****

实验报告

|  |  |
| --- | --- |
| 姓名： | 强珂阳 |
| 学号： | 57118106 |

东南大学网络空间安全学院

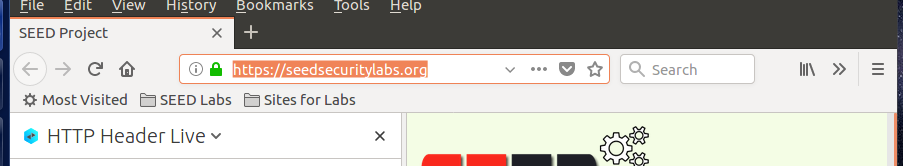
School of Cyber Science & Engineering

Southeast University

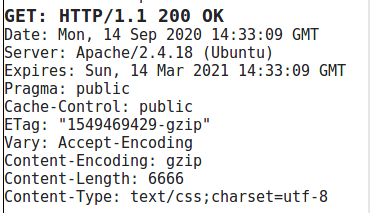
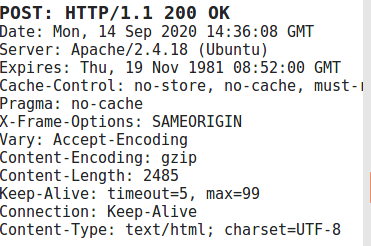
2020年9月

TASK1：Observing HTTP Request

首先更新HTTP Header Live扩展插件，并打开：



打开Elgg网站并登录随意一个账号，出现Post和Get请求内容：

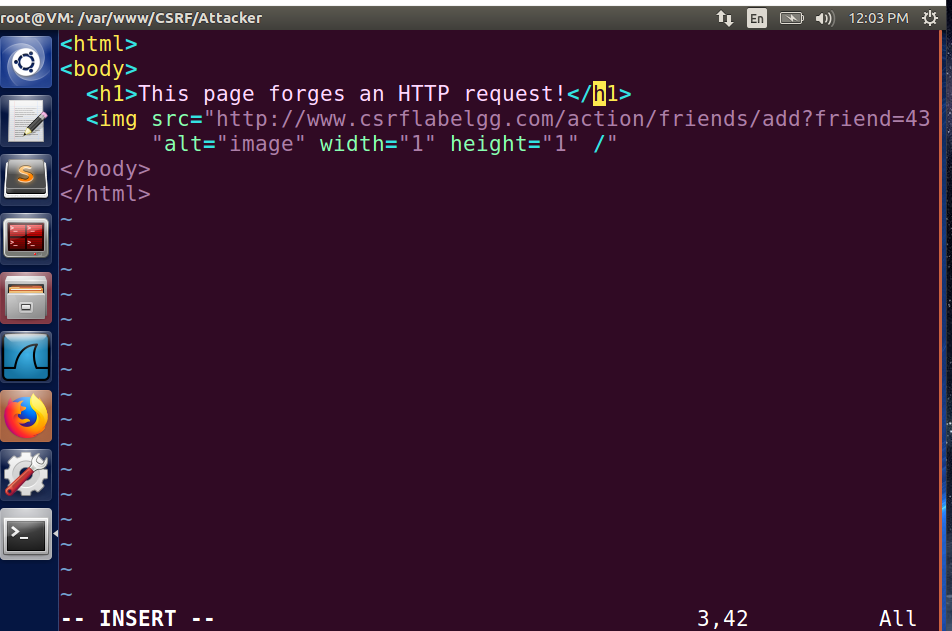


TASK2：**CSRF Attack using GET Request**

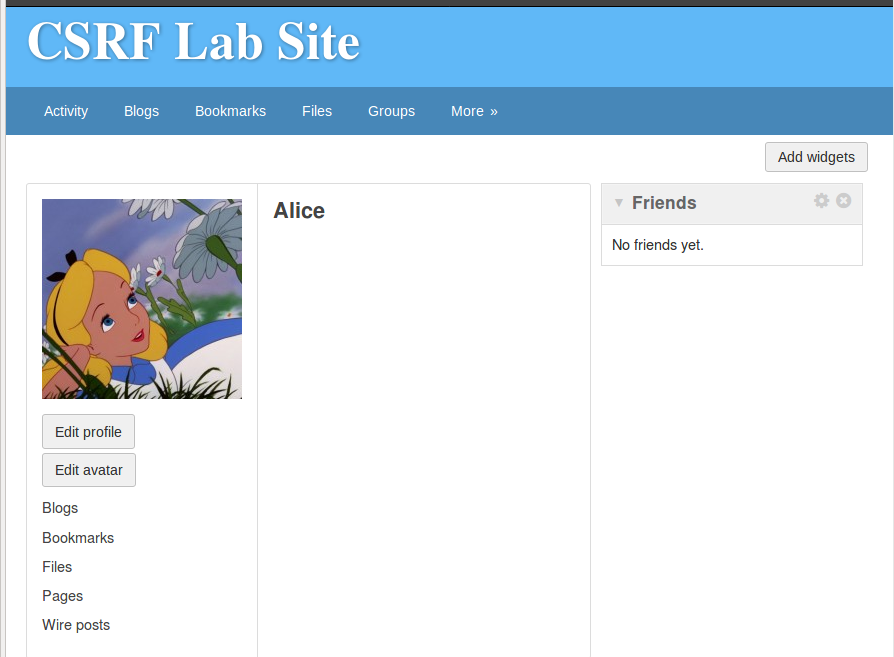
随意添加一个好友，查看HTTP Header Live中的GET请求：



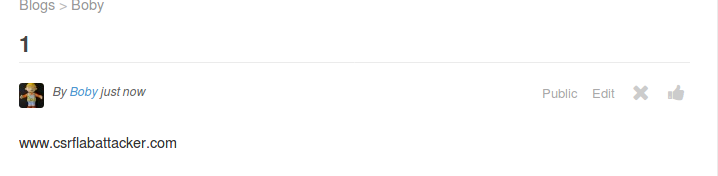
进入网页代码/var/www/CSRF/Attacker/按照上述合法的HTTP请求来编辑attack.html：



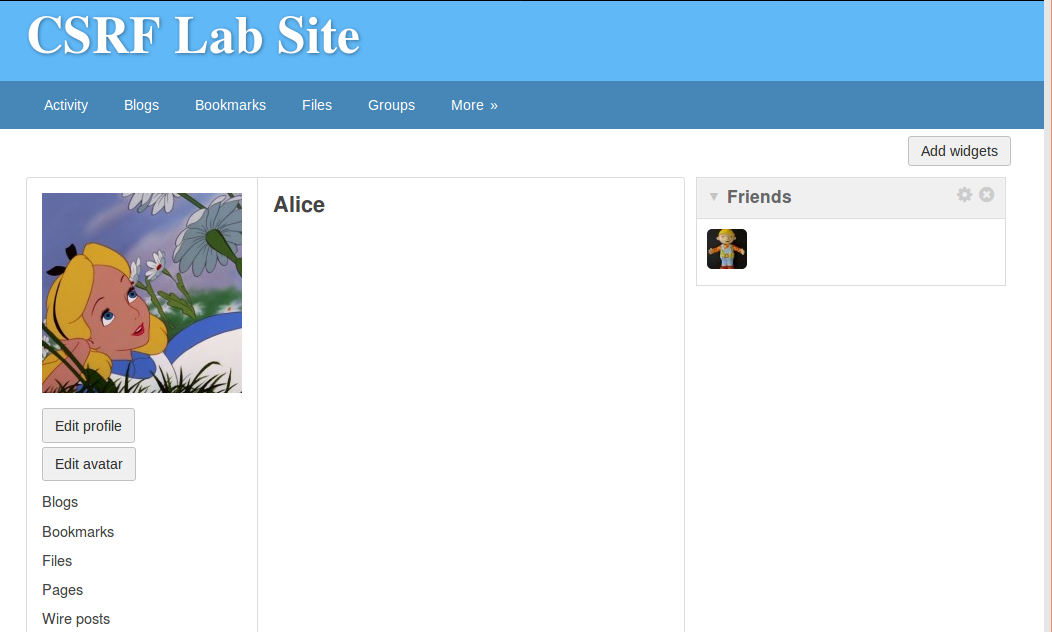
先登录Alice的账号，发现Alice并未添加任何人为好友：



用boby的账号发送一条动态，写着攻击网站，吸引Alice去访问。

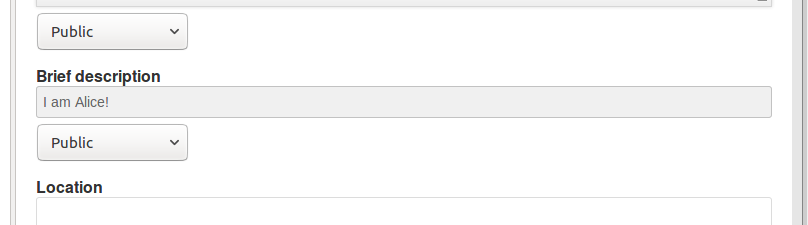


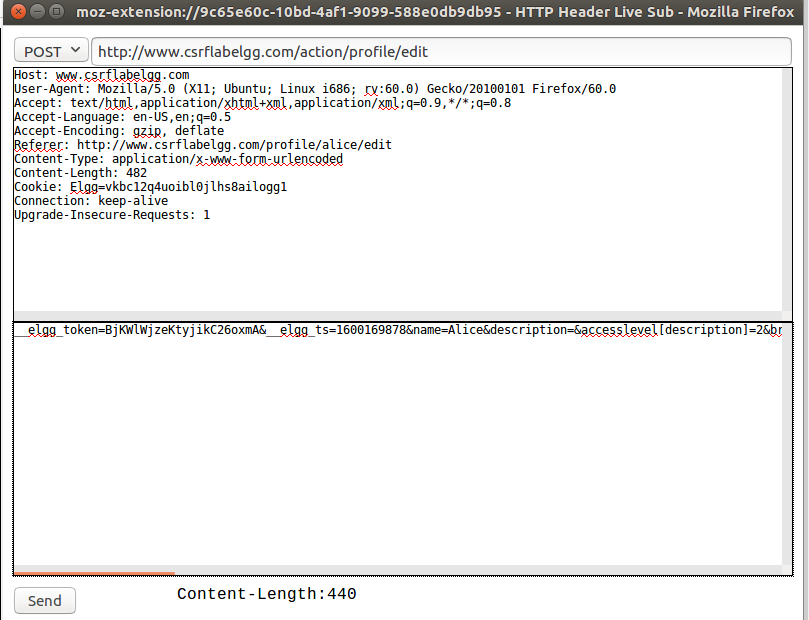
登录Alice账号点击进入网站，再返回Alice主页，发现已经添加boby为好友：



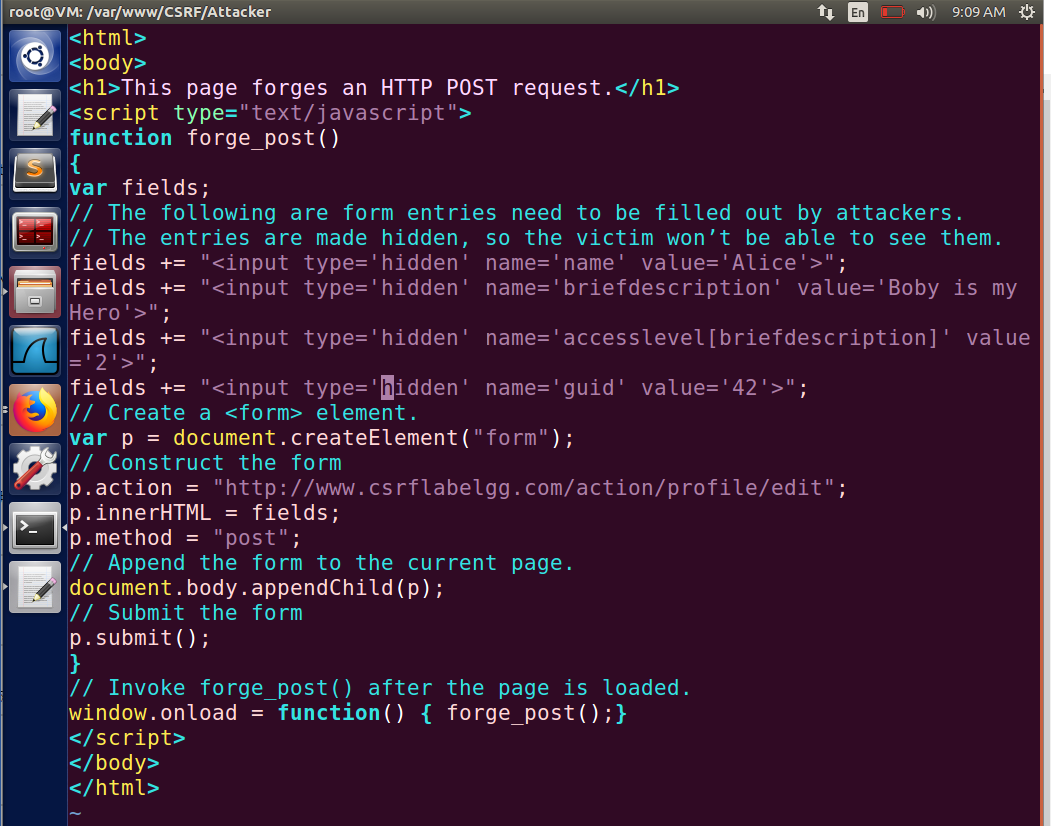
TASK3：**CSRF Attack using POST Requst**

先用Alice的账号修改个人资料，查看POST请求：

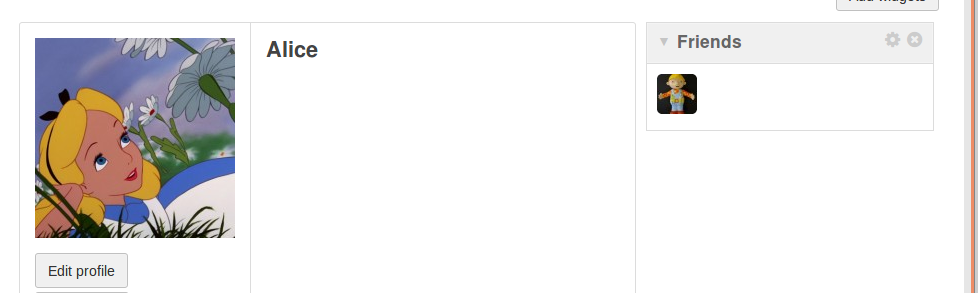




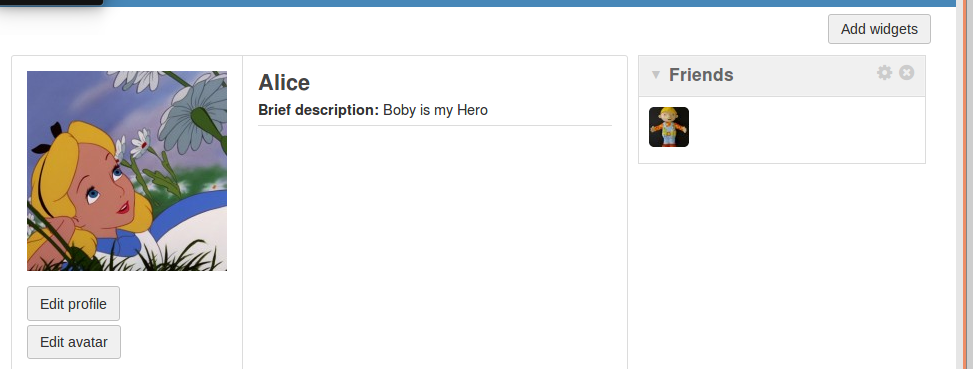
得到了相关的参数，再去之前的attack.html中修改攻击代码。

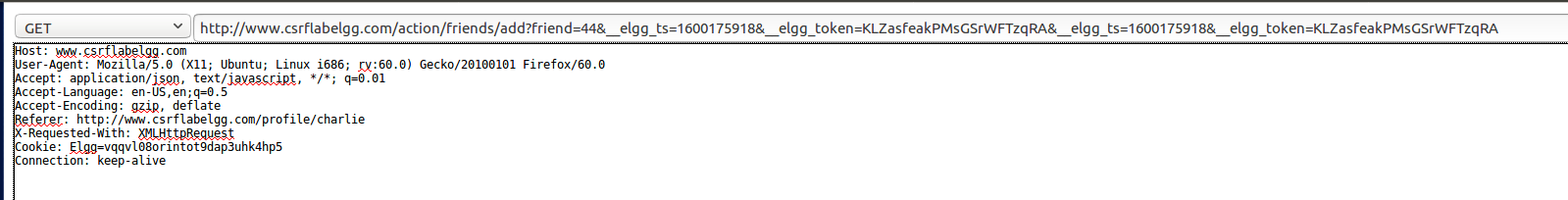


先更改Alice自我介绍为空，查看Alice的自我介绍确认为空：



点击网站后跳转到Alice的主页，并且自我介绍已经更改为“Boby is my Hero”：



问题一：可以先加对方的好友，并用HTTP Header Live截取，尝试用Alice的账号加Charlie好友，可以截取到

已知Alice的guid为42，所以截取到的44是Charlie的guid。由此可见该方法可行。

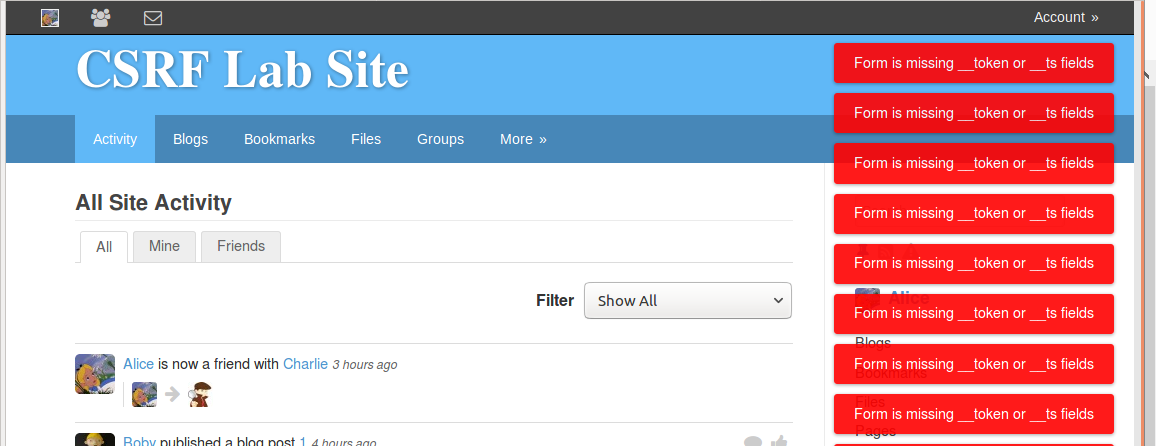
问题二：必须要知道对方的guid才能进行这样的攻击，在编写代码时有一栏guid是必填项，所以如果事先不知道谁会访问，则不能进行攻击。

TASK4：**Implementing a countermeasure for Elgg**

注释掉/var/www/CSRF/Elgg/vendor/elgg/elgg/engine/classes/Elgg/ActionsService.php中gatekeeper函数里的return ture;语句：



再次让Alice账号点击网站，出现失败警告：



Elgg向JavaScript添加了安全令牌，而安全令牌是由时间戳，sessionID和随机字符串的通过MD5加密后的值，在密码学上难以破译，所以攻击者无法获取安全令牌，也就无法进行攻击。

**总结：**

在这次实验中，我初步了解了CDSRF攻击，学会运用HTTP Header Live扩展插件来查看POST和GET请求。这次实验总体完成比较顺畅，并没有遇到很大的困难。

这次试验让我知道了对于不熟悉的网站要保持警惕，并且了解了一些防御方法，可以通过密码学的方式来对网站来源进行核对检查达到增加安全性的目的。