



## Assignment 2

### Cross-Site Scripting (XSS) Attack

Submission Date: February 15, 2024

*by*

1905052

Bijoy Ahmed Saiem

Under the supervision of

Dr. Md. Shohrab Hossain

Md. Toufikuzzaman

A.K.M. Mehedi Hasan

Abdur Rashid Tushar

Bangladesh University of Engineering and Technology  
BUET



## Contents

1	Task 1	1
2	Task 2	2
3	Task 3	4
4	Task 4	7



## 1 Task 1

I was given the code of task 1 in XSSDemo.txt except the sendurl. So i had to find the sendurl. For that i logged in to the charlie's profile and send a friend request to samy while monitor the network part of the inspect. Here i find the url which is shown to the below picture.

The screenshot shows a web browser at [www.seed-server.com/profile/samy](http://www.seed-server.com/profile/samy). The page displays a user profile for 'Samy' with a profile picture of a black hat. The browser's developer tools are open, showing the Network tab. A GET request is highlighted, showing the URL: [http://www.seed-server.com/action/friends/add?friend=596\\_\\_elgg\\_ts=17079238776\\_\\_elgg\\_token=BHGc9lmi-1jzvWYp5Orw6\\_\\_elgg\\_token=BHGc9lmi-1jzvWYp5Orw6](http://www.seed-server.com/action/friends/add?friend=596__elgg_ts=17079238776__elgg_token=BHGc9lmi-1jzvWYp5Orw6__elgg_token=BHGc9lmi-1jzvWYp5Orw6). The status is 200 OK, and the response headers show Cache-Control: must-revalidate, no-cache, no-store, private; Connection: Keep-Alive; Content-Length: 386.



## 2 Task 2

Here, i was given the code of task 2 in XAADemo.txt except the sendurl and content. So, i logged in samy's profile and went to the edit profile section . Where i change the description and submit it. At that time i monitor the network section in the inspect. Where i found the sendurl (post) given in the below picture.

The screenshot shows a web browser at [www.seed-server.com/profile/samy](http://www.seed-server.com/profile/samy). The page displays the profile of 'samy' with an 'About me' section. The Chrome DevTools Network tab is open, showing a list of network requests. The selected request is a POST to <http://www.seed-server.com/action/profile/edit> with a status of 302 Found. The response headers are visible, including Cache-Control, Connection, Content-Length, Content-Type, and Date.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server...	edit	document	html	4.21 kB	16.77 kB
200	GET	www.seed-server...	samy	document	html	4.26 kB	16.77 kB
200	GET	www.seed-server.com	59large.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...	favicon-128.png	FaviconLoader.sys...	png	cached	4.33 kB
200	GET	www.seed-server...	favicon.svg	FaviconLoader.sys...	svg	cached	6.50 kB
200	GET	www.seed-server...	sprint.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server...	en.js	require.js:127 (script)	js	cached	0 B

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, 14 Feb 2024 15:34:19 GMT



Here, i wanted to find out the content. So i checked the Request section in the inspect while clicking on the submit button of the edit profile section. And i got the content shown on the below picture.

The screenshot shows a web browser at [www.seed-server.com/profile/samy](http://www.seed-server.com/profile/samy). The page displays a user profile for 'Samy' with a profile picture of a hat and an 'About me' section. The browser's developer tools are open to the 'Network' tab, showing a list of requests. The selected request is a POST to 'edit' with a status of 302. The 'Request payload' is visible on the right, showing a form data token and a JavaScript payload injected into the 'description' field.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings
302	POST	www.seed-server...	edit	document	html	4.21 kB	16.77 kB					
200	GET	www.seed-server...	samy	document	html	4.26 kB	16.77 kB					
200	GET	www.seed-server.com	59large.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...	favicon-128.png	FaviconLoader.sys...	png	cached	4.33 kB					
200	GET	www.seed-server...	favicon.svg	FaviconLoader.sys...	svg	cached	6.50 kB					
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					

Request payload

```
.....74147455023560372382062125840
Content-Disposition: form-data; name="_elgg_token"
GJz15laCtwBzMeBxG8RIVQ
.....74147455023560372382062125840
Content-Disposition: form-data; name="elgg_ts"
1707924838
.....74147455023560372382062125840
Content-Disposition: form-data; name="name"
Samy
.....74147455023560372382062125840
Content-Disposition: form-data; name="description"
<script type="text/javascript">
  window.onload = function () {
    // ...
  }

```



### 3 Task 3

Here i had to find the sendurl,content and profile link of the samy to complete this task 3.  
So, i logged in as samy and went to the wire to post on behalf of samy to monitor the network section where i got the sendurl(post type) shown on the below picture.

The screenshot shows a web browser at [www.seed-server.com/thewire/all](http://www.seed-server.com/thewire/all). The page displays a post by 'Samy' with the text 'hi, i am samy!'. Below the post, there are links for 'RSS', 'Bookmark this page', and 'Report this'. The page is powered by Elgg.

The Chrome DevTools Network tab is open, showing a list of network requests. The selected request is a POST to <http://www.seed-server.com/action/thewire/add>. The request headers are visible, showing a status of 302 Found, version HTTP/1.1, and a content type of text/html.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server...	add	document	html	4.53 kB	18.59 kB
200	GET	www.seed-server...	all	document	html	4.58 kB	18.59 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...	init.js	require.js:127 (script)	js	cached	370 B

The selected POST request details are as follows:

- Status: 302 Found
- Version: HTTP/1.1
- Transferred: 4.53 kB (18.59 kB size)
- Referrer Policy: strict-origin-when-cross-origin
- Request Priority: Highest
- DNS Resolution: System
- Response Headers (395 B):
  - Cache-Control: must-revalidate, no-cache, no-store, private
  - Connection: Keep-Alive
  - Content-Length: 398
  - Content-Type: text/html; charset=UTF-8



Then i checked the Request section where i got the content.

The screenshot shows a web browser window with the URL [www.seed-server.com/thewire/all](http://www.seed-server.com/thewire/all). The page displays a post by a user named 'Samy' with the text 'hi, i am samy!'. Below the post, there are links for 'RSS', 'Bookmark this page', and 'Report this', and a note 'Powered by Elgg'. The browser's developer tools are open, showing the 'Network' tab. The list of requests includes a POST request to 'add' and several GET requests for various JavaScript files. The 'Request' tab for the first POST request is selected, showing the request payload. The payload is a form data object with two fields: 'elgg\_token' and 'elgg\_ts'. The 'elgg\_token' field contains a long alphanumeric string, and the 'elgg\_ts' field contains a timestamp. The 'body' field contains the text 'hi, i am samy!'.

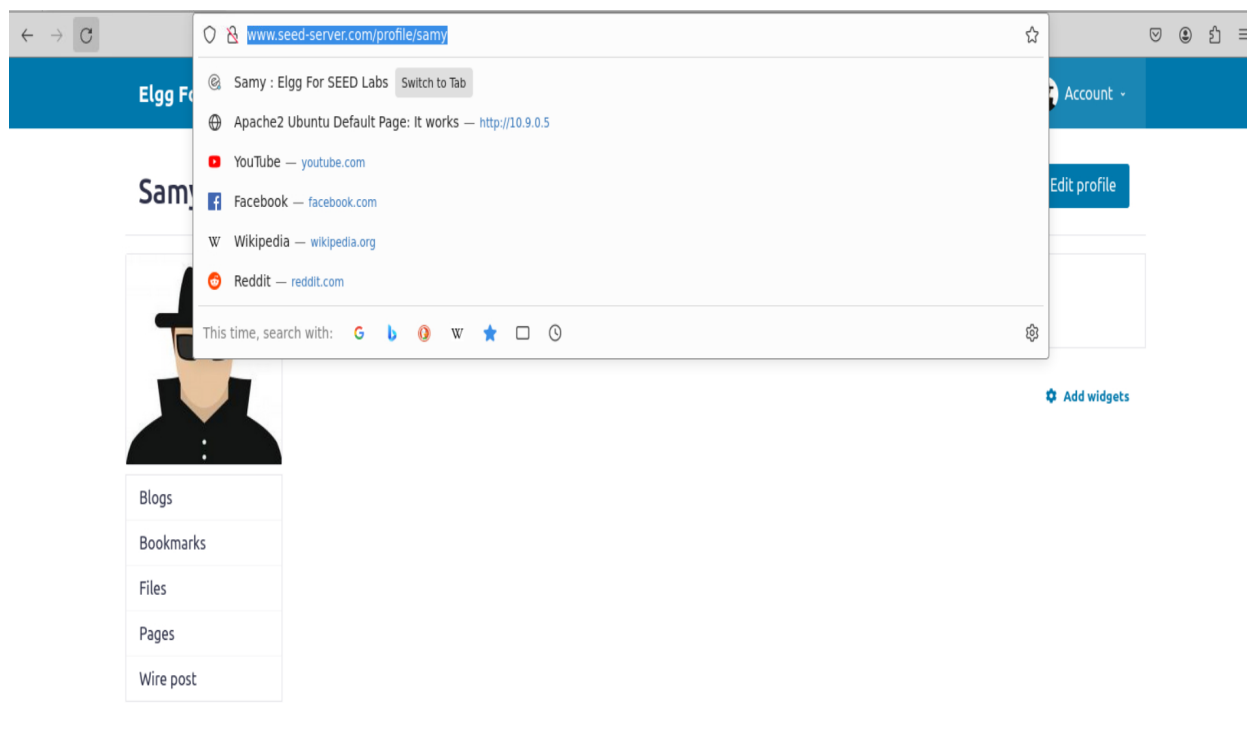
Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings
302	POST	www.seed-server...	add	document	html	4.53 kB	18.59 kB					
200	GET	www.seed-server...	all	document	html	4.58 kB	0 B					
200	GET	www.seed-server...	jquery.js	script	js	cached	0 B					
200	GET	www.seed-server...	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...	init.js	require.js:127 (script)	js	cached	370 B					

Request payload

```
1 .....21704507314207349171922889401
2 Content-Disposition: form-data; name="__elgg_token"
3 .....
4 rbWUXqrcQLSKj0QB9AR4pg
5 .....21704507314207349171922889401
6 Content-Disposition: form-data; name="__elgg_ts"
7 .....
8 1707926755
9 .....21704507314207349171922889401
10 Content-Disposition: form-data; name="body"
11 .....
12 hi, i am samy!
13 .....21704507314207349171922889401..
14 .....
```



Finally , i need the profile link of the samy profile . So , i copied the profile link of the samy shown in the picture.







## 4 Task 4

Here , i had to design a self propagating worm. The worm code can use DOM APIs to retrieve a copy of itself from the web page and an example of using DOM APIs has been provided with me in the XSSDemo.txt. So , first i copy the code to send a friend request to samy like task 1. Then i use the provided code with me to edit the victim's description. Finally i copy the code of task 3 to post the victim's profile in the wire.



thank you