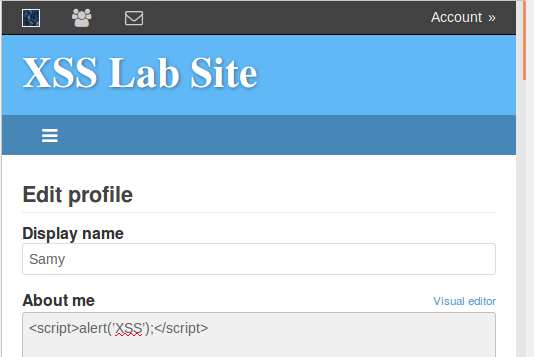
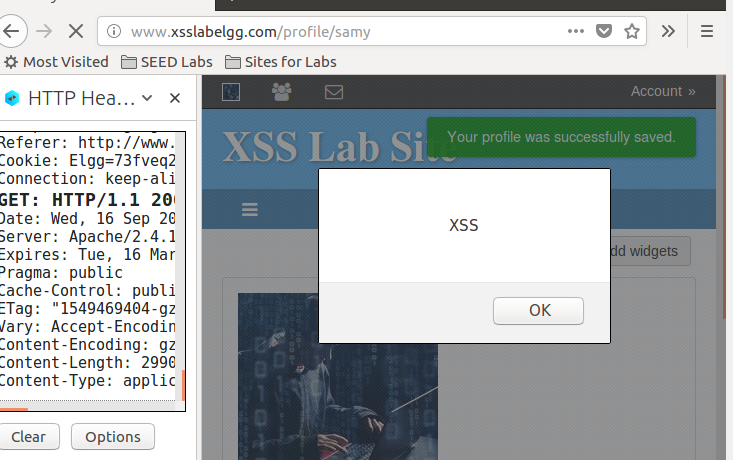
**Lab 5实验报告**

57118110 杨紫瑄

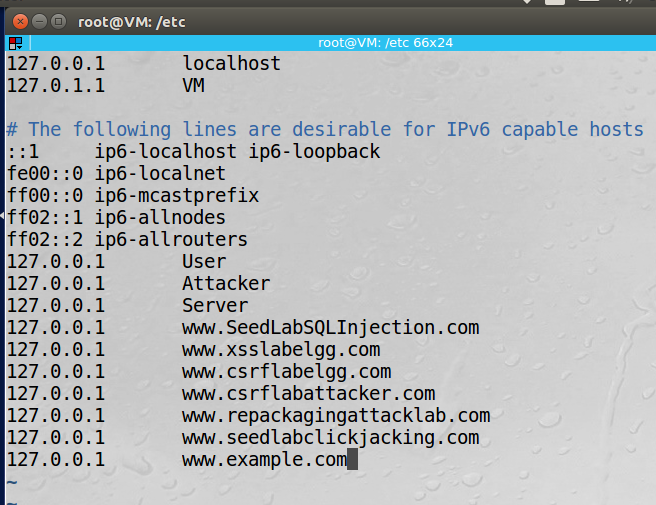
**Task1: Posting a Malicious Message to Display an Alert Window**



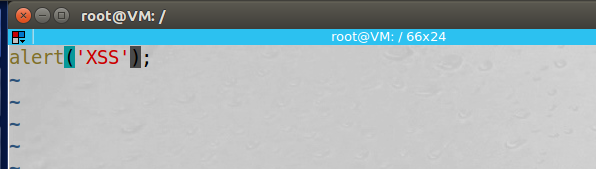
登录Samy的账号并在profile里写入代码



保存后成功跳出弹窗XSS



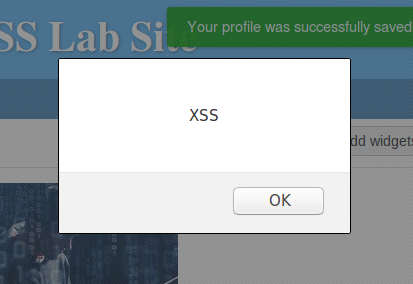
进入终端，在/etc/hosts文件里加入127.0.0.1 www.example.com



在/var/www/html中创建myscripts.js文件并写入代码alert(‘XSS’);

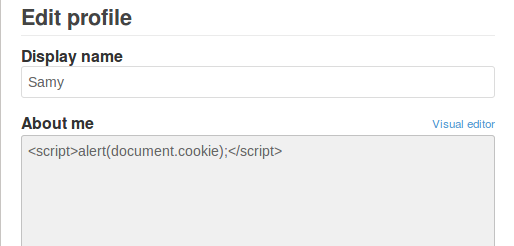


在Samy的profile中写入代码

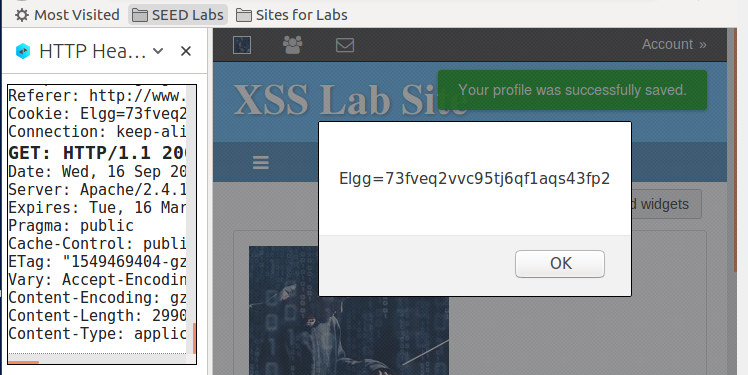


保存后成功弹出警告窗口

**Task2: Posting a Malicious Message to Display Cookies**



在Samy的profile里写入代码来获取cookies



保存后成功弹出获取到cookies的窗口

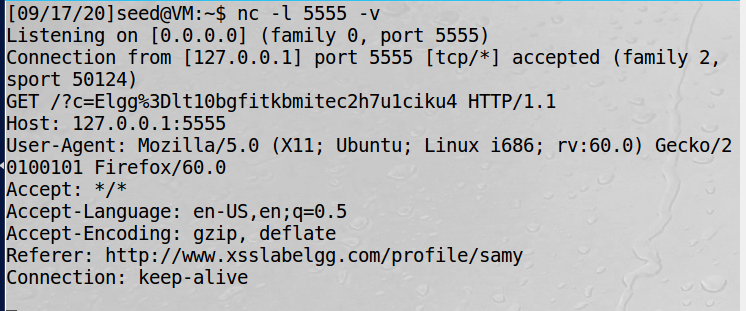
**Task 3: Stealing Cookies from the Victim’s Machine**



在Samy的profile中写入以下代码来监听获取cookies

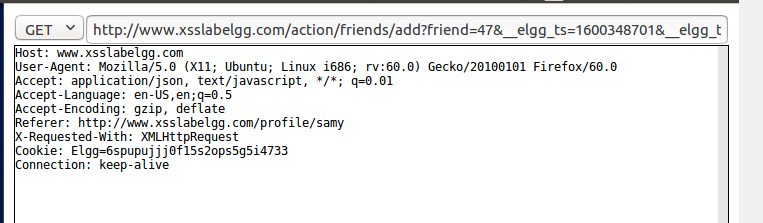


进入终端输入代码开始监听

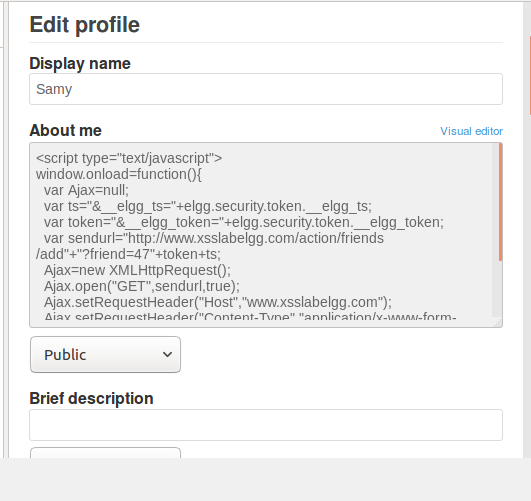


用Alice登录并打开Samy主页，Samy通过监听获取到对方的cookies

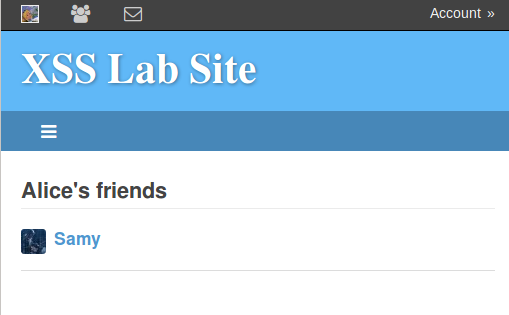
**Task 4: Becoming the Victim’s Friend**



先登录Boby账号并加Samy为好友，用HTTP Header Live抓包后获取guid



在Samy主页中写入代码并保存



登录Alice账号浏览Samy主页，发现自动成功加Samy为好友

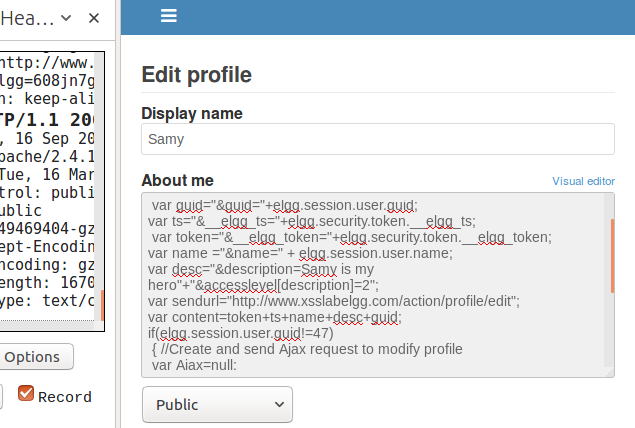
**问题1：Explain the purpose of Lines ① and ②, why are they are needed?**

答：1和2分别表示获得的时间戳和秘密令牌的值，因为所有Elgg请求都需要这两个值，只有有了这两个值才能够攻击成功。

**问题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?**

答：可以。可以用其他客户端来发送请求，达到攻击的效果，并不一定必须要使用浏览器。

**Task 5: Modifying the Victim’s Profifile**



在Samy的profile中写入代码并保存



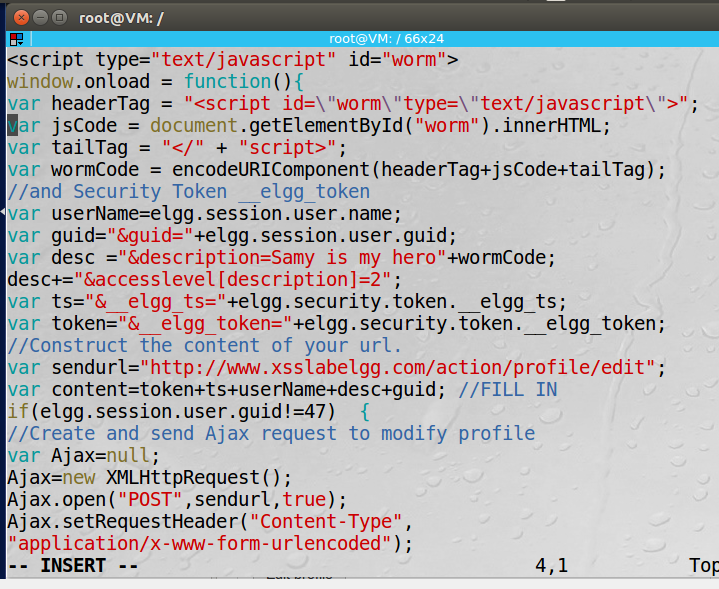
用Alice的账号访问Samy主页，发现Alice的主页被成功修改

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

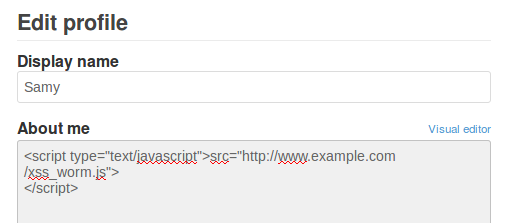
答：这一行代码是用来判断uid是否为Samy自己的uid,如果去掉这行，在保存完这段代码之后Samy的主页就会自动加上Samy is my hero

**Task 6: Writing a Self-Propagating XSS Worm**

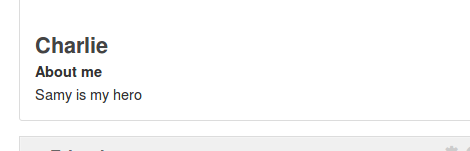
**链接：**



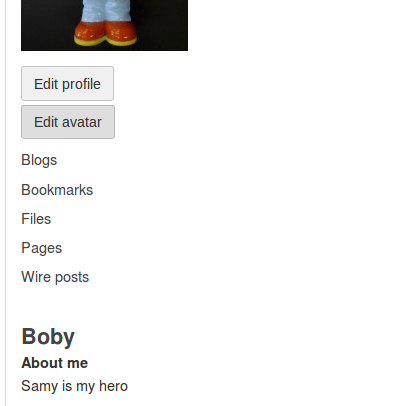
在/var/www/html中创建xxx\_worm.js文件并写入以上代码



在Samy的主页中写入代码调用xxs\_worm.js文件中的代码

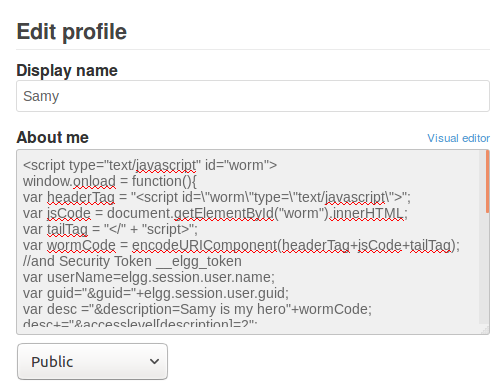


用Charlie的账号登录并访问Samy主页发现Charlie主页被成功修改

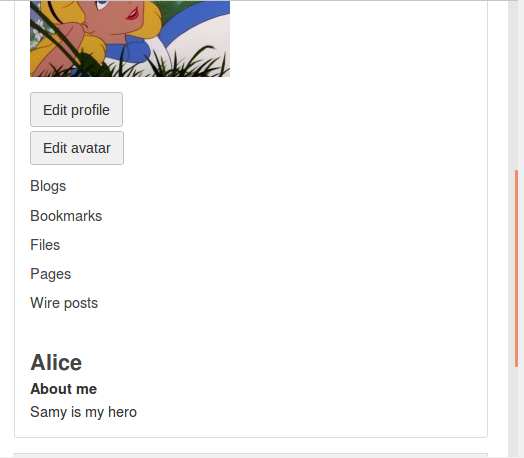


再登录Boby账号访问Charlie主页，发现Boby主页也被成功修改

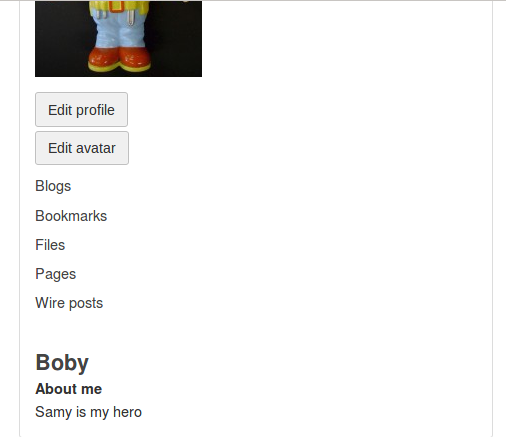
**DOM:**



在Samy的主页中写入以上代码

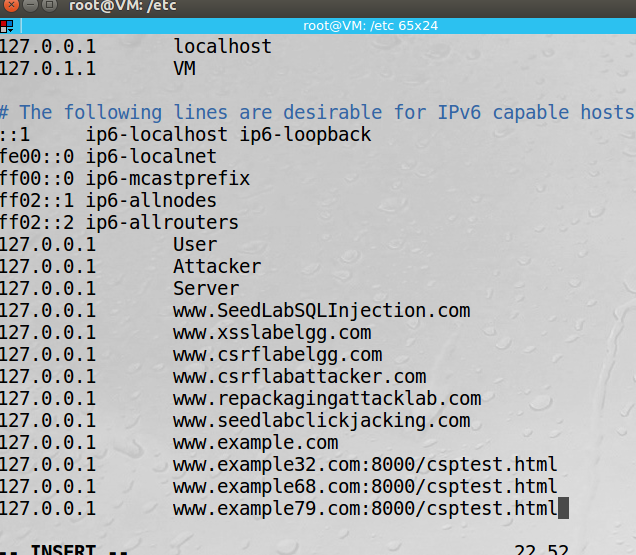


登录Alice账号并访问Samy主页发现Alice的主页被修改

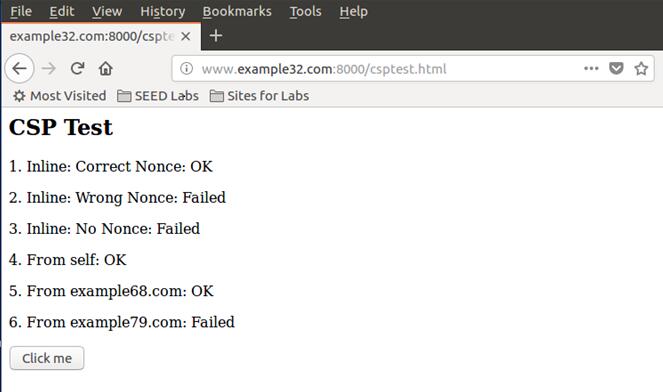
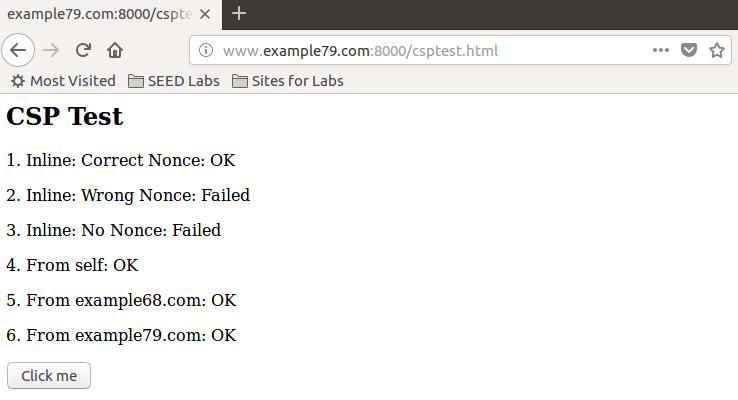
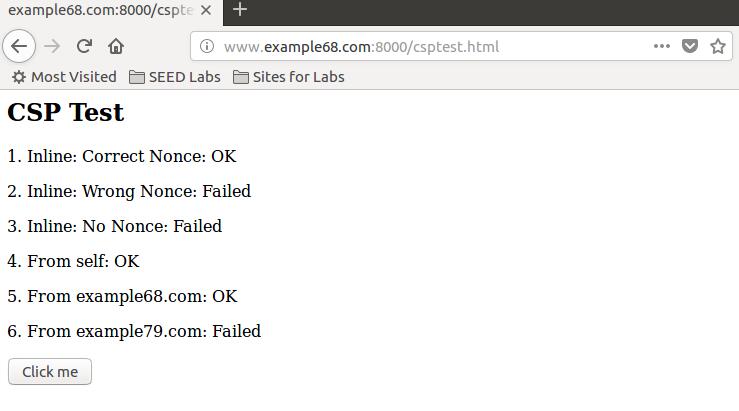


删除Boby主页中的信息后访问Alice主页，发现Boby主页也被成功修改

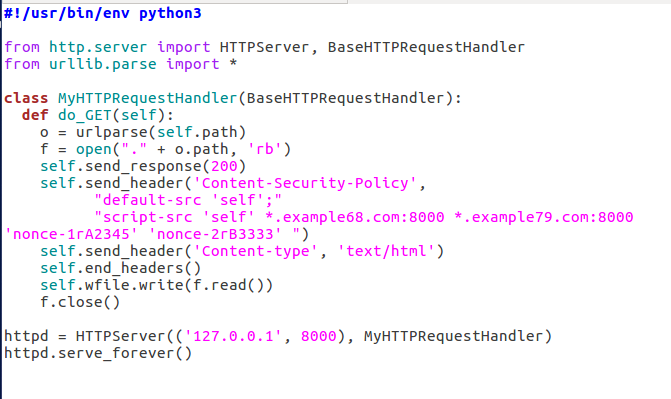
**Task 7: Defeating XSS Attacks Using CSP**



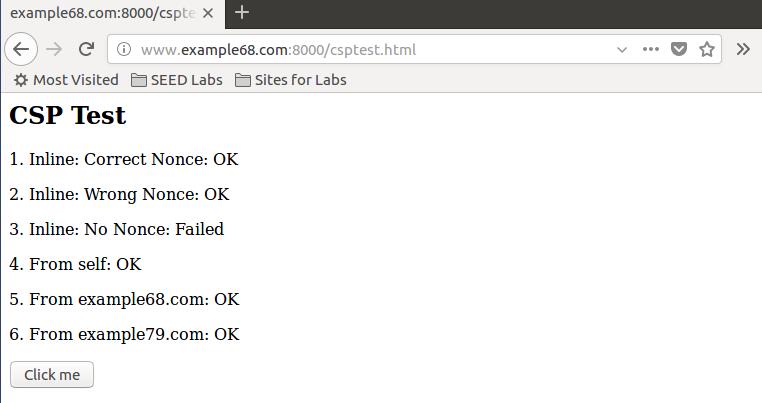
在/etc/hosts文件中添加三个网址

****

下载csp.zip，解压后运行http\_server.py并访问三个网址得到以上结果



修改http\_server.py文件后再次打开网页发现1,2,4,5,6成功全部显示OK



实验总结：此次试验和上次CSRF实验很相似，本次实验的主要对象XSS攻击会在网站数据中放入代码并可能会传染其他用户造成大规模的感染病毒遭受攻击的情况，通过学习这些攻击的方法，我们也能更好地学习到怎样阻止类似的攻击，对网络空间安全有重要的意义。