

CSE406
Assignment 2
Cross-Site Scripting (XSS) Attack

Report

Prepared by: Wasif Jalal (1905084)

Clarifications:

I have used the native fetch() of Javascript instead of Ajax. The exact fetch() code can be very easily be obtained from right clicking the request in Firefox Developer Tools' Network Analysis tab.

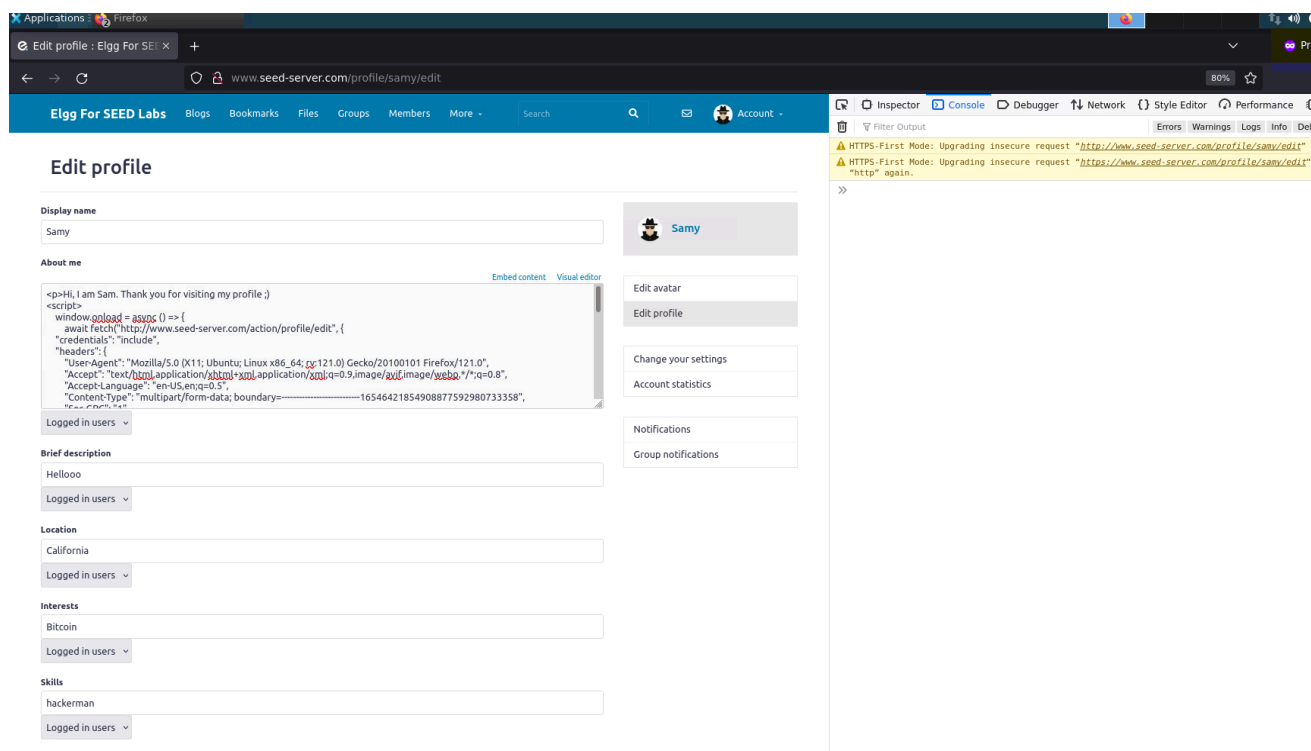
Task 1:

I could identify the following parameters:

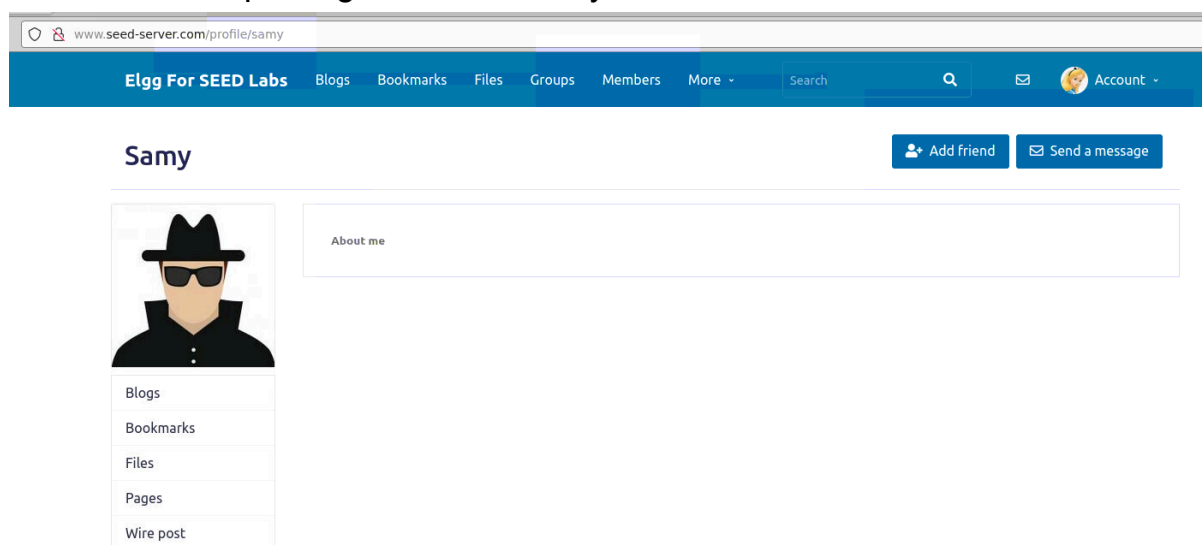
- User GUID
- User security token
- User security ts

They could be found in the elgg.security object. The elgg.session object also contained some very useful variables.

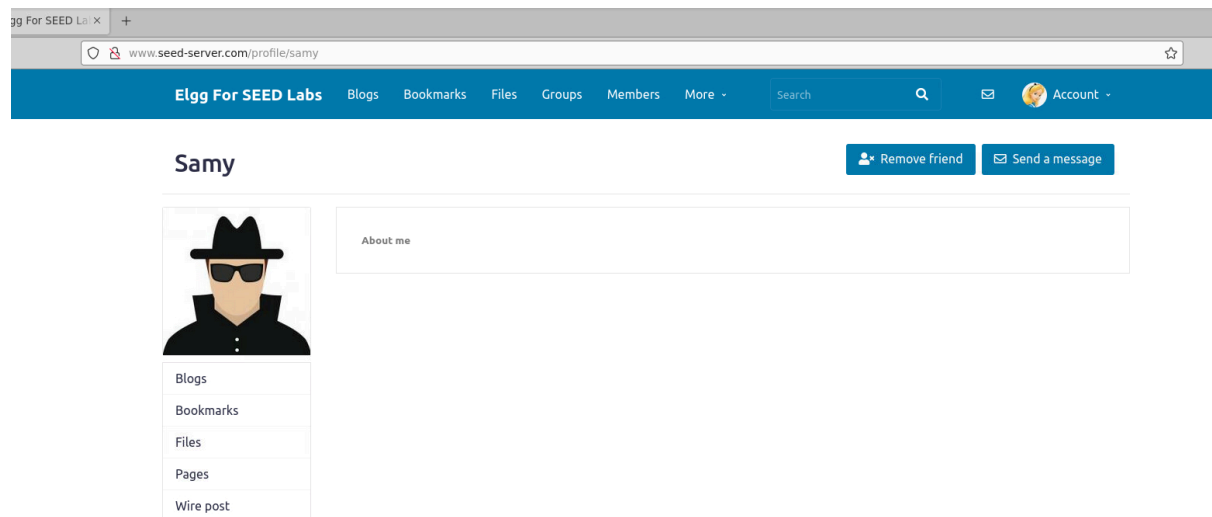
I substituted those variables into the fetch() call and updated Samy's profile with the <script/>



Then, an unsuspecting Alice could only see this:

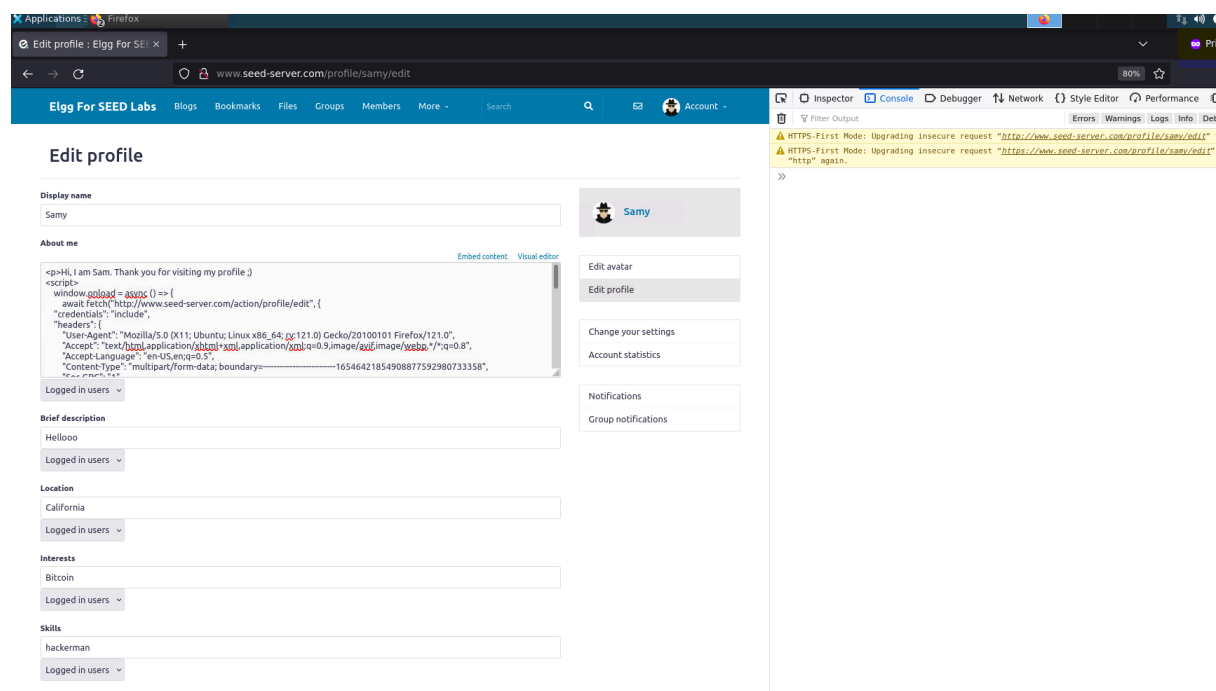


But upon reloading it is observed that Samy is her friend now:



Task-2

I updated Samy's profile in a way similar to the task, and captured the post request's fetch() code from the network tab. Substituted the 3 variables previously mentioned (GUID, token, ts).



Then again Alice could only see this in Samy's profile:

Samy

[Remove friend](#)[Send a message](#)[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

Brief description
Hellooo

Location
[California](#)

Interests
[Bitcoin](#)

Skills
[hackerman](#)

Contact email
samy@samy1234.com

Telephone
[911](#)

Mobile phone
[5551234567](#)

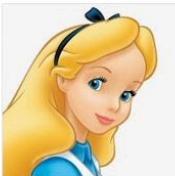
Website
<http://www.samy1234.com>

Twitter username
[samyX](#)

But her own profile had been edited

[Elgg For SEED Labs](#)[Blogs](#)[Bookmarks](#)[Files](#)[Groups](#)[Members](#)[More ▾](#)[Search](#)[Account ▾](#)

Alice

[Edit avatar](#)[Edit profile](#)[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

Brief description
Hellooo

Location
[California](#)

Interests
[Bitcoin](#)

Skills
[hackerman](#)

Contact email
samy@samy1234.com

Telephone
[911](#)

Mobile phone
[5551234567](#)

Website
<http://www.samy1234.com>

Twitter username
[samyX](#)

About me
[1905084](#)

Task 3

Elgg For SEED Labs

BlogsBookmarksFilesGroupsMembersMore

Search

Account

Wire posts

All wire posts

AllMineFriends

What's happening?

Post

140 characters remaining

By **Samy** 9 minutes ago

It's a really nice day, isn't it?

InspectorConsoleDebuggerNetworkStyle EditorPerformanceMemory

Filter URLs

Filter Request Parameters

St	M	Do...	File	Int...	%	tra...	S
38	OK	...	add	de...	no	4	1
39	OK	...	all	ob...	no	4	1
40	OK	...	jquery.js	scr...	js	ca...	0
41	OK	...	jquery-ui.js	scr...	js	ca...	0
42	OK	...	require_config.js	scr...	js	ca...	76
43	OK	...	require.js	scr...	js	ca...	0
44	OK	...	elgg.js	scr...	js	ca...	0
45	OK	...	sprintf.js	de...	js	ca...	0
46	OK	...	en.js	de...	js	ca...	0
47	OK	...	weekmap-polyfill	de...	js	ca...	0
48	OK	...	formdata-polyfill	de...	js	ca...	0
49	OK	...	init.js	de...	js	ca...	37
50	OK	...	ready.js	de...	js	ca...	12
51	OK	...	lightbox.js	de...	js	ca...	0
52	OK	...	thewire.js	de...	js	ca...	1
53	OK	...	form.js	de...	js	ca...	1
54	OK	...	dropdown.js	de...	js	93...	1
55	OK	...	likes.js	de...	js	88...	1
56	OK	...	topbar.js	de...	js	ca...	17
57	OK	...	reportviewcontent	de...	js	ca...	0
58	OK	...	Plugin.js	de...	js	ca...	14
59	OK	...	jquery.colorbox.js	de...	js	ca...	0
60	OK	...	Ajax.js	de...	js	ca...	0
61	OK	...	spinner.js	de...	js	ca...	75
62	OK	...	favicon-128.png	de...	pn	ca...	4
63	OK	...	favicon.svg	de...	sv	ca...	6

26 requests55.45 KB / 10.94 KB transfer

Elgg For SEED Labs

BlogsBookmarksFilesGroupsMembersMore

Search

Account

Wire posts

All wire posts

AllMineFriends

What's happening?

Post

140 characters remaining

By **Alice** just now

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

By **Samy** 9 minutes ago

It's a really nice day, isn't it?

Task 4:

Alice

[Edit avatar](#)[Edit profile](#)[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

Brief description
Hellooo

Location
[California](#)

Interests
[Bitcoin](#)

Skills
[hackerman](#)

Contact email
samy@samy1234.com

Telephone
[911](#)

Mobile phone
[5551234567](#)

Website
<http://www.samy1234.com>

Twitter username
[samyX](#)

About me
Hi I am Alice ;)


Wire posts

All wire posts

AllMineFriends



What's happening?


Post140 characters remaining



By [Alice](#) · just now



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


 



By [Alice](#) · just now



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


 



By [Alice](#) · 2 minutes ago



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


 



By [Alice](#) · 20 minutes ago



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



By [Samy](#) · 30 minutes ago

It's a really nice day, isn't it?


Wire posts

All wire posts

AllMineFriends



What's happening?


Post140 characters remaining



By [Alice](#) · just now



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


 



By [Alice](#) · just now



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


 



By [Alice](#) · 2 minutes ago



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


 



By [Alice](#) · 20 minutes ago

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



By [Samy](#) · 30 minutes ago

It's a really nice day, isn't it?

