**CSRF Attack Lab**

**实验报告**

57118112-王怡乐

**Task 1:Observing HTTP Request**

使用HTTP Header Live插件抓取HTTP请求。



**POST报文分析：**

Host: [www.csrflabelgg.com](http://www.csrflabelgg.com) //表示接受请求的服务器地址，此处为域名

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 //表示发送请求的应用程序名称

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 //客户端希望接受的数据类型的格式

Accept-Language: en-US,en;q=0.5 //通知服务端可以发送的语言

Accept-Encoding: gzip, deflate //通知服务端可接受的文本压缩算法

Referer: <http://www.csrflabelgg.com/> //表示发出请求的地址

Cookie: Elgg=cqk47busdrvd2otfdci74s3t31 //是一种身份证明

Connection: keep-alive //HTTP连接方式为持久连接

Upgrade-Insecure-Requests: 1 //向服务器发送一个客户端对HTTPS加密和认证响应良好，并且可以成功处理的信号，请求所属网站所有的HTTPS资源。

ps: Content-Length参数在页面下方另外显示，未出现在显示的报文内容中。



**GET报文分析：**

Host: [www.csrflabelgg.com](http://www.csrflabelgg.com) //表示接受请求的服务器地址，此处为域名

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0 //表示发送请求的应用程序名称

Accept: text/css,\*/\*;q=0.1//客户端希望接受的数据类型的格式

Accept-Language: en-US,en;q=0.5//通知服务端可以发送的语言

Accept-Encoding: gzip, deflate//通知服务端可接受的文本压缩算法

Referer: http://www.csrflabelgg.com/activity//表示发出请求的地址

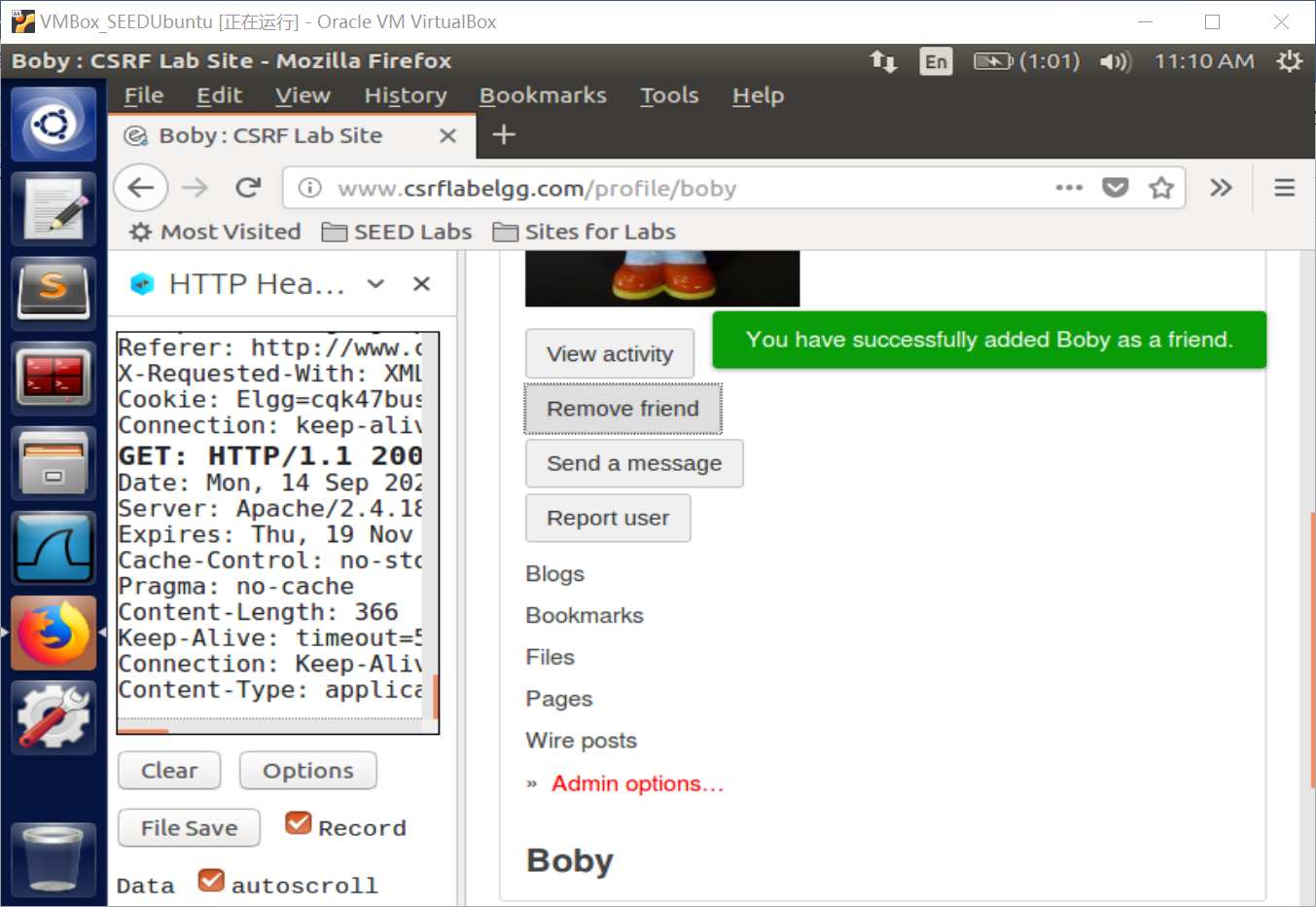
Cookie: Elgg=cqk47busdrvd2otfdci74s3t31//是一种身份证明

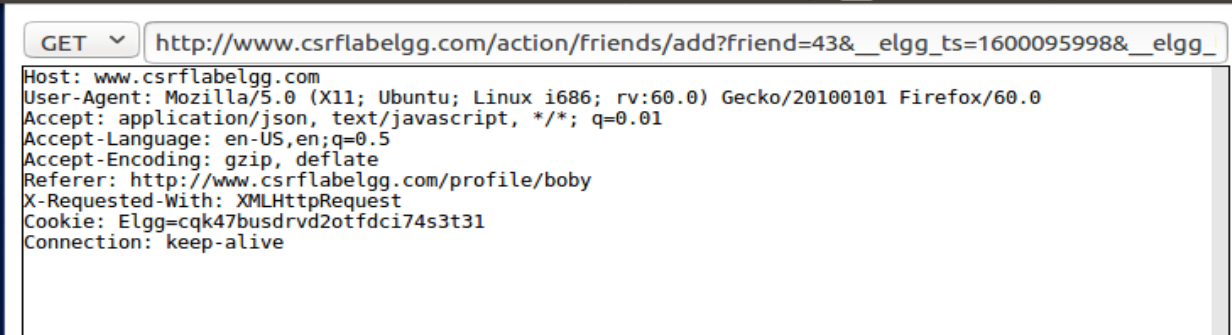
Connection: keep-alive//HTTP连接方式为持久连接

需要注意的是，GET报文的请求参数在URL后（放在请求行中），而POST，报文的请求参数则放于请求数据中，这一点在截图中未显示。

**Task2:CSRF Attack using Get Request**

登录Samy的账号，加Boby为好友，用HTTP Header Live插件抓取相应的GET请求报文。

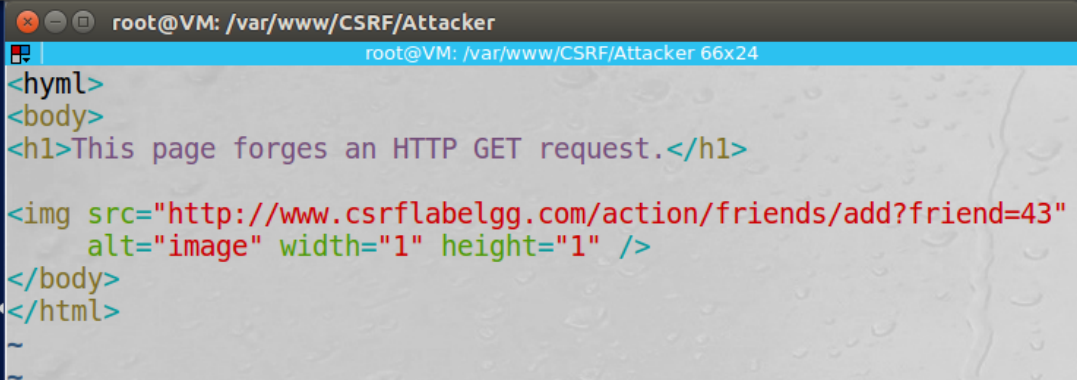


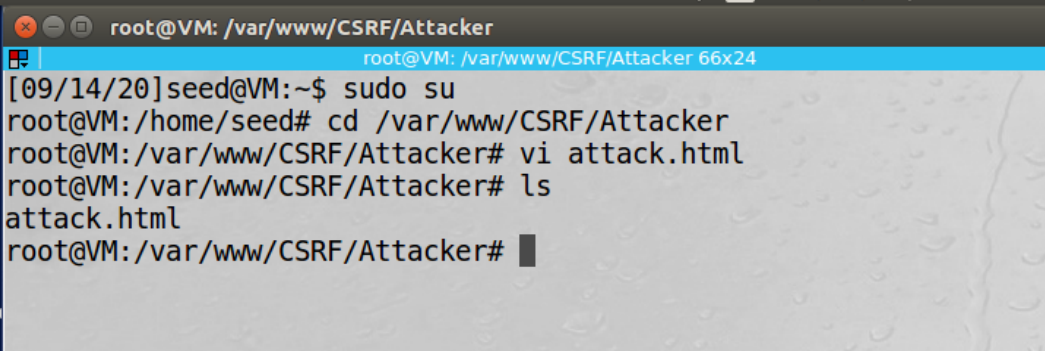


记录下Boby的GUID为43。

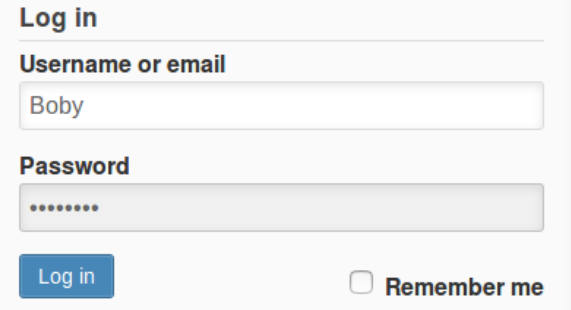
<http://www.csrflabelgg.com/action/friends/add?friend=43&__elgg_ts=1600095998&__elgg_token=EnEHikpzsqB6qXbakgrezw&__elgg_ts=1600095998&__elgg_token=EnEHikpzsqB6qXbakgrezw>

构造恶意Web页面。其中，加Boby为好友的URL被嵌入在图片中，该图片极小，不可见。

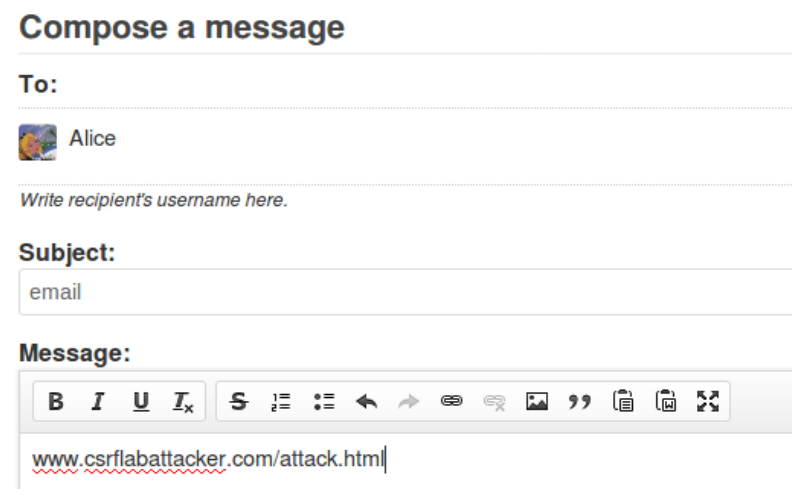




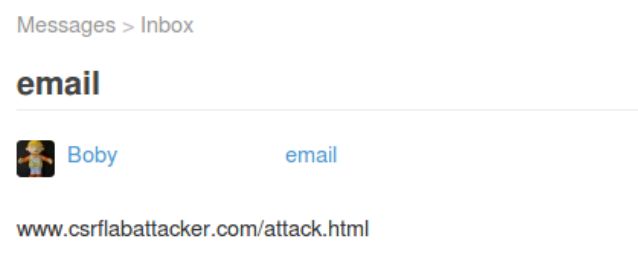
登录Boby的账户。

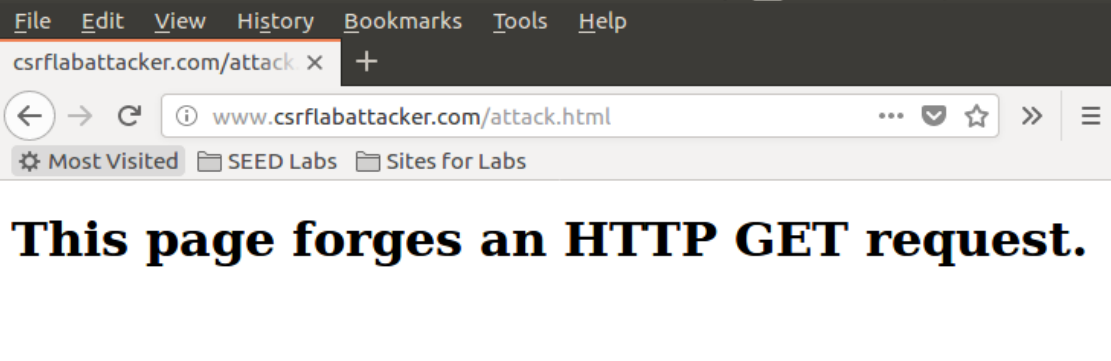


向Alice发送内容为恶意网址的邮件。

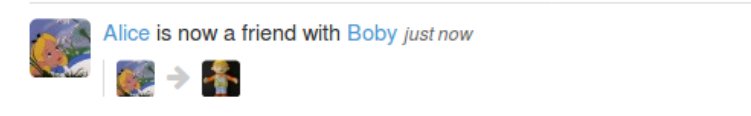


登录Alice的账户，打开Boby发来邮件中的网址，跳转到下图界面。



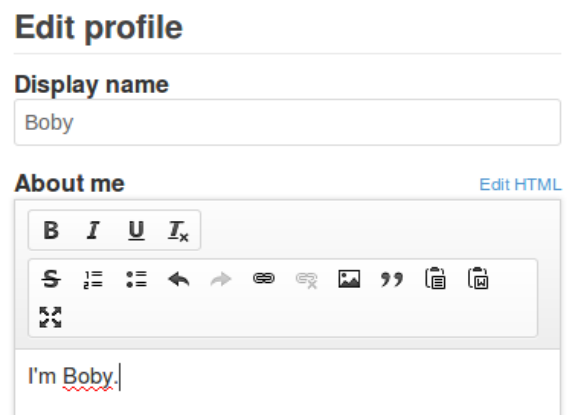
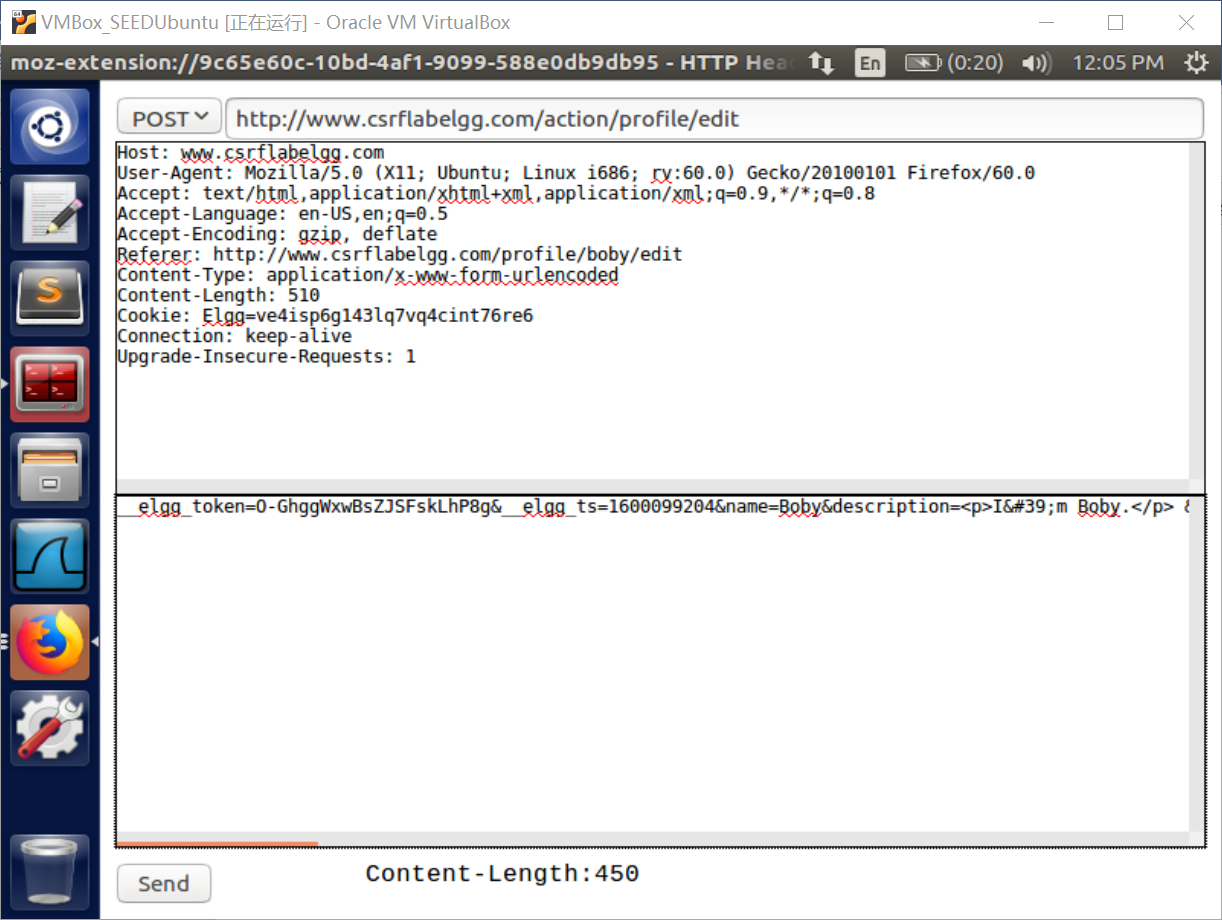


Alice和Boby成为好友。



**Task3:CSRF Attack using POST Request**

修改Boby的profile,观察相关的POST报文格式。

Host: www.csrflabelgg.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.csrflabelgg.com/profile/boby/edit

Content-Type: application/x-www-form-urlencoded

Content-Length: 510

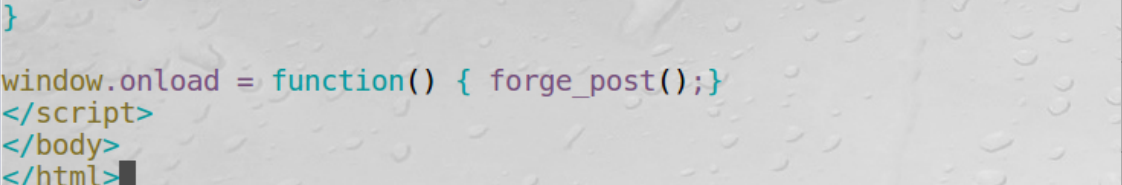
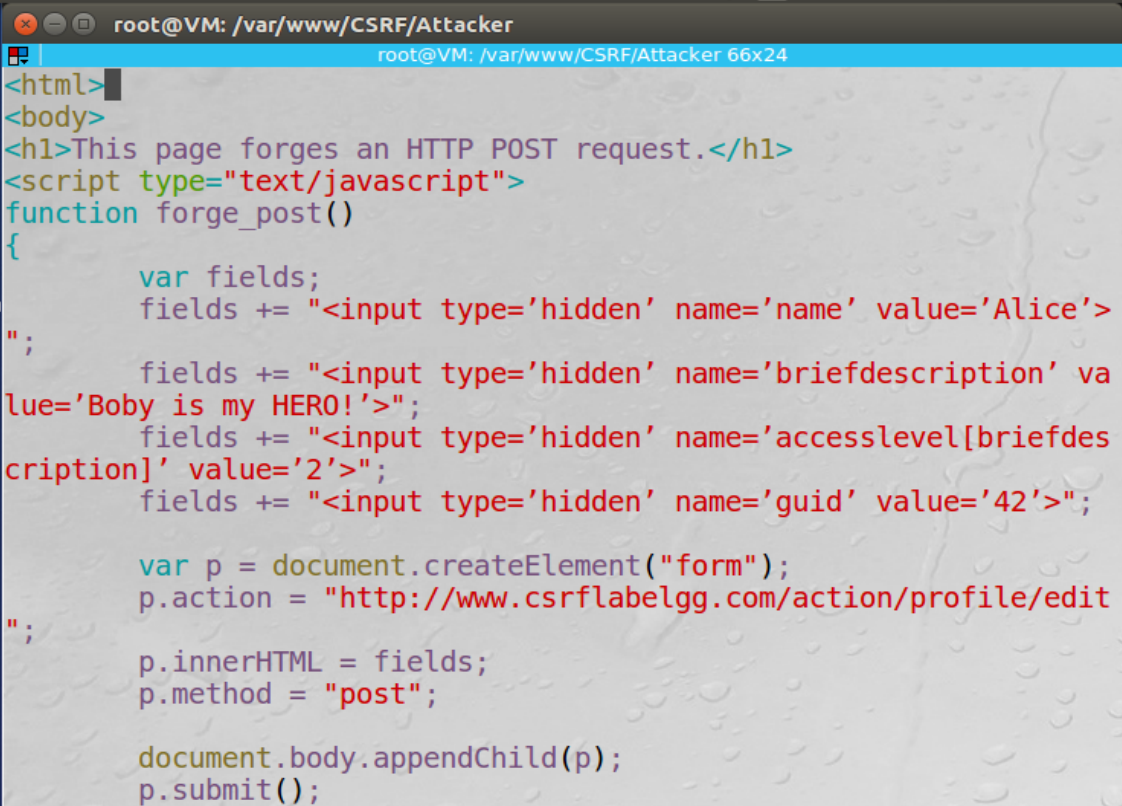
Cookie: Elgg=ve4isp6g143lq7vq4cint76re6

Connection: keep-alive

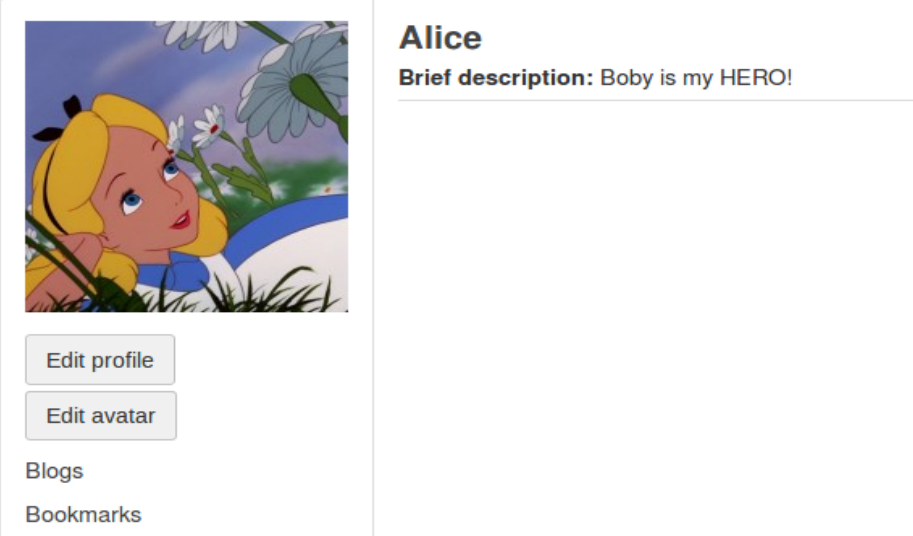
Upgrade-Insecure-Requests: 1

\_\_elgg\_token=O-GhggWxwBsZJSFskLhP8g&\_\_elgg\_ts=1600099204&name=Boby&description=<p>I&#39;m Boby.</p> &accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=43

编写代码，构建恶意网页。



Alice的主页中出现“Boby is my HERO!”。



Question1: 伪造的HTTP请求需要Alice的用户id (guid)才能正常工作。如果波比目标是Alice，在攻击之前，他需要找到获取Alice的用户id的方法。Boby不知道Alice的Elgg密码，所以他无法登录Alice的账户获取信息。请描述如何解决这个问题。

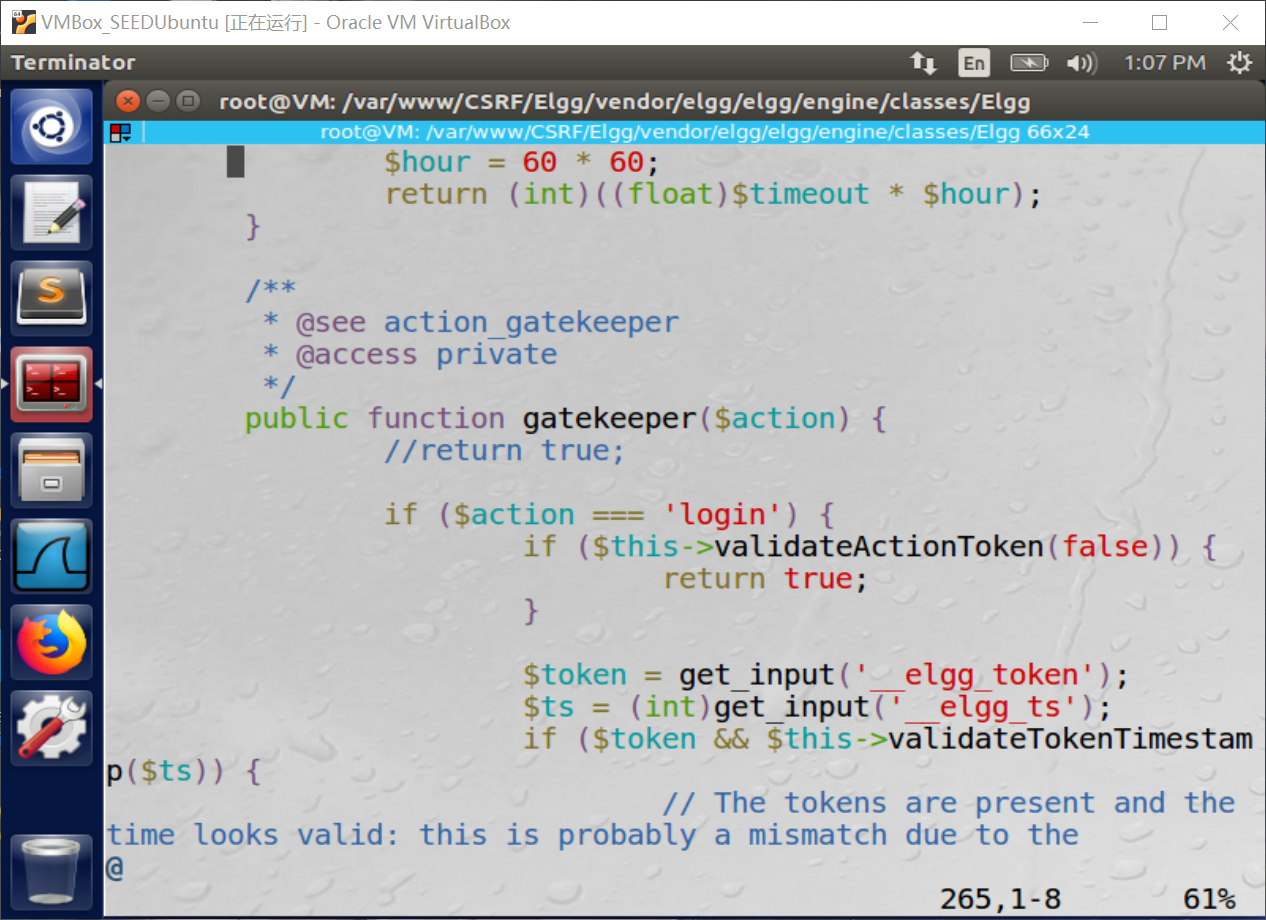
答：Boby只需申请成为Alice的好友，捕获申请的GET请求报文，便可以从中获得Alice的guid。

Question2：如果Boby想对访问其恶意网页的任何人发起攻击。在这种情况下，他事先不知道谁正在访问web页面。他还能启动CSRF修改受害者elgg档案吗?请解释一下。

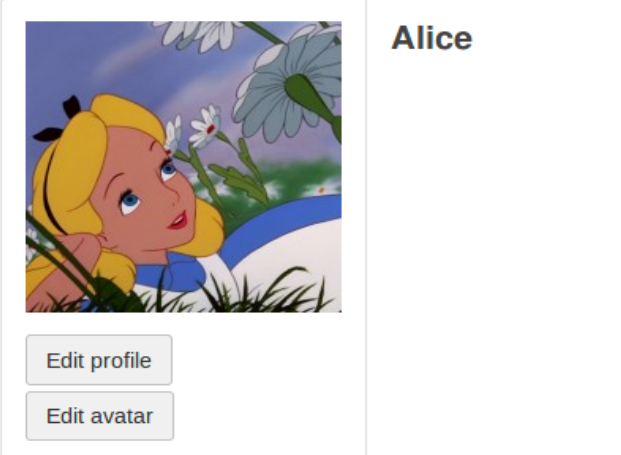
答：不能。因为在无法确定对方的身份，因此不能知道对方的guid.当然，也可以用穷举攻击，遍历所有用户的guid，但这样代价较大。

**Task4:Implementing a countermeasure for** Elgg

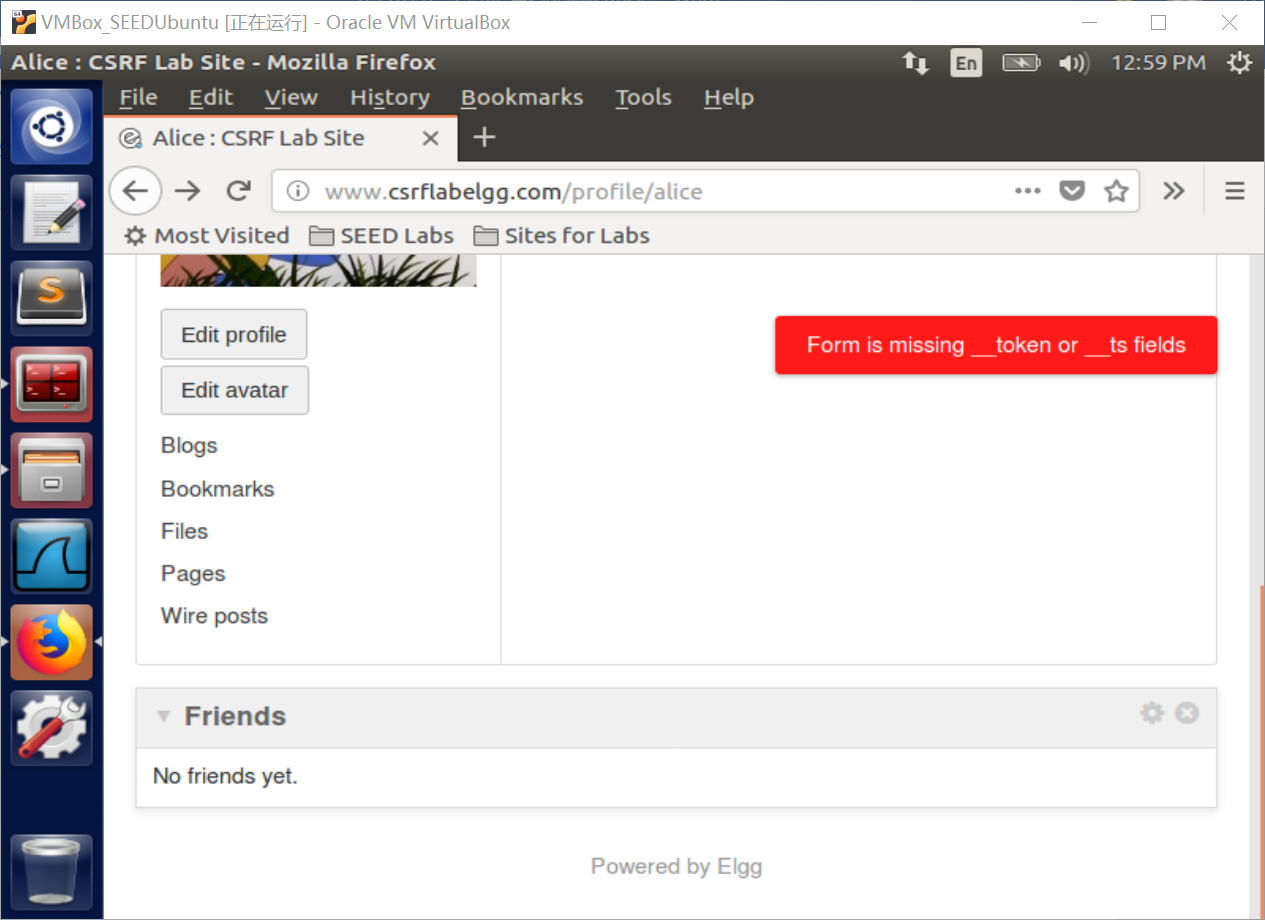
注释掉ActionsService.php中的return true,此时CSRF攻击不成功



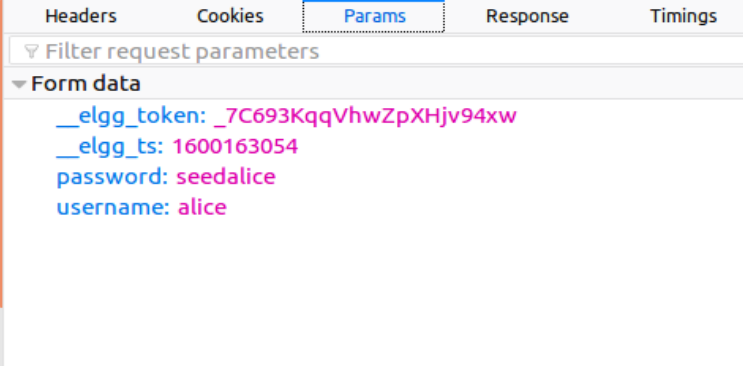
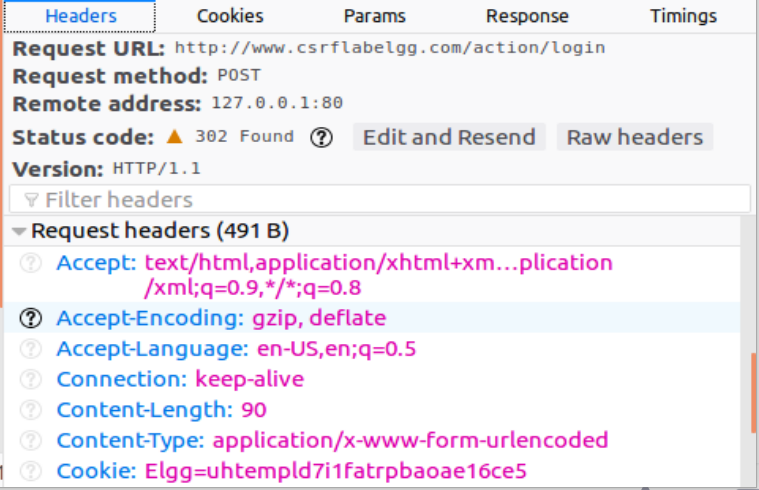
Alice主页未被修改。



Boby 未能成功添加Alice为好友。



Question: 请指出使用Firefox的HTTP检查工具捕获的HTTP请求中的秘密令牌，请解释攻击者在CSRF攻击中为什么不能发送这些秘密令牌，是什么阻止他们从网页中发现秘密令牌?



答：根据提示可以知道，攻击失败的原因是token的缺失。这是因为注释掉return true后，gatekeeper函数可以执行，该函数会调用secret\_token validation函数，secret\_token validation函数中有个存在MD5加密，即便攻击者知道guid，由于密钥缺失，也不能伪造出正确的token。

**实验总结**

这次实验让我对网络攻击有了初步的了解。在实验之前我对HTTP报文不甚了解，为了完成task1我查阅了有关于HTTP报文的资料，对其类型以及格式等等都有了比价清晰的认识。除此之外，我也初步涉及了CSRF攻击的知识，虽然对有些概念一知半解，但仍能在手册的指引下完成实验。完成后回顾让我感觉收获很大。