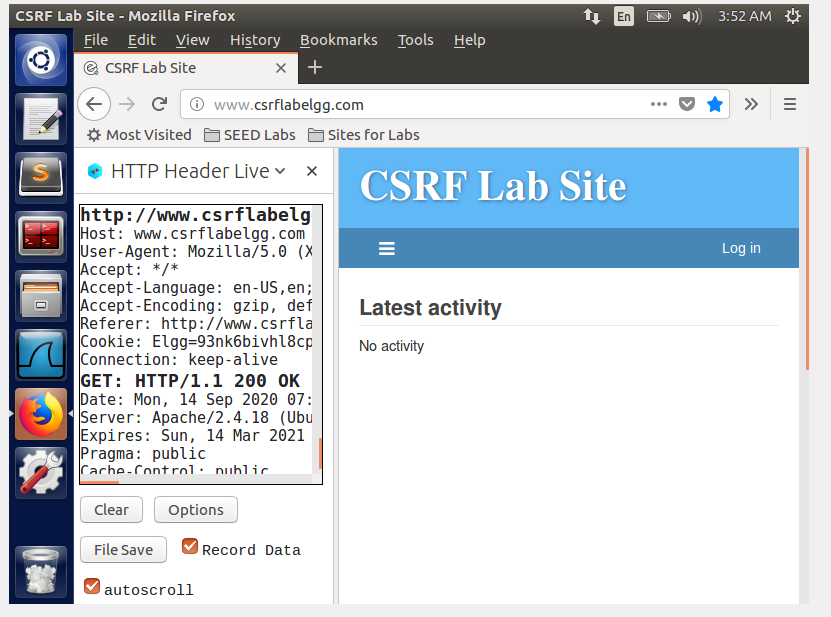
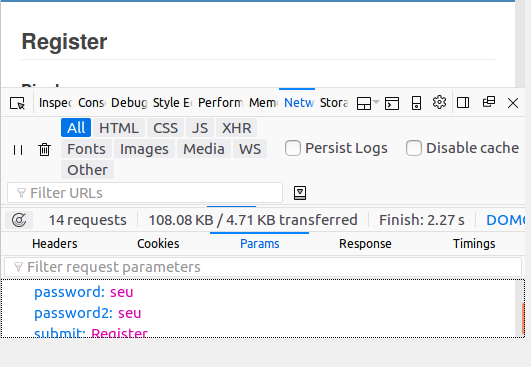
**Lab 4**

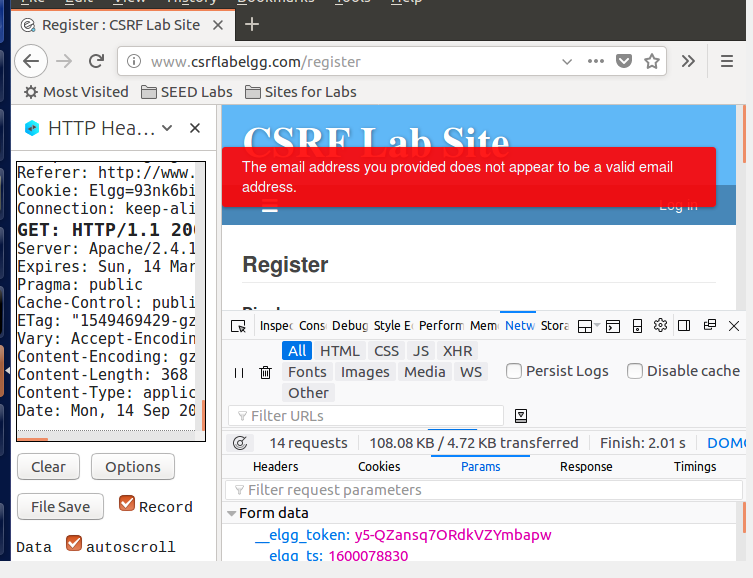
57118110 杨紫瑄

**Task1: Observing HTTP Request.**

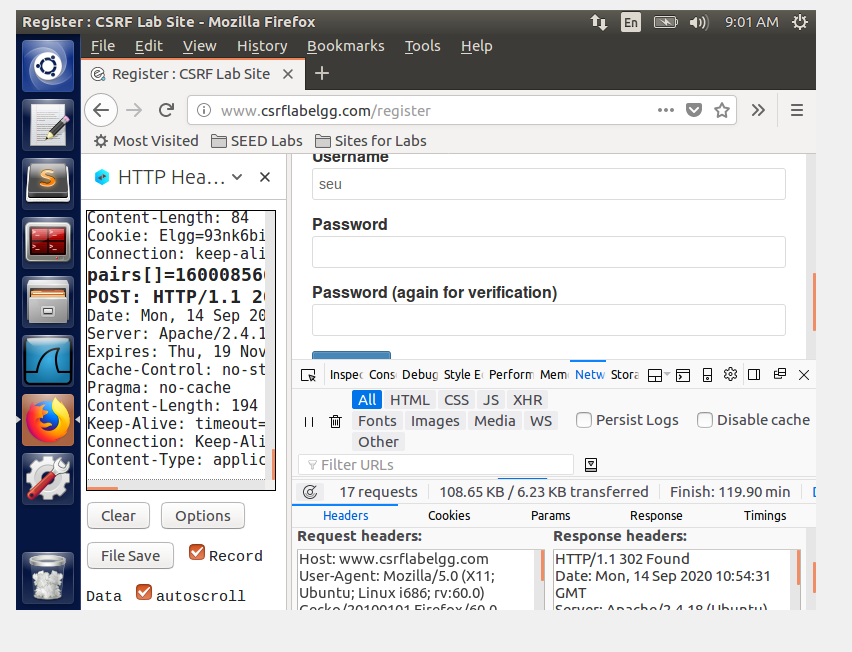


首先获取了HTTP Header Live插件登录[www.csrflabelgg.com](http://www.csrflabelgg.com)并进行抓包



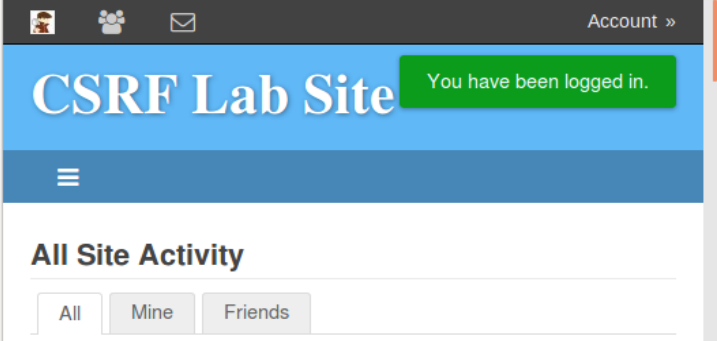


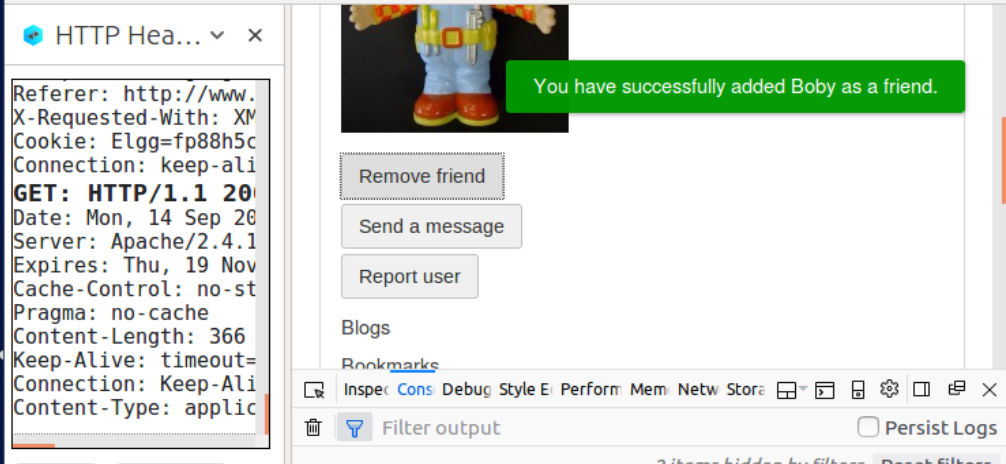
可以通过查看params和旁边HTTP Header Live的抓包查看POST报文

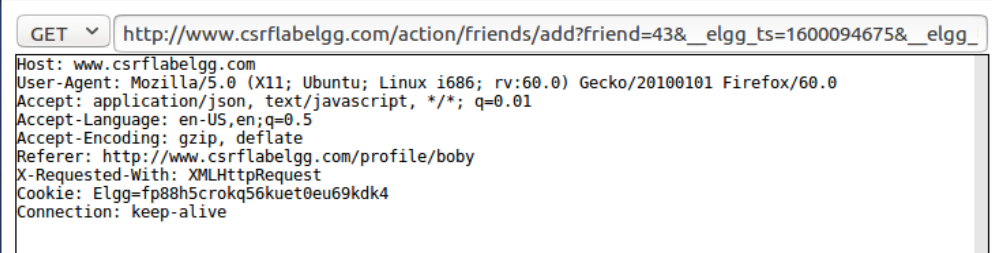


 **Task2: CSRF Attack using GET Request**

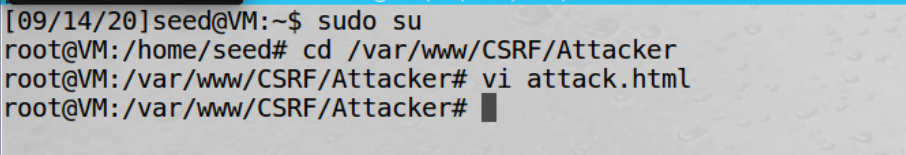
首先登录Charlie账号，然后添加Boby为好友：



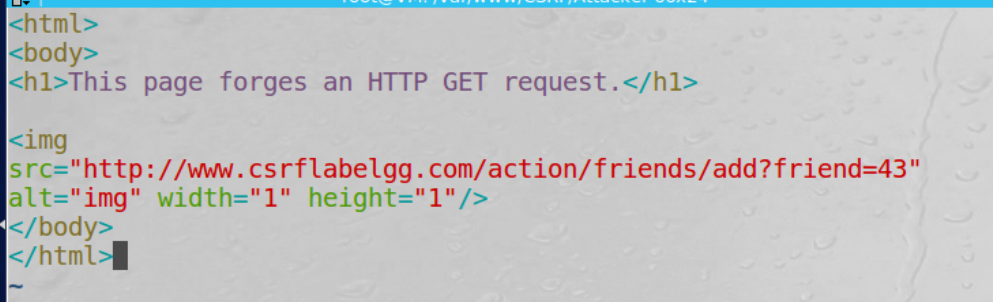




使用HTTP Header live抓包后得到boby的ID为43

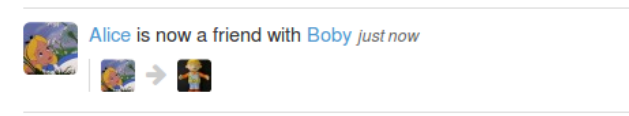


在文件夹/var/www/CRSF/Attacker中新建文件attack.html



登录Boby账号并向Alice发送邮件，内容为http://www.csrflabattacker.com/attack.html





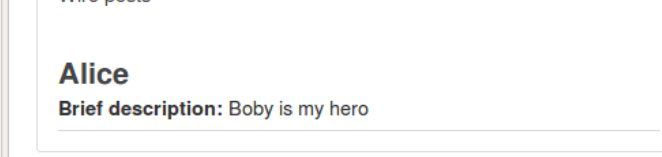
Alice点开连接后自动添加Boby为好友

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

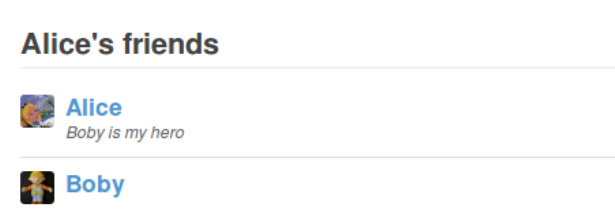
首先，登录Boby账号访问Alice主页，通过HTTP Header Live 抓包发现Alice的ID为42



在/var/www/CRSF/Attacker文件夹中新建test.html，修改Alice的description为‘Boby is my hero’



并再次向Alice发送邮件及链接，当Alice再次点开链接，发现Alice的简介自动被修改。



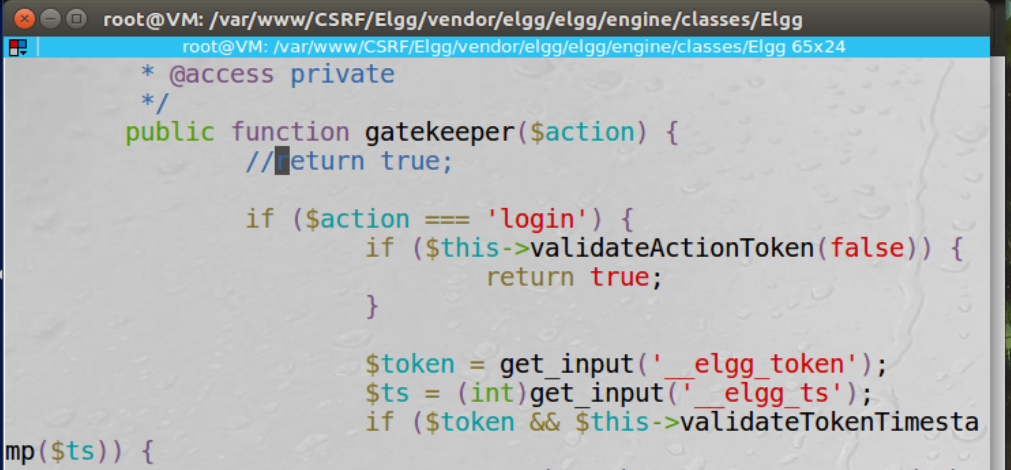
问题1: 伪造的HTTP请求需要Alice的用户id (guid)才能正常工作。如果Boby目标  
特别是Alice，在攻击之前，他可以找到获取Alice的用户id的方法。Boby不知道Alice的Elgg密码，所以他无法登录Alice的账户获取信息。请描述如何解决这个问题。

答：Alice输入账号密码成功登录Elgg后，网页保存了Alice的cookie，Alice点开Boby发送的恶意网站链接后，浏览器就携带Alice登录后认证通过的cookie信息访问这个恶意链接的网站，就会执行恶意请求，Boby可通过一些抓包软件抓取到Alice的用户信息。

•问题2:Boby是否想对访问其恶意网页的任何人发起攻击。在这种情况下，他事先并不知道谁正在访问网页。他还能发动CSRF攻击来修改受害者的Elgg档案吗?请解释

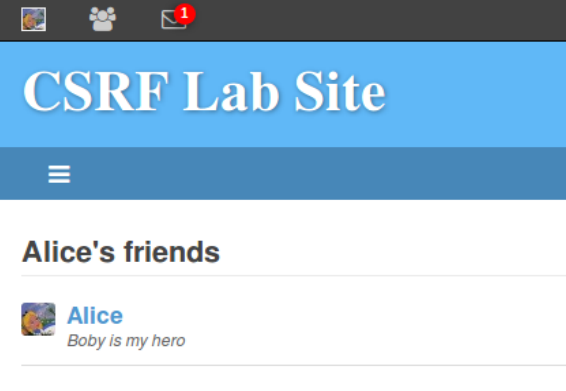
答：可以。用户登录账户的信息被存在了cookie里，Boby可以在不知道验证信息的情况下直接利用用户自己的cookie来通过安全验证，从而进入该用户账号来修改其Elgg档案。

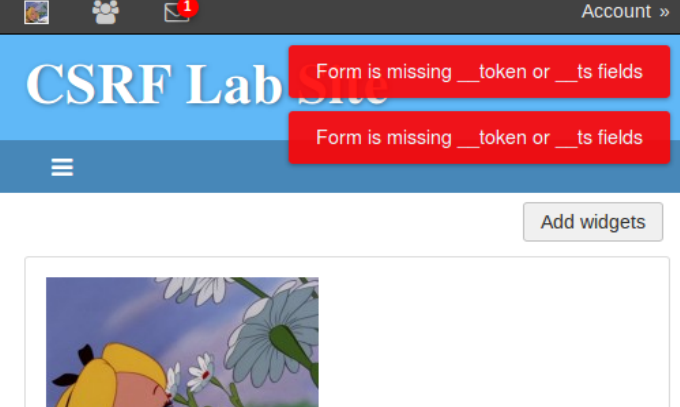
**Task 4: Implementing a countermeasure for Elgg**

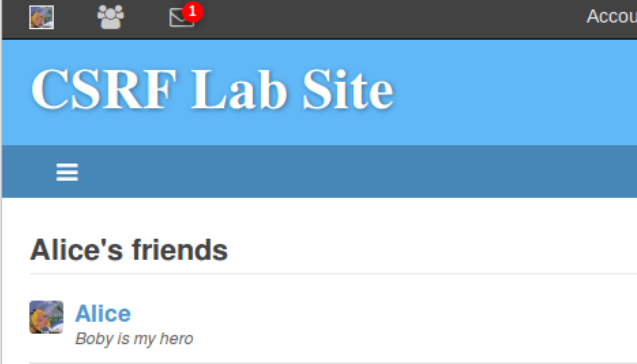


进入/var/www/CSRF/Elgg/vendor/elgg/engine/classes/Elgg.ActionsService.php文件，修改注释return true来关闭Elgg的防护措施，之前实际上是让所有的请求都通过验证。注释之后如果重复之前的攻击，攻击会失败。

再重复之前的攻击，登录Alice账号删除Boby好友，再点击恶意链接



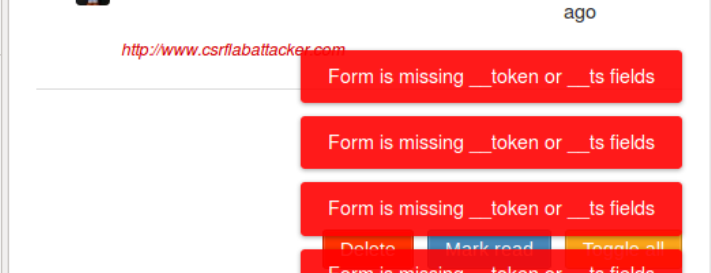


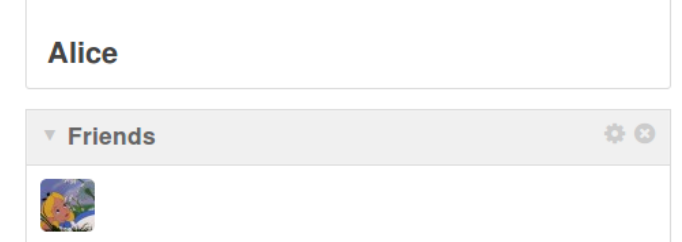


网页提示丢失\_\_elgg\_ts和\_\_elgg\_token，并且Alice没有成功添加Boby好友



删除Alice的简介，并点击恶意链接





也出现了同样的错误并没有编辑成功

问题：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：根据显示的错误可知，攻击失败的是因为token的缺失，因为注释掉return true后，Elgg保护措施关闭，重复之前的攻击就会失败。浏览器的访问控制机制会阻止攻击者的恶意网页的JavaScript代码访问Elgg页面，也就能够阻止他们从网页中发现秘密令牌。

实验总结：本次实验让我们了解了CSRF的攻击和防御机制，通过此次的学习，我对网络安全有了更深和更实际的认识，也充分认识到恶意代码的可怕。在此次试验中一开始因为对于实验环境的不熟悉，遇到了一些困难，但是在请教助教，同学和查阅资料后都得到了解决。