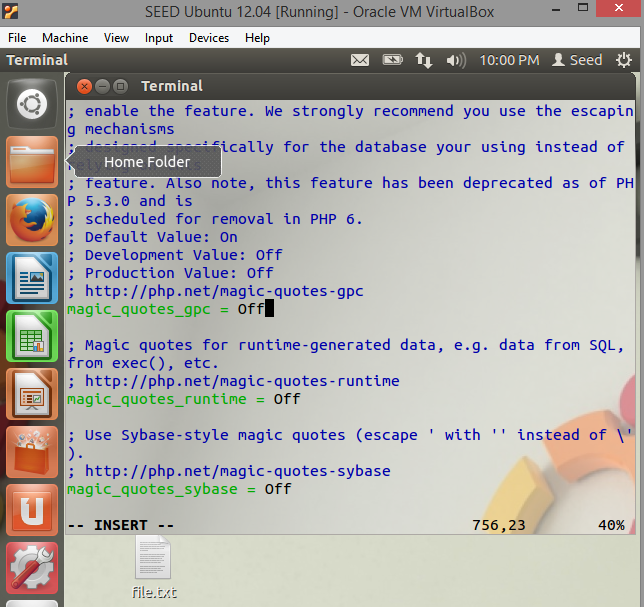
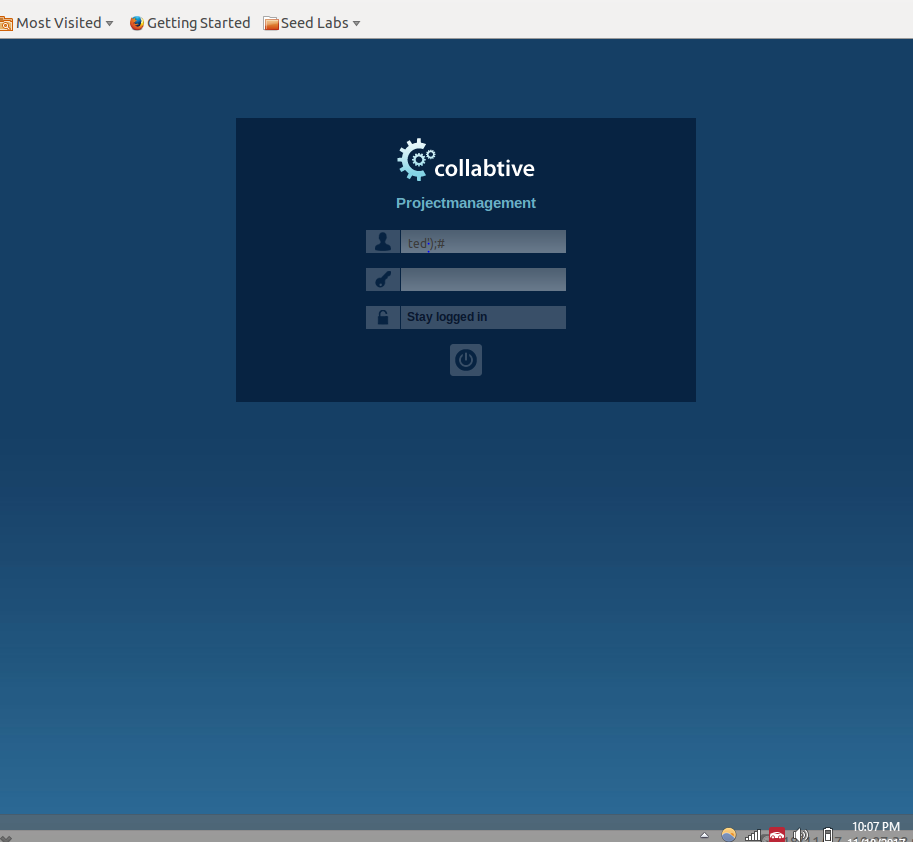
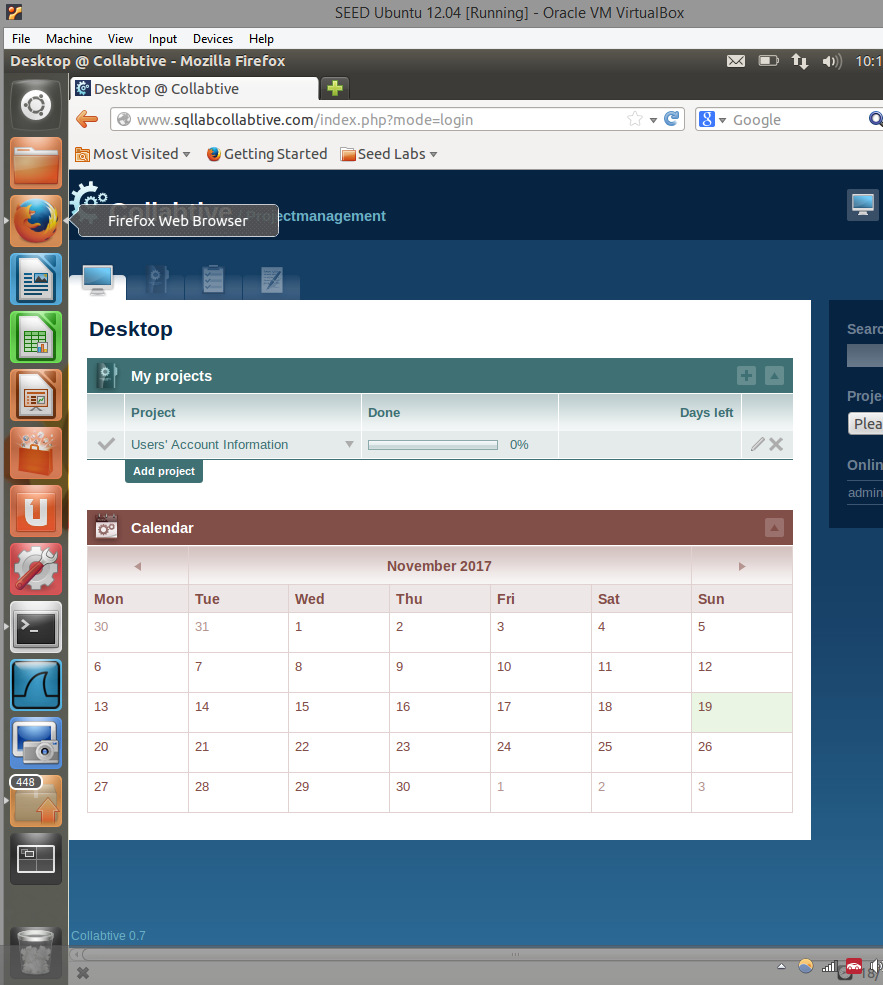
Maya Lake

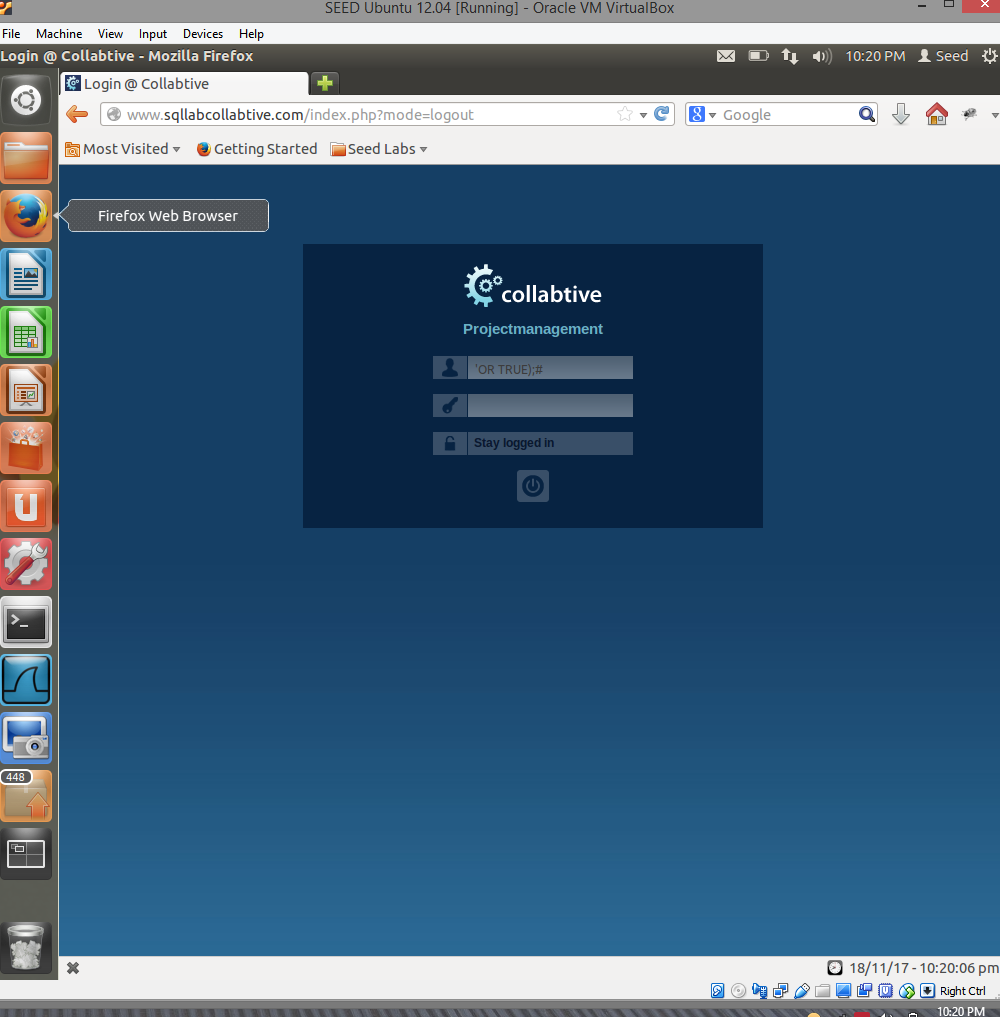




We are able to login using: ted’);# as the user login. The ‘ finishes the string entry, the ); finishes the parameter entry, and # will comment out the rest of the code so that the script reads in the user name and returns true as logged in.



We are able to login as admin the same way we are able to login as ted.



To login as an empty string, we must put in ‘OR TRUE);#. The script will read OR TRUE and or the empty string with True, which will always return True. The remaining );# exist for the same reason as mentioned above.

EXTRA CREDIT:

First, you manually change Ted’s password to alice in the edit panel on the website.

After you change Ted’s password, you log in using Ted and Alice. You can then inject new variables in some of the form entries. I attempted to change the password from the User form entry as a String array. Unfortunately I miscalculated what to input into the form entry, and set the password to another string I didn’t mean to, and have locked myself out of the account and can no longer log in so I was unable to finish the extra credit. However I understand the basic concept and pinpointed the code in the PHP file that we were suppose to look at to solve the extra credit.