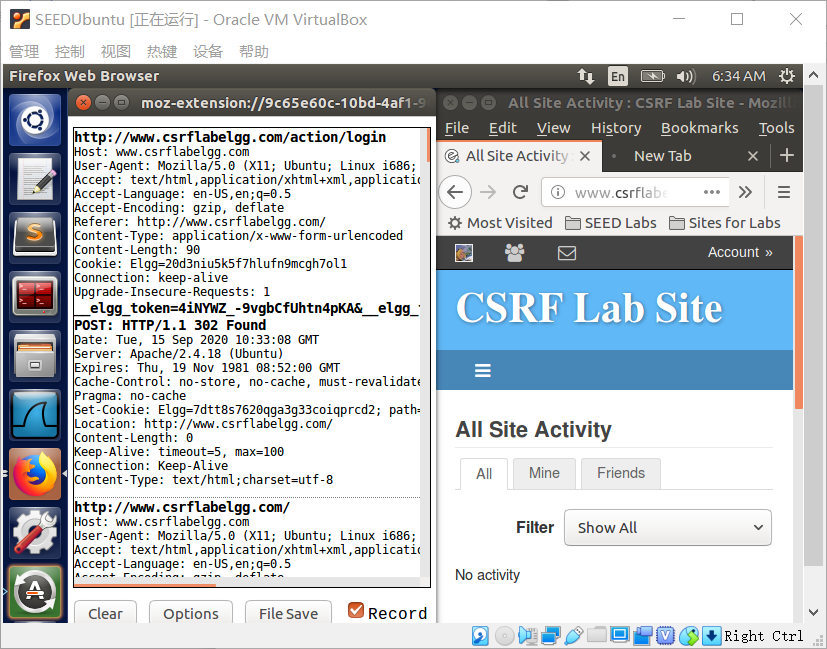
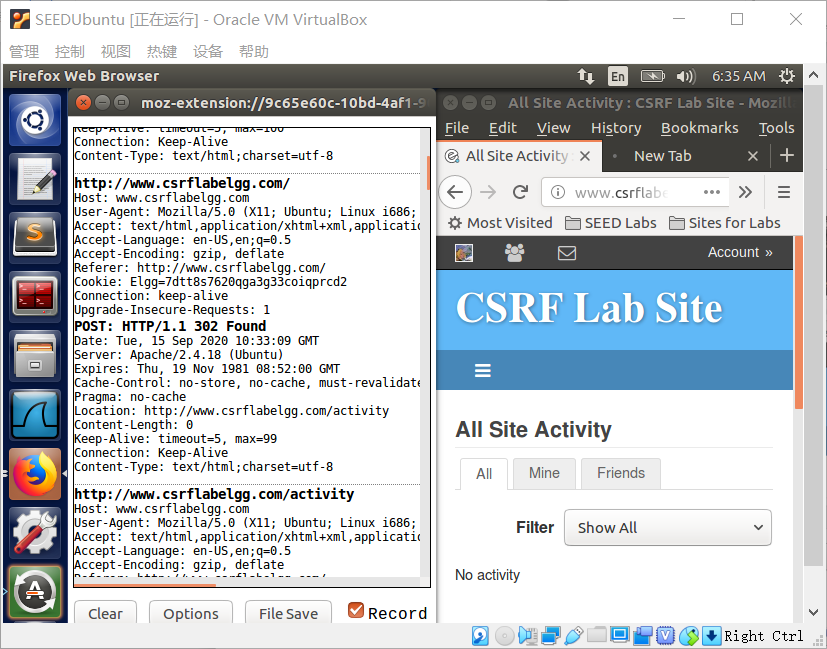
**Cross-Site Request Forgery (CSRF) Attack Lab**

57118135 许皓钦

**Task 1: Observing HTTP Request**

在firefox中打开HTTP Header Live插件，登录[www.csrflabelgg.com](http://www.csrflabelgg.com)。输入用户名和密码，抓取报文。





HTTP POST的参数是\_elgg\_token和\_elgg\_ts

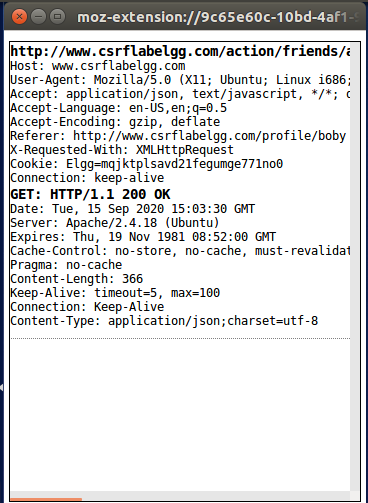


HTTP GET没有参数。

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

首先我们登录admin的账号，打开HTTP Header Live，点击添加boby为好友，通过抓包，我们得到了添加的链接是

http://www.csrflabelgg.com/action/friends/add?friend=43&\_\_elgg\_ts=1600182203&\_\_elgg\_token=NBYLLMbz1FUftz0-cIzV-g&\_\_elgg\_ts=1600182203&\_\_elgg\_token=NBYLLMbz1FUftz0-cIzV-g



然后我们创建一个php文件放到/var/www/CRSF/Attacker文件夹中，php里的代码如下：

<html>

<body>

<h1>this is a page forges an HTTP GET Request.</h1>

<img

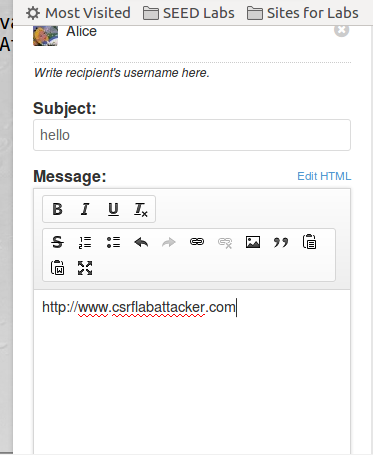
src="http://www.csrflabelgg.com/action/friends/add?friend=42"

alt="image" width="1" height="1" />

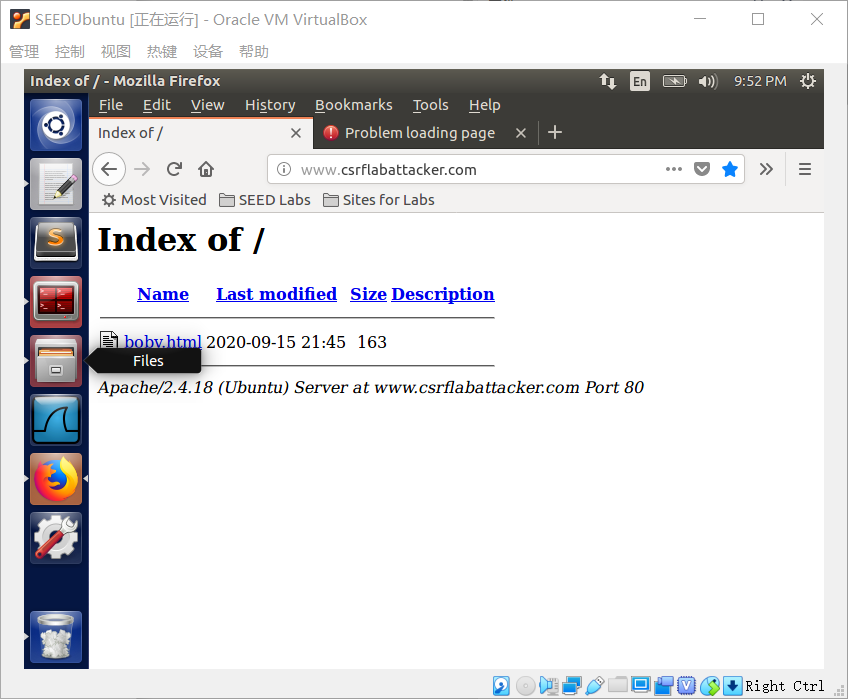
</body>

</html>

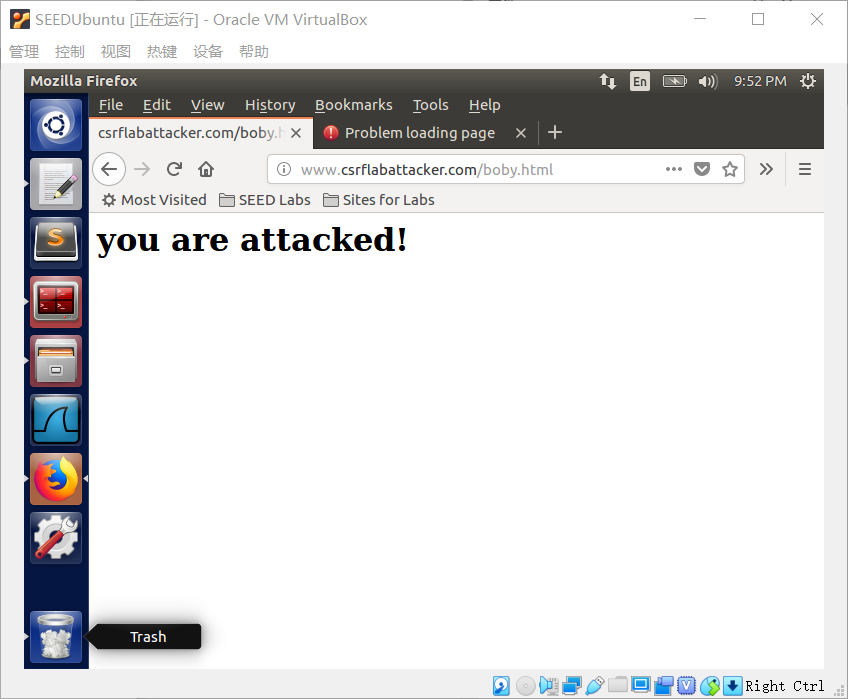
接着我们登录boby的账号发送一个邮件给alice，邮件内容为<http://www.csrflabattacker.com>这个网址。



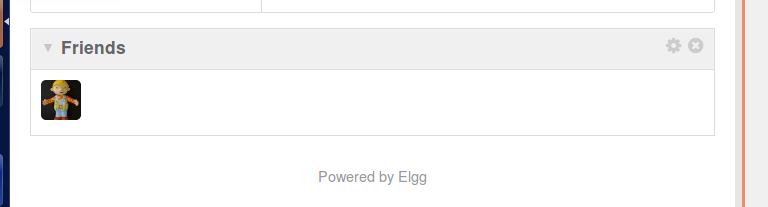
然后我们登录Alice的账号，点击刚才的邮件，出现下面的情况。



点击诱导网页后



最后我们来到Alice的friend里面一看，发现boby已经在里面了。

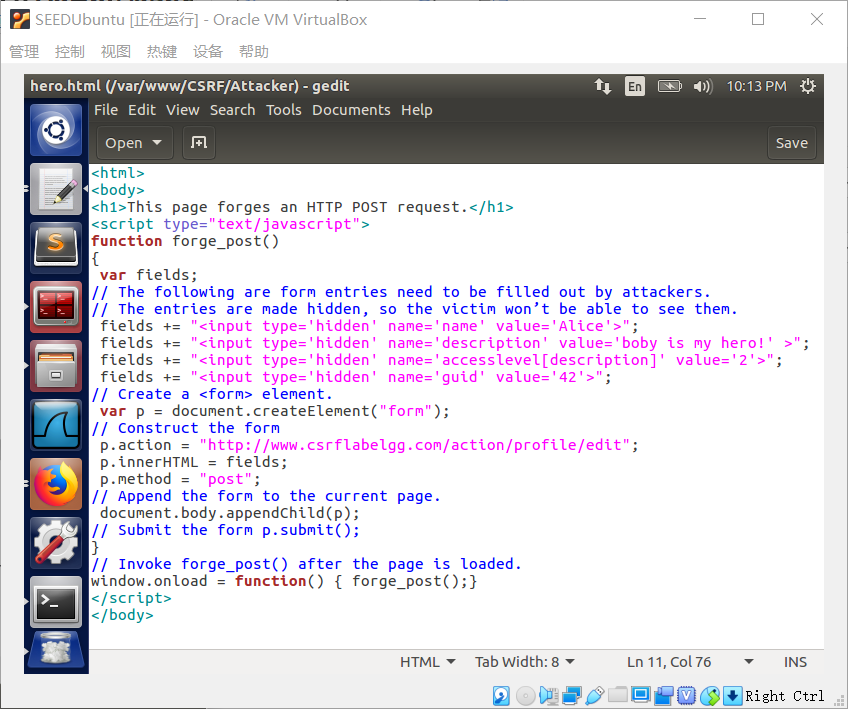


**Task 3: CSRF Attack using POST Request**

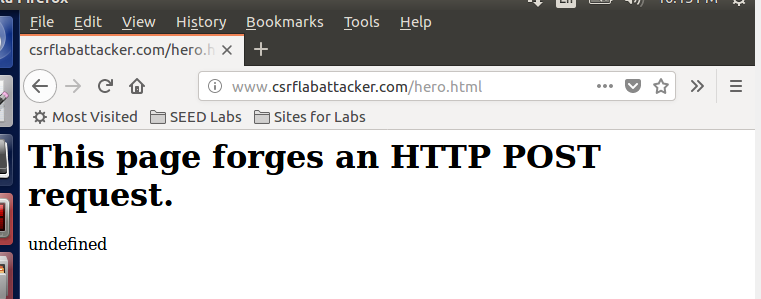
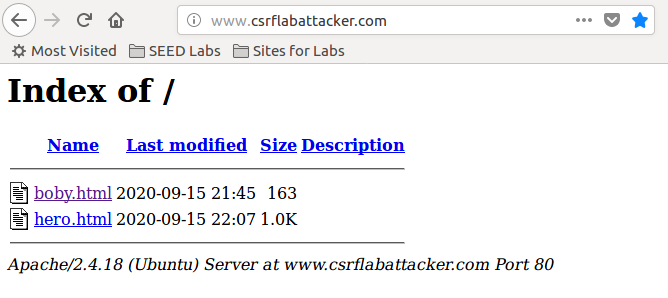
首先用boby的账号访问Alice的主页，抓包获得alice的guid是42



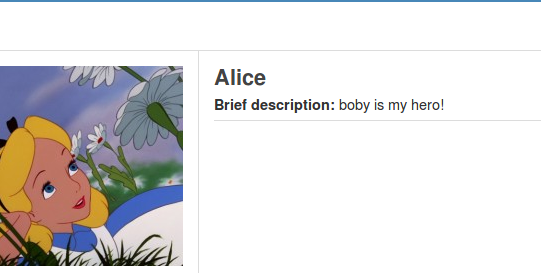
重新编写文件，放在同一目录下，内容如下



再次用boby的账号发送一个邮件给Alice，Alice收到后点开，出现



这时转到profile，Alice查看自己的profile发现已经修改成功



问题1：伪造的HTTP请求需要Alice的用户id (guid)才能正常工作。如果Boby的目标是Alice，在攻击之前，他可以找到获取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。请描述一下是如何解决这个问题的

Boby可以通过HTTP Header Live工具进行抓包，然后登录自己的帐号对Alice进行好友申请，这时候会抓到一个带有Alice账号响应的包，在其中我们可以获得Alice的guid。

问题2：如果Boby想要对访问他的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。他还能发动攻击来修改受害者的Elgg档案吗

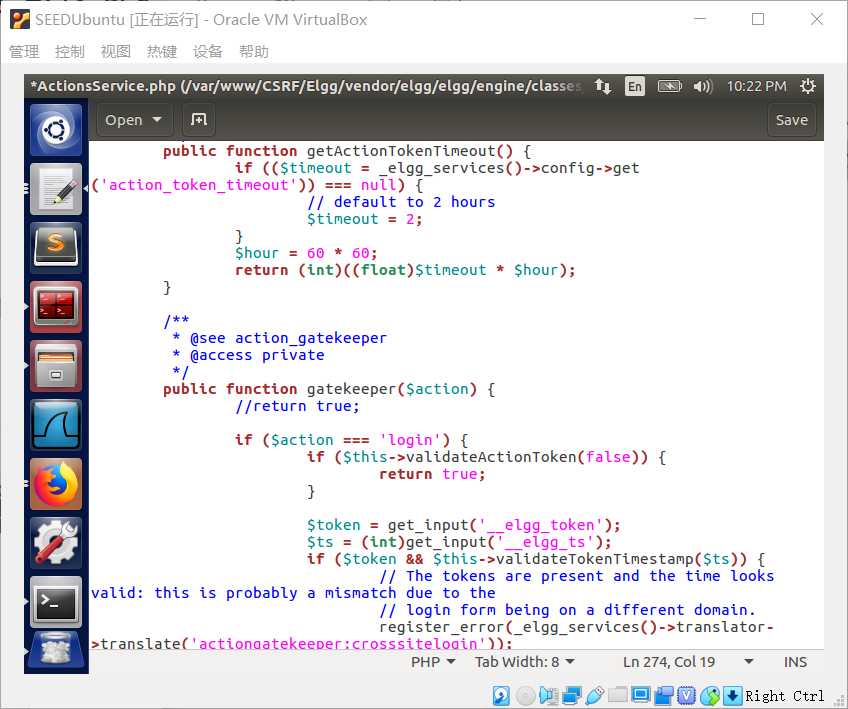
可以。首先，要使CSRF攻击成功的前提是必须拥有用户的guid，我们可以通过使用csrf来先获取用户的guid，然后自动提交到guid的位置，这样不论是谁，只要他没有退出elgg系统，同时访问了我们的攻击url就会自动编辑他们的资料。

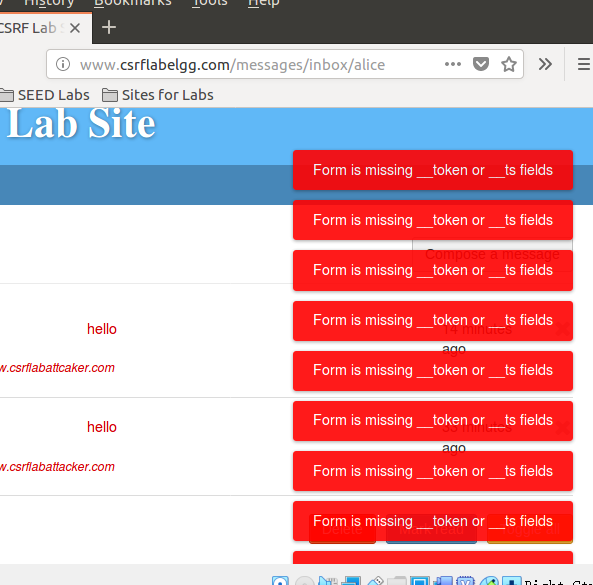
**Task 4: Implementing a countermeasure for** Elgg

在/var/www/CSRF/Elgg/vendor/elgg/elgg/engine/classes/Elgg

目录下找到ActionsService.php文件，找到函数gatekeeper()，注释掉return true;这句话。

然后重新进行上面的攻击。





在添加注释之后，开启了Elgg对CSRF的防御措施，重复task 2 3的实验，发现CSRF攻击无效

这是因为elgg应用程序验证生成的令牌和时间戳来抵御CSRF攻击，每一个用户都有一个验证机制，如果令牌不存在或失效，用户操作将被拒绝并被重定向。