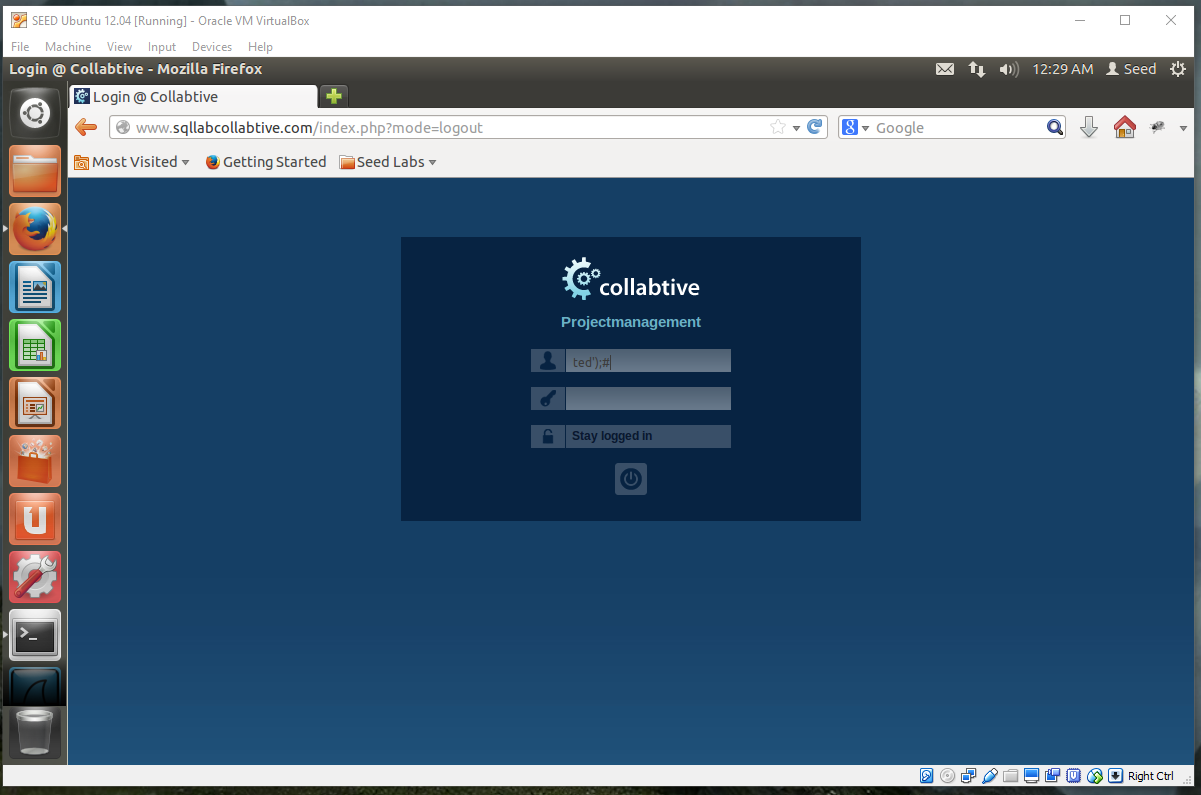
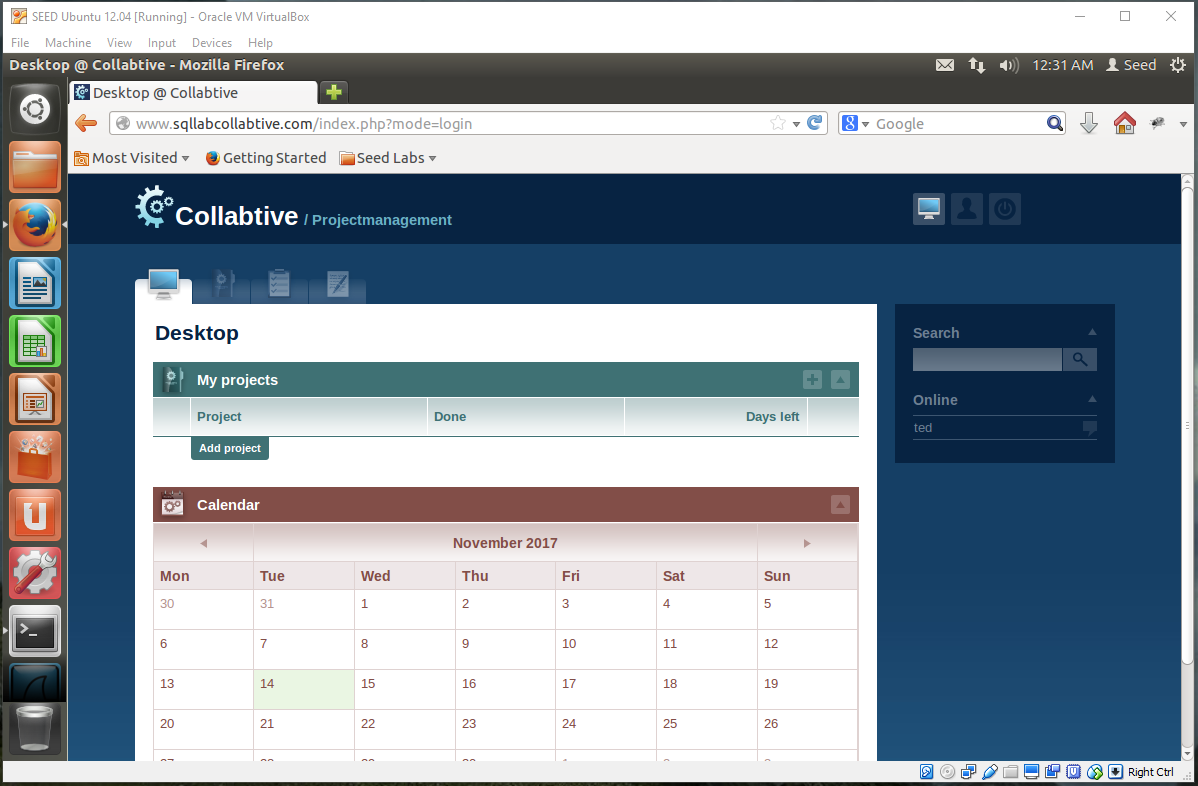
William Kenji Kiplinger

<https://github.com/Kenjum/CS380-EX6>

**Logging in as ted:**

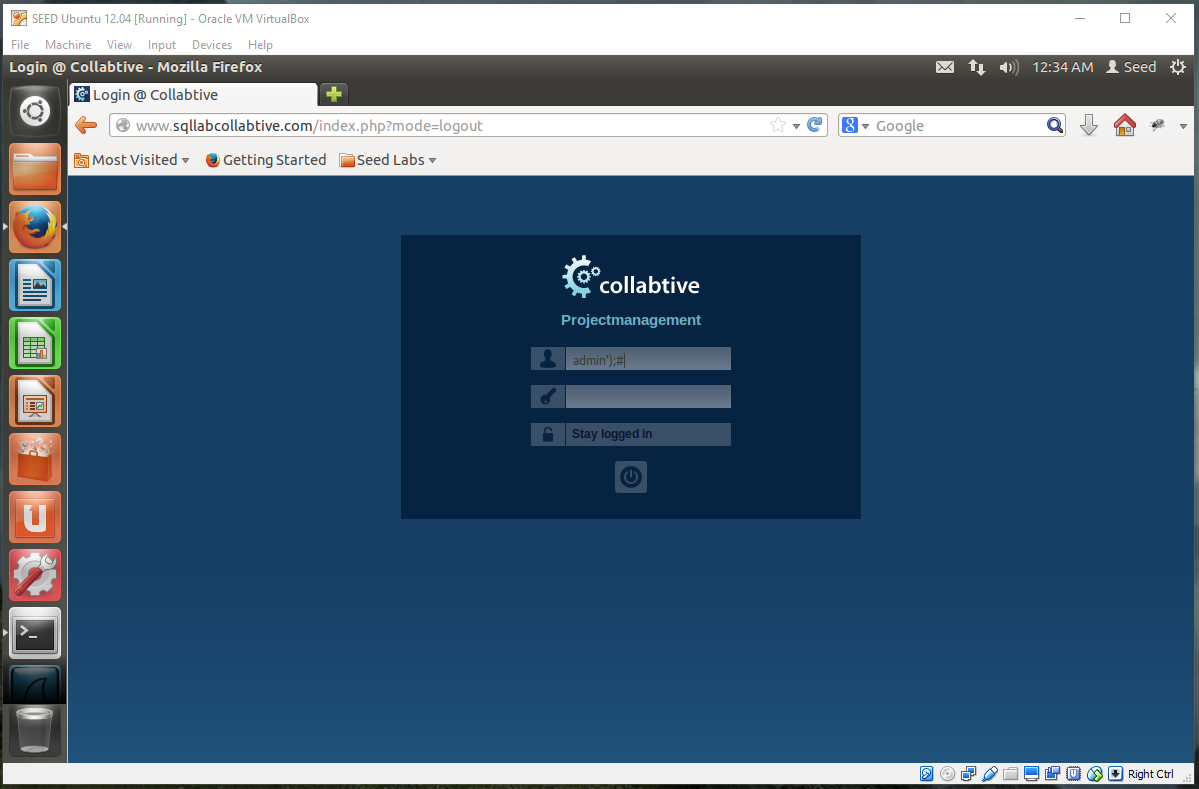
After editing the apache2 security, we bypass the password requirements with an SQL inject. With our knowledge of the code, we fill in the user field and close that off with a ‘); and have a # following it. # in SQL means that everything after it is commented out, so anything after ted’); will be ignored. This works well since the authentication is on one line of code.

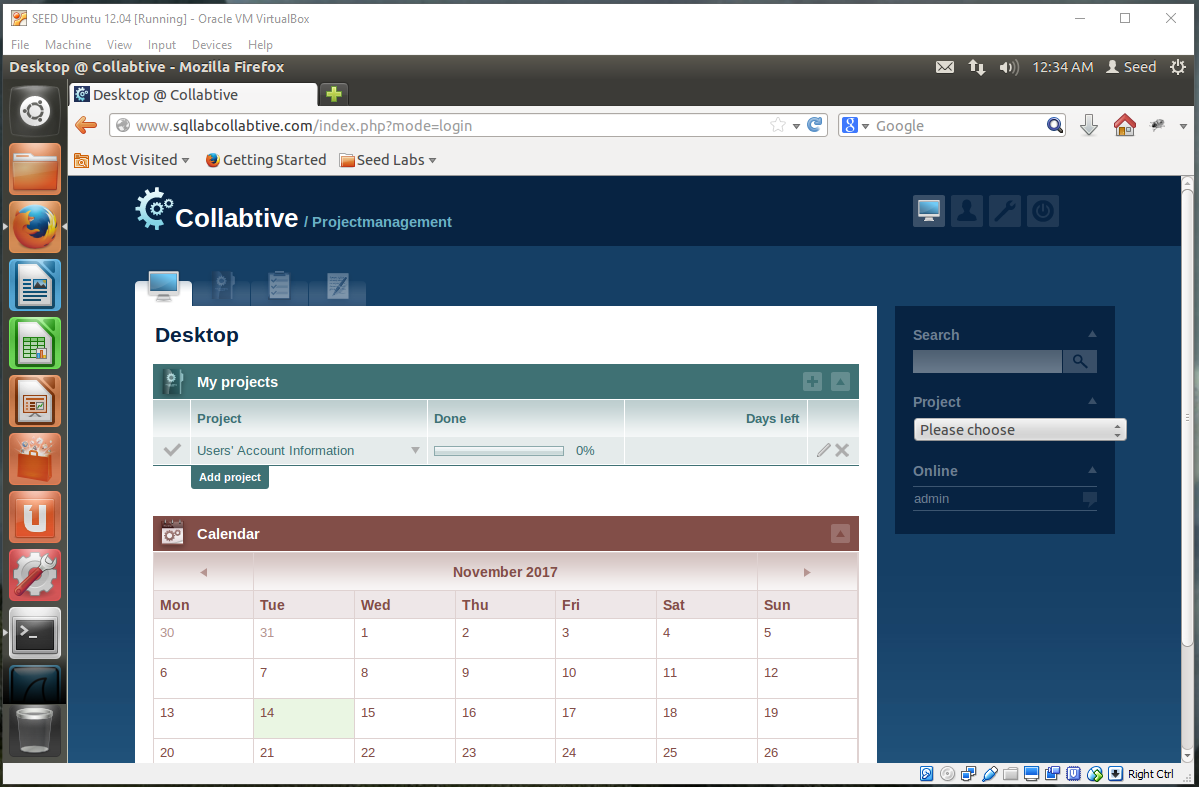




**Logging in as admin:**

The same steps were followed as the login for ted. This time, the name ted was replaced with admin.





**Logging in as blank:**

The way the SQL code is set up allows for us to pass a user and/or a true value. This will trick the machine into thinking it caught a hit and go with it. Here, it defaulted to the admin account. The );# as stated above apply to here too.

