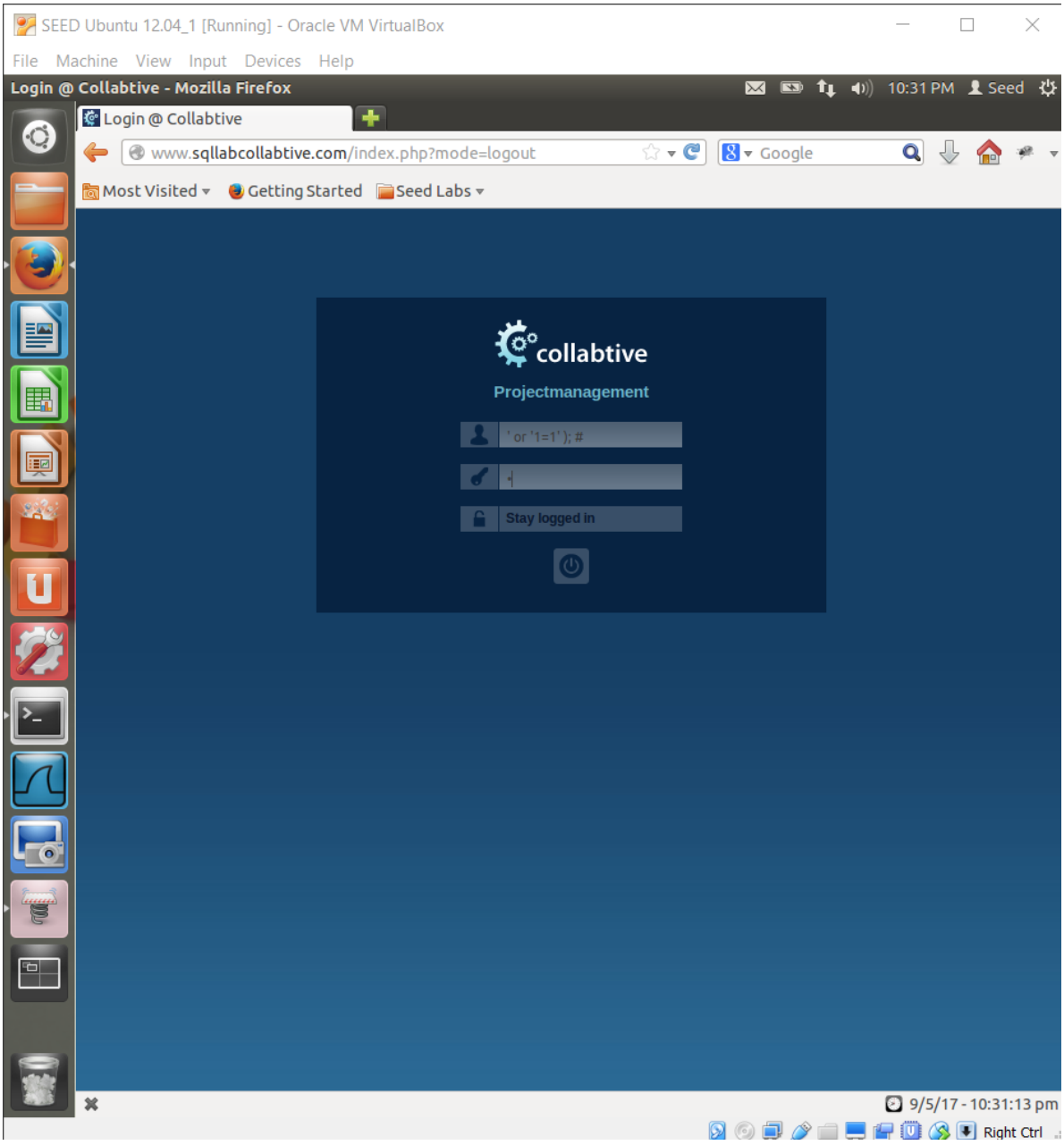


To be able to login with making the query appear blank, one must enter to following characters for the user:

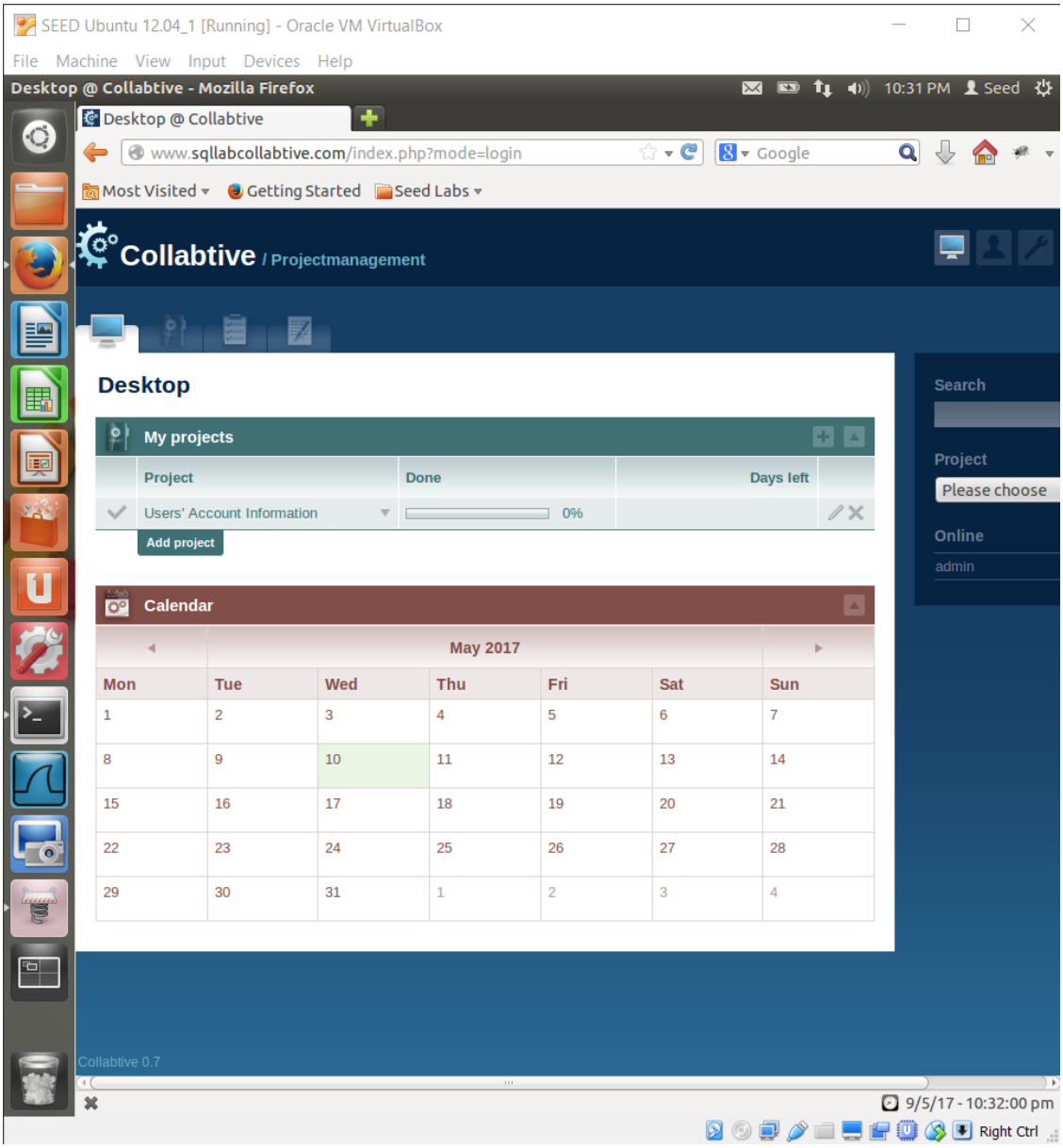
‘ or ‘1=1’); #

The above works by setting the user query to true and by commenting the rest of the WHERE statement. Setting the user query to true makes the SQL return all the rows from the user table. When one attempts to login using the characters mentioned above, the website thinks that the person logging in in is the admin.

Screenshot of input



Screenshot of login


SEED Ubuntu 12.04_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Desktop @ Collabtive - Mozilla Firefox
10:31 PM Seed
Desktop @ Collabtive
www.sqllabcollabtive.com/index.php?mode=login
Google
Most Visited
Getting Started
Seed Labs
Collabtive / Projectmanagement
Desktop
My projects
Project
Done
Days left
Users' Account Information
0%
Add project
Calendar
May 2017
Mon Tue Wed Thu Fri Sat Sun
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31 1 2 3 4
Search
Project
Please choose
Online
admin
Collabtive 0.7
9/5/17 - 10:32:00 pm
Right Ctrl