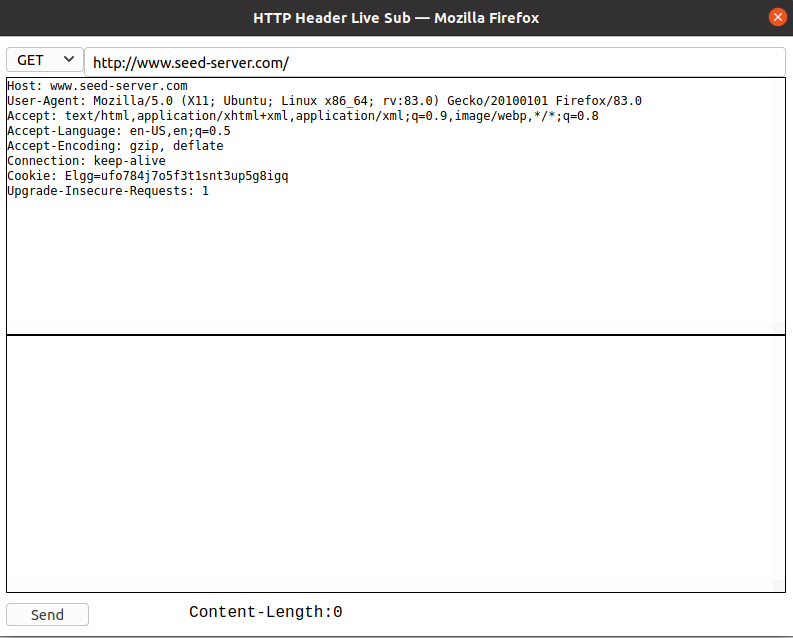
**Lab4-report**

**57119122 刘恒睿**

**Task1:Observing HTTP Requests**

Get请求：

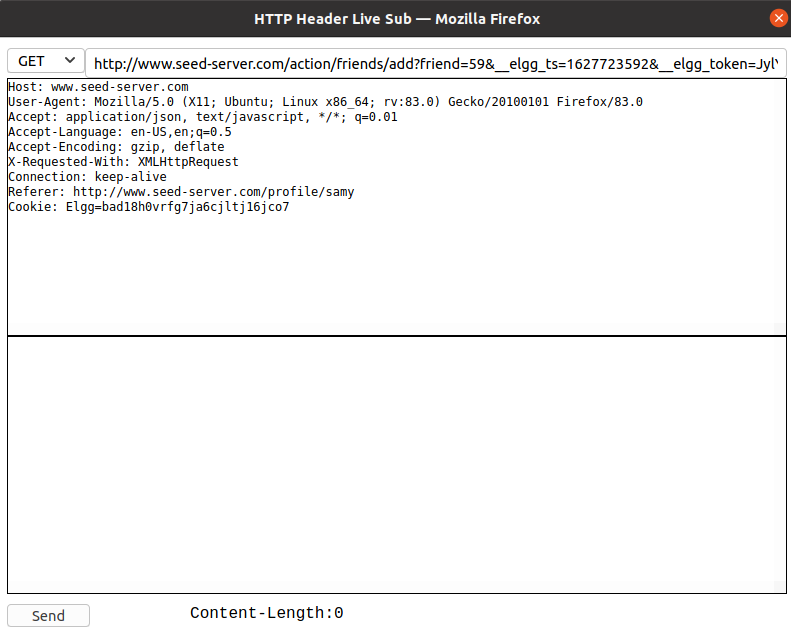


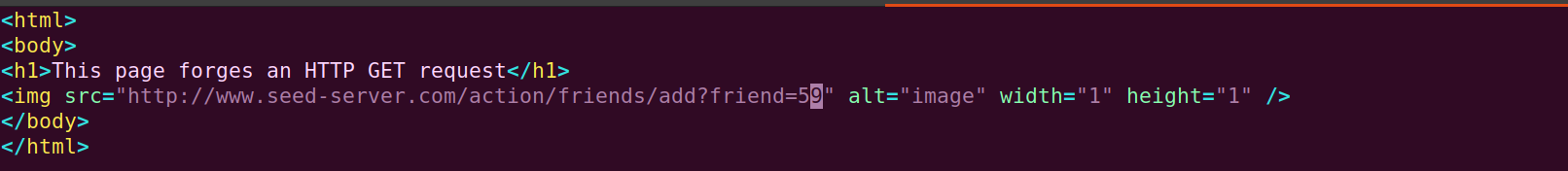
Post请求：



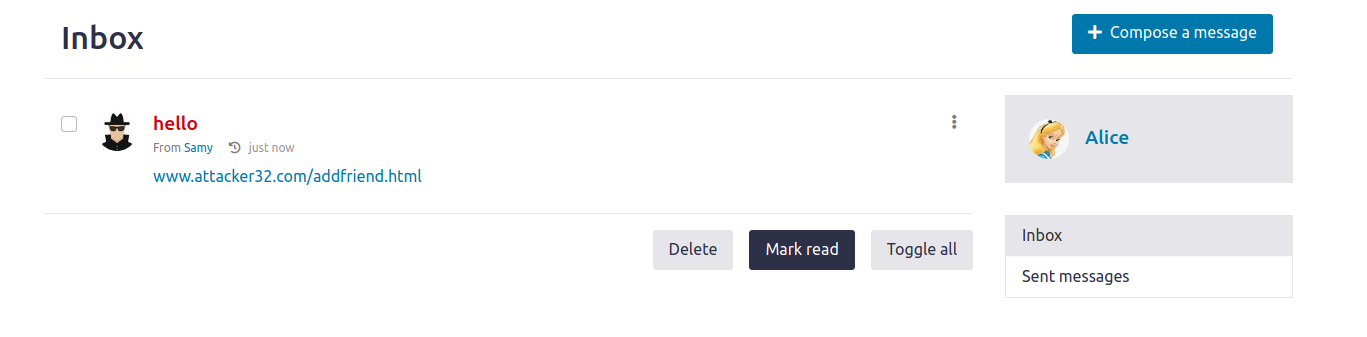
**Task2：CSRF Attack using GET Request**

登录boby账号添加Samy好友，获取添加Samy为好友的http请求报文：

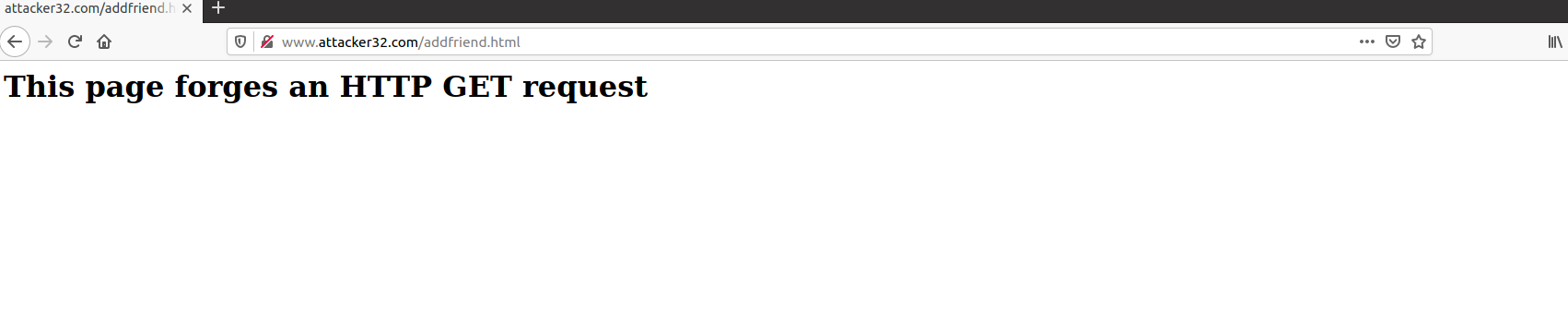


搭建攻击网站：  


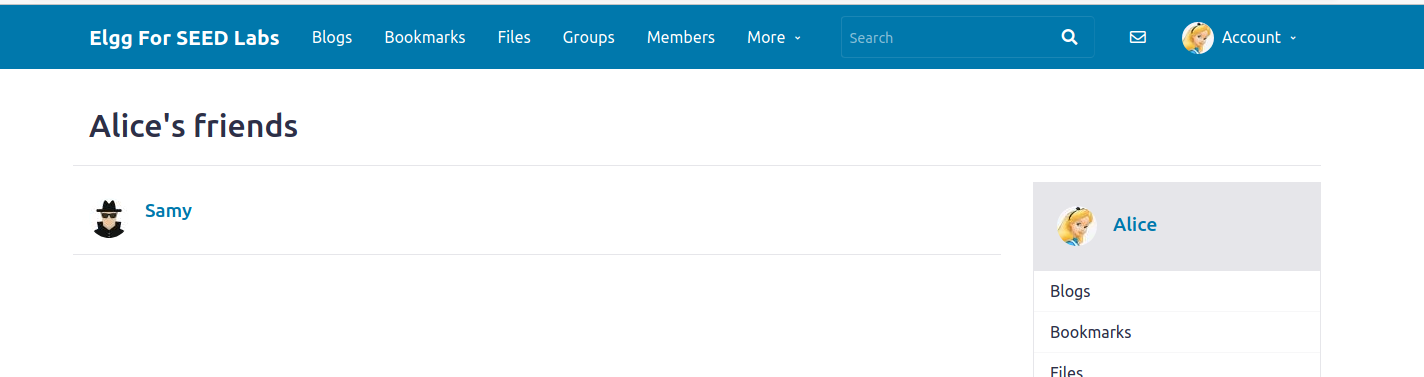
登录Samy给Alice发送邮件：



Alice打开邮件中的网站：

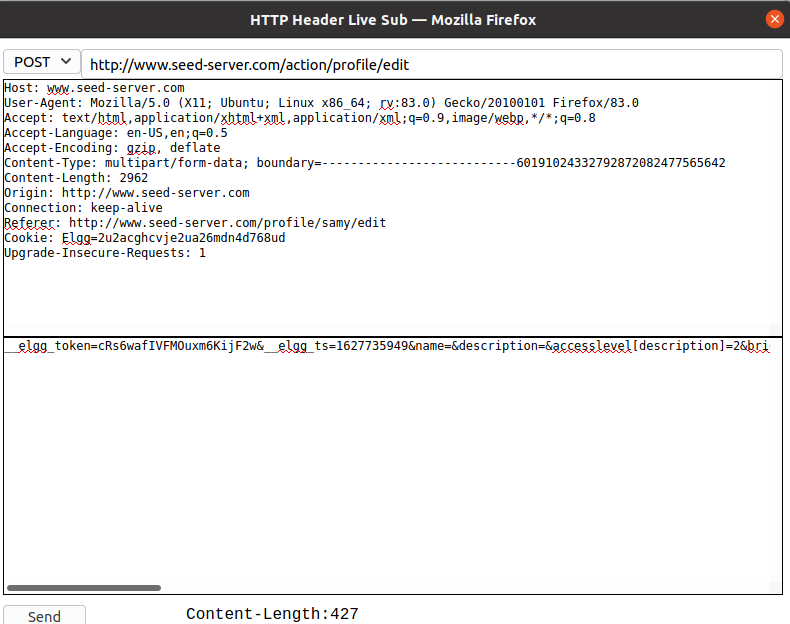


成功添加Samy为好友：



**Task3:CSRF Attack using POST Request**

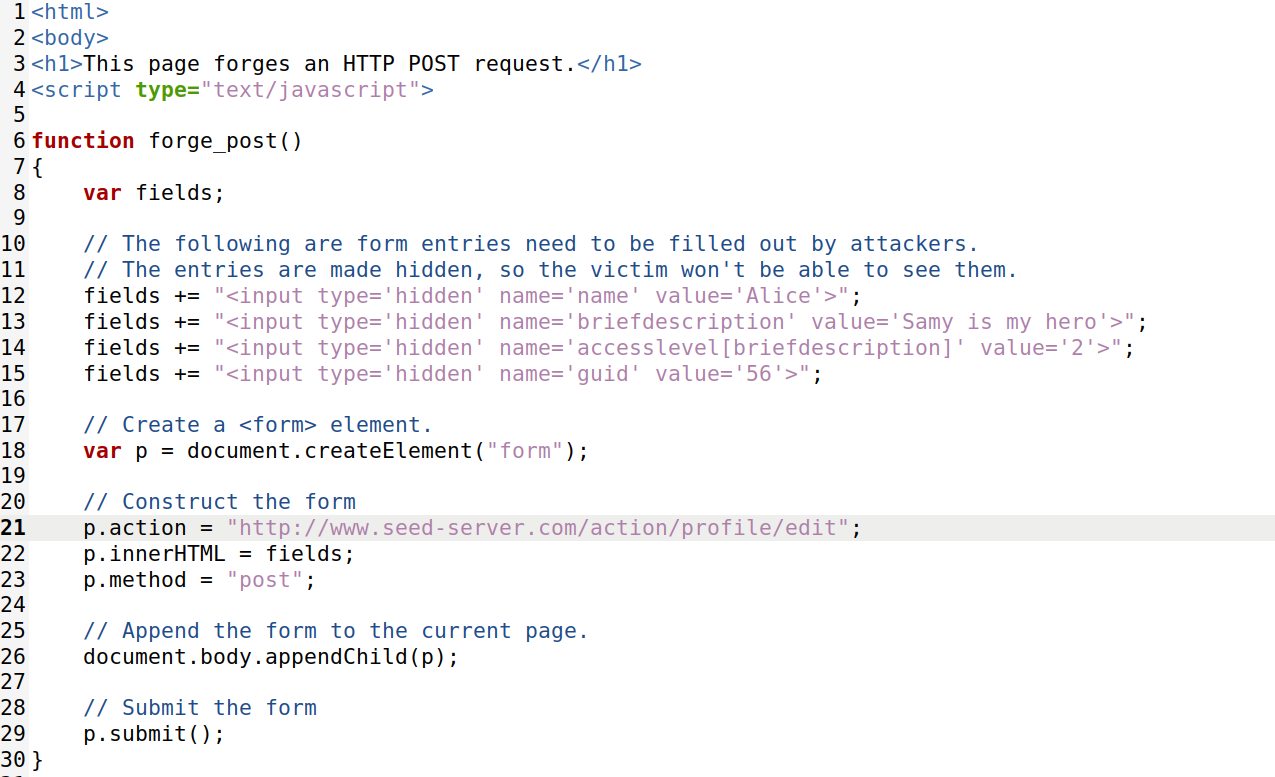
Samy修改自己的profile获取post报文：



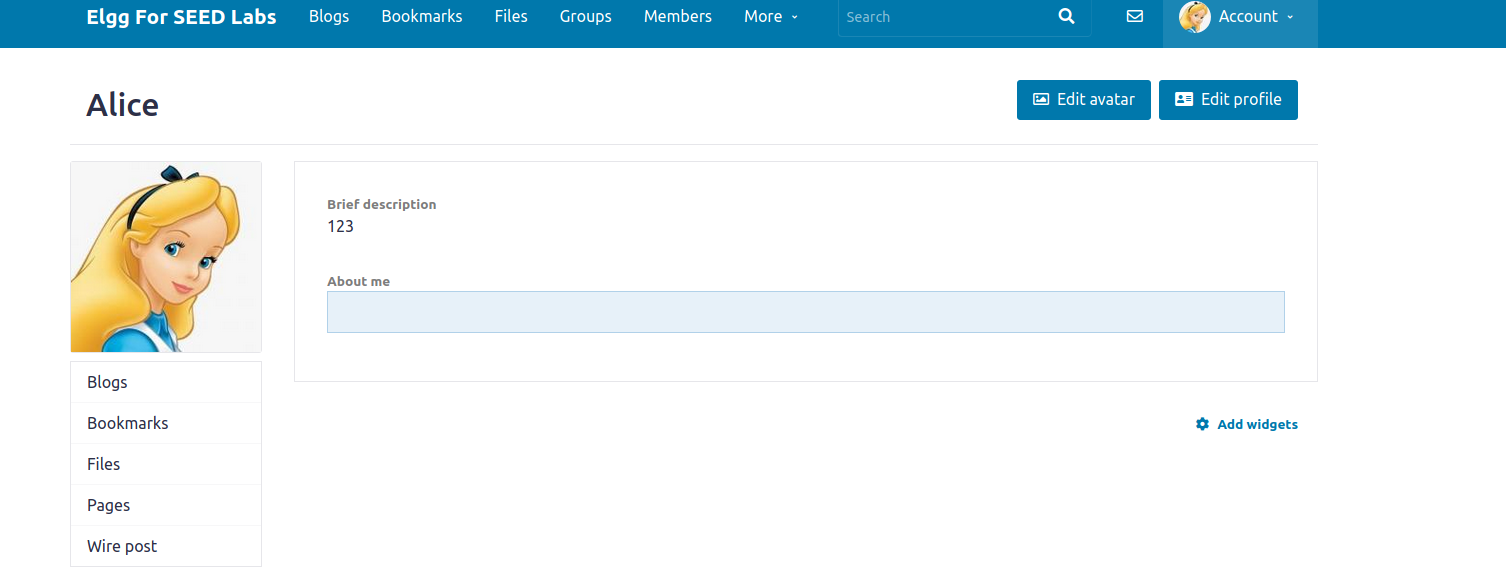
访问Alice主页,查看网页原码，获取Alice的guid：



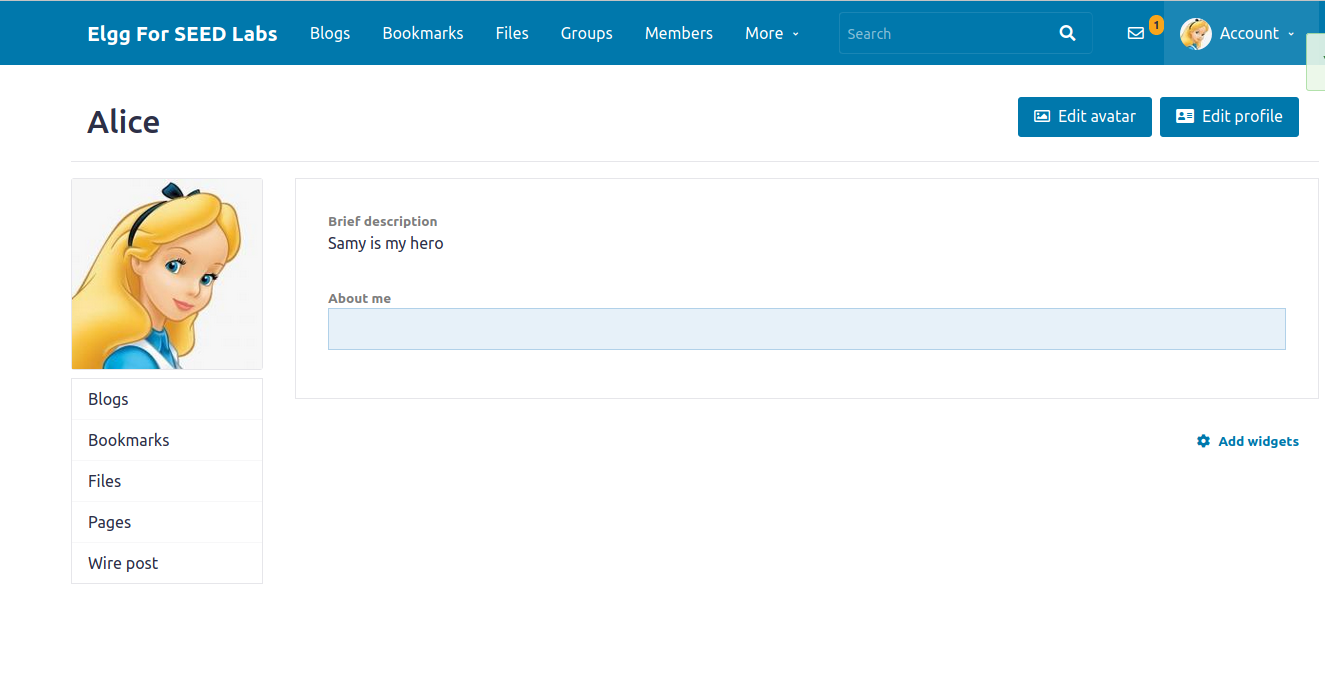
JavaScript攻击程序：



浏览攻击网站前：



浏览攻击网站后：



攻击成功！

**Question 1:**

Body 进入 Alice 的主页，查看页面源代码，在其中搜索关键字 uid，便可以找到Alice的uid。

**Question 2:**  
由于此网站uid可通过访问用户主页源代码查出，所以我们可以通过暴力手段在我们的代码中插入所有用户的uid(即枚举所有用户id)，使得无论哪个用户访问我们的钓鱼网站，他都会被攻击。