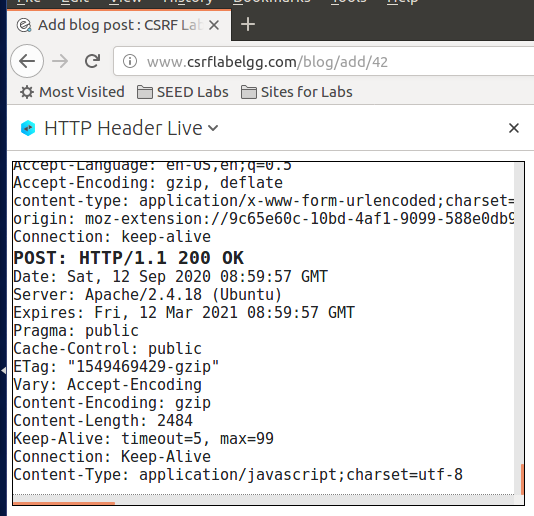
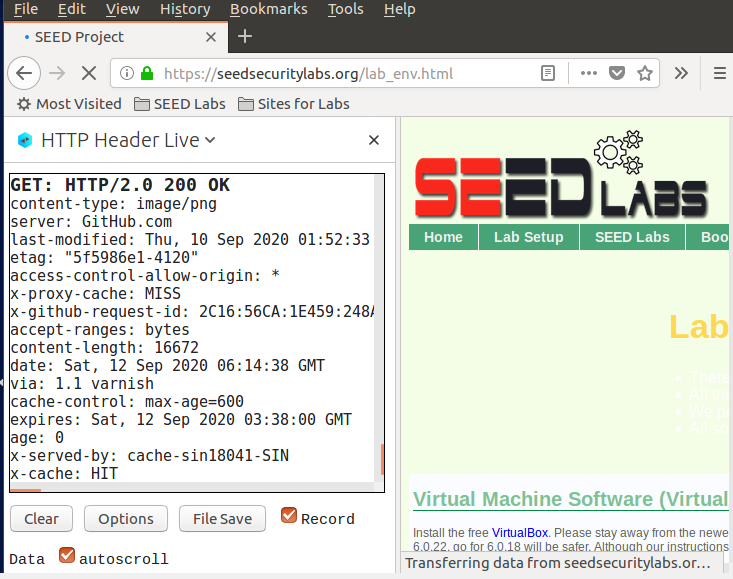
**Cross-Site Request Forgery Attack Lab**

**——57118125施祺**

**Task 1:Observing HTTP Request**

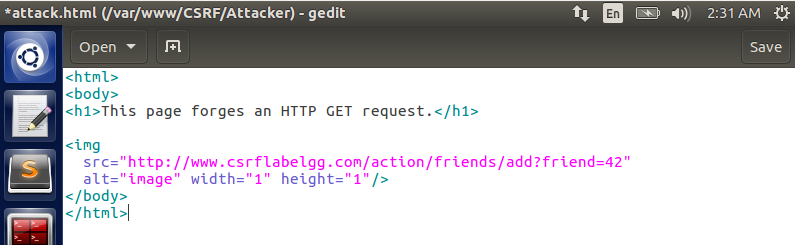
在firefox中打开HTTP Header Live插件，再点击网页任意一个按钮，即可抓取HTTP请求报文。



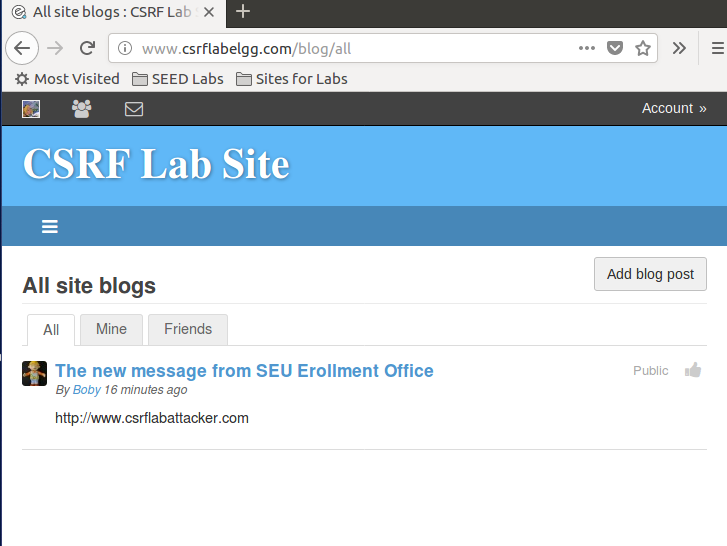
**Task 2: CSRF Attack using GET Reques**t

在文件夹/var/www/CSRF/Attacker文件夹中创建一个html文件，在其中写入制作好的网页。

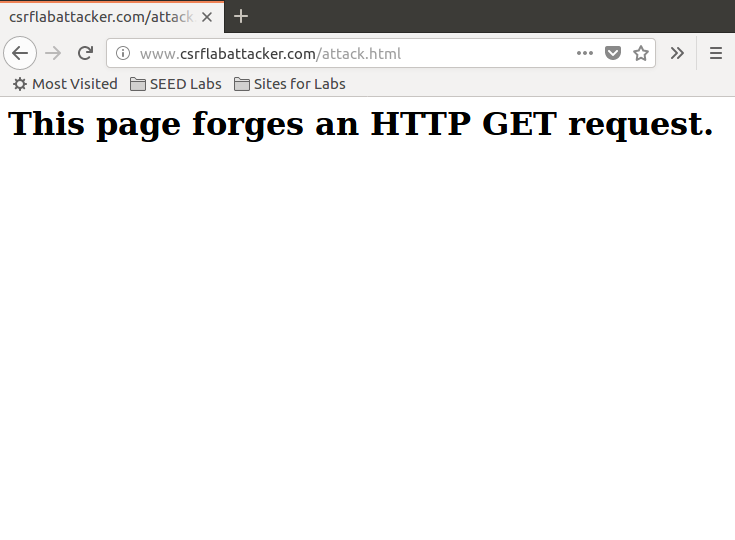
Img标签将自动触发一个HTTP GET请求。这个标签是用于将图像包含进网页中的。当浏览器在显示网页的过程中遇到img标签时，它会自动向由src属性的URL发送一个HTTP GET请求。这个URL是任意的，因此可以是跨站的，这样就允许一个网页包含其他网站的图像。该URL并没用返回图像，为了不让目标用户起疑，故意设置图像的大小为1\*1像素，非常微小，难以被发现。

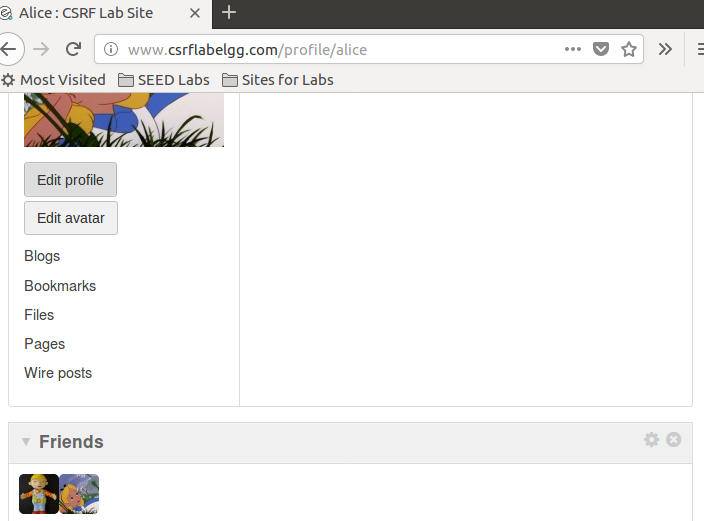


我们登录Boby的账号，发表一篇博文，标题为SEU教务处的通知，博客内容为恶意网站，以此吸引Alice点击。



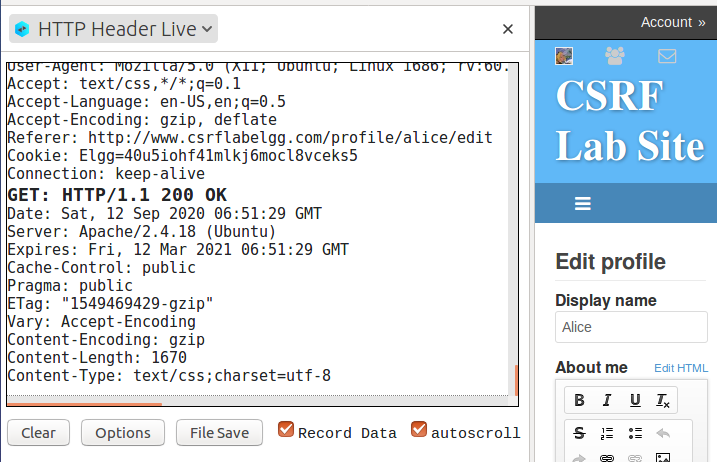
点击成功后界面显示如下，说明Alice已经成功掉入了圈套。



再次查看Alice的朋友列表，可以发现多了Boby，说明CSRF攻击成功。

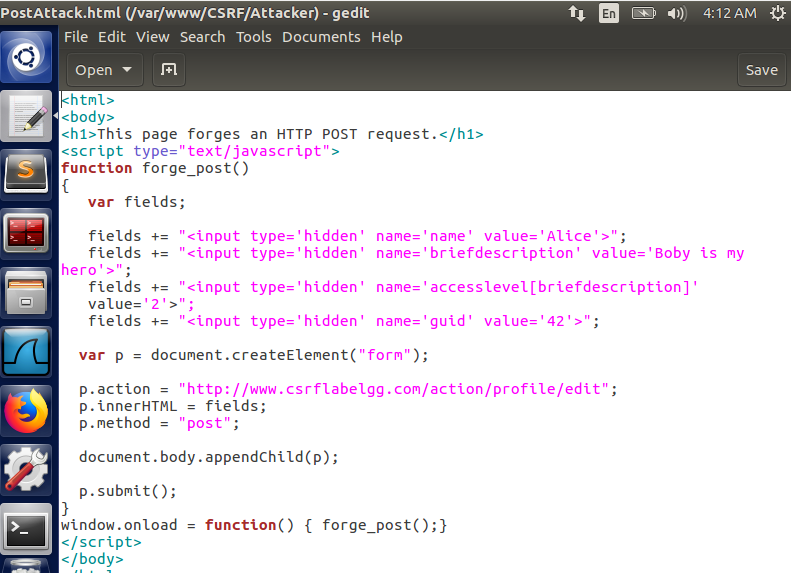
**Task 3: CSRF Attack using POST Request**

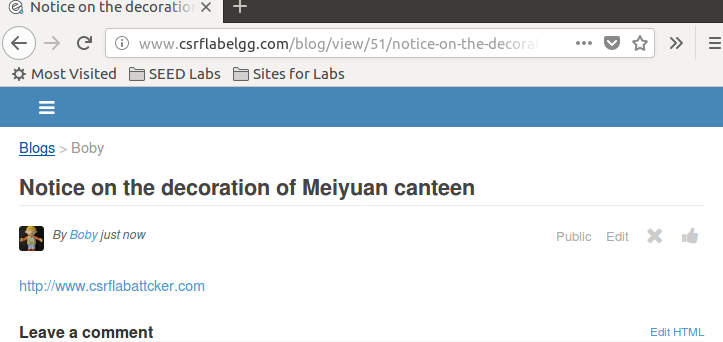
利用Header Live插件，我们可以得到Alice的guid为42。

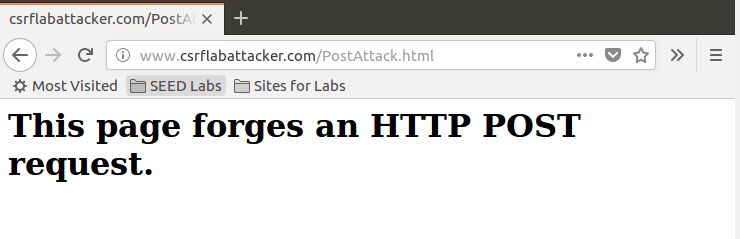


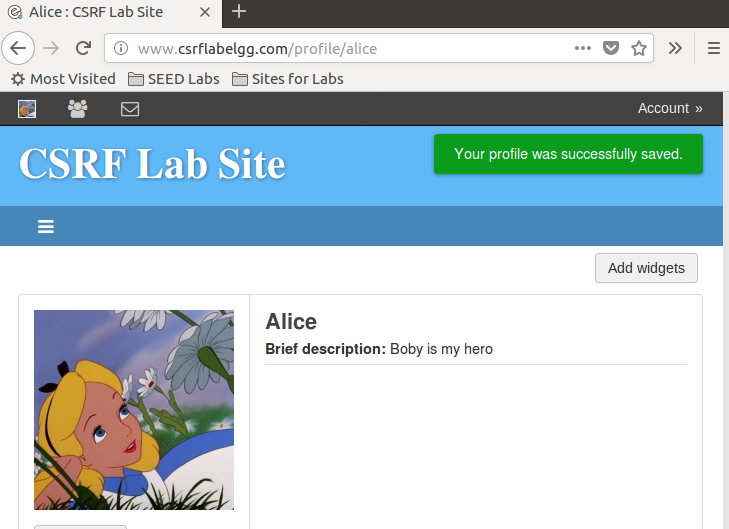


我们使用HTML代码构建一个恶意网页PostAttack.html，并将其存储到/var/www/CSRF/Attacker目录中，具体代码内容如下：

接下来我们登录Boby的账号，发布一个带有恶意网站信息的blog。



登录Alice的账号点击该网页，HTTP POST攻击启动。

再次返回，我们可以看到Alice的个人资料已经被修改。

**有关问题的回答：**

**Question1:**

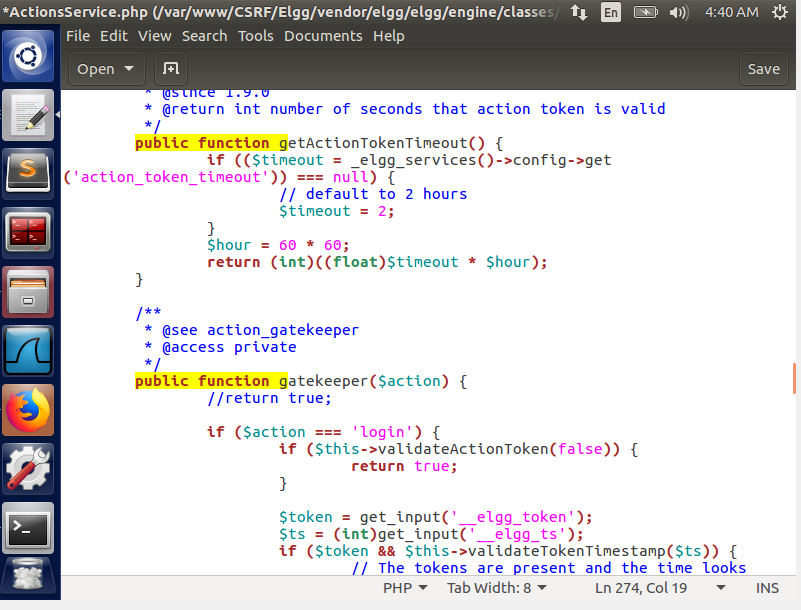
Boby可以通过HTTP Header Live工具进行抓包，然后登录自己的帐号对Alice进行好友申请，这时候会抓到一个带有Alice账号响应的包，在其中我们可以获得Alice的guid。

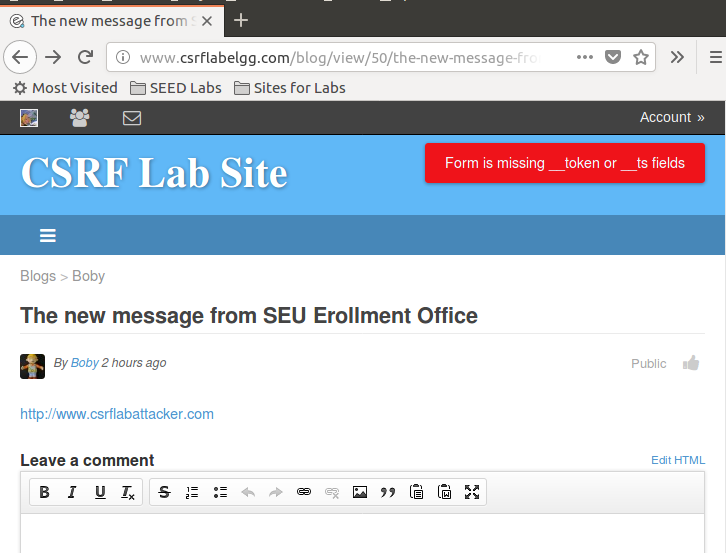
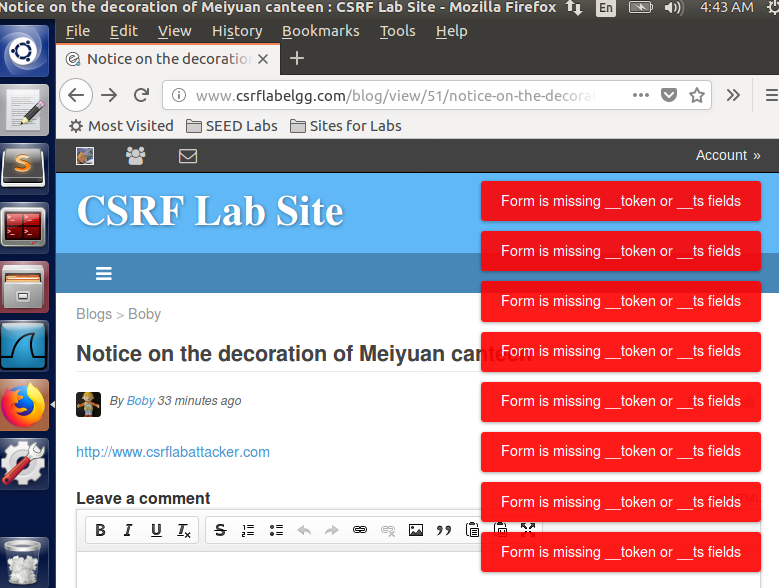
**Question2:**

不可以。CSRF攻击是通过html代码来实现，而代码中明确写入了被攻击者的guid。如果陌生人点开这个恶意网站，由于没有他的guid，因此攻击也无法进行。

**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，打开进行编辑，找到函数gatekeeper()，注释掉return true;这句话。





再次执行CSRF攻击，可以看到攻击失效，原因是缺少\_token or \_ts fields。

**原因分析：**

Elgg使用了秘密令牌来抵御CSRF攻击，在它的所有页面都内嵌了两个机密值：\_\_elgg\_ts和\_\_elgg——token。Elgg的安全令牌是一条包含4条信息的MD5摘要：网站机密值、时间戳、用户会话ID以及一个随机生成的会话字符串，在处理每个用户请求之前都会验证安全令牌。如果用户请求没有提供安全令牌或者安全令牌无效，那么该请求会被拒绝。因此，在该实验中，攻击者需要了解秘密令牌的值以及目标用户的Elgg页面内嵌的时间戳。然而，浏览器的访问机制会组织攻击者网页的JS代码访问Elgg页面的任何内容。