**跨站请求伪造(CSRF)攻击实验室**

姓名：钱煜 学号：57118105

1. 实验目的

了解跨站请求伪造(CSRF)攻击。

二、实验内容

1.观察HTTP请求；

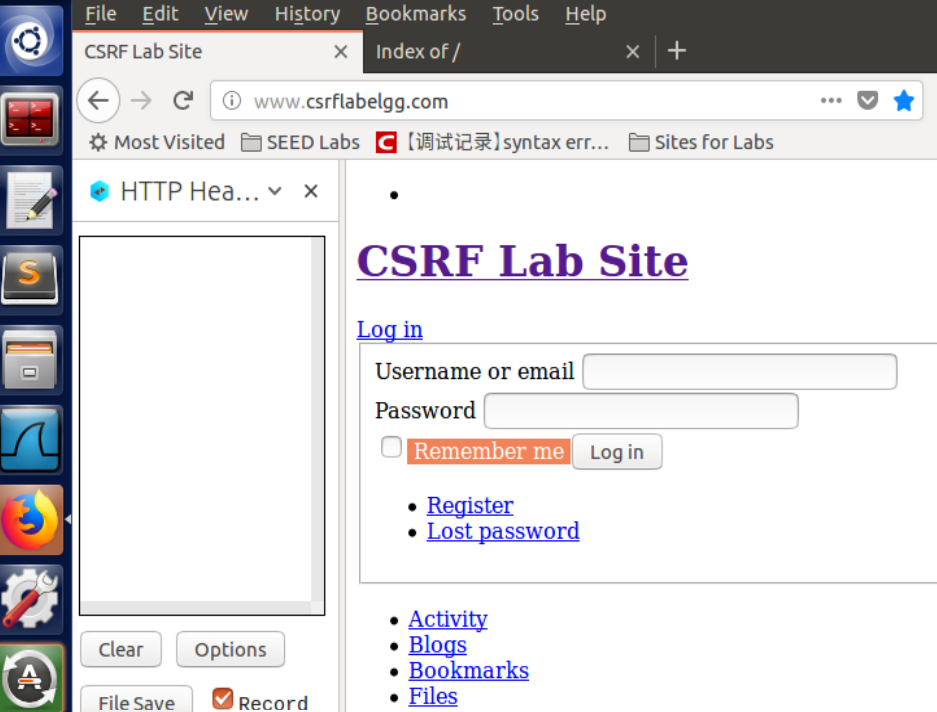
三、实验环境

Virtual Box，Seed Ubuntu 16.04。

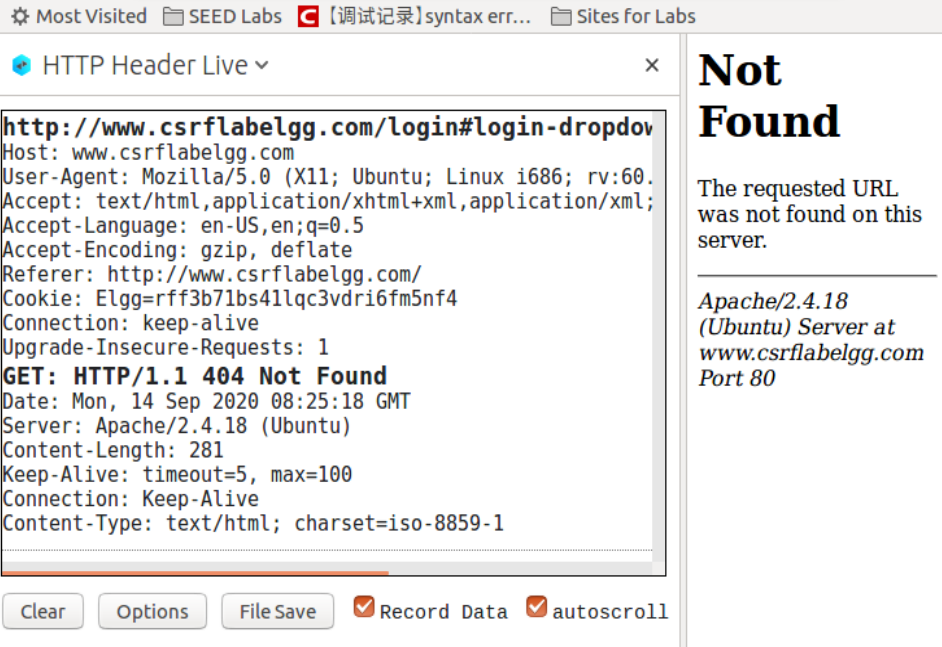
1. 实验

**Task 1.观察HTTP请求**

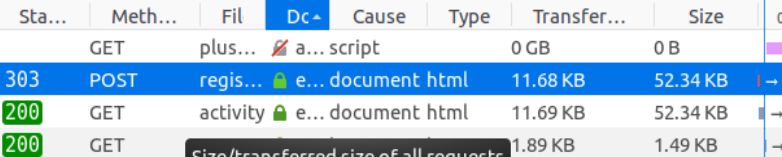
首先打开HTTP Header Live：

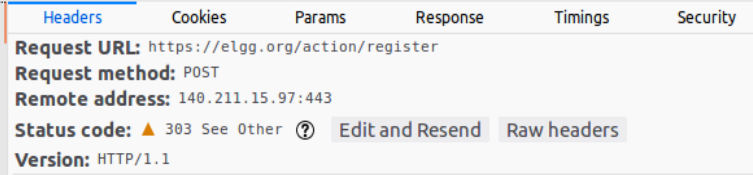


单击Log in，得到：



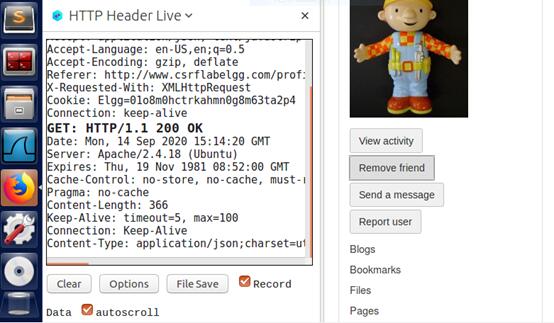
获取POST及其详细信息：



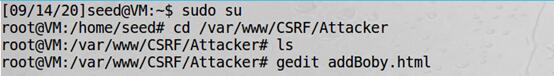


**Task 2.使用GET请求进行CSRF攻击**

登录：



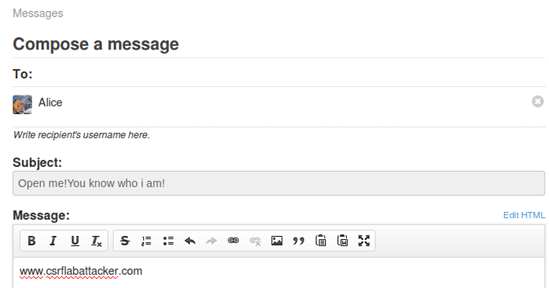
Captured HTTP Header：

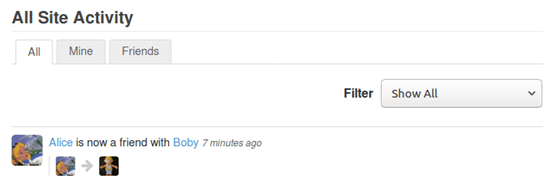


imp文件：



向被攻击方发送：

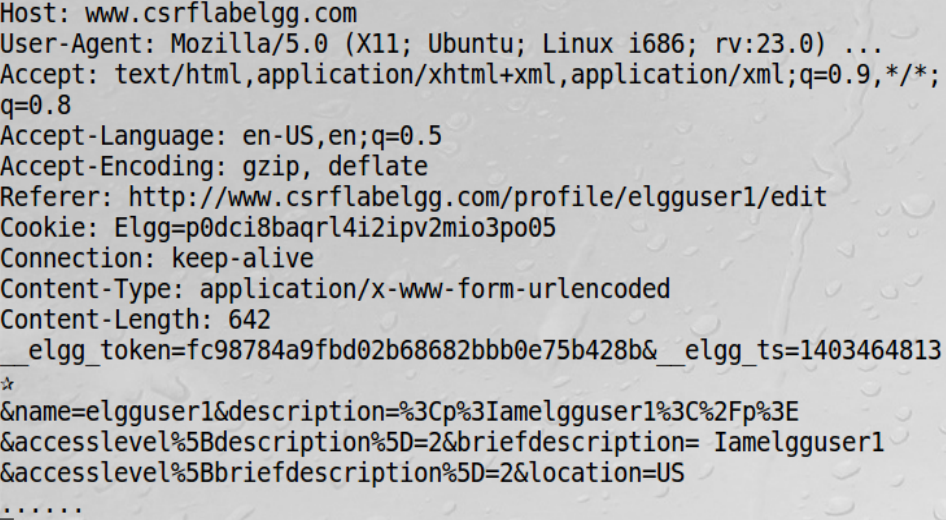




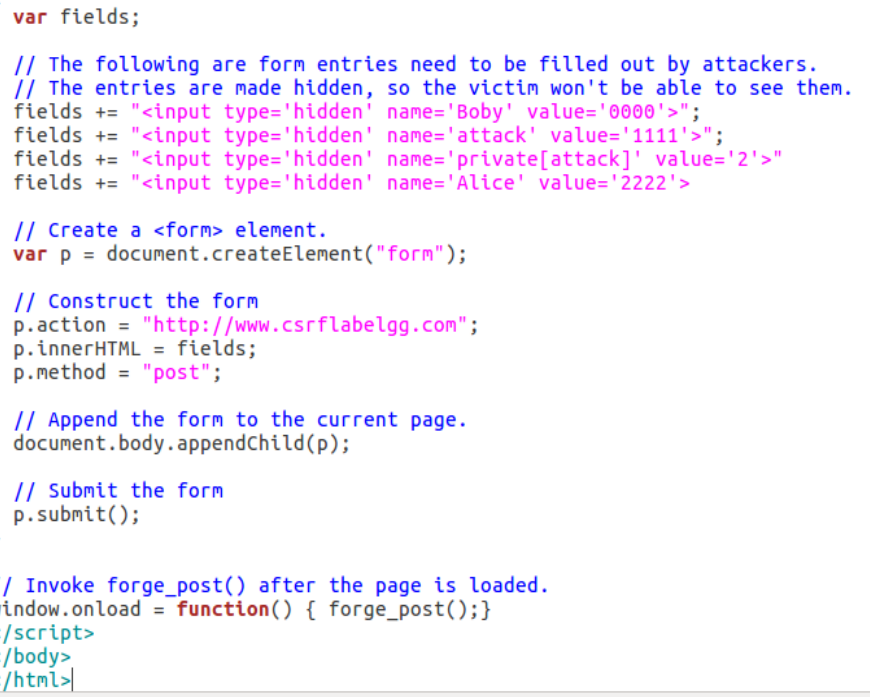
添加成为好友。

**Task 3.使用POST请求进行CSRF攻击**

修改使用POST：



修改html文件：



Question 1：在Alice登录网站的时候，网站向Alice返回Cookie，Boby向服务器发送命令请求执行，以获取其中的uid。

Question 2：在CSRF攻击中，可设置特定URL，仅能使用特定返回的Cookie发起POST请求进行攻击。

Task 4.Elgg实现对策

修改HTTP：

