

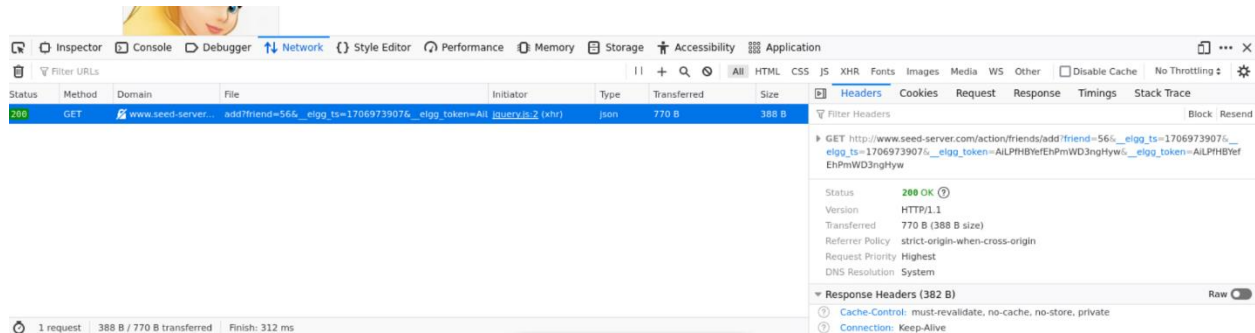
# Report on Offline 2 on XSS

## CSE 406 – Computer Security Sessional

### Roll : 1905014

#### Task -1:

To become the victim's friend, the url for adding a friend was to be determined. I did this by examining the GET request that is sent when a user adds someone as a friend.



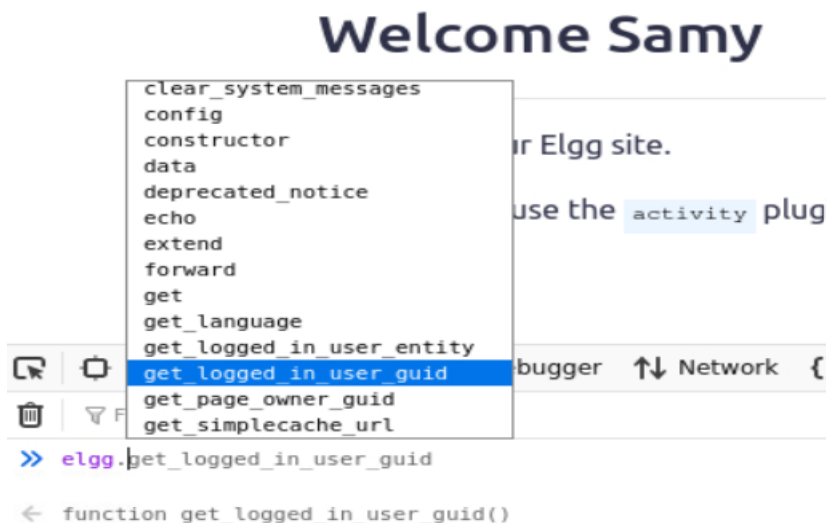
I had to determine the id number of Samy's profile. When the "View Page Source" of Samy's starting page is clicked, the guid and other information is found at the bottom of the page:

```

57     return false;
58 };
59 }
60
61 var elgg = {"config":{"lastcache":1587931381,"viewtype":"default","simplecache_enabled":1,"current_language":"en"},"security":{"token":
{"_elgg_ts":1706973256,"_elgg_token":"KRJ4ce0_pbctu0qAlw44Sg"}}, "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":"2020-04-
\\profile\\samy","name":"Samy","username":"samy","language":"en","admin":false,"token":"ZViKRdTHbCeVHjWCWEYhee"},"_data":{}}};
62 </script><script src="http://www.seed-server.com/cache/1587931381/default/jquery.js"></script><script src="http://www.seed-server.com/cache/158
src="http://www.seed-server.com/cache/1587931381/default/elgg/require_config.js"></script><script src="http://www.seed-server.com/cache/1587931
server.com/cache/1587931381/default/elgg.js"></script><script>
63 require([
64     "page/elements/topbar",
65     "input/form",
66     "elgg/reportedcontent"
67 ]);
68 </script>

```

There are also the elgg functions found through Console tab of “Inspect” which are used to determine the current (logged in) user’s name, username, guid, profile url etc.



## Task – 2:

For task 2, at first the input format of the fields are determined by adding random input to the fields in Samy's profile:

Public

Contact email

a

Please enter an email address.

Telephone

Public

Website

a

Please enter a URL.

The url for editing profile, request body of the change along with access code and the user's name were found by simply examining the POST request in the Network tab of "Inspect".

Status	Method	Domain	File	Initiator	Type	Transferred	S...	Headers	Cookies	Request	Response	Timings
302	POST	www.seed-server.com	edit	document	html	3.83 kB	1...	POST http://www.seed-server.com/action/profile/edit				
200	GET	www.seed-server.com	samy	document	html	3.83 kB	1...	Status 302 Found				
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	8...	Version HTTP/1.1				
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B	Transferred 3.83 kB (15.66 kB size)				
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B	Referrer Policy strict-origin-when-cross-origin				
200	GET	www.seed-server.com	require_config.js	script	js	cached	7...	Request Priority Highest				
200	GET	www.seed-server.com	require.js	script	js	cached	0 B	DNS Resolution System				
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B					
200	GET	www.seed-server.com	favicon-128.png	img	png	cached	4...	Response Headers (396 B)				
200	GET	www.seed-server.com	favicon.svg	img	svg	cached	6...	Cache-Control: must-revalidate, no-cache, no-store, private				
200	GET	www.seed-server.com	sprintf.js	script	js	cached	0 B	Connection: Keep-Alive				
200	GET	www.seed-server.com	en.js	script	js	cached	0 B	Content-Length: 402				
200	GET	www.seed-server.com	weakmap-polyfill.js	script	js	cached	0 B	Content-Type: text/html; charset=UTF-8				
200	GET	www.seed-server.com	formdata-polyfill.js	script	js	cached	0 B	Date: Sat, 03 Feb 2024 15:49:56 GMT				
200	GET	www.seed-server.com	widgets.js	script	js	cached	0 B	expires: Thu, 19 Nov 1981 08:52:00 GMT				
200	GET	www.seed-server.com	init.js	script	js	cached	9...	Keep-Alive: timeout=5, max=100				
								Location: http://www.seed-server.com/profile/samy				
								pragma: no-cache				

Status	Method	Domain	File	Initiator	Type	Transferred	S...
200	GET	www.seed-server.com	topbar.js	require.js:127	js	cached	1...
200	GET	www.seed-server.com	sprintf.js	require.js:127	js	cached	0 B
200	GET	www.seed-server.com	spinner.js	require.js:127	js	cached	7...
200	GET	www.seed-server.com	samy	document	html	4.23 kB	1...
200	GET	www.seed-server.com	require_config.js	script	js	cached	7...
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	reportedcontent.js	require.js:127	js	cached	0 B
200	GET	www.seed-server.com	ready.js	require.js:127	js	cached	1...
200	GET	www.seed-server.com	Plugin.js	require.js:127	js	cached	1...
200	GET	www.seed-server.com	lightbox.js	require.js:127	js	cached	0 B
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery.colorbox.js	require.js:127	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js:127	js	cached	3...
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127	js	cached	0 B
200	GET	www.seed-server.com	form.js	require.js:127	js	cached	1...
200	GET	www.seed-server.com	favicon.svg	FaviconLoader.sys...	svg	cached	6...
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.sys...	png	cached	4...
200	GET	www.seed-server.com	en.js	require.js:127	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
502	POST	www.seed-server.com	edit	document	html	4.19 kB	1...
200	GET	www.seed-server.com	Ajax.js	require.js:127	js	cached	0 B
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4...

25 requests | 55.87 kB / 8.42 kB transferred | Finish: 1.83 s | DOMContentLoaded: 1.29 s | load: 1.29 s

The user's name was determined by the elgg function to obtain logged in user's entity.

```

>> elgg.get_logged_in_user_entity()
← Object { guid: 59, type: "user", subtype: "user", owner_guid: 59, container_guid: 0, time_created: "2020-04-26T15:23:51-04:00", time_updated: "2024-02-04T09:30:30-05:00", url: "http://www.seed-server.com/profile/samy", name: "Samy", username: "samy", ... }
  admin: false
  container_guid: 0
  guid: 59
  language: "en"
  name: "Samy"
  owner_guid: 59
  subtype: "user"
  time_created: "2020-04-26T15:23:51-04:00"
  time_updated: "2024-02-04T09:30:30-05:00"
  type: "user"
  url: "http://www.seed-server.com/profile/samy"
  username: "samy"
  <prototype>: Object { constructor: ElggUser(a) {}, isAdmin: isAdmin() {} }

>> elgg.get_logged_in_user_entity().url
← "http://www.seed-server.com/profile/samy"
>>

```

## Task – 3:

Here, the url for posting on the wire and its request body was to be determined. This was done by again examining the POST request in the Network tab of “Inspect”.

Wire posts

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	S...	Headers	Cookies	Request	Response	Timings
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.sys...	png	cached	4...	Filter Headers				Block Resend
200	GET	www.seed-server.com	favicon.svg	FaviconLoader.sys...	svg	cached	6...					
200	GET	www.seed-server.com	sprint.js	require.js 127 (scri...	js	cached	0 B			POST http://www.seed-server.com/action/thewire/add		
200	GET	www.seed-server.com	en.js	require.js 127 (scri...	js	cached	0 B	Status: 302 Found				
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js 127 (scri...	js	cached	0 B	Version: HTTP/1.1				
200	GET	www.seed-server.com	formdata-polyfill.js	require.js 127 (scri...	js	cached	0 B	Transferred: 4.52 kB (18.57 kB size)				
200	GET	www.seed-server.com	init.js	require.js 127 (scri...	js	cached	3...	Referrer Policy: strict-origin-when-cross-origin				
200	GET	www.seed-server.com	ready.js	require.js 127 (scri...	js	cached	1...	Request Priority: Highest				
200	GET	www.seed-server.com	lightbox.js	require.js 127 (scri...	js	cached	0 B	DNS Resolution: System				
200	GET	www.seed-server.com	thewire.js	require.js 127 (scri...	js	cached	1...	Response Headers (395 B)				Raw
200	GET	www.seed-server.com	form.js	require.js 127 (scri...	js	cached	1...	Cache-Control: must-revalidate, no-cache, no-store, private				
200	GET	www.seed-server.com	dropdown.js	require.js 127 (scri...	js	cached	1...	Connection: Keep-Alive				
200	GET	www.seed-server.com	likes.js	require.js 127 (scri...	js	932 B	1...	Content-Length: 398				
200	GET	www.seed-server.com	topbar.js	require.js 127 (scri...	js	884 B	1...	Content-Type: text/html; charset=UTF-8				
200	GET	www.seed-server.com	reportedcontent.js	require.js 127 (scri...	js	cached	1...	Date: Sat, 03 Feb 2024 15:48:05 GMT				
200	GET	www.seed-server.com	Plugin.js	require.js 127 (scri...	js	cached	1...	expires: Thu, 19 Nov 1981 08:52:00 GMT				
200	GET	www.seed-server.com	jquery.colorbox.js	require.js 127 (scri...	js	cached	0 B	Keep-Alive: timeout=5, max=100				
200	GET	www.seed-server.com	Ajax.js	require.js 127 (scri...	js	cached	0 B	Location: http://www.seed-server.com/thewire/all				
200	GET	www.seed-server.com	spinner.js	require.js 127 (scri...	js	cached	7...	pragma: no-cache				

26 requests 55.39 kB / 10.91 kB transferred Finish: 1.29 s DOMContentLoaded: 934 ms load: 948 ms

Request Headers (620 B)

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Wire posts

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

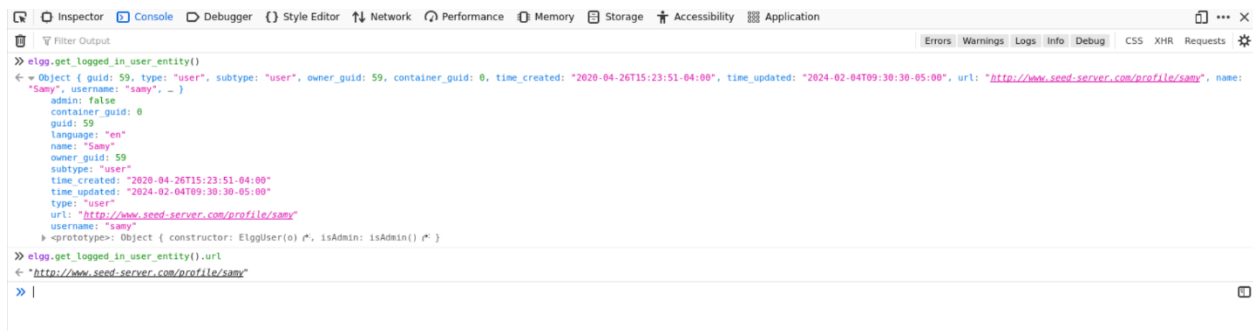
Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	S...	Headers	Cookies	Request	Response	Timings
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.sys...	png	cached	4...	Filter Request Parameters				
200	GET	www.seed-server.com	favicon.svg	FaviconLoader.sys...	svg	cached	6...					
200	GET	www.seed-server.com	sprint.js	require.js 127 (scri...	js	cached	0 B	Request payload				
200	GET	www.seed-server.com	en.js	require.js 127 (scri...	js	cached	0 B	1 .....-25086862441497857554189949151				
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js 127 (scri...	js	cached	0 B	2 Content-Disposition: form-data; name="__elgg_token"				
200	GET	www.seed-server.com	formdata-polyfill.js	require.js 127 (scri...	js	cached	0 B	3 w1o1WR0q3Hrch29Jj6GwA				
200	GET	www.seed-server.com	init.js	require.js 127 (scri...	js	cached	0 B	4 .....-25086862441497857554189949151				
200	GET	www.seed-server.com	ready.js	require.js 127 (scri...	js	cached	3...	5 Content-Disposition: form-data; name="__elgg_ts"				
200	GET	www.seed-server.com	lightbox.js	require.js 127 (scri...	js	cached	1...	6 1786975236				
200	GET	www.seed-server.com	thewire.js	require.js 127 (scri...	js	cached	1...	7 .....-25086862441497857554189949151				
200	GET	www.seed-server.com	form.js	require.js 127 (scri...	js	cached	1...	8 Content-Disposition: form-data; name="body"				
200	GET	www.seed-server.com	dropdown.js	require.js 127 (scri...	js	932 B	1...	9 abc				
200	GET	www.seed-server.com	likes.js	require.js 127 (scri...	js	884 B	1...	10 .....-25086862441497857554189949151...				
200	GET	www.seed-server.com	topbar.js	require.js 127 (scri...	js	cached	1...	11				
200	GET	www.seed-server.com	reportedcontent.js	require.js 127 (scri...	js	cached	0 B	12				
200	GET	www.seed-server.com	Plugin.js	require.js 127 (scri...	js	cached	1...	13				
200	GET	www.seed-server.com	jquery.colorbox.js	require.js 127 (scri...	js	cached	0 B	14				
200	GET	www.seed-server.com	Ajax.js	require.js 127 (scri...	js	cached	0 B					
200	GET	www.seed-server.com	spinner.js	require.js 127 (scri...	js	cached	7...					

26 requests 55.39 kB / 10.91 kB transferred Finish: 1.29 s DOMContentLoaded: 934 ms load: 948 ms

## Task – 4:

Task 4 is a combination of all the previous tasks. Here, the wormcode needs to be propagated with DOM API, whose code was already provided. The difference is that instead of Samy's profile for task 3, the infected user had to link their own profile in The Wire post. The url of a person's profile is determined through the elgg function to get the user's entity and url.



```
<> Inspector Console Debugger {} Style Editor ⚡ Network ⚙ Performance 🧠 Memory 🗄 Storage 🦿 Accessibility 🖨 Application ⌵ ... ✕
⌵ Filter Output Errors Warnings Logs Info Debug CSS XHR Requests ⚙
>> elgg.get_logged_in_user_entity()
← ◀ Object { guid: 59, type: "user", subtype: "user", owner_guid: 59, container_guid: 0, time_created: "2020-04-26T15:23:51-04:00", time_updated: "2024-02-04T09:30:30-05:00", url: "http://www.seed-server.com/profile/samy", name: "Samy", username: "samy", ... }
  admin: false
  container_guid: 0
  guid: 59
  language: "en"
  name: "Samy"
  owner_guid: 59
  subtype: "user"
  time_created: "2020-04-26T15:23:51-04:00"
  time_updated: "2024-02-04T09:30:30-05:00"
  type: "user"
  url: "http://www.seed-server.com/profile/samy"
  username: "samy"
  ▶ <prototype>: Object { constructor: ElggUser(a) ⚙, isAdmin: isAdmin() ⚙ }
>> elgg.get_logged_in_user_entity().url
← ◀ "http://www.seed-server.com/profile/samy"
>> |
```