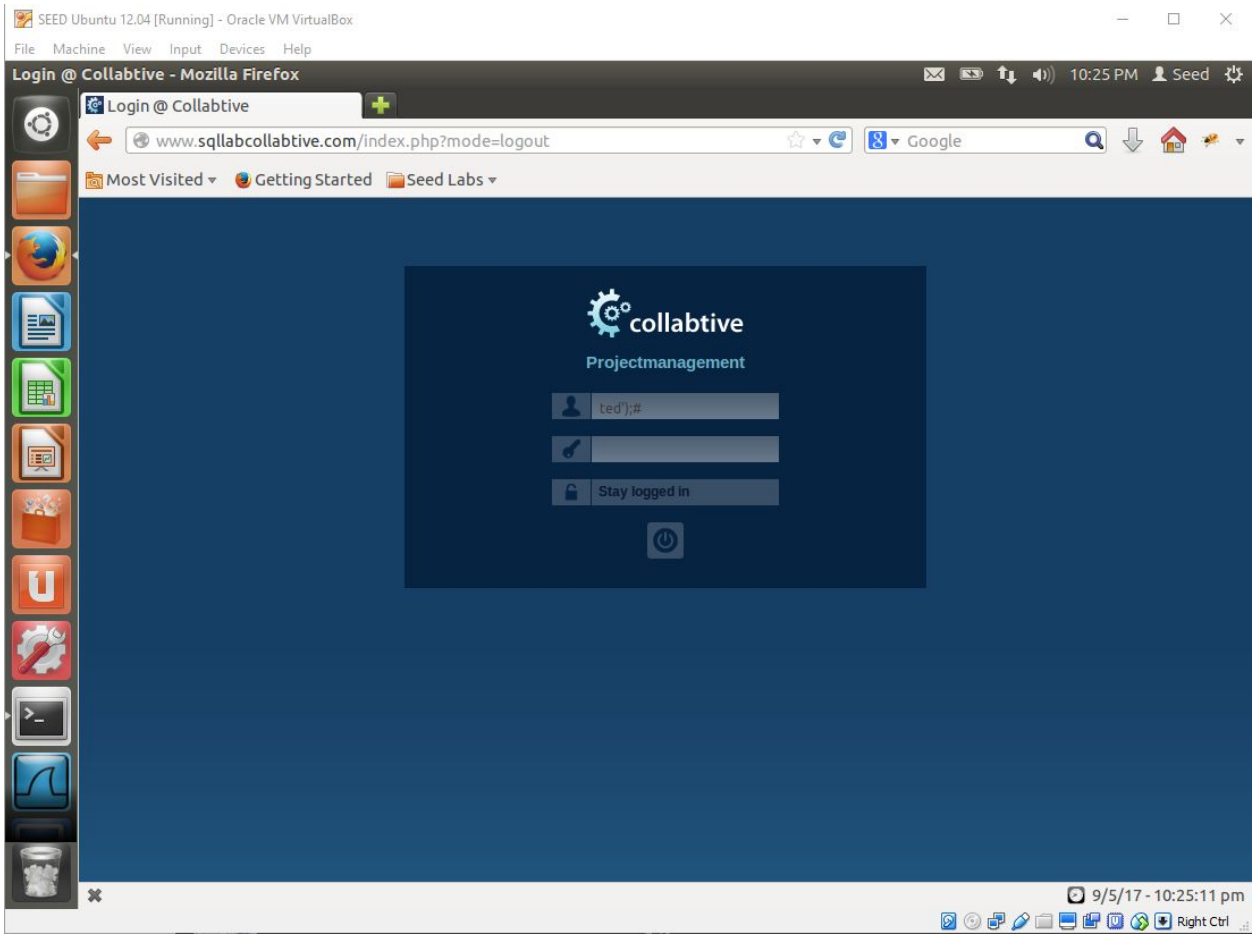
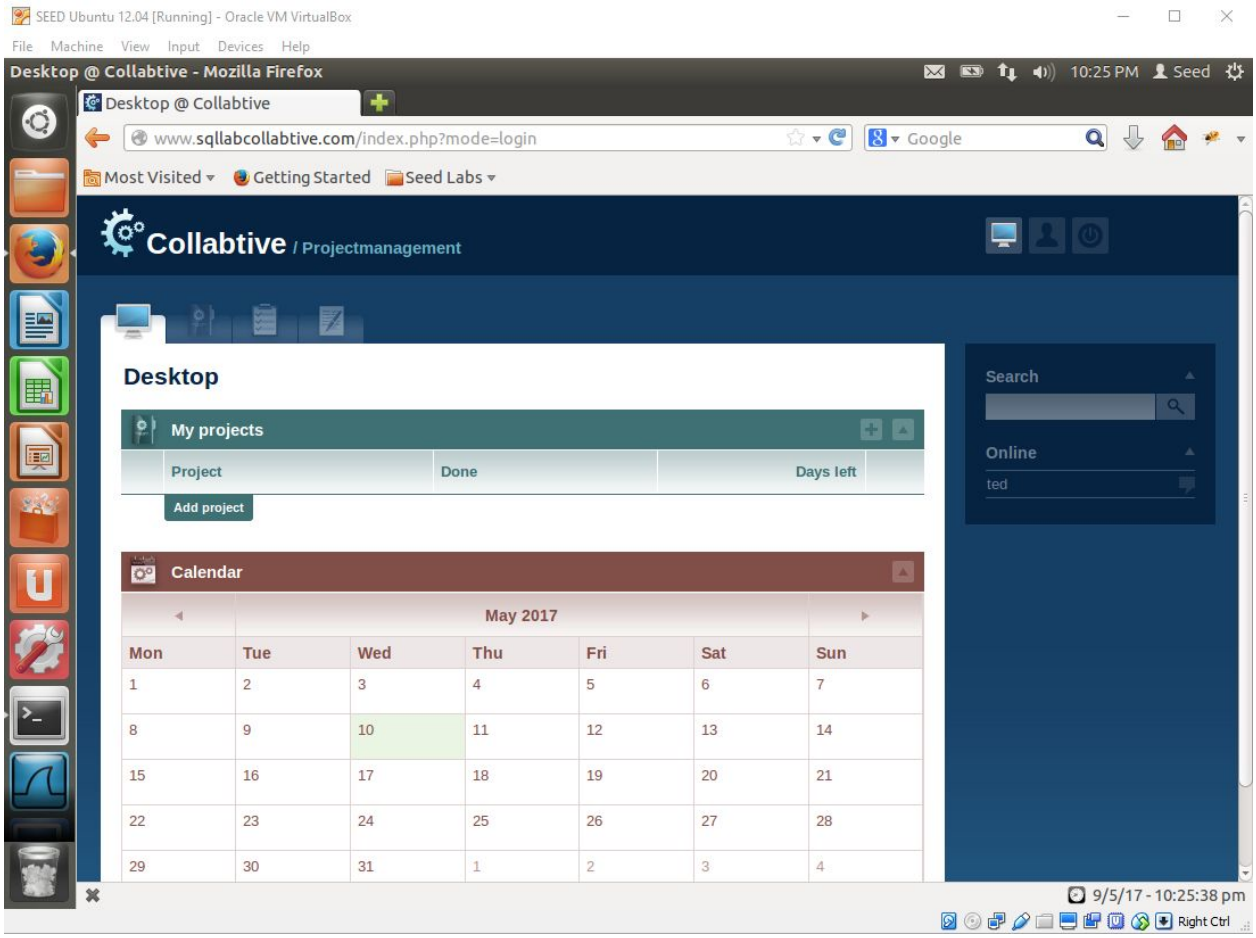
Jorge Luis Carrera
5-8-2017
CS380

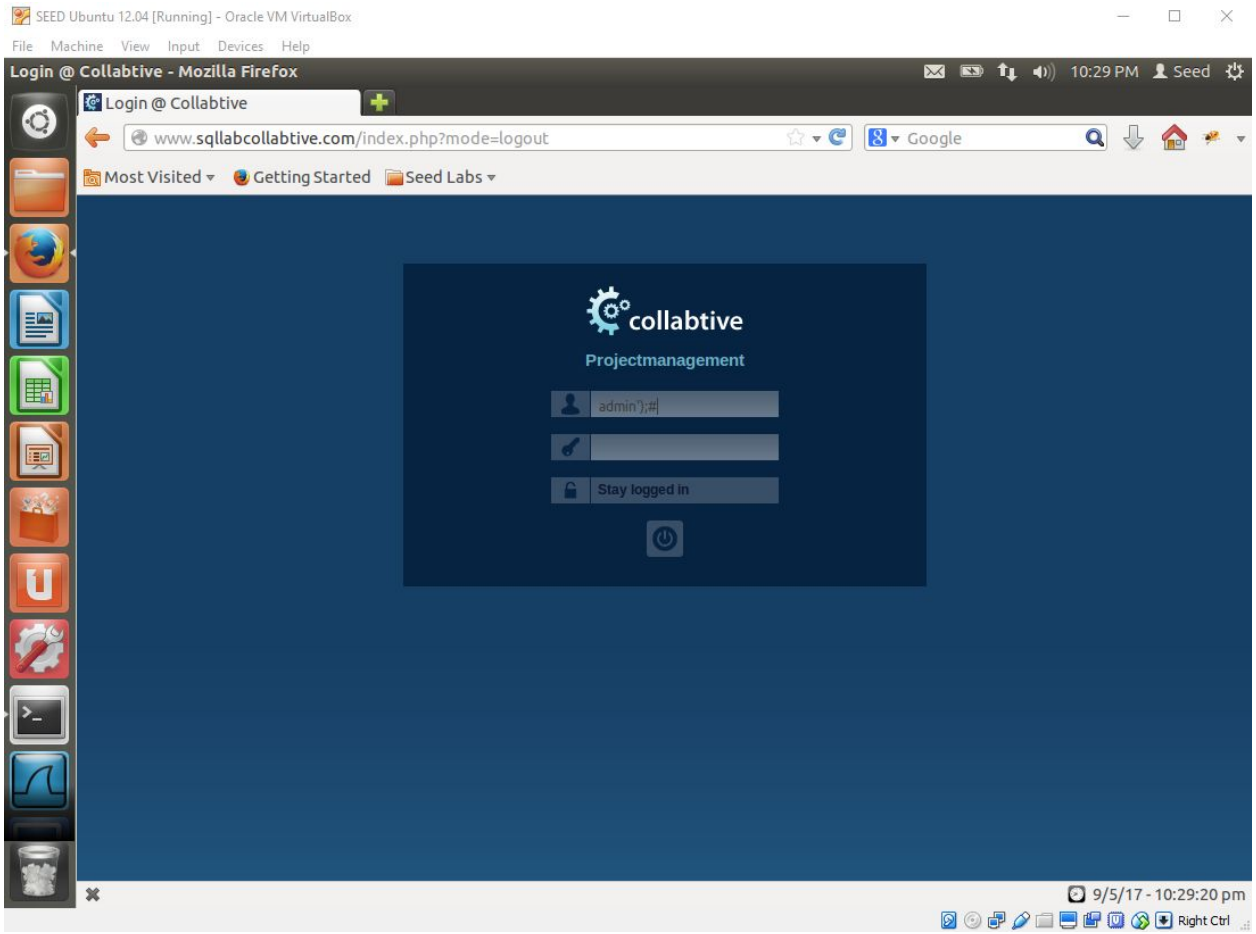
Exercise 6

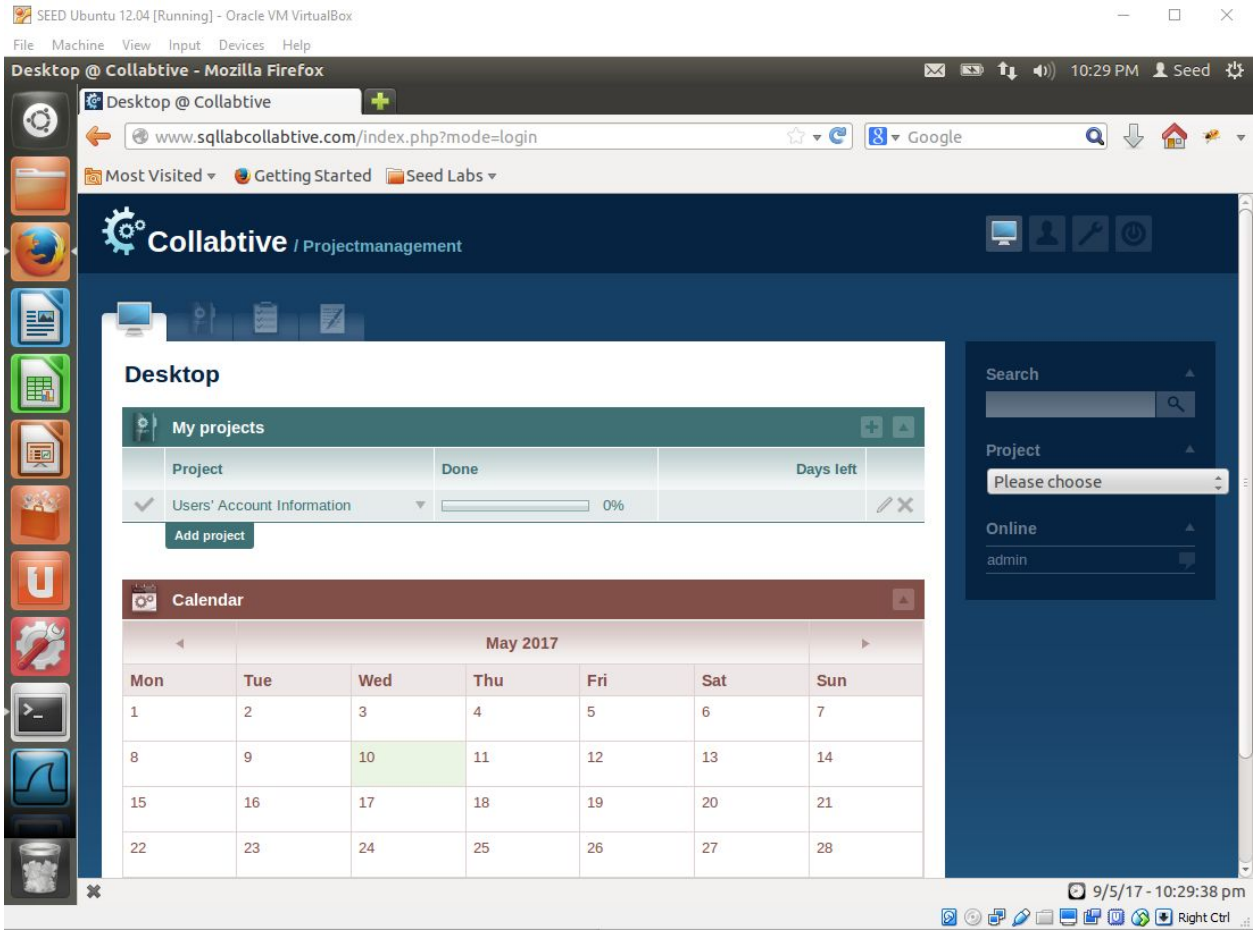
I viewed the code that handled user login for www.sqllabcollabtive.com and focused on any section that included $user. I eventually was able to come up with an input that logged me in as ted by bypassing the password check, the input was ted');# .



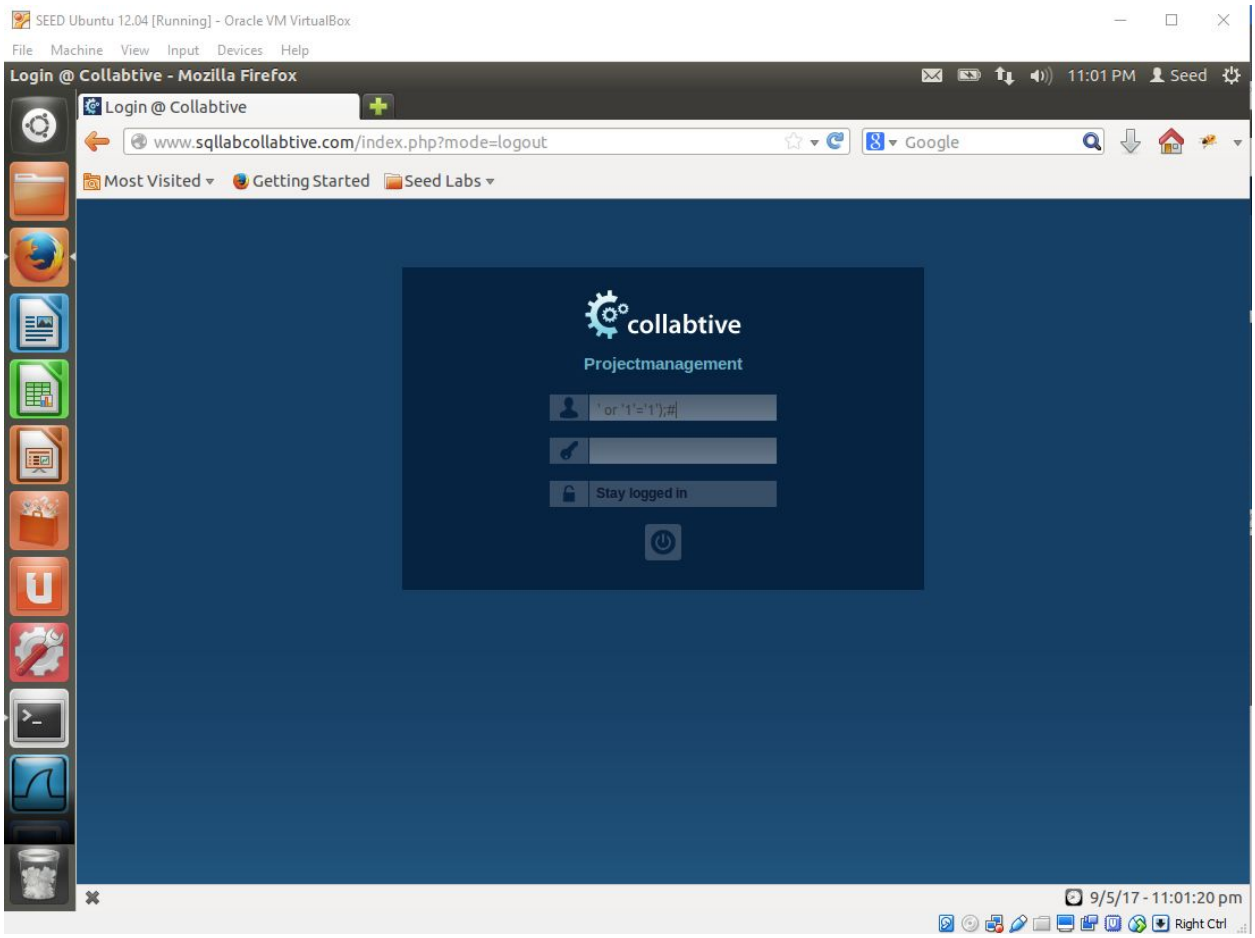


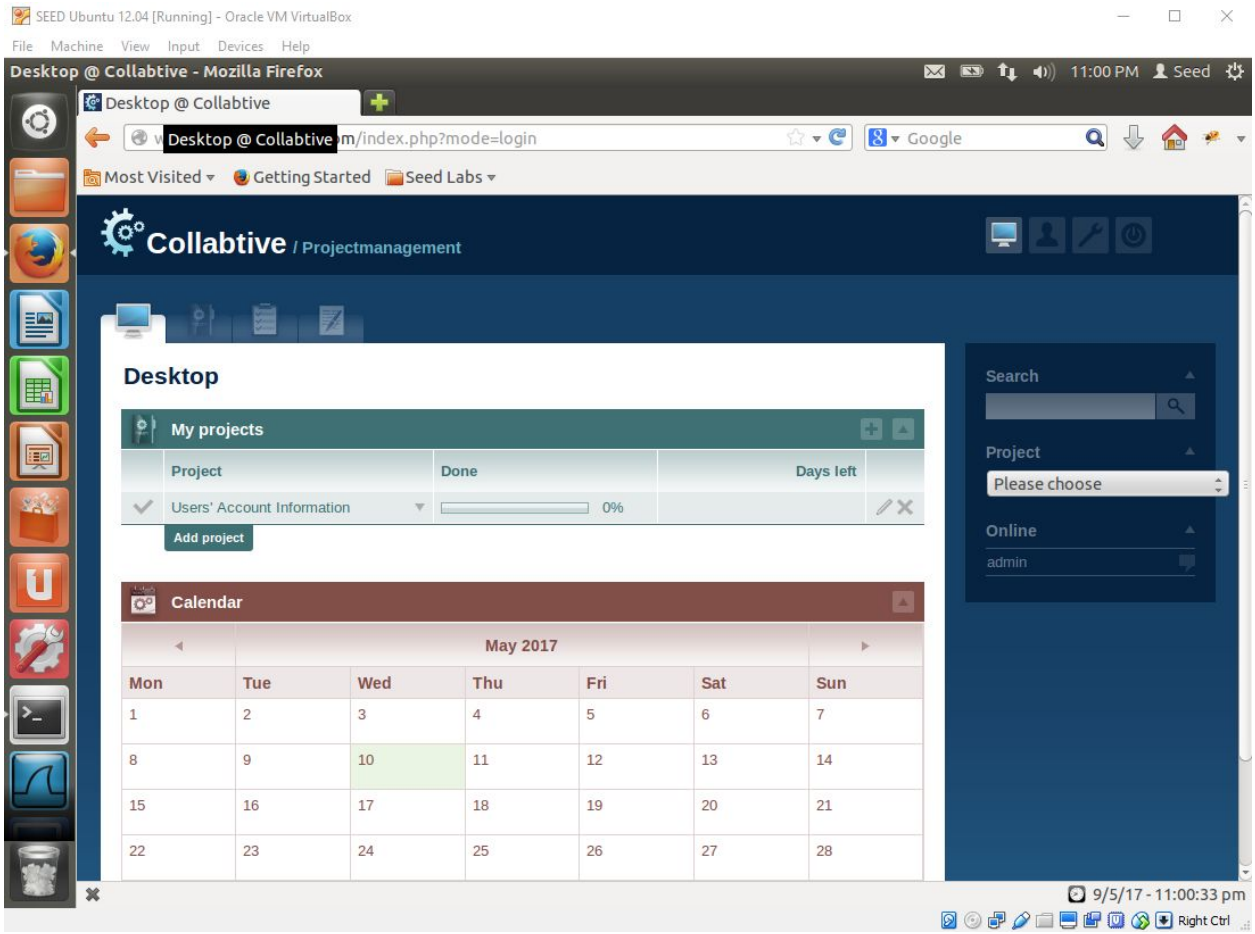
I tested out a similar input for the admin account and it also processed.


SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Login @ Collabtive - Mozilla Firefox
10:29 PM Seed
Login @ Collabtive
www.sqllabcollabtive.com/index.php?mode=logout
Google
Most Visited
Getting Started
Seed Labs
collabtive
Projectmanagement
admin');#
Stay logged in
9/5/17 - 10:29:20 pm
Right Ctrl



I also found a way to enter the site without formally addressing a name, and just inputting SQL commands to bypass the username/password checking. The end result was logging into the admin page.


SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Login @ Collabtive - Mozilla Firefox
11:01 PM Seed
Login @ Collabtive
www.sqllabcollabtive.com/index.php?mode=logout
Google
Most Visited
Getting Started
Seed Labs
collabtive
Projectmanagement
' or '1'='1');#
Stay logged in
9/5/17 - 11:01:20 pm
Right Ctrl


SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Desktop @ Collabtive - Mozilla Firefox
11:00 PM Seed
Desktop @ Collabtive
Desktop @ Collabtive m/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
Search
Project
Please choose
Online
admin
9/5/17 - 11:00:33 pm
Right Ctrl