SQL Injection

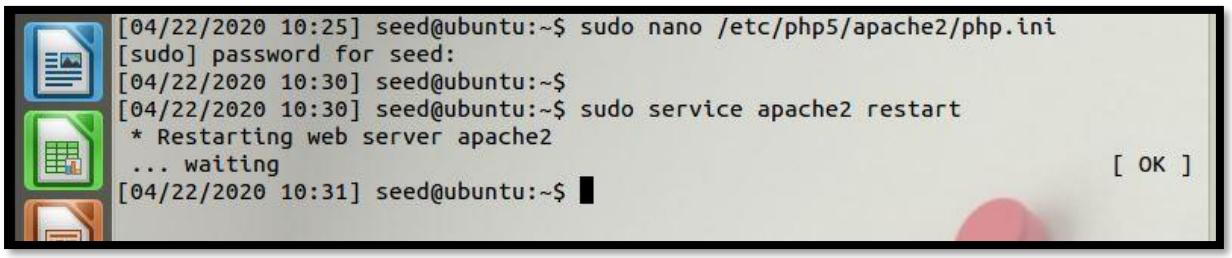
Alizeh Jafri

Task 1:

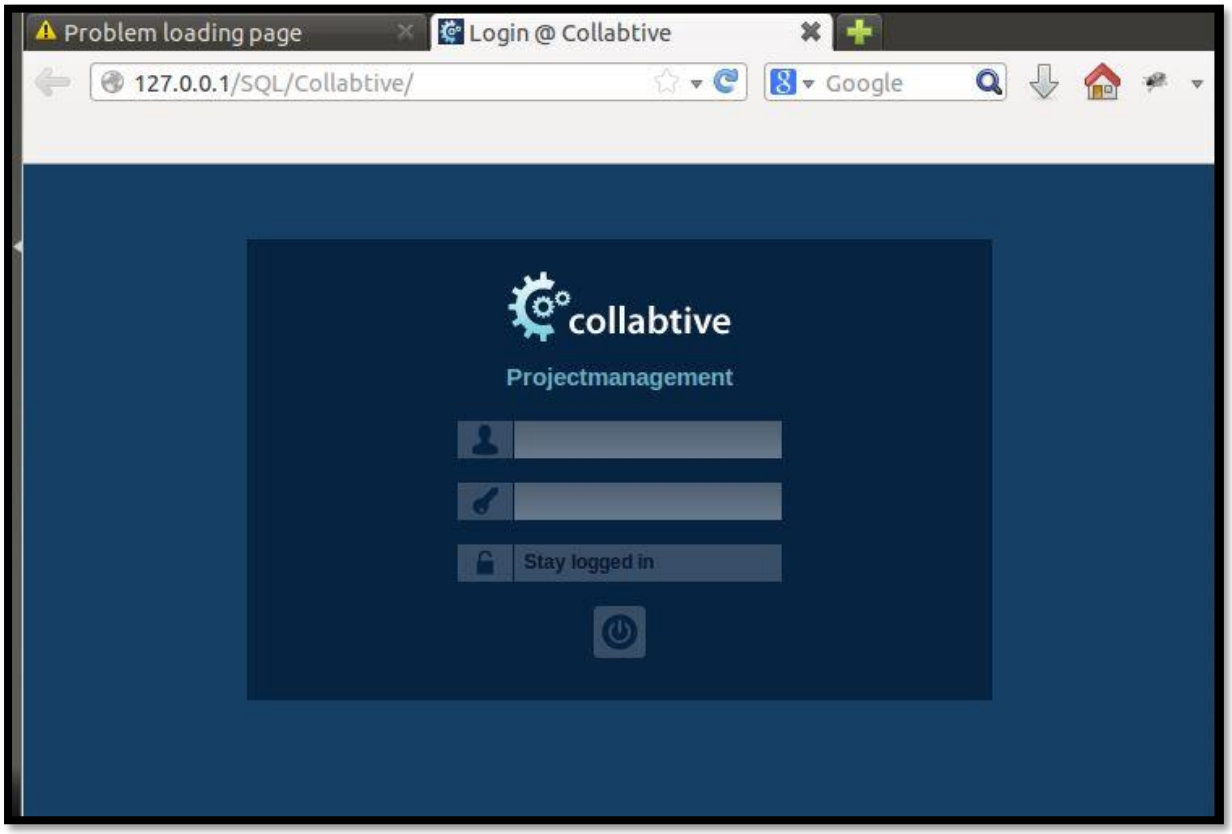
To set up the lab:

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:

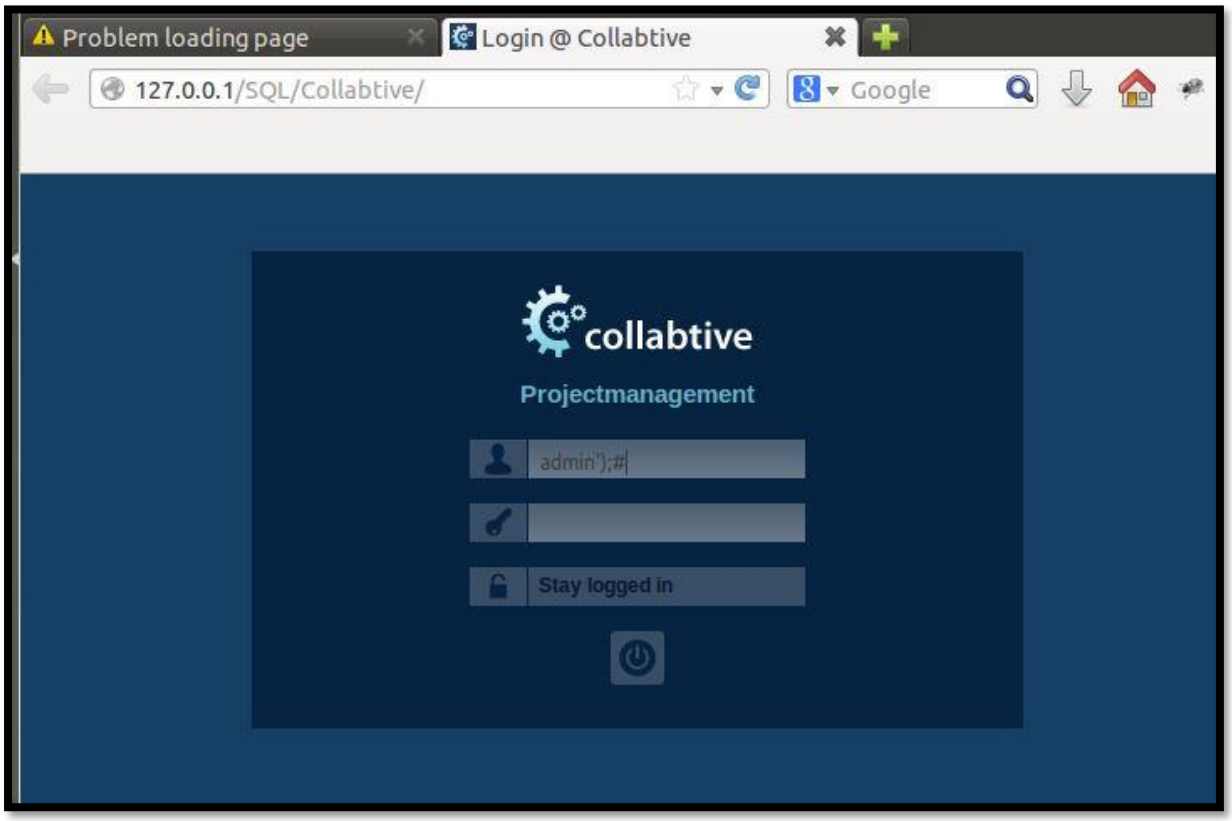
Then I came back to the terminal and typed sudo service apache2 restart:



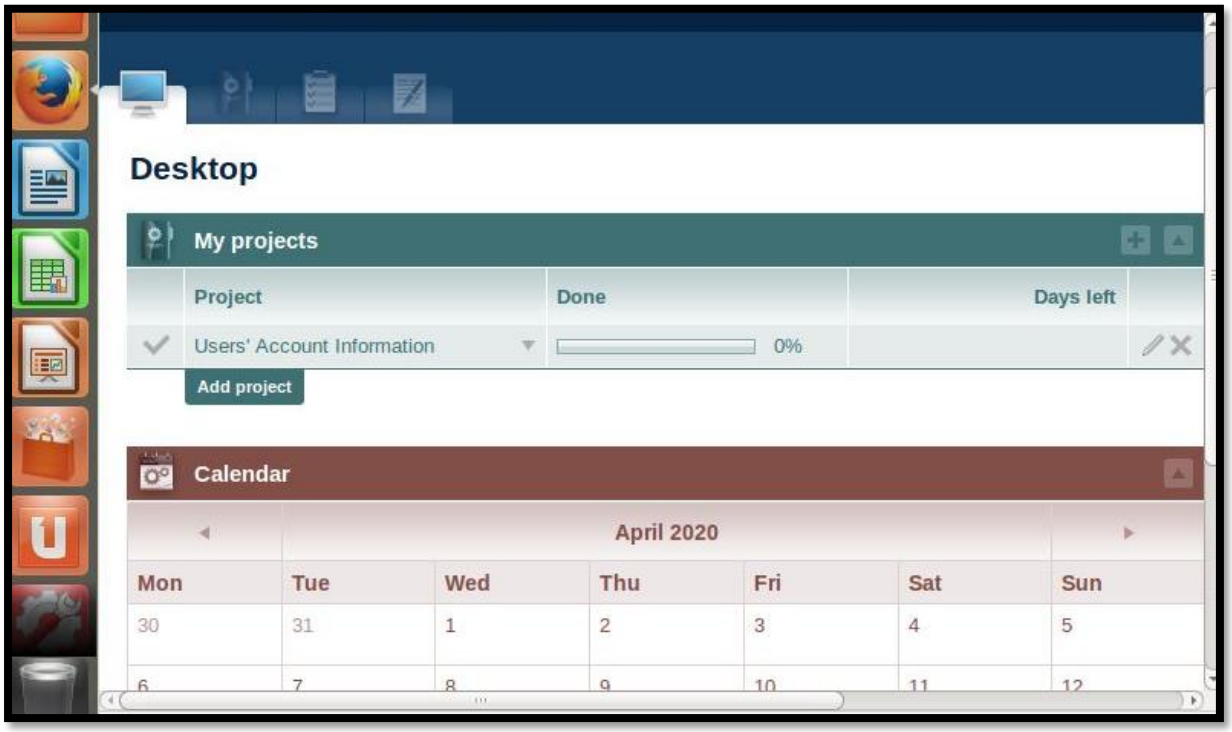
Next, I entered the URL using my IP/SQL/Collabtive:



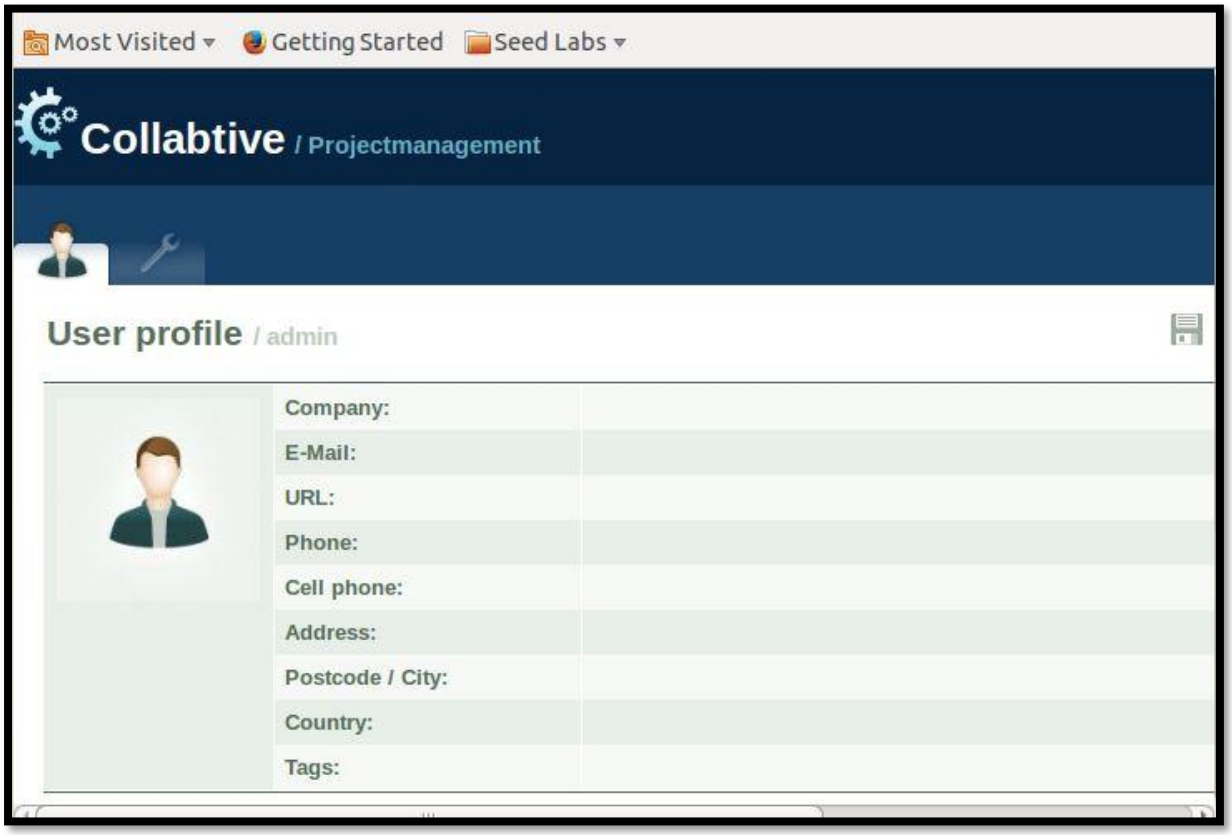
So, the web page is now visible for me to login, I entered the following, for password you can type anything:



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

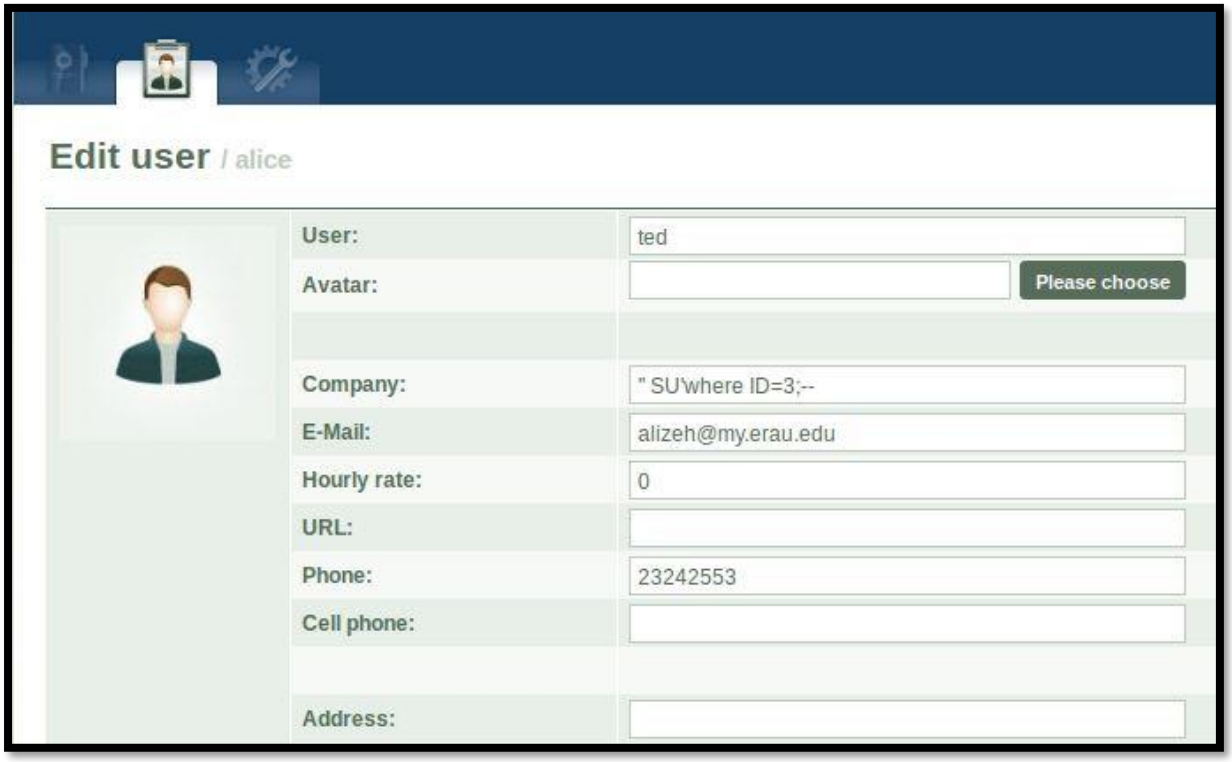


Task 2:



I logged into the website with username “alice” and password “alice”.

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



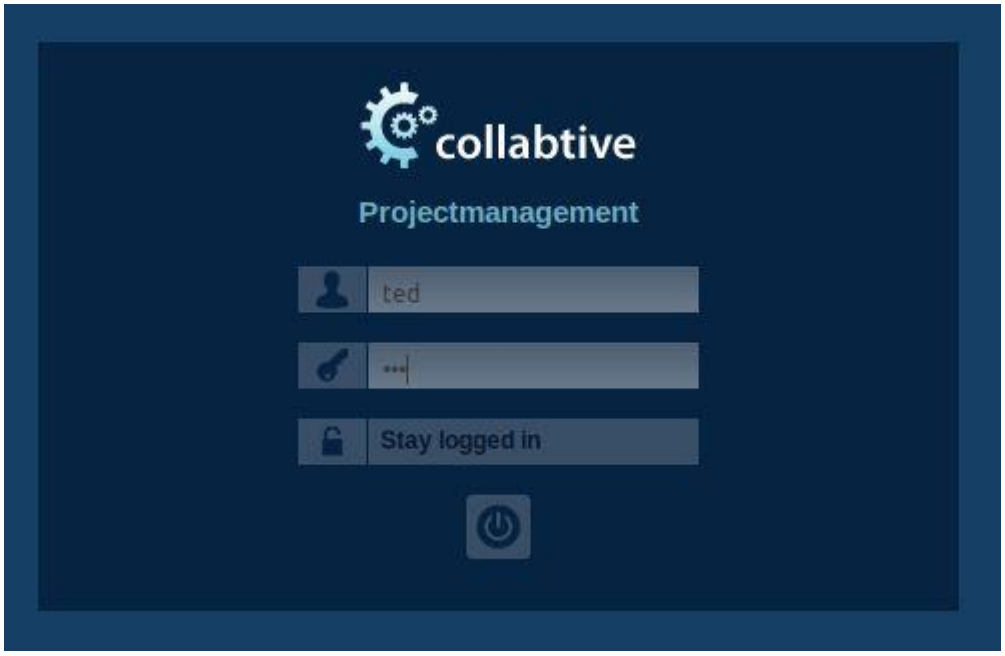
Then I logged in as ted and Ted's profile has been modified successfully!

Task 3:

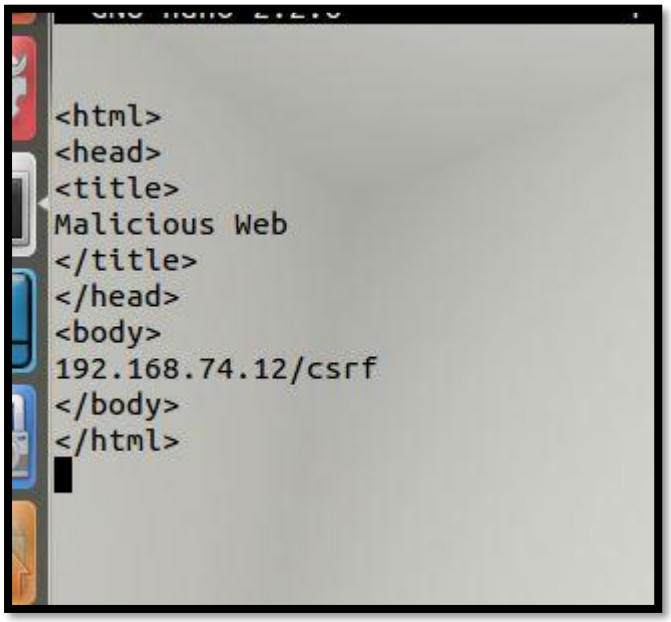
I logged into the service using user ‘admin’ and (password is “admin”).

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:



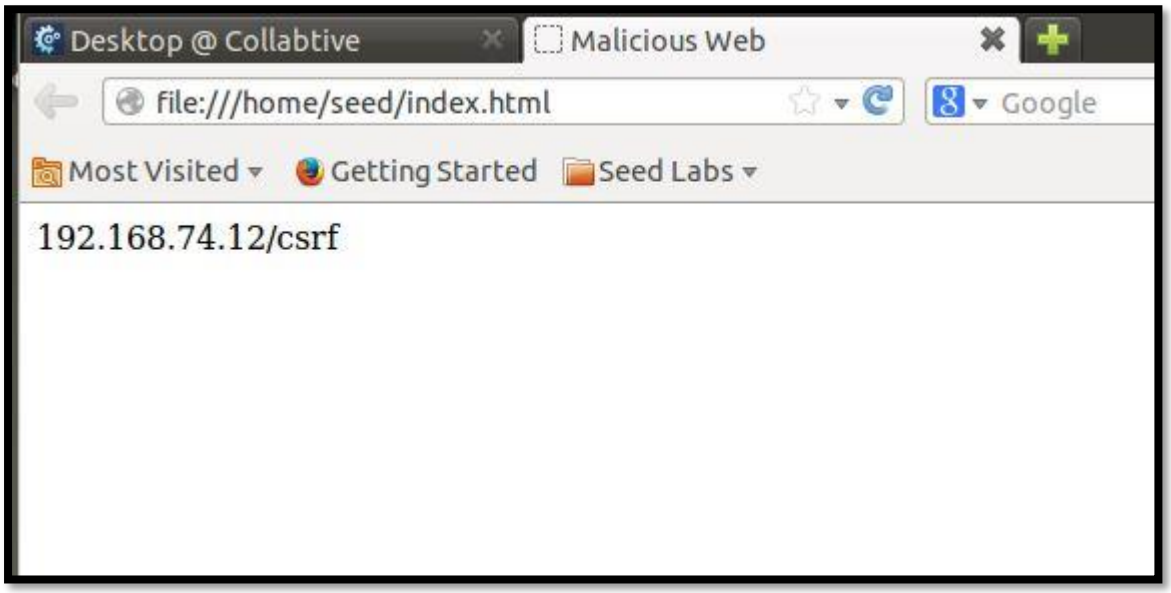
Next, I edited the content of the file using nano:



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 13:56 file
-rw-rw-r--  1 seed seed       0 Apr 22 19:07 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: