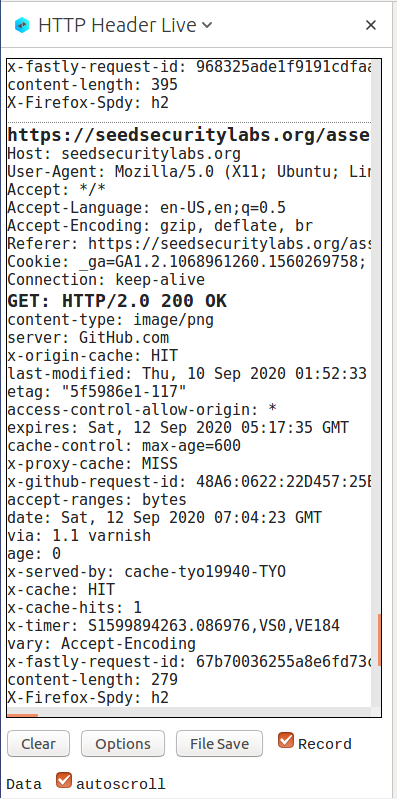
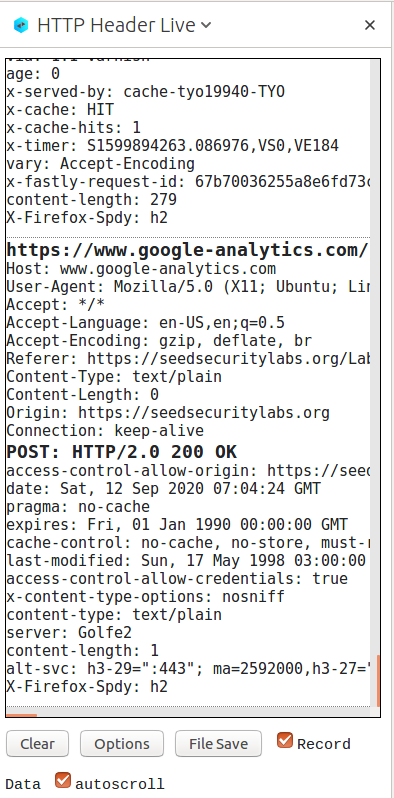
**网络空间安全实训Lab[4]**

**实验报告**

**57118117 谌雨阳**

**Task 1: Observing HTTP Request**

1、安装了http header live扩展程序并进行了试运行。



识别出的参数有：

Language

Cookie

Age

Content-length

**Task 2: CSRF Attack using GET Request**

吸引Alice点击链接的方法：

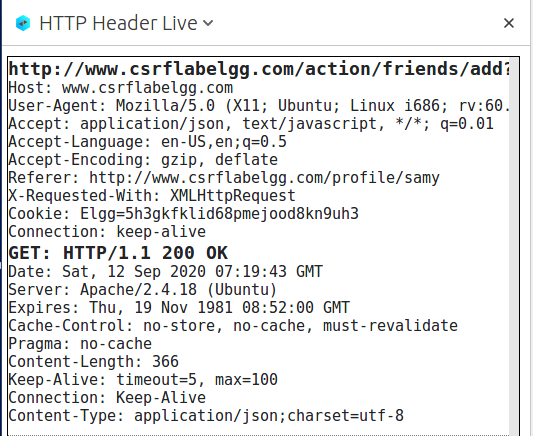
1、发送私人信息。

2、使用吸引人的标题或内容引导。

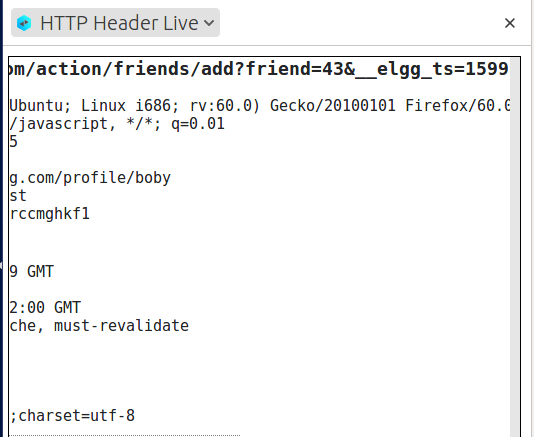
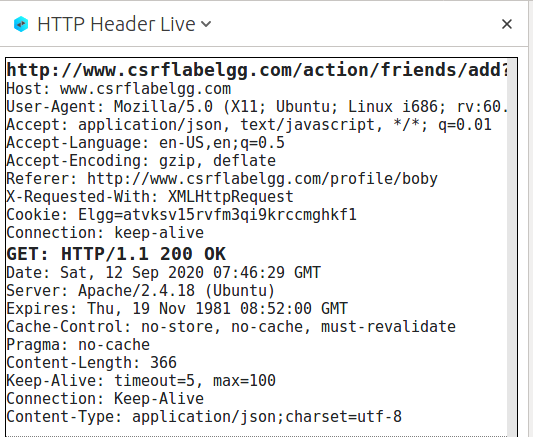
**实验过程：**

1、登录了Alice 的账号并熟悉了操作界面。打开http header live用于抓取请求。

2、点击进Samy 的主页，进行添加好友的尝试。此操作中工具抓取的请求如下：



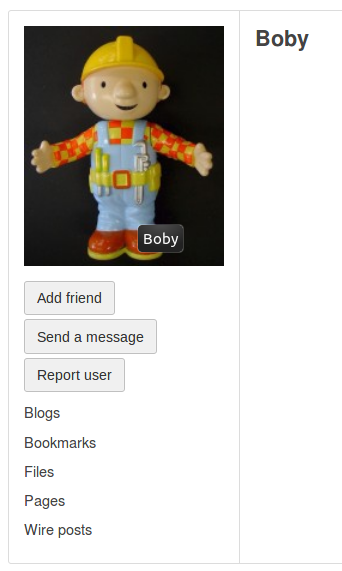
3、发现添加好友与用户ID有关，于是点进Boby主页并进行添加好友尝试，得到Boby的ID为43。



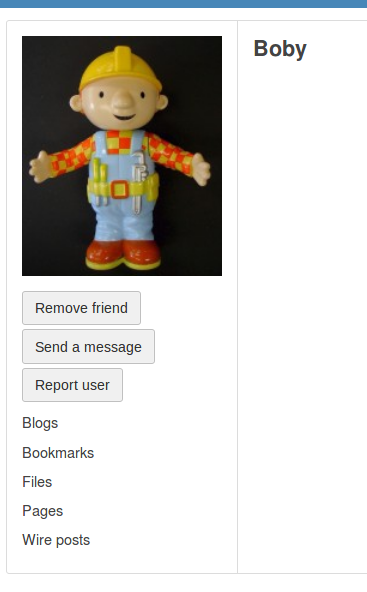
4、在/var/www/CSRF/Attacker中新建index.html文件，并填入如下代码。攻击网站制作完成。



5、登录Alice 的账号，点击Boby的主页，显示不是好友。



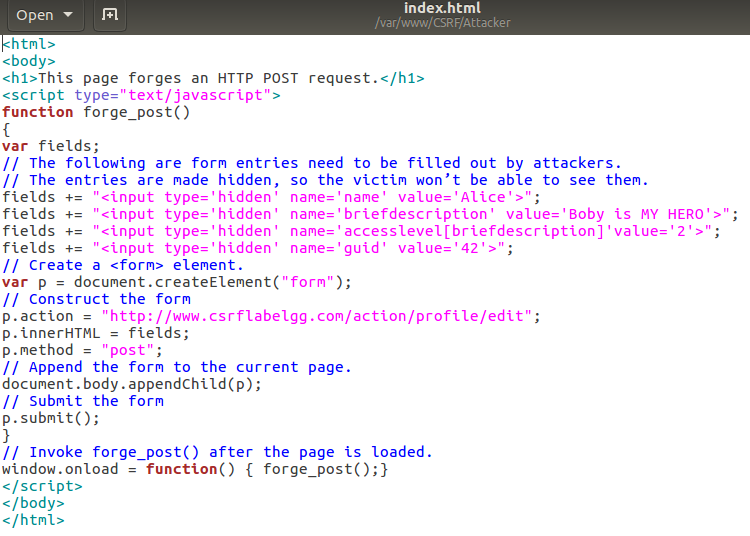
6、在登录状态下访问刚刚添加的攻击网页，回Boby主页进行刷新，发现已经和Boby成为好友。



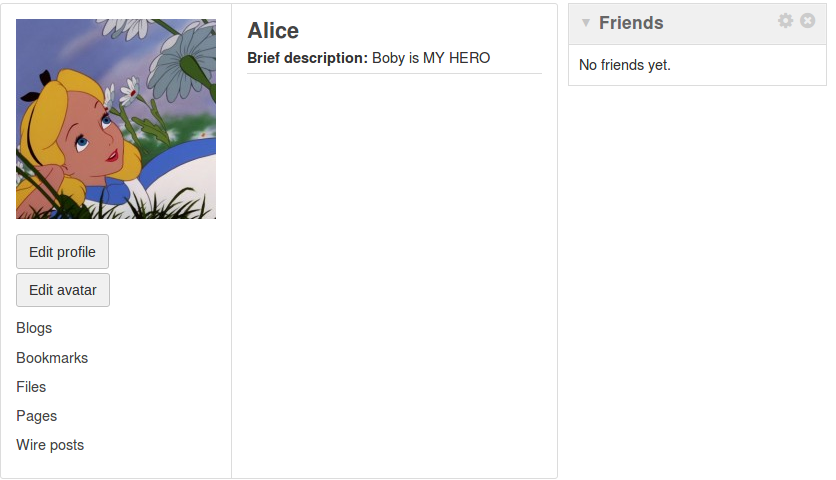
**Task 3: CSRF Attack using POST Request**

1、先从别的账号中通过加好友得知Alice的ID为42。

2、更改index.html为如下代码：



3、在以Alice的账户登录后访问攻击网页显示如下，攻击成功。



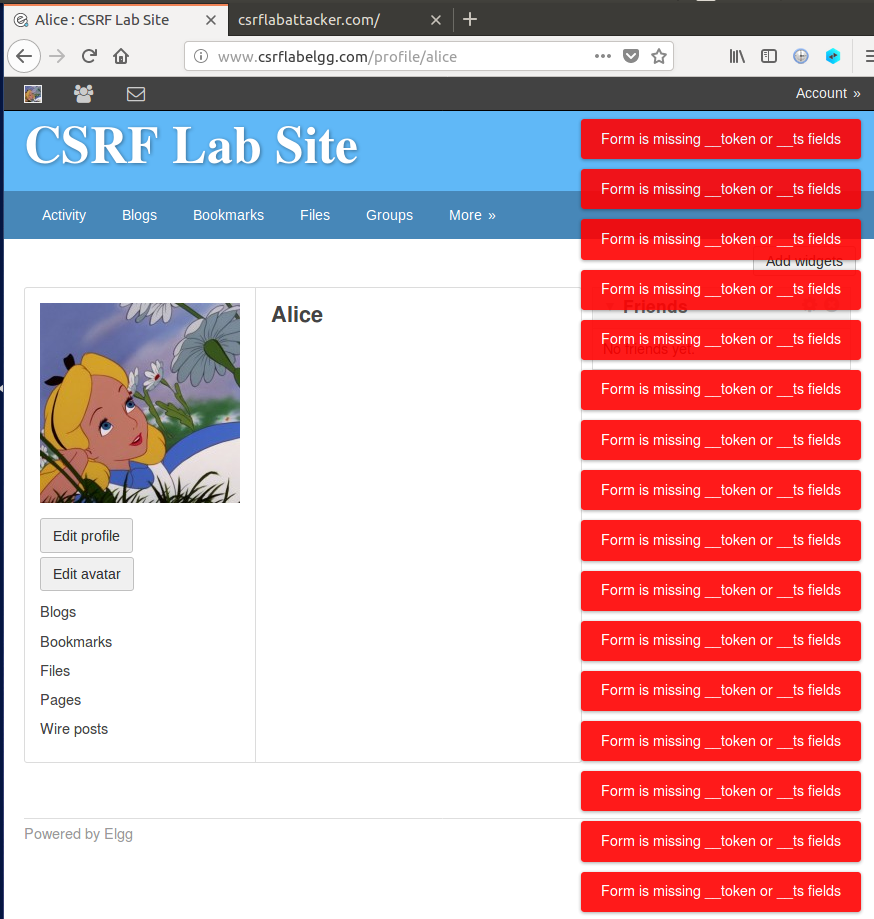
两个问题：

1、获取Alice的ID：可以在开着http header live进行加好友操作，从抓取的命令当中获得Alice的ID。

2、能否攻击解释：不能，在不能输对guid的情况下该脚本是无法选择攻击对象的。

**Task 4: Implementing a countermeasure for Elgg**

1. 注释掉return true代码后访问攻击网站结果如下：



解释：打开的防御机制是验证session的token和timestamp，恢复代码之后攻击就无法奏效了。