

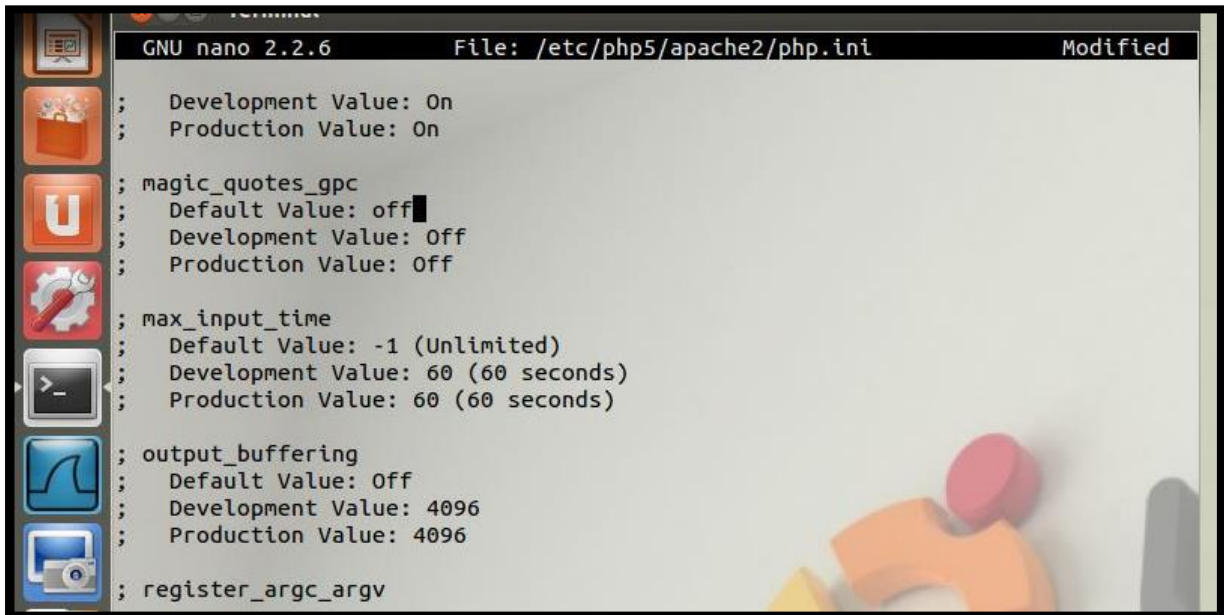
SQL Injection

Alizeh Jafri

Task 1:

To set up the lab:

Firstly, I turned off the protection for built-in SQL injection. For that, I opened the terminal in Ubuntu and typed the command: `sudo nano /etc/php5/apache2/php.ini` to switch it OFF:



```
GNU nano 2.2.6      File: /etc/php5/apache2/php.ini      Modified
; Development Value: On
; Production Value: On

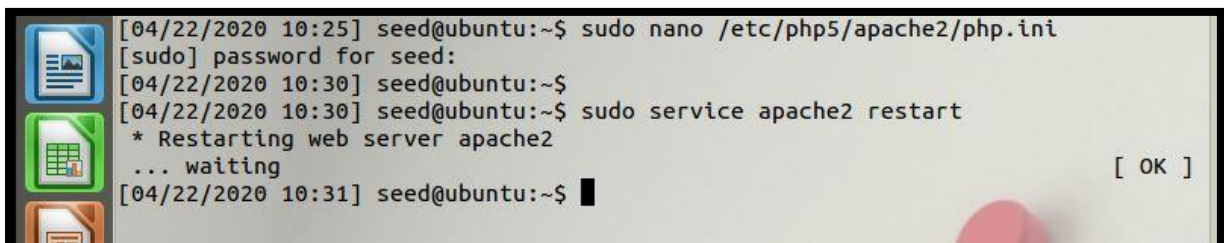
; magic_quotes_gpc
; Default Value: off
; Development Value: Off
; Production Value: Off

; max_input_time
; Default Value: -1 (Unlimited)
; Development Value: 60 (60 seconds)
; Production Value: 60 (60 seconds)

; output_buffering
; Default Value: Off
; Development Value: 4096
; Production Value: 4096

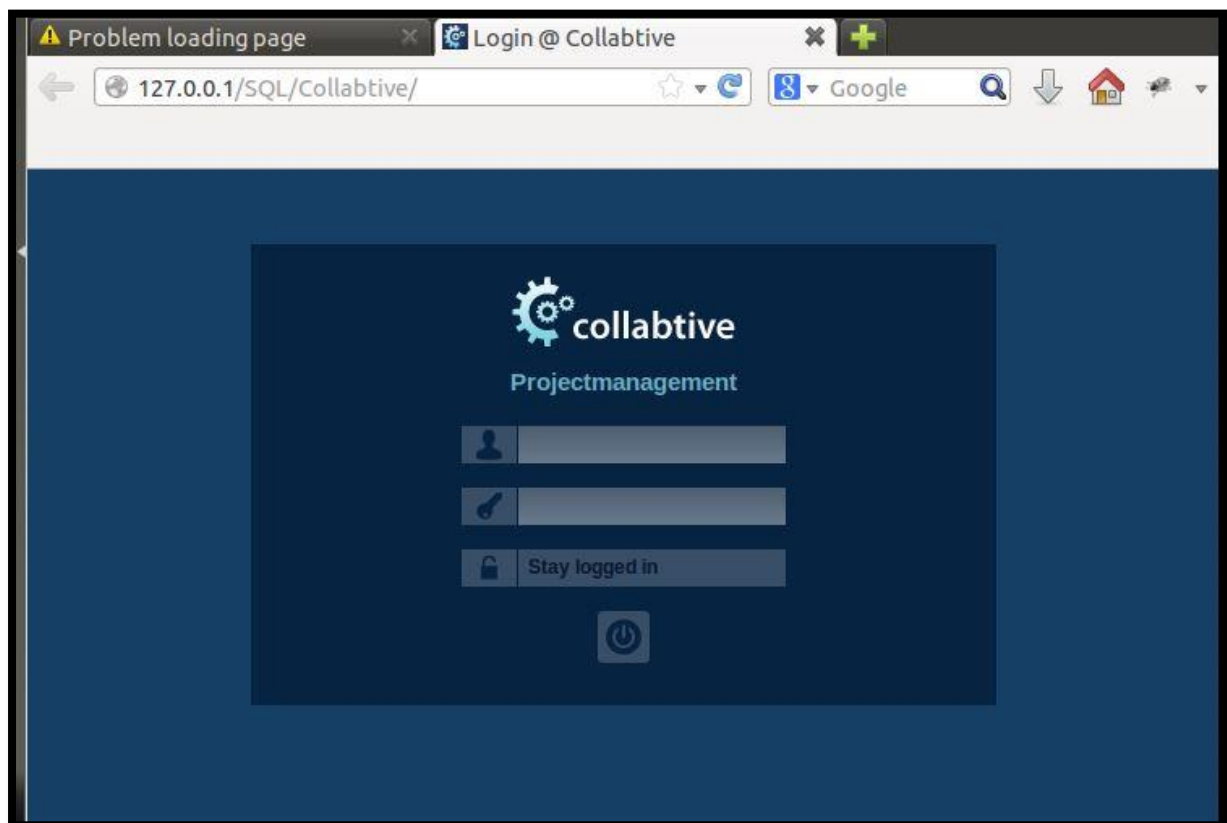
; register_argc_argv
```

Then I came back to the terminal and typed `sudo service apache2 restart`:

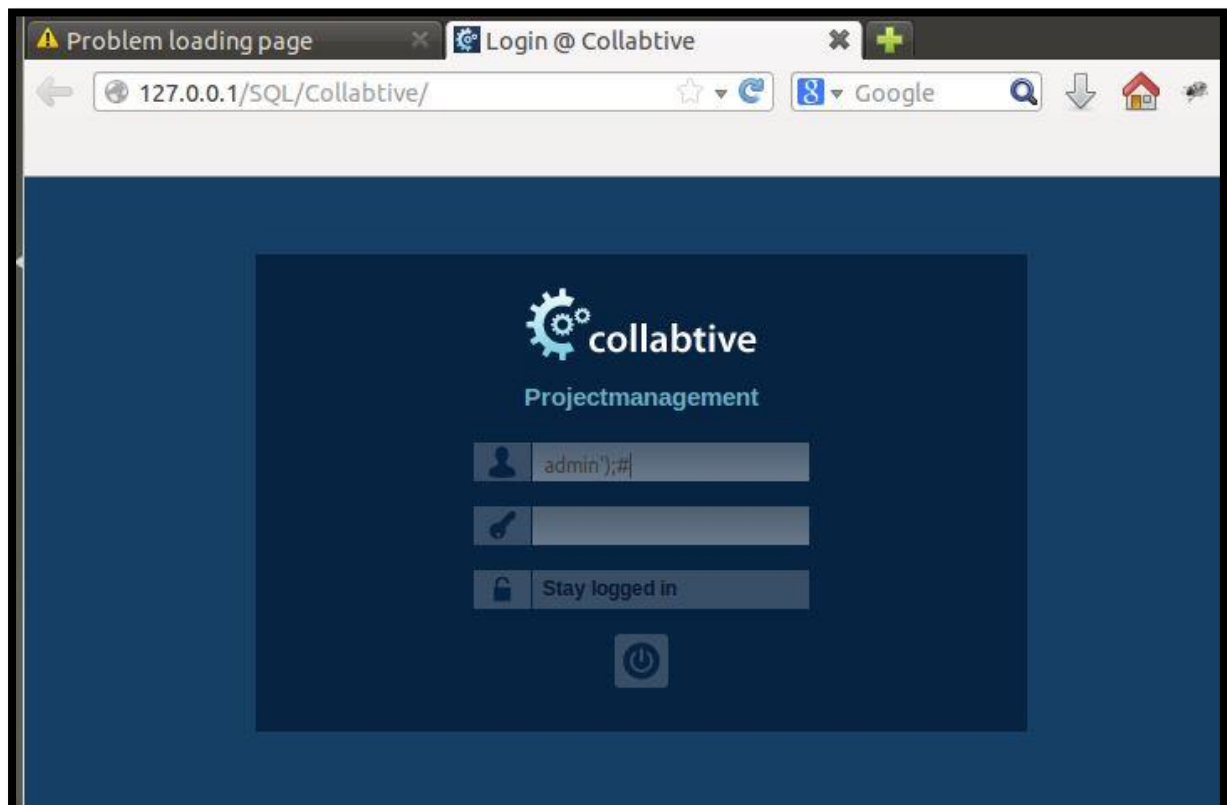


```
[04/22/2020 10:25] seed@ubuntu:~$ sudo nano /etc/php5/apache2/php.ini
[sudo] password for seed:
[04/22/2020 10:30] seed@ubuntu:~$
[04/22/2020 10:30] seed@ubuntu:~$ sudo service apache2 restart
* Restarting web server apache2
... waiting
[04/22/2020 10:31] seed@ubuntu:~$ [ OK ]
```

Next, I entered the URL using my IP/SQL/Collabtive:



So, the web page is now visible for me to login, I entered the following, for password you can type anything:



Now, I successfully entered the webpage after I logged in:

The screenshot displays a web application interface with a dark blue header bar. On the left, a vertical sidebar contains several icons: a globe, a document, a calendar, a folder, a shopping bag, a 'U' logo, and a trash can. The main content area is titled 'Desktop' and features two primary widgets.

The first widget, 'My projects', has a dark green header. Below it is a table with the following structure:

Project	Done	Days left
✓ Users' Account Information	<div><div></div></div> 0%	

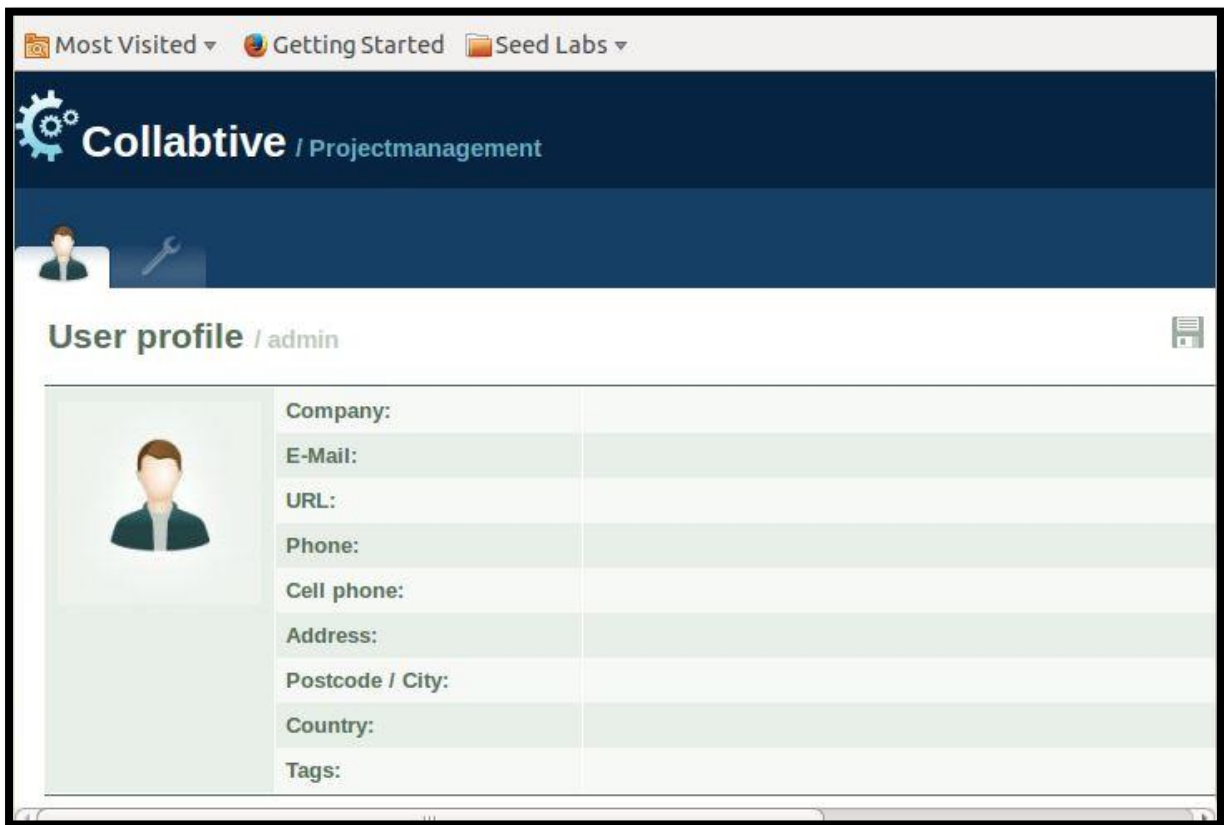
Below the table is a green 'Add project' button.

The second widget, 'Calendar', has a dark red header. It displays a calendar for April 2020 with the following layout:

April 2020						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
30	31	1	2	3	4	5
6	7	8	9	10	11	12


Navigation arrows are visible on the left and right sides of the calendar grid.

Task 2:



The screenshot shows a web browser window with the following elements:

- Browser tabs: "Most Visited", "Getting Started", "Seed Labs".
- Page header: "Collabative / Projectmanagement" with a gear icon.
- User profile section: "User profile / admin" with a user icon and a wrench icon.
- Form fields for user profile:

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

I logged into the website with username "alice" and password "alice".

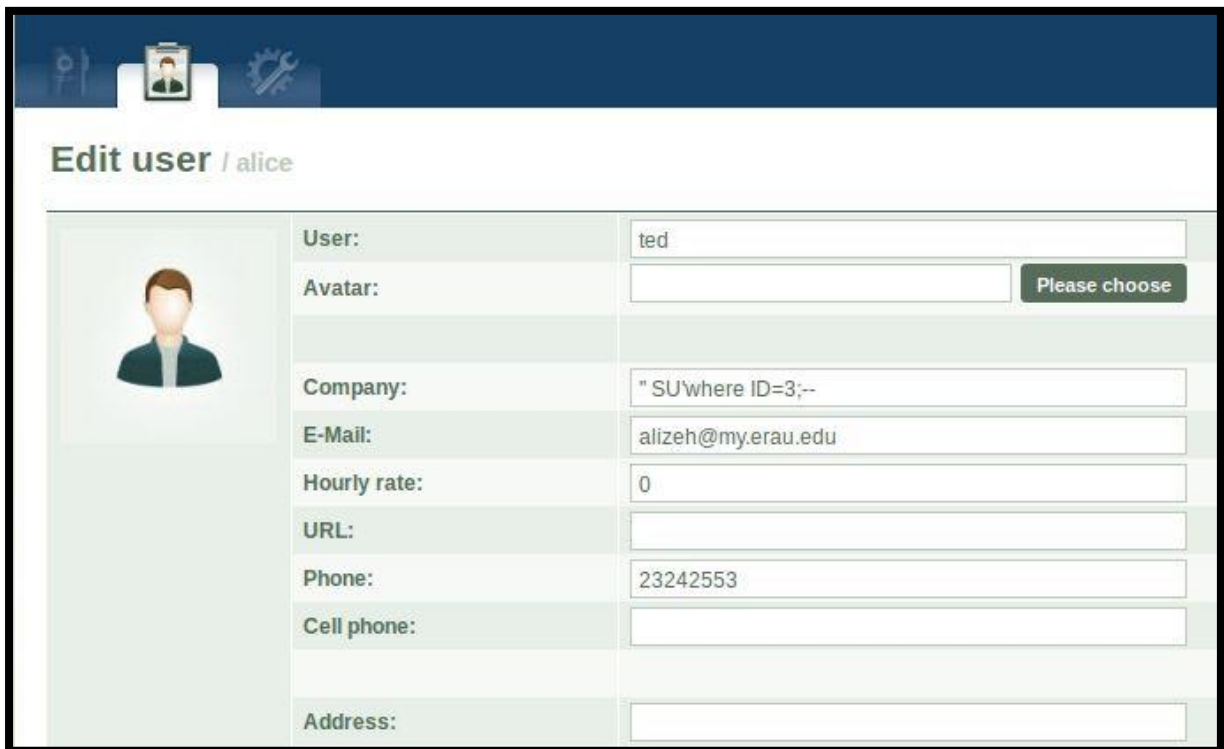


The screenshot shows the login page of the Collabative Projectmanagement system. It features the Collabative logo and the text "Projectmanagement". Below the header, there are three input fields:

- Username field: "alice"
- Password field: "*****"
- Stay logged in checkbox: "Stay logged in"

At the bottom, there is a power button icon.

Now, I modified the user ted's email information and password by updating Alice's profile, shown in the screen shot below:



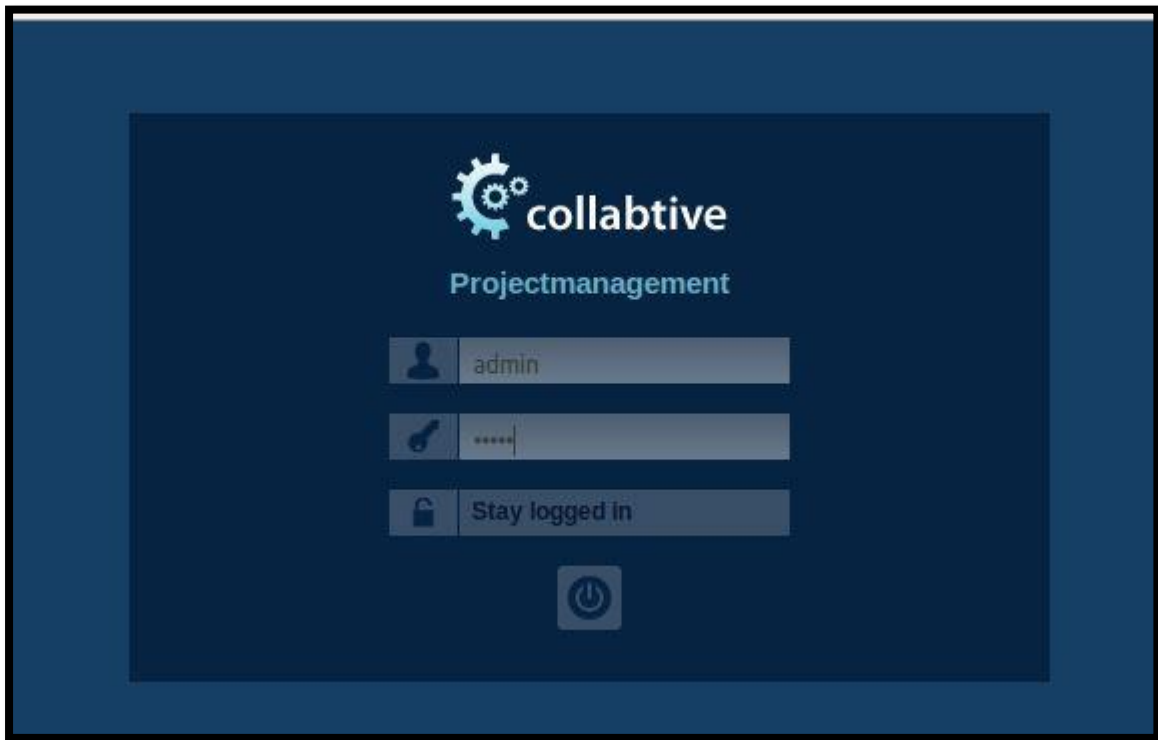
The screenshot shows a web interface for editing a user profile. The title is "Edit user / alice". On the left is a placeholder for a user avatar. To the right is a form with the following fields:

User:	ted
Avatar:	<input type="text"/> Please choose
Company:	" SU\where ID=3;--
E-Mail:	alizeh@my.erau.edu
Hourly rate:	0
URL:	<input type="text"/>
Phone:	23242553
Cell phone:	<input type="text"/>
Address:	<input type="text"/>

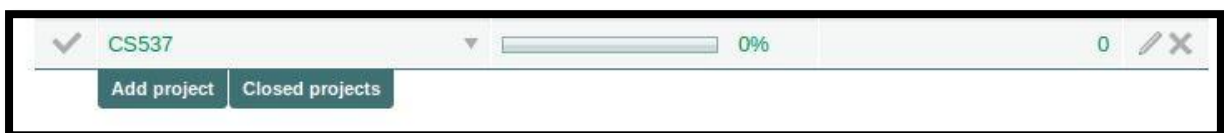
Then I logged in as ted and Ted's profile has been modified successfully!

Task 3:

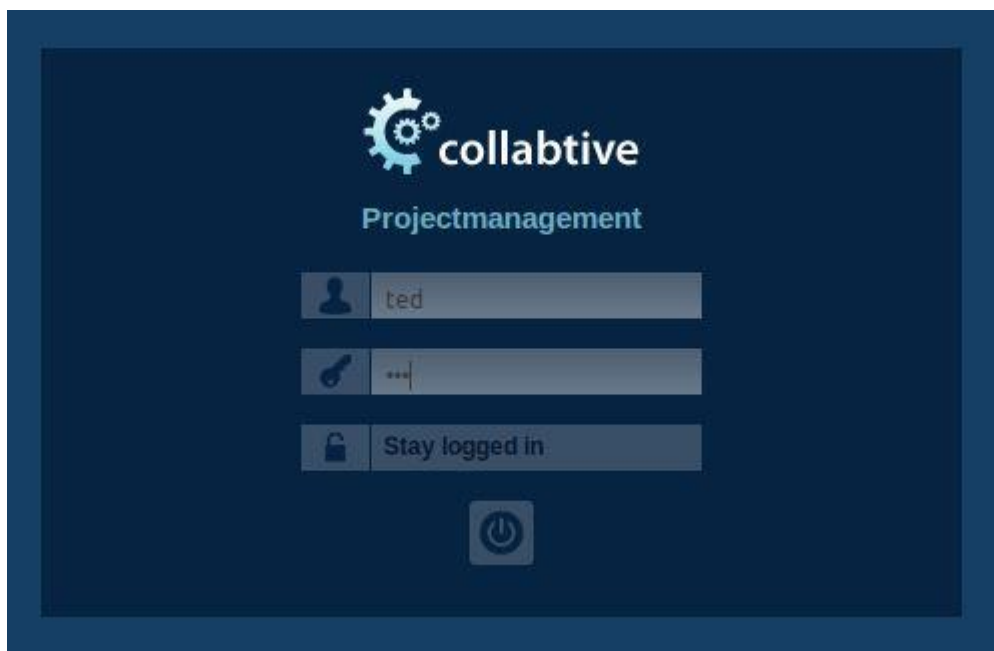
I logged into the service using user 'admin' and (password is "admin").



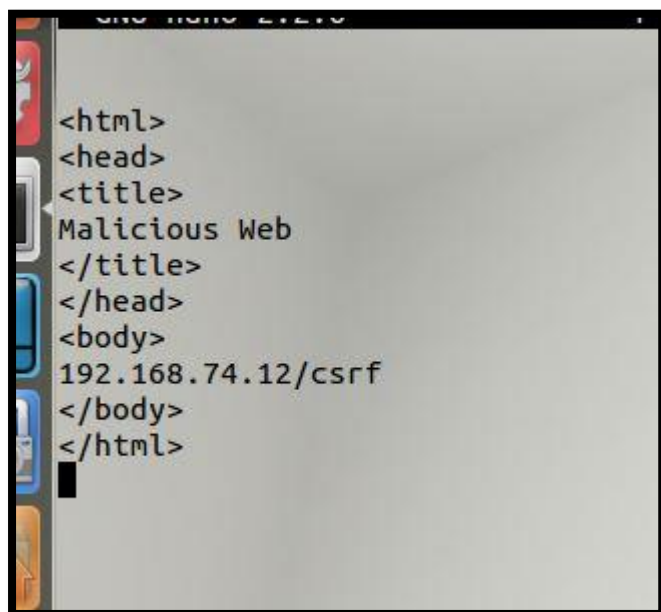
Step2: I created a project with name **cs537** and added ted as well as admin into the project:



Logged out the admin account, and login as ted (password is "pass"). My login was successful:



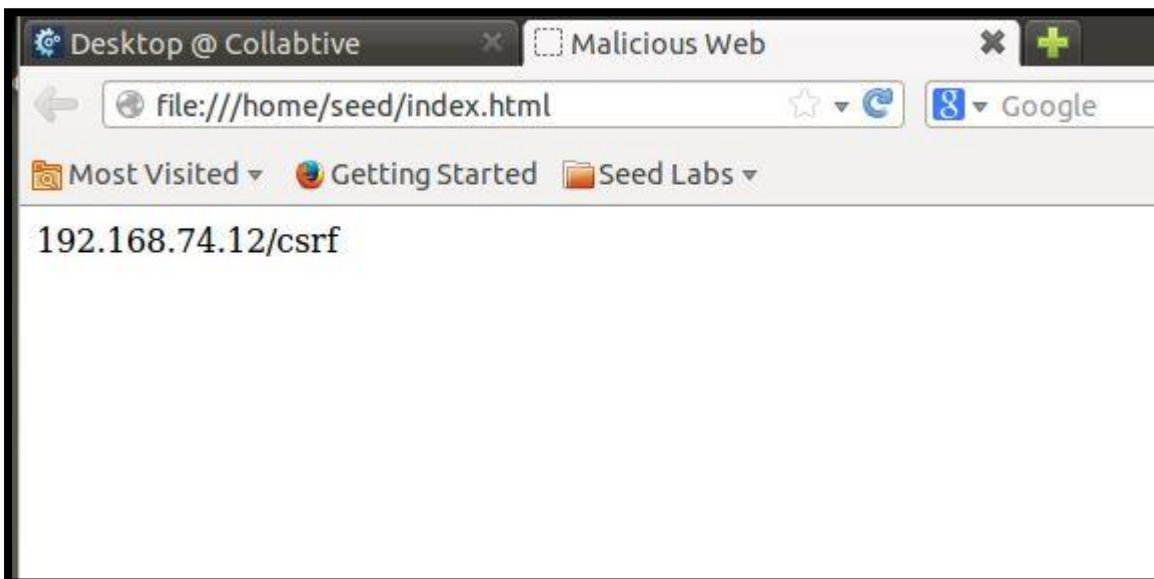
Next, I edited the content of the file using nano:



I used the command `ls -l` to view the files:

```
[04/22/2020 19:07] seed@ubuntu:~$ ls -l
total 4544
drwxr-xr-x  4 seed seed    4096 Dec  9  2015 Desktop
drwxr-xr-x  3 seed seed    4096 Dec  9  2015 Documents
drwxr-xr-x  2 seed seed    4096 Sep 17  2014 Downloads
drwxrwxr-x  6 seed seed    4096 Sep 16  2014 elggData
-rw-r--r--  1 seed seed   8445 Aug 13  2013 examples.desktop
-rw-rw-r--  1 seed seed     96 Apr 22  2013 file
-rw-rw-r--  1 seed seed      0 Apr 22  2013 index.html
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Music
drwxr-xr-x 24 root root    4096 Jan  9  2014 openssl-1.0.1
-rw-r--r--  1 root root 132483 Jan  9  2014 openssl_1.0.1-4ubuntu5.11.debian.ta
r.gz
-rw-r--r--  1 root root   2382 Jan  9  2014 openssl_1.0.1-4ubuntu5.11.dsc
-rw-r--r--  1 root root 4453920 Mar 22  2012 openssl_1.0.1.orig.tar.gz
drwxr-xr-x  2 seed seed    4096 Aug 25  2013 Pictures
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Public
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Templates
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Videos
```

Malicious index.html file content:



Ted can use this function to send his malicious website to the admin. The Screen shot of the message is shown below:

The screenshot shows a web application window titled "CS537". Inside, there is a section labeled "Add message". The "Title:" field contains the text "CS537 project". The "Text:" field is a rich text editor with a toolbar containing bold, italic, underline, font size, bulleted list, numbered list, link, unlink, image, and text color icons. The text area of the editor contains the URL "192.168.74.12/csrf". Below the text editor, there are "Files" and "Tags:" labels, each followed by an "Add" and an "Attach" button. At the bottom, the "Milestone:" label is followed by a dropdown menu currently showing "Please choose".

CS537

Add message

Title: CS537 project

Text:

B *I* U | Font size | |

192.168.74.12/csrf

Files

Tags:

Milestone: Please choose