**Lab5-report**

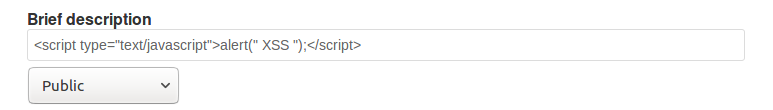
**57118132 吴嘉琪**

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

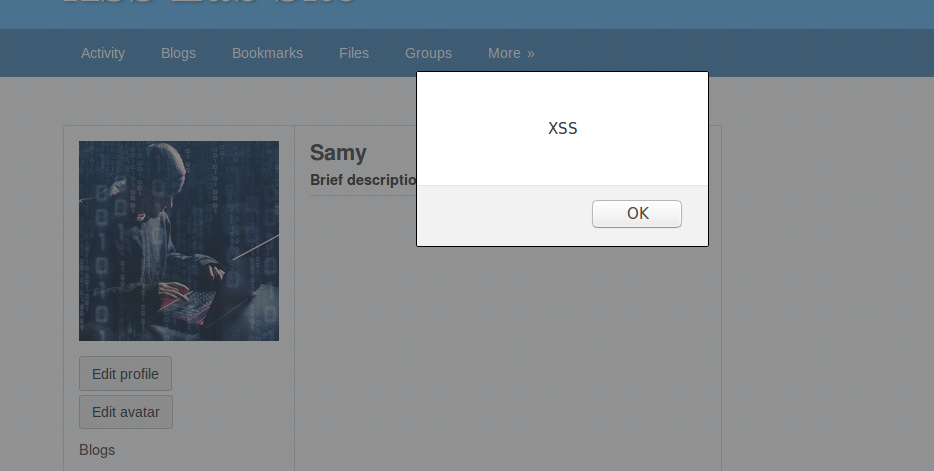
此任务的目标是在elgg配置文件中嵌入一个JavaScript程序，一遍当其他用户查看配置文件时，将执行该程序并显示出一个警告窗口。在本例中Javascript代码很短，可以在brief description字段中输入。

在Samy用户的brief description里面添加js脚本。

<script>alert(‘XSS’);</script>



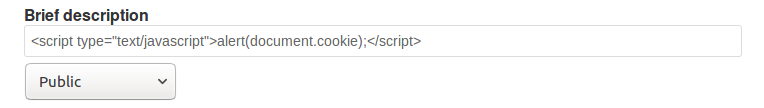
保存后，再次进入Samy的主页，会见到警告窗口弹出



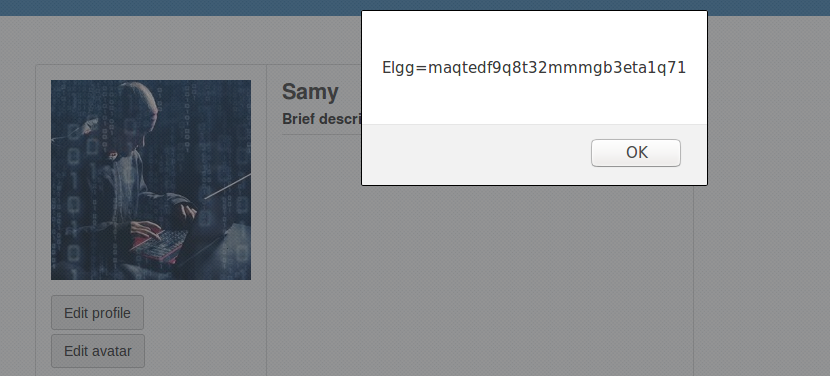
**Task2:** **Posting a Malicious Message to Display Cookies**

在Samy用户的brief description里面添加js脚本。

<script type="text/javascript">alert(document.cookie);</script>



保存后，再次进入Samy的主页，会见到警告窗口弹出

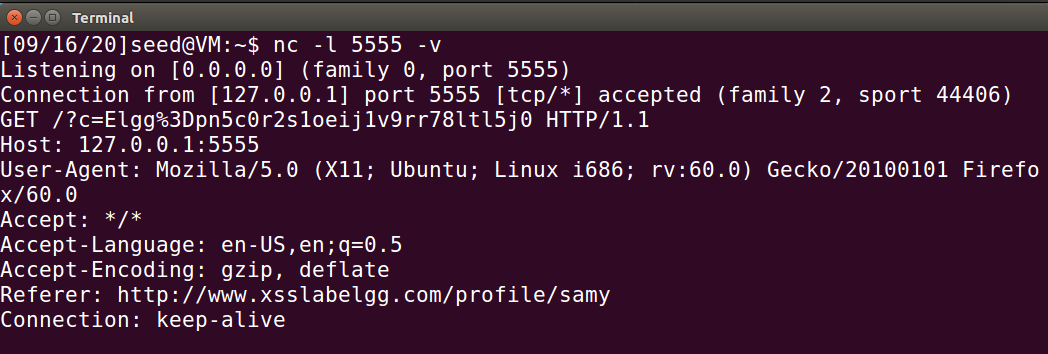


**Task3:** **Stealing Cookies from the Victim’s Machine**

在Samy用户的About me里面添加js脚本，向攻击者的服务器回传cookie



如下的操作显示了客户端浏览器回传的get请求。其中附带了Elgg网站的cookie

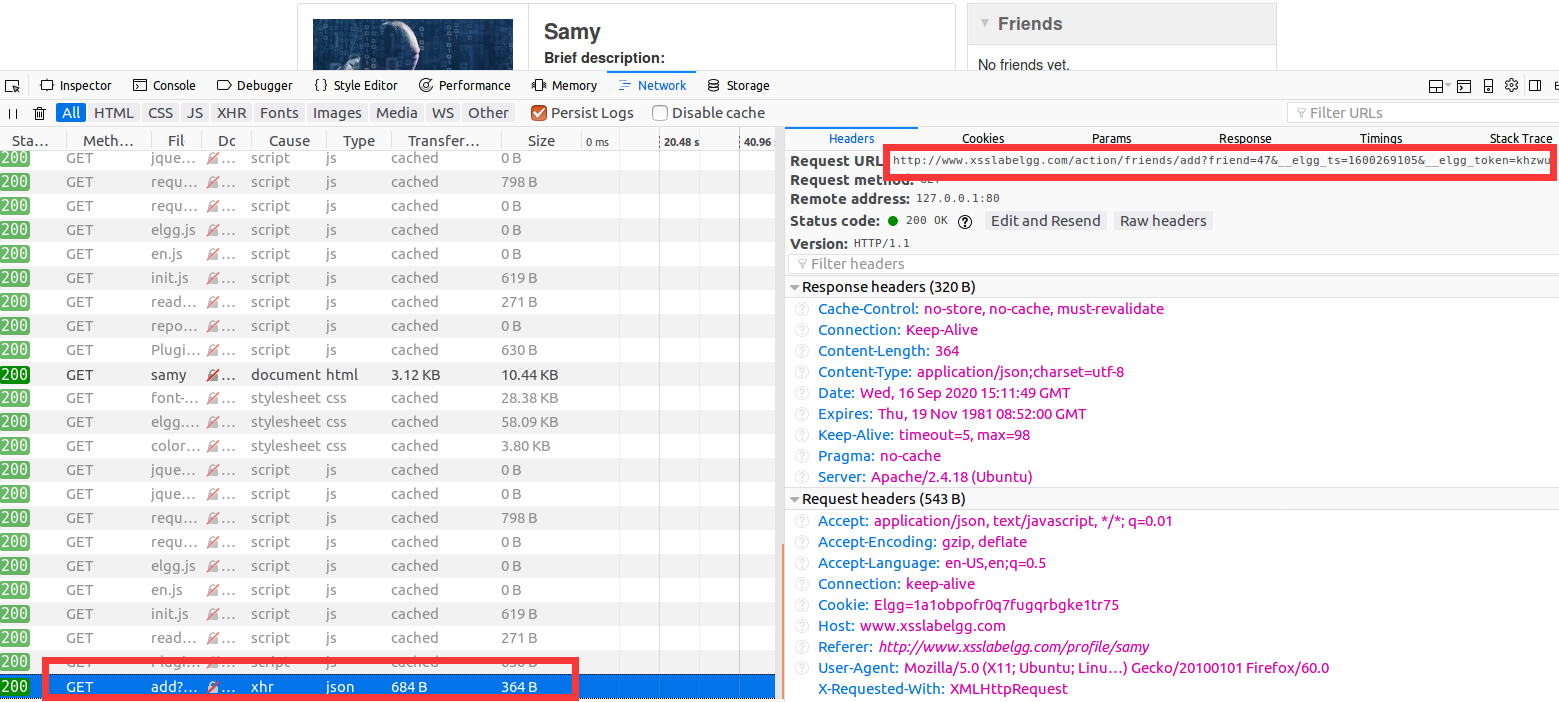


**Task4:** **Becoming the Victim’s Friend**

首先查看samy的guid

在Firefox中，打开tool->webconsole，选中all标签。

以charlie身份登录，添加samy为好友，可以看到一个addfriend的get 请求。

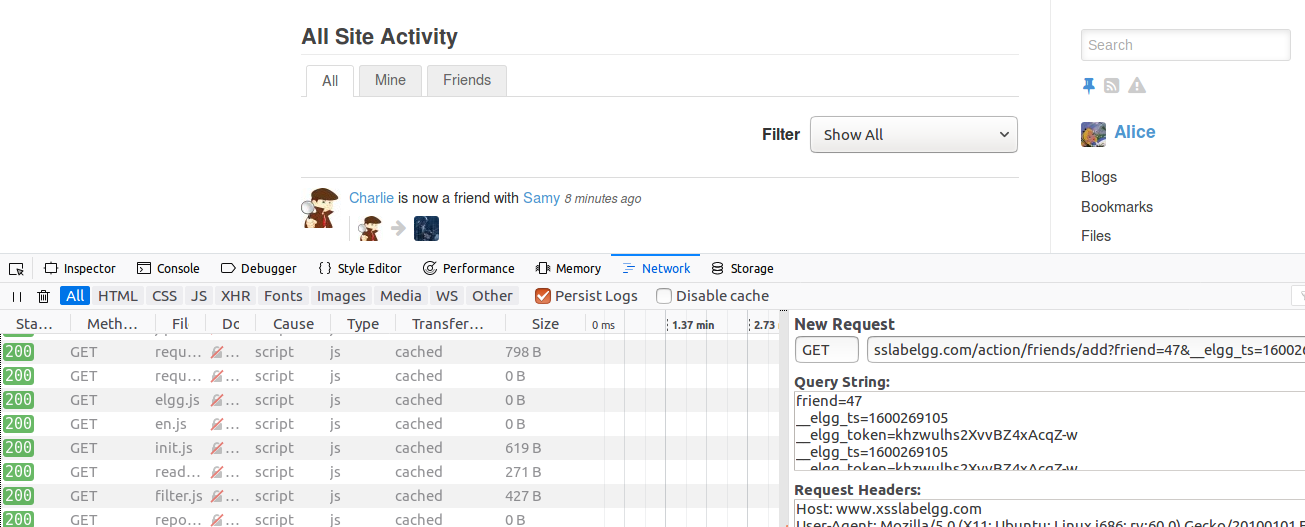


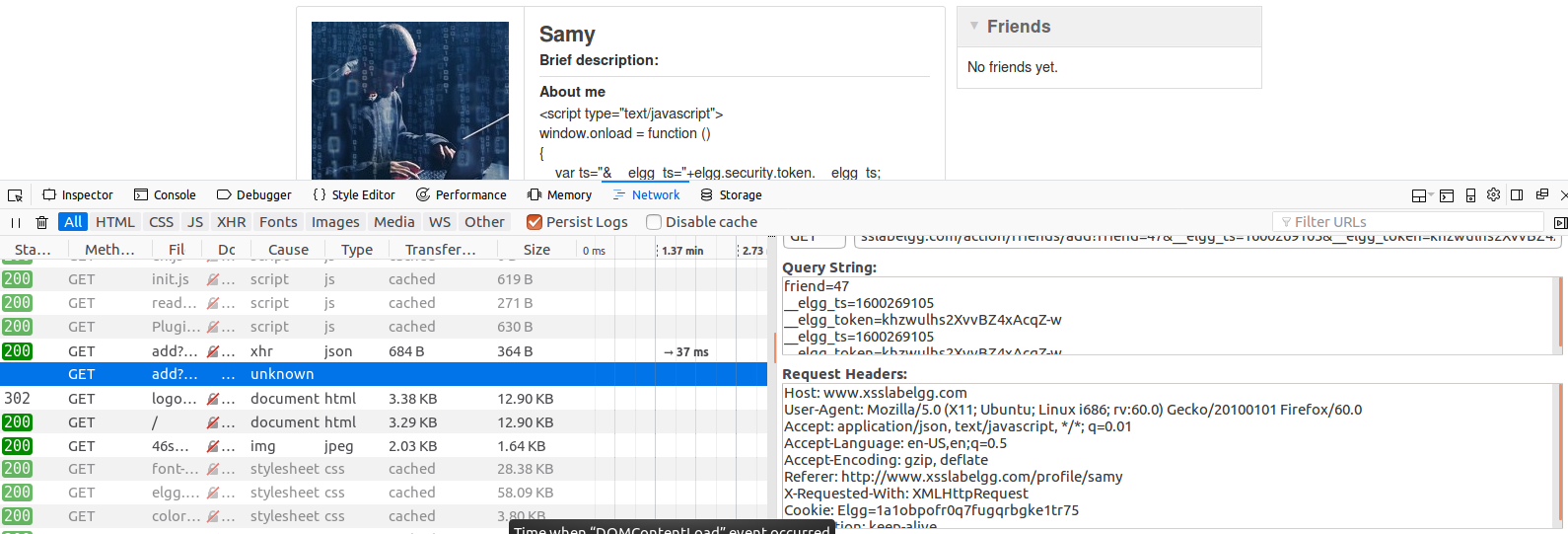
在右边的requesturl中可以看到friend是47

然后以samy登录，进入profile edit页面，在About me部分里面添加js脚本

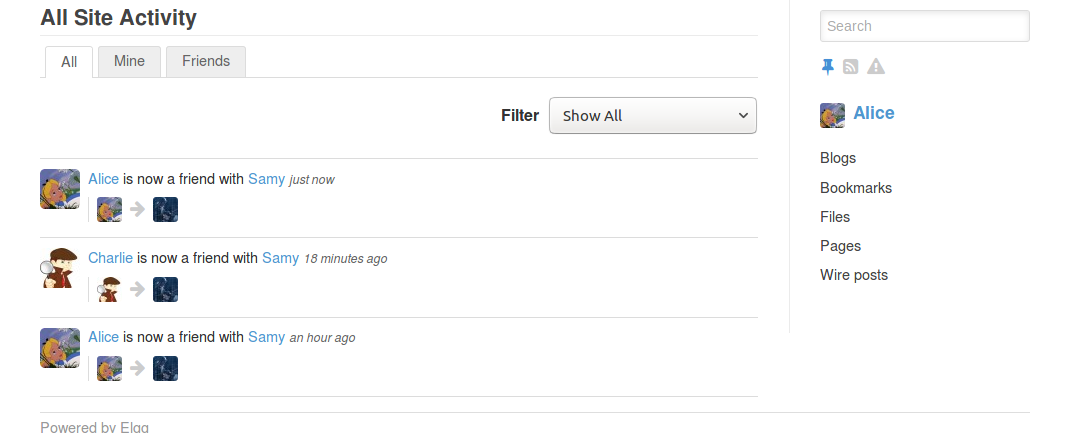
提交，再以alice登录，然后再查看samy的主页

可以看到发出了get请求，添加47作为好友





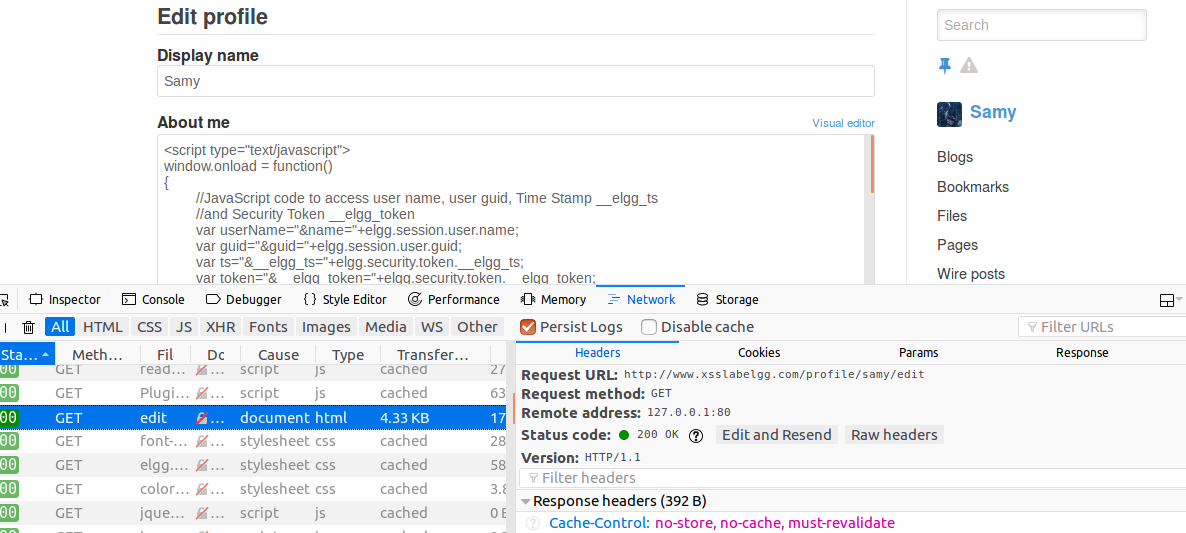
Activity里面可以看到，Alice添加了samy作为好友



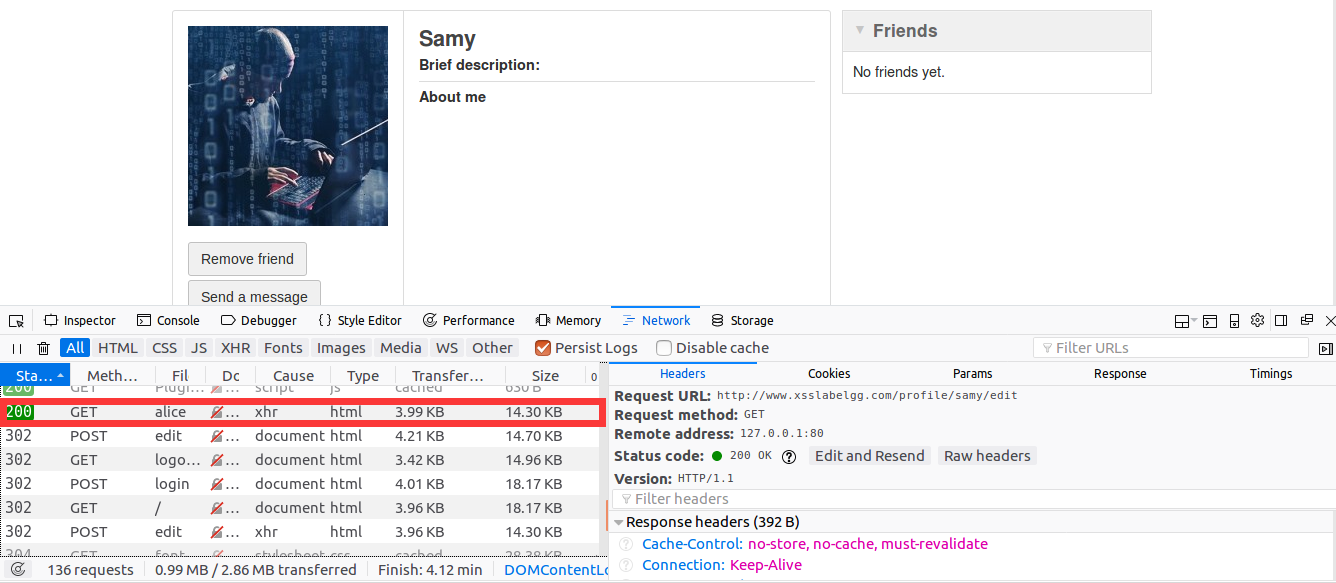
**Task5:** **Modifying the Victim’s Profile**

已知Samy的用户id是47

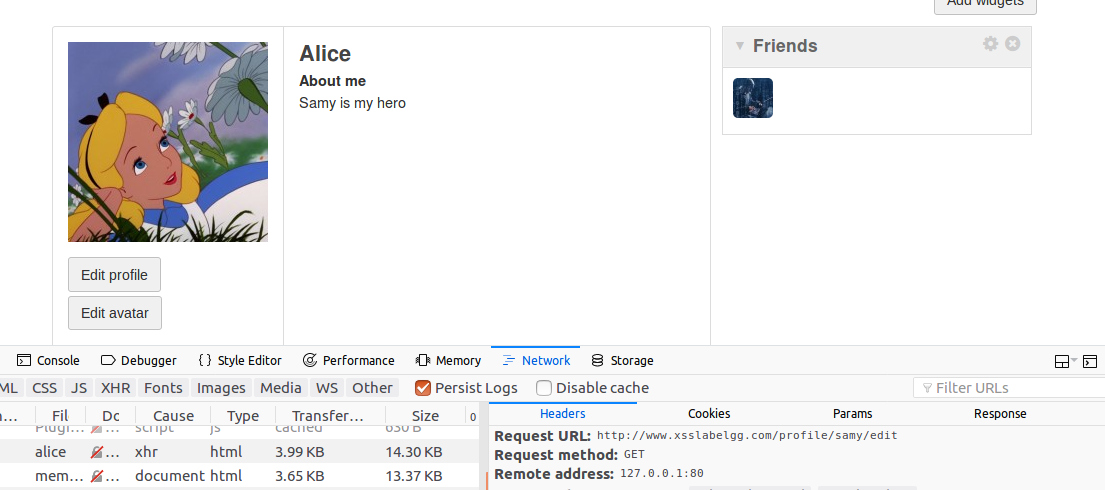
以Samy登录，进入profile edit页面，在About me部分里面添加js脚本



然后提交，保存，然后Alice登陆并查看Samy的主页的时候，自动发送了edit profile的post请求



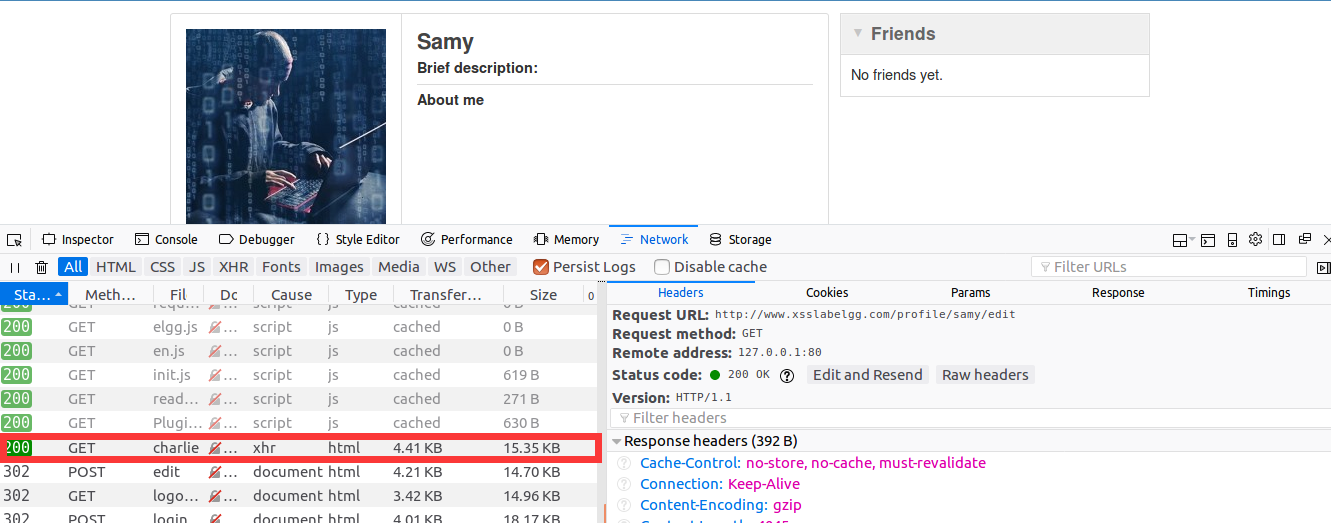
Alice的主页已经被更新



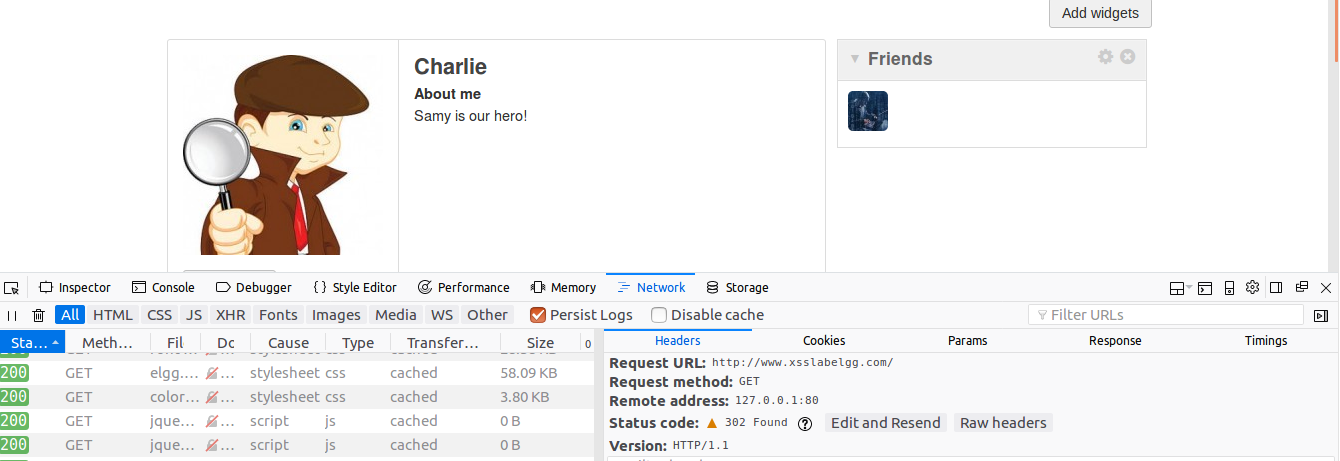
**Task6:** **Writing a Self-Propagating XSS Worm**

以Samy登录，进入profile edit页面，在About me部分里面添加js脚本

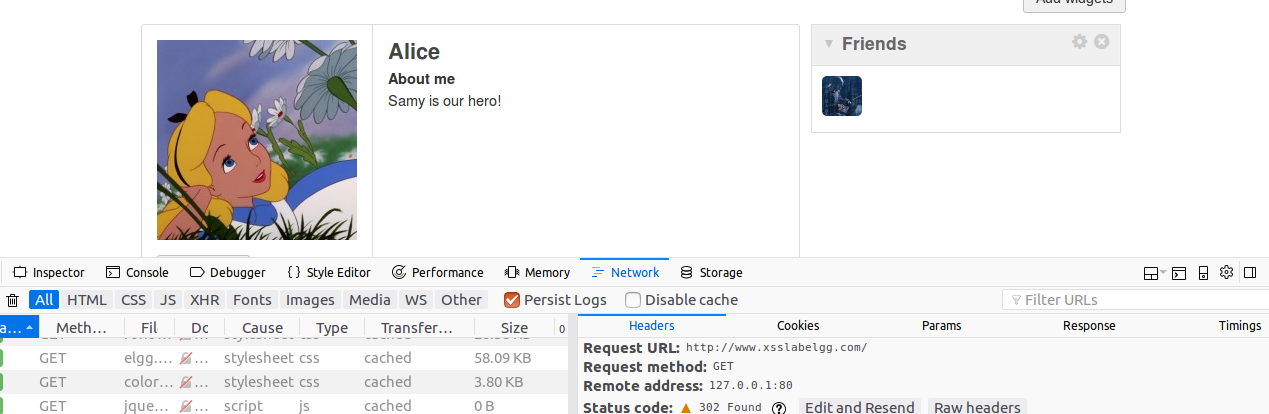
再以Charlie登陆，并查看Samy的主页，发现post了更新主页的请求



然后再以Alice登陆，并查看Charlie的主页，发现Charlie的主页已经更新

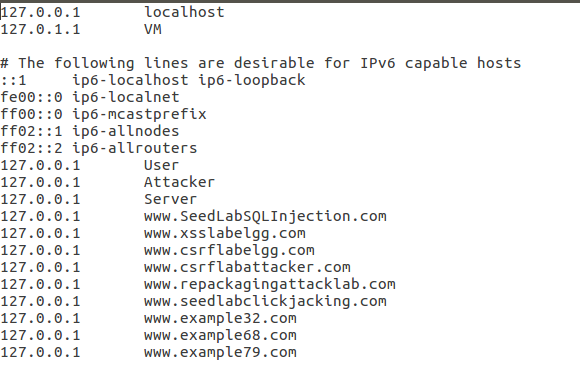


查看Alice 的主页，已经再次被更新

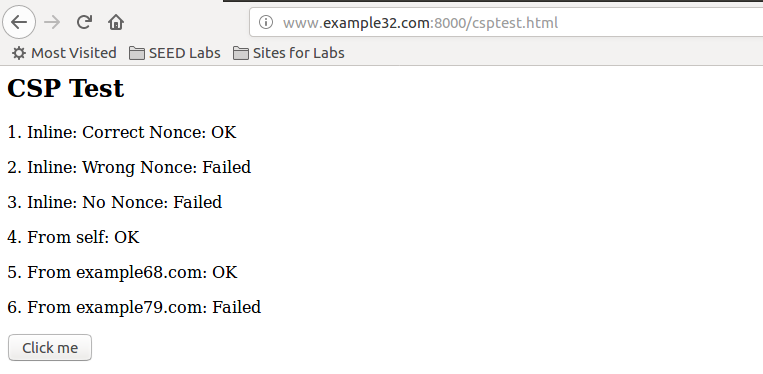


**Task7:** **Defeating XSS Attacks Using CSP**

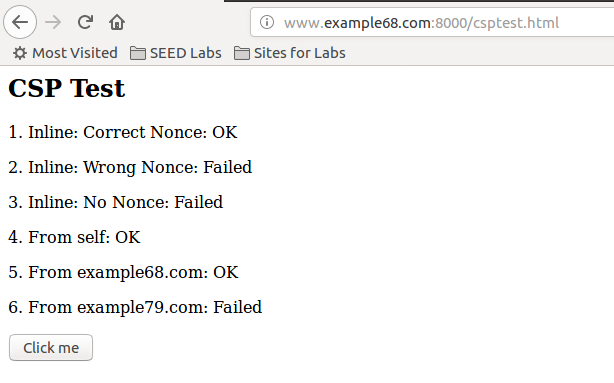
将以下三个条目添加到/etc/hosts文件中



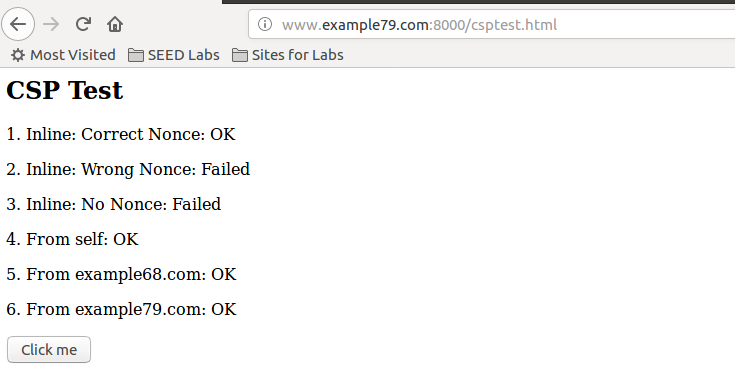
http://www.example32.com:8000/csptest.html



http://www.example68.com:8000/csptest.html



http://www.example79.com:8000/csptest.html



**修改后的http\_server代码**

#!/usr/bin/env python3

from http.server import HTTPServer, BaseHTTPRequestHandler

from urllib.parse import \*

class MyHTTPRequestHandler(BaseHTTPRequestHandler):

def do\_GET(self):

o = urlparse(self.path)

f = open("." + o.path, 'rb')

self.send\_response(200)

self.send\_header('Content-Security-Policy',

"default-src 'self';"

"script-src 'self' \*.example68.com:8000 \*.example79.com:8000 'nonce-1rA2345' 'nonce-2rB3333'")

self.send\_header('Content-type', 'text/html')

self.end\_headers()

self.wfile.write(f.read())

f.close()

httpd = HTTPServer(('127.0.0.1', 8000), MyHTTPRequestHandler)

httpd.serve\_forever()

修改后的网页显示，1，2，4，5，6均为ok

