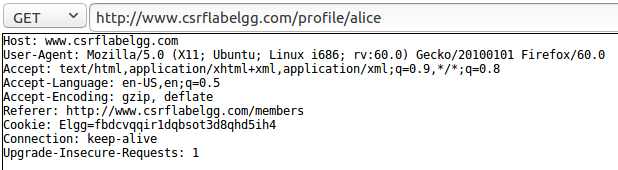
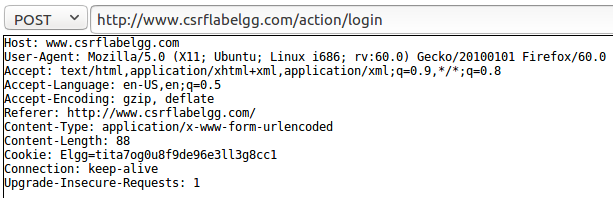
**Lab[4]-report**

57118123刘康辉

**Task 1**



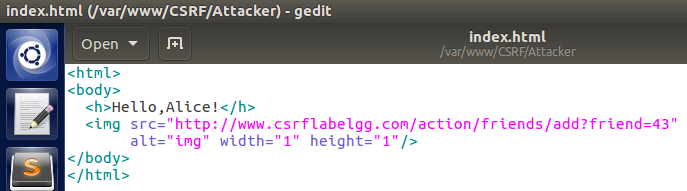


抓取的HTTP GET和POST请求如上图所示，使用的参数有Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Referer、Cookie、Connection以及Content-Type、Content-Length等。

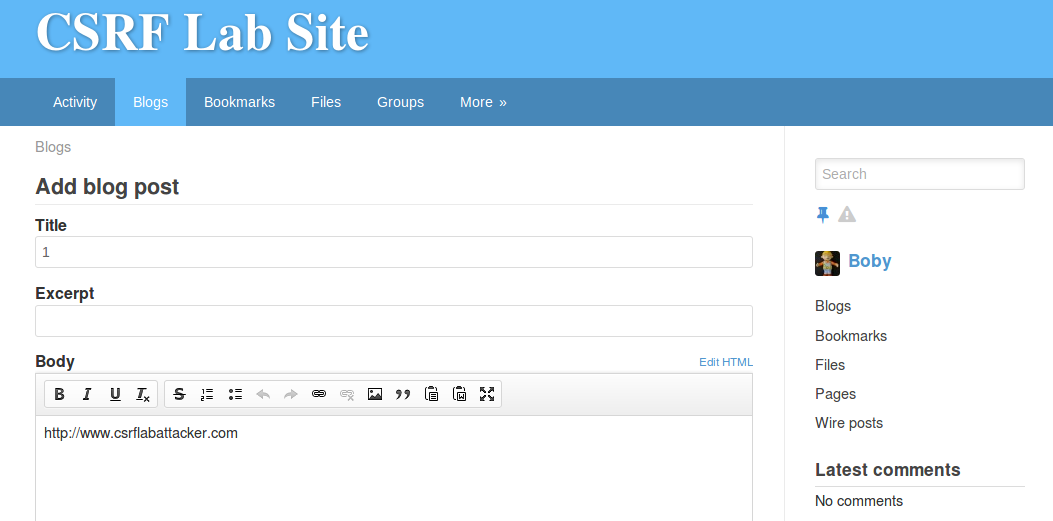
**Task 2**



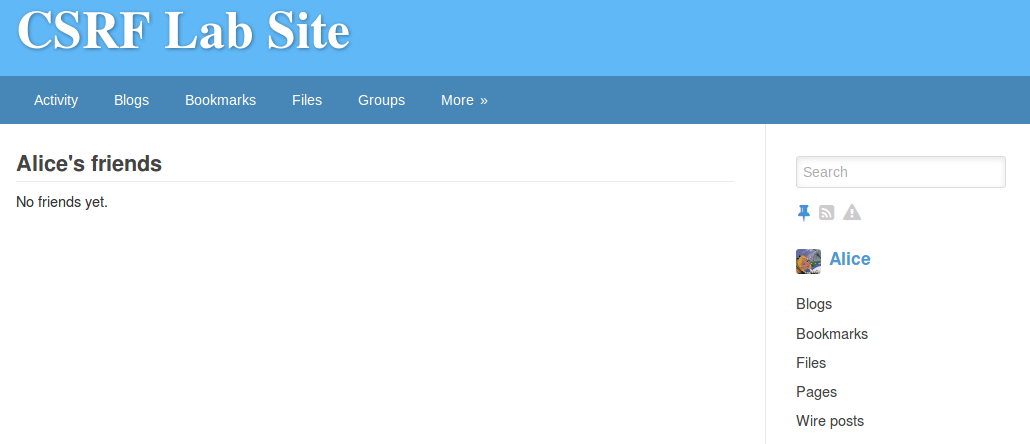
抓取的添加好友的HTTP GET请求如上图所示。



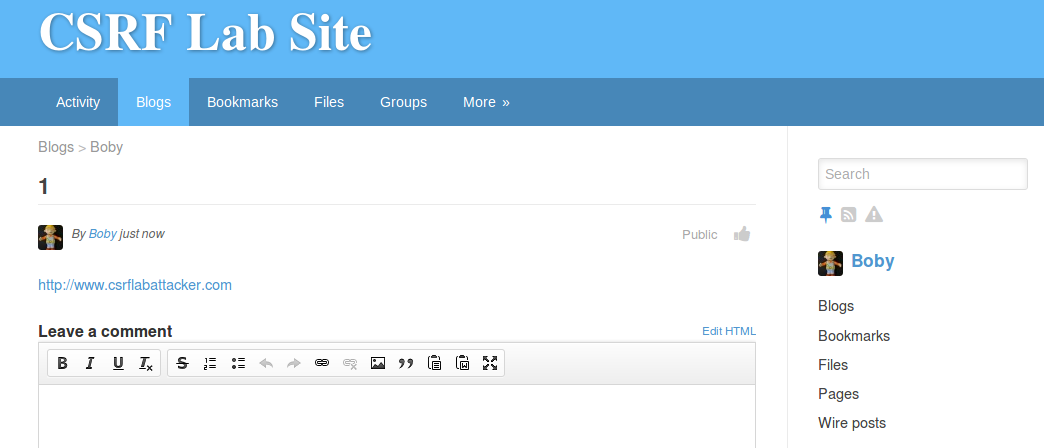
在/var/www/CSRF/Attacker/下创建文件index.html，并且添加代码如上图所示。



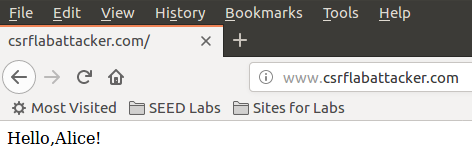
登录Boby的账户，发布blog，其中内容如上图所示。

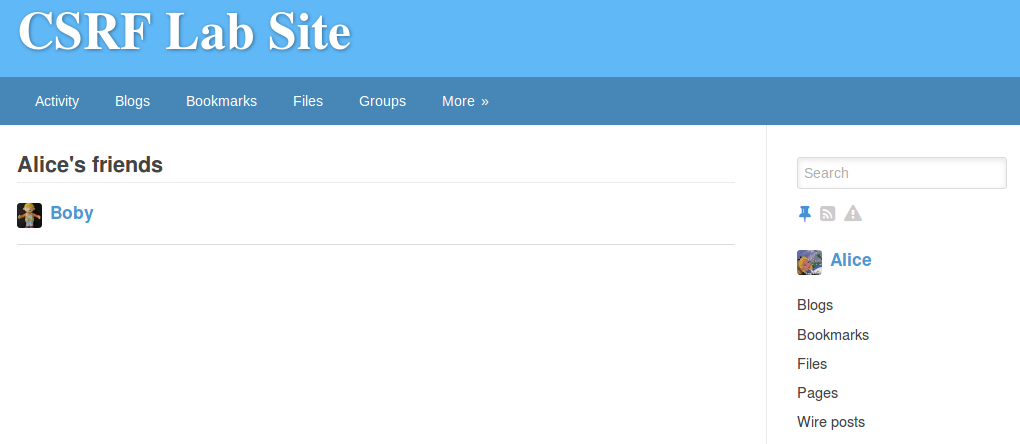


登录Alice的账户，进入好友界面发现未添加好友。



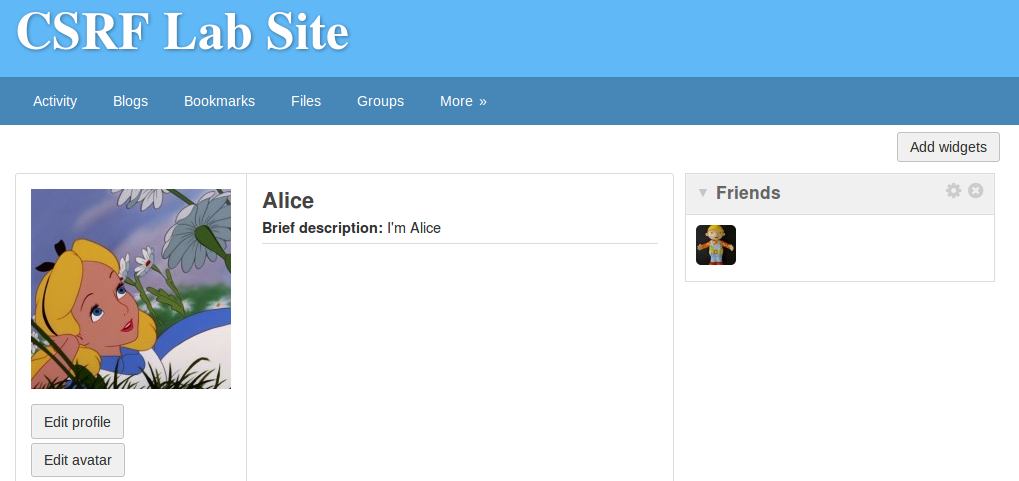
Alice打开Boby的blog，并且点击链接。





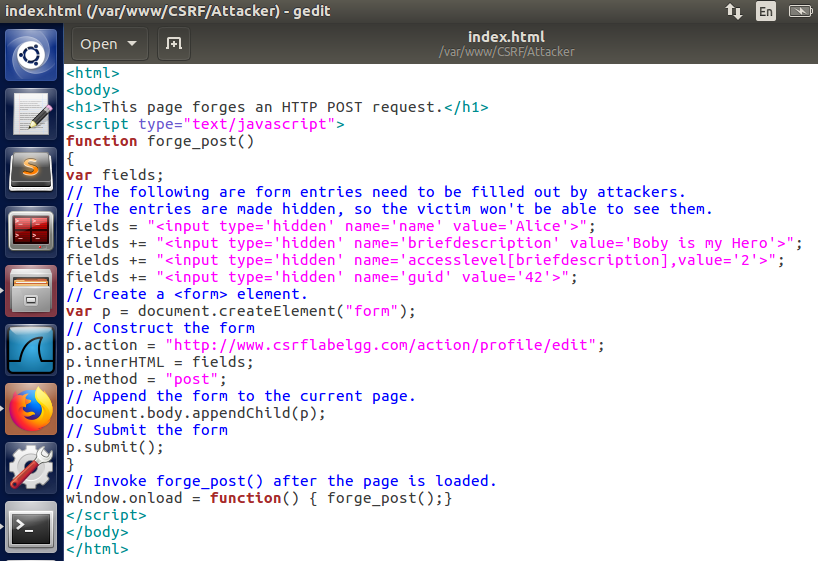
页面会跳转到[www.csrflabarracker.com](http://www.csrflabarracker.com)，然后回到Alice的好友界面发现已经添加了Boby为好友。根据实验结果可知，使用HTTP GET请求的CSRF攻击成功。

**Task 3**

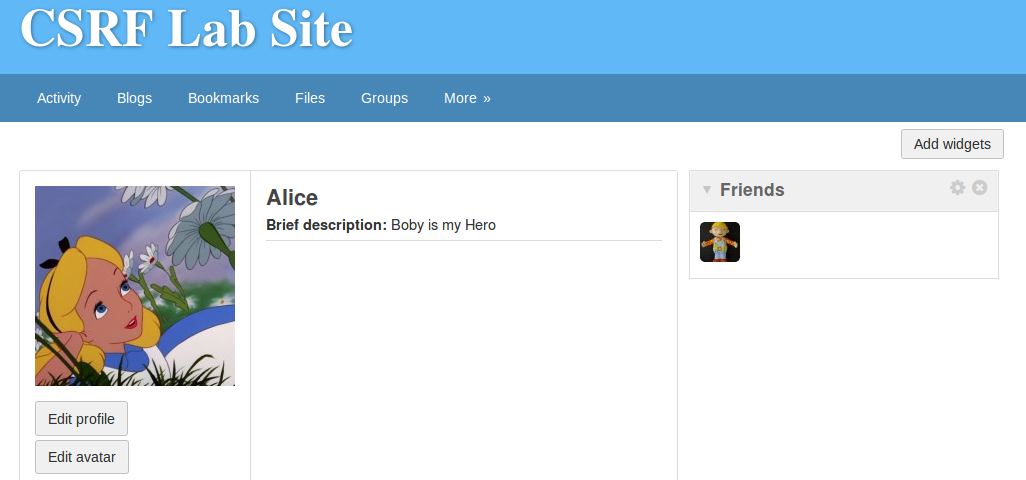




登录Alice的账户，修改签名并且抓取查看HTTP POST请求。



修改文件/var/www/CSRF/Attacker/index.html，并且代码如上图所示。



打开Boby的blog，并且点击链接，页面会跳转到[www.csrflabarracker.com](http://www.csrflabarracker.com)然后自动跳回，发现签名已经被修改为Boby is my Hero。根据实验结果可知，使用HTTP POST请求的CSRF攻击成功。

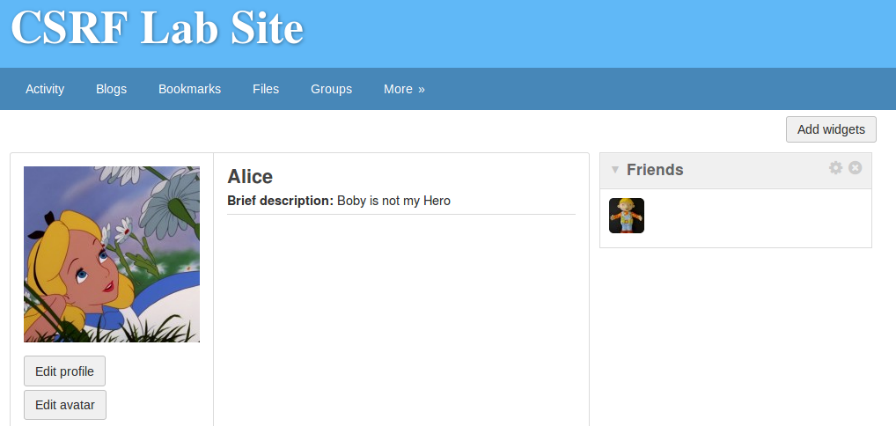
**Question 1**

Boby可以先把Alice添加到自己的好友列表，抓取添加好友的HTTP请求，查看friend参数指明的用户id，即为Alice的用户id，再利用此用户id就能够实现CSRF攻击。

**Question 2**

不能；因为Boby的CSRF攻击需要使用到用户姓名及其id，而在不知道访问该网站的用户身份的情况下，更难以获得其用户id。只有当访问该网站的用户姓名及其id与网站中的相一致时，才能实现CSRF攻击，修改受害者的用户资料，否则无法实现CSRF攻击。

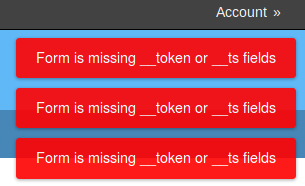
**Task 4**



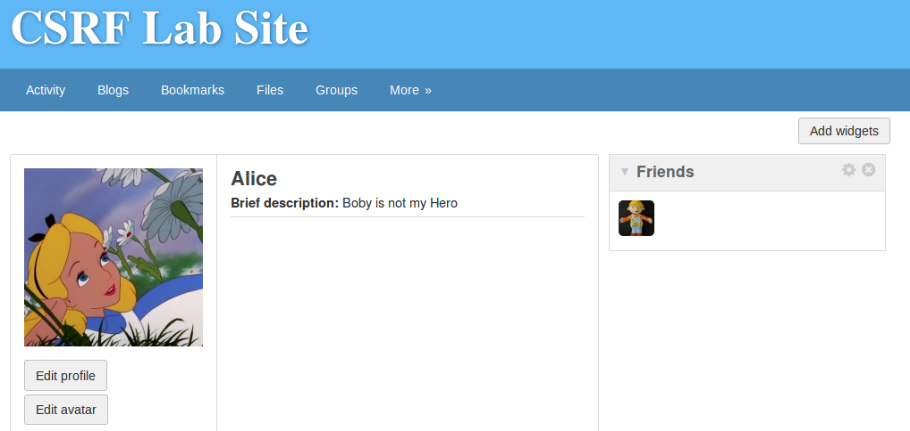
登录Alice的账户，修改签名如上图所示。



修改/var/www/CSRF/Elgg/vendor/elgg/elgg/engine/classes/Elgg中的文件ActionsService.php，注释掉gatekeeper()函数中的return true，如上图所示。



打开Boby的blog，并且点击链接，页面会跳转到[www.csrflabarracker.com](http://www.csrflabarracker.com)后不断自动刷新，退出后发现右侧会提示错误。



返回Alice的个人信息界面查看签名发现没有被修改。根据实验结果可知，防御手段成功。



在完成防御手段后，再次尝试CSRF并且抓取查看HTTP POST请求，可知秘密令牌是\_elgg\_ts和\_elgg\_token，并且非常复杂，攻击者难以猜测。通过修改上述的gatekeeper()函数，使得请求需要提供正确的安全指令才不会被拒绝，而浏览器的访问控制机制会阻止攻击者在网页中寻找秘密令牌。因此，CSRF攻击会失败。