

CSE 406 Assignment 2

Cross-Site Scripting (XSS)

Attack

ID:1905040

TASK 1

Becoming the Victim's Friend

At first, I logged into Samy's account and sent a friend request to Bobby. We have already opened inspect tab to check the status and link of our GET request.

Bobby

Remove friend

Send a message



Blogs

Bookmarks

Network | Style Editor | Performance | Memory | Storage | Accessibility | Application

File	Initiator	Type	Transferred	Size
add?friend=57%__elgg_ts=1707926551%__elgg_token=ROv_6t8ylsmfrpPZOcwEQ	jQuery.js:2 (xhr)	json	768 B	386 B

Headers | Cookies | Request | Response | Timings | Stack Trace

GET http://www.seed-server.com/action/friends/add?friend=57%__elgg_ts=1707926551%__elgg_token=ROv_6t8ylsmfrpPZOcwEQ

Status: 200 OK

Version: HTTP/1.1

Transferred: 768 B (386 B size)

TASK 1

Becoming the Victim's Friend

Then we checked the page source to find the guid of samy, which is 59. This is to prevent his friend request to himself.

These information are stored in elgg variable. We can also find the information needed for token and ts from here.

```
}  
  
var elgg = {"config":{"lastcache":1587931381,"viewtype":"default","simplecache_enabled":1,"current_language":"en"},"security":{"token":{"__elgg_ts":1707927544,"__elgg_token":"W03Ng6S0sJmyNqlfZxUVwA"}}, "session":{"user":{"guid":59,"type":"user","subtype":"user","ow  
</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><script src="http://www.seed-server.com/cache/1587931381/default/elgg/require_conf  
require([  
  "navigation/menu/elements/item_toggle",  
  "page/elements/topbar",  
  "input/form",  
  "elgg/reportedcontent"  
]);
```

TASK 2

Modifying the Victim's Profile

Again we will check how to edit profile using Samy's ID.

In inspect,we see 302 status in our POST request,in which if we check the header,we will find the link,which is www.seed-server.com/action/profile/edit

In Request tab, we can see the fields for which we have to change the values(e.g Logged in Users have a value 1)

The following images depict the above mentioned scenarios:

Changing Samy's ID values and checking the Headers' content for sending_url.

The screenshot shows a web browser with the address bar displaying `www.seed-server.com/profile/samy`. The page header is blue with the text "Elgg For SEED Labs" and navigation links: Blogs, Bookmarks, Files, Groups, Members, More. A search bar and an "Account" link are also present.

The main content area shows the profile of "Samy". It includes an avatar of a person wearing a black hat and sunglasses. To the right of the avatar, there is a "Brief description" section with the text "Meh", a "Location" section with the text "Guatemala", and an "Interests" section with the text "Talking to the moon". There are two buttons: "Edit avatar" and "Edit profile".

The bottom of the screenshot shows the Chrome DevTools Network tab. The "Network" panel is active, displaying a list of requests. The first request is a POST to `http://www.seed-server.com/action/profile/edit` with a status of 302. The "Headers" panel is expanded, showing the "Response Headers" for the 302 status. The headers include:

- Cache-Control: must-revalidate, no-cache, no-store, private
- Connection: Keep-Alive
- Content-Length: 402
- Content-Type: text/html; charset=UTF-8
- Date: Thu, 15 Feb 2024 07:32:19 GMT
- expires: Thu, 19 Nov 1981 08:52:00 GMT
- Keep-Alive: timeout=5, max=100

The "Network" panel also shows a list of requests with columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size. The requests are as follows:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	edit	document	html	4.57 kB	19.35 kB
200	GET	www.seed-server.com	samy	document	html	4.61 kB	19.35 kB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.57 kB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	require.js:127 (script)	js	cached	0 B

Field name, like "location", "accesslevel[location]" and their values found in Request Tab when we modified Samy's ID:

The screenshot shows a web browser's developer tools with the 'Request' tab selected. The 'Request payload' section displays a multipart/form-data request. The payload consists of several parts, each starting with a 'Content-Disposition: form-data; name=' header. The parts are: 'accesslevel[description]' with value '1', 'briefdescription' with value 'Meh', 'accesslevel[briefdescription]' with value '1', 'location' with value 'Guatemala', 'accesslevel[location]' with value '1', and 'interests' with value '1'. Each part is followed by a long string of dashes and a unique identifier.

Line	Content
37	Content-Disposition: form-data; name="accesslevel[description]"
38	
39	1
40	-----18630840322578346751950944685
41	Content-Disposition: form-data; name="briefdescription"
42	
43	Meh
44	-----18630840322578346751950944685
45	Content-Disposition: form-data; name="accesslevel[briefdescription]"
46	
47	1
48	-----18630840322578346751950944685
49	Content-Disposition: form-data; name="location"
50	
51	Guatemala
52	-----18630840322578346751950944685
53	Content-Disposition: form-data; name="accesslevel[location]"
54	
55	1
56	-----18630840322578346751950944685
57	Content-Disposition: form-data; name="interests"

The result is like this:

seed-server.com/profile/alice

Alice

Edit avatar

Edit profile



Blogs

Bookmarks

Files

Pages

Wire post

Brief description

Meh

Location

Gaza

Interests

Hacking

Skills

Nothing

Contact email

tobey@gmail.com

Telephone

123456789

Mobile phone

123456789

Website

http://ggwp.com

Twitter username

Point break

About me

Network Style Editor Performance Memory Storage Accessibility Application

|| + Q All HTML CSS JS XHR Fonts Images Media

TASK 3

Posting on the Wire on Behalf of the Victim

The screenshot shows the 'Headers' tab in a web browser's developer tools. The request is a POST to `www.seed-server.com/action/thewire/add` from the address `10.9.0.5:80`. The status is `302 Found`. The response headers are visible, including `Cache-Control: must-revalidate, no-cache, no-store, private`, `Connection: Keep-Alive`, `Content-Length: 402`, `Content-Type: text/html; charset=UTF-8`, `Date: Thu, 15 Feb 2024 08:43:47 GMT`, `expires: Thu, 19 Nov 1981 08:52:00 GMT`, `Keep-Alive: timeout=5, max=97`, and `Location: http://www.seed-server.com/profile/samy`.

JS XHR Fonts Images Media WS Other ☐ Disable Cache No Throttling ⚙

Headers Cookies Request Response Timings Stack Trace

Filter Headers Block Resend

POST

Scheme: http
Host: www.seed-server.com
Filename: /action/thewire/add

Address: 10.9.0.5:80

Status: 302 Found ⓘ
Version: HTTP/1.1
Transferred: 4.61 kB (19.41 kB size)
Referrer Policy: strict-origin-when-cross-origin
DNS Resolution: System

Response Headers (395 B) Raw

Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 402
Content-Type: text/html; charset=UTF-8
Date: Thu, 15 Feb 2024 08:43:47 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=97
Location: http://www.seed-server.com/profile/samy

The screenshot shows a web browser displaying a confirmation message: "Your message was successfully posted to the wire." The page title is "Elgg For SEED Lab" and the user name "Samy" is visible. There are two buttons: "Remove friend" and "Send a message".

JS XHR Fonts Images Media WS Other ☐ Disable Cache No Throttling ⚙

Headers Cookies Request Response Timings Stack Trace

HTML Raw

Elgg For SEED Lab

Your message was successfully posted to the wire.

Samy

Remove friend Send a message

Explanation of last slides' photos

As this is a POST request ,just like task 2, our procedure is completely same.We find the field name and set its value accordingly.

At first we will get the link from the Header as usual,and then modify the body field.

TASK 4

Design a Self-Propagating Worm

The work in this task comprises the tasks of other three files. So we are not adding the similar photos again.

The worm propagation code was provided in assignment resources, so we used that code snippet.

GET and POST requests being executed for the script.

Activities TigerVNC Viewer ১৫ ফেব ১৫ ২৩:৫৬ Overflow.2g0pslu01quevfmdwsgjylxc.zx.internal.cloudapp.net:1 (seed) - TigerVNC

Applications: Samy : Elgg For SEED La... seed@Overflow: ~/Docu... [Labsetup - File Manager]

Samy : Elgg For SEED La... +

www.seed-server.com/profile/samy

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

Samy

Remove friend Send a message

Brief description
Meh

Location
Guatemala

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	GET	www.seed-server.com	samy	document	html	5.01 kB	21.16 kB	83 ms
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B	0 ms
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B	0 ms
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B	0 ms
200	GET	www.seed-server.com	require.js	script	js	cached	0 B	0 ms
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B	0 ms
302	GET	www.seed-server.com	add?friend=59&_elgg_ts=1708019767&_elgg_ts=1708019767&_elgg_token=akdCHAZpaqR9P3hsq6IAQ6	samy:99 (xhr)	html	5 kB	21.33 kB	95 ms
302	POST	www.seed-server.com	edit	samy:107 (xhr)	html	4.98 kB	21.27 kB	1419 ms
302	POST	www.seed-server.com	add	samy:116 (xhr)	html	4.95 kB	21.16 kB	330 ms
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.seed-server.com	widgets.js	require.js:127 (script)	js	cached	0 B	0 ms
200	GET	www.seed-server.com	init.js	require.js:127 (script)	js	cached	370 B	0 ms
200	GET	www.seed-server.com	ready.js	require.js:127 (script)	js	cached	123 B	0 ms

30 requests 163.75 kB / 35.02 kB transferred Finish: 1.79 s DOMContentLoaded: 236 ms load: 239 ms

Samy has been added to the friend List after visiting Alice's ID who has been formerly attacked visiting Samy's ID. We can see his posts in friends tab here.

Friends' wire posts

All

Mine

Friends

What's happening?

Post

140 characters remaining



By Samy 9 hours ago

life is horrible



Charlie

Blogs

Bookmarks

Files

Pages

s/charlie


Debugger [Network](#) [Style Editor](#) [Performance](#) [Memory](#) [Storage](#) [Accessibility](#) [Application](#)

Wire-post addition after visiting Alice's account



AllMineFriends


What's happening?

Post140 characters remaining



By Charlie · 2 minutes ago

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



By Charlie · 3 minutes ago

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



BloggsBookmarksFilesPagesWire post


RSSBookmark this pageReport this


Powered by Elgg

DebuggerNetworkStyle EditorPerformanceMemoryStorageAccessibilityApplication

Time	Method	URL	File	Size	Cache	Time	Size
200	GET	www.seed-server.com/en.js	require.js.1.2.7 (script)	0 B	cached	0 ms	0 ms
200	GET	www.seed-server.com/webpack-polyfill.js	require.js.1.2.7 (script)	0 B	cached	0 ms	0 ms
200	GET	www.seed-server.com/formdata-polyfill.js	require.js.1.2.7 (script)	0 B	cached	0 ms	0 ms
200	GET	www.seed-server.com/widgets.js	require.js.1.2.7 (script)	0 B	cached	0 ms	0 ms
200	GET	www.seed-server.com/init.js	require.js.1.2.7 (script)	370 B	cached	0 ms	0 ms
200	GET	www.seed-server.com/ready.js	require.js.1.2.7 (script)	123 B	cached	0 ms	0 ms

30 requests163.75 kB / 35.02 kB transferredFinish: 1.79 sDOMContentLoaded: 236 msload: 239 ms





THANKS!