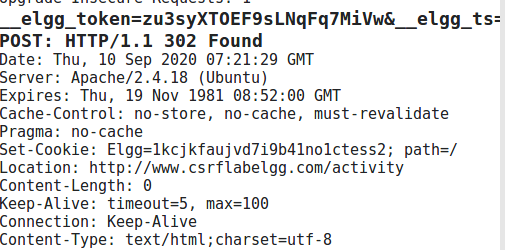
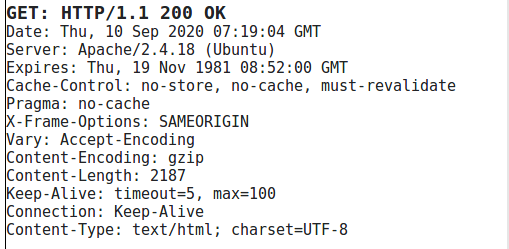
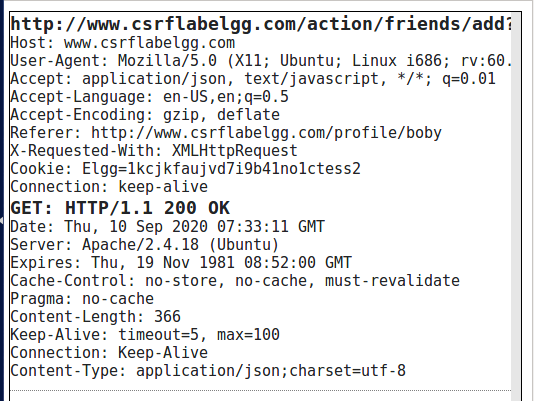
Task1:

抓到的HTTP GET请求和HTTP POST如下

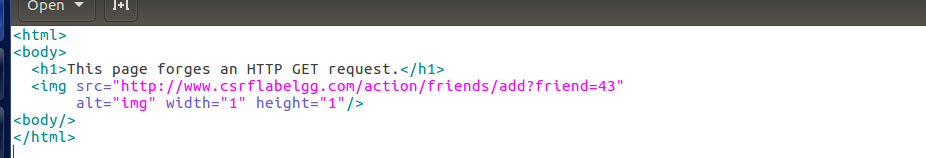


Task2:

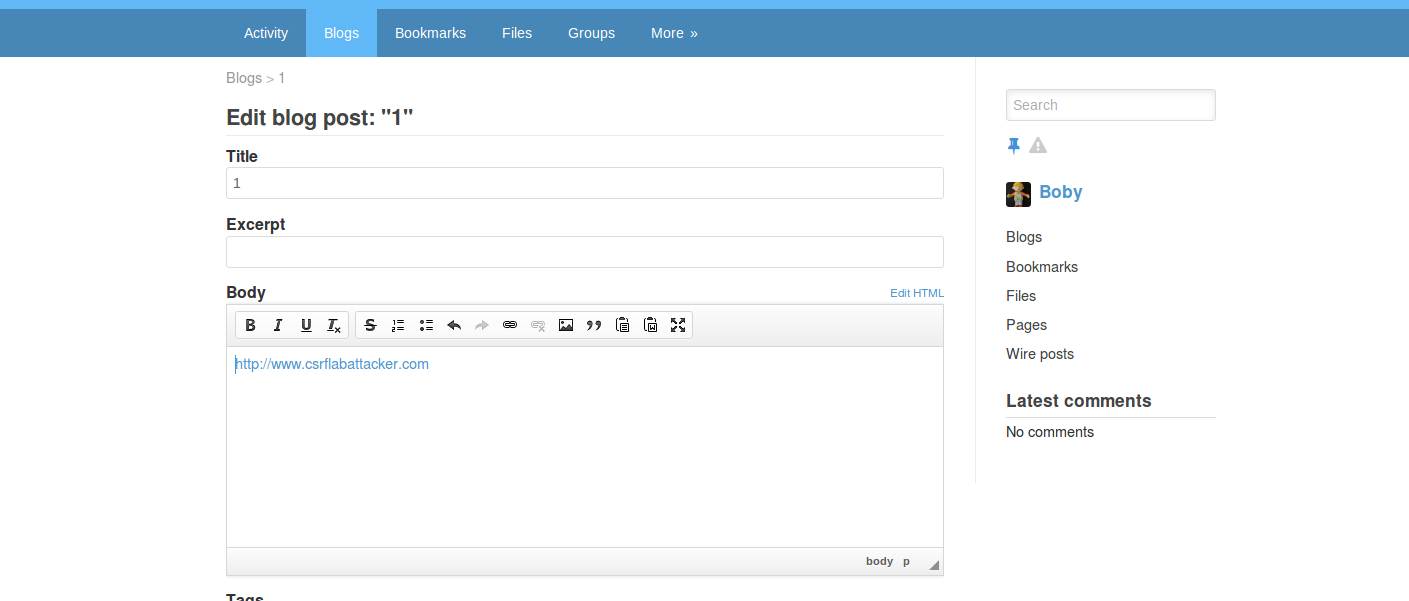
抓到添加好友的GET请求如图



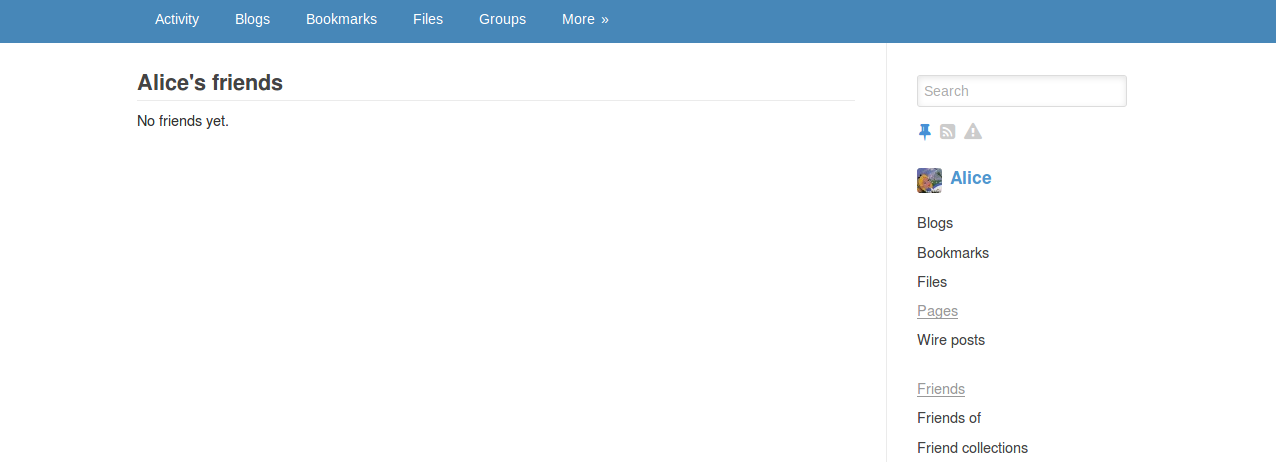
在目录/var/www/CSRF/Attacker/下添加index.html，代码如图



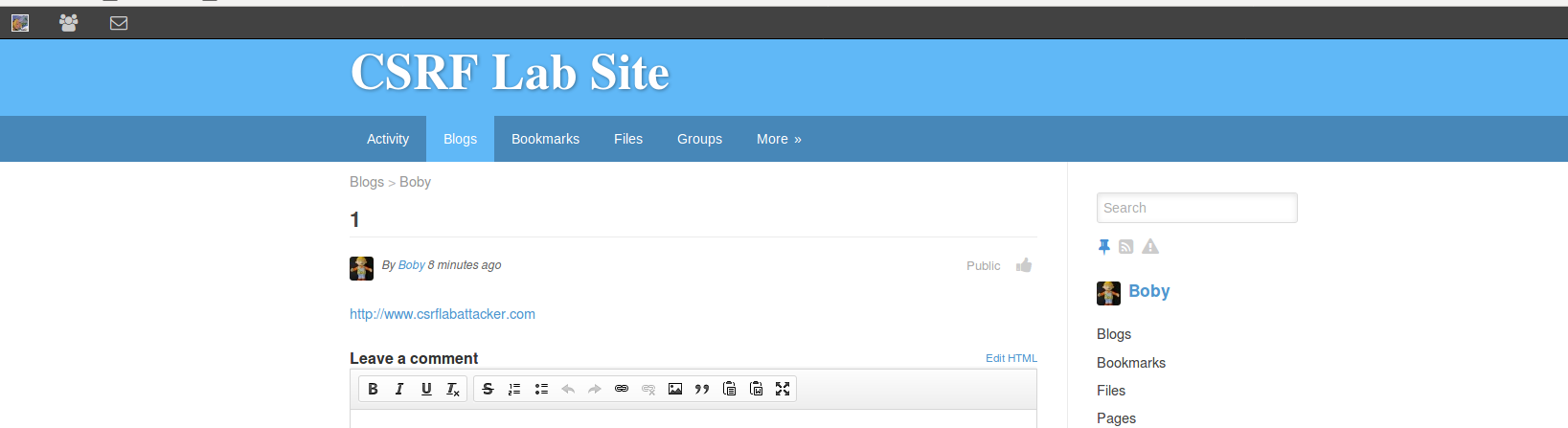
登陆Boby账户发blog



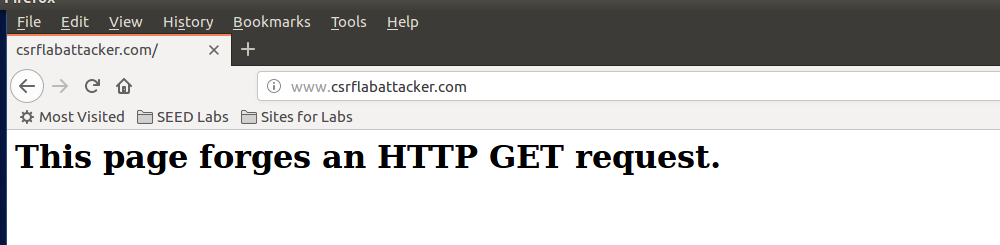
登陆Alice账户，起初没有好友



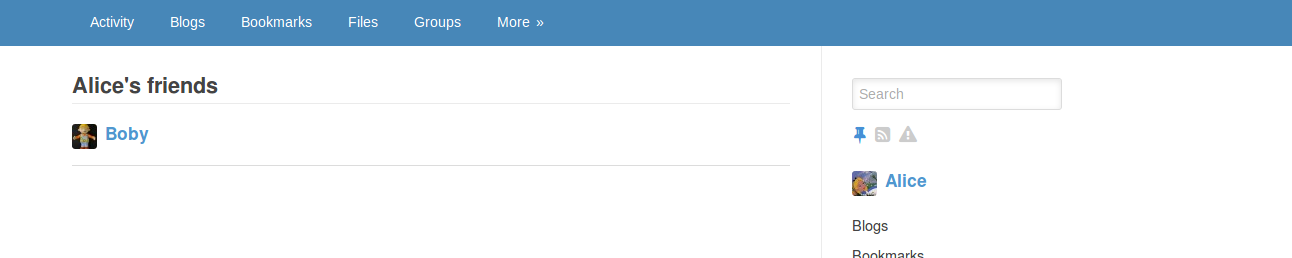
打开Boby的博客，点击链接



跳转到www.csrflabarracker.com

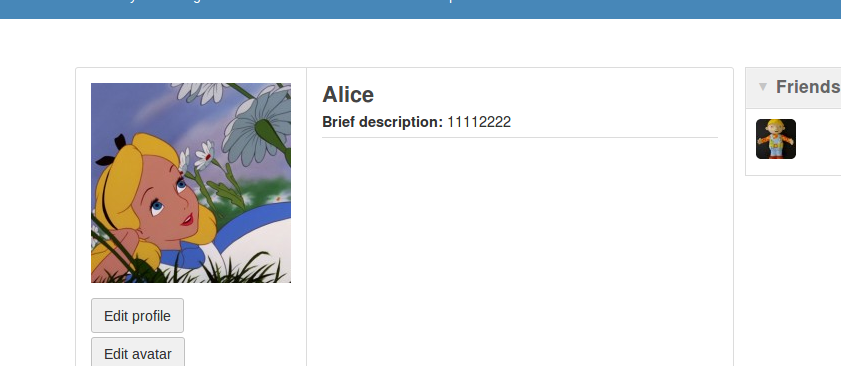


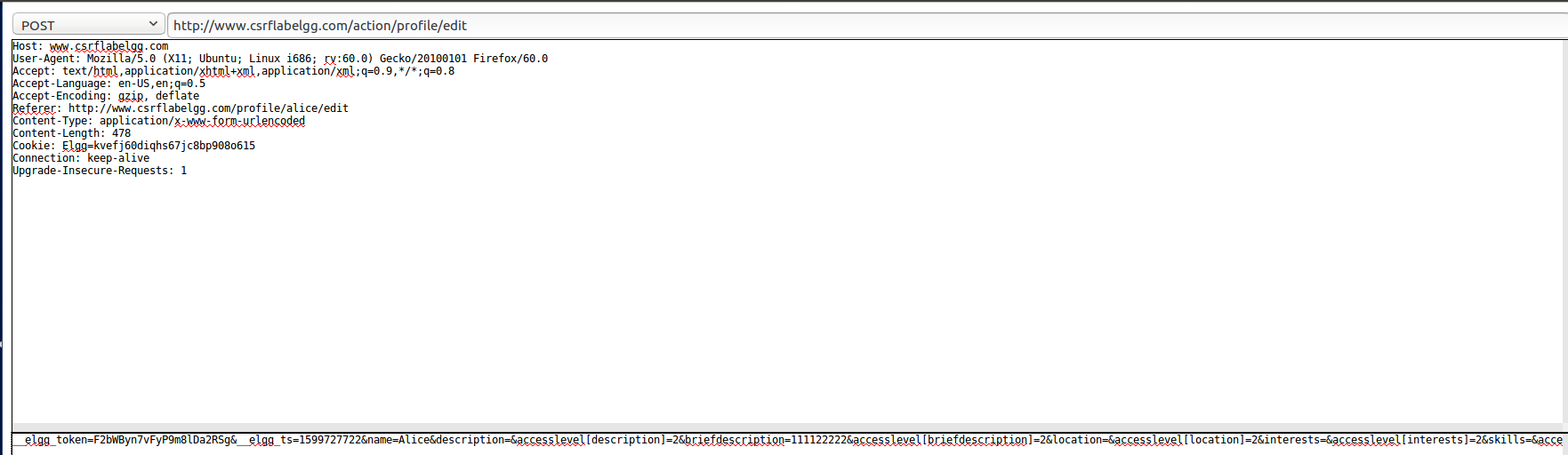
回到Alice好友界面发现多了Boby的好友



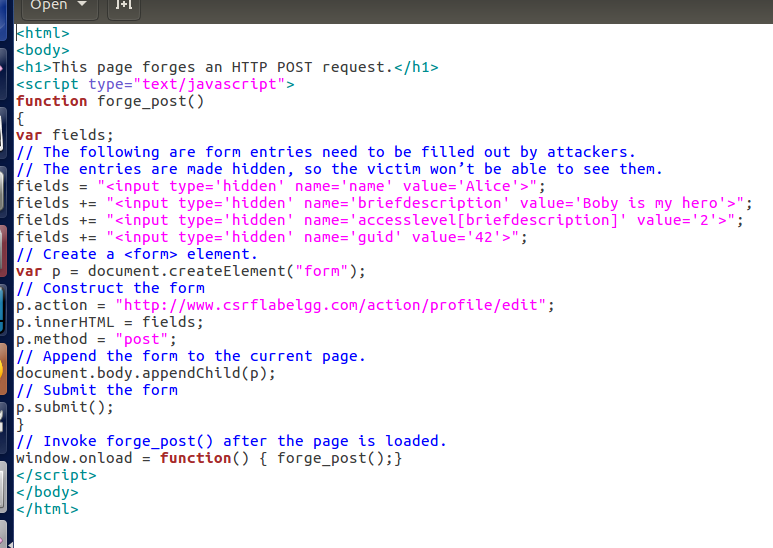
Task3:

正常修改签名并查看POST请求各字段值

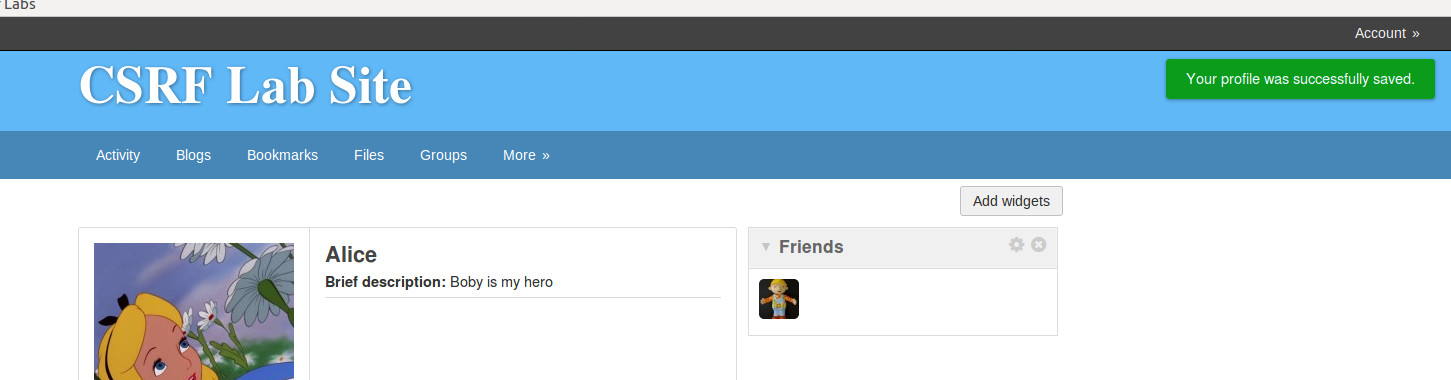




修改/var/www/CSRF/Attacker/index.html，如图

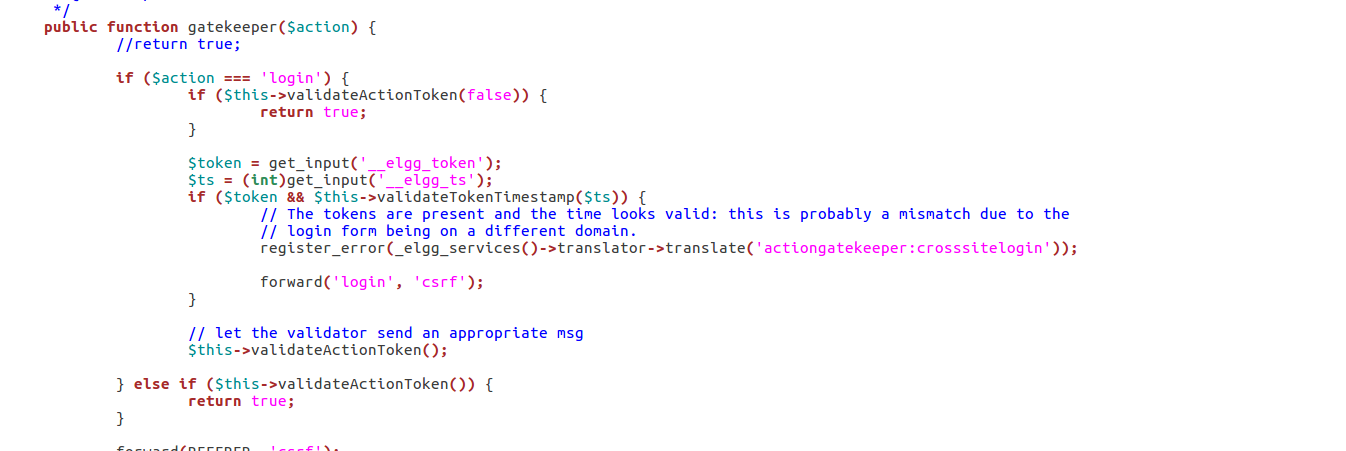


之后再次点击Boby的博客中的链接，跳转到[www.csrfattacker.com](http://www.csrfattacker.com)后自动跳回，然后发现签名已经被修改

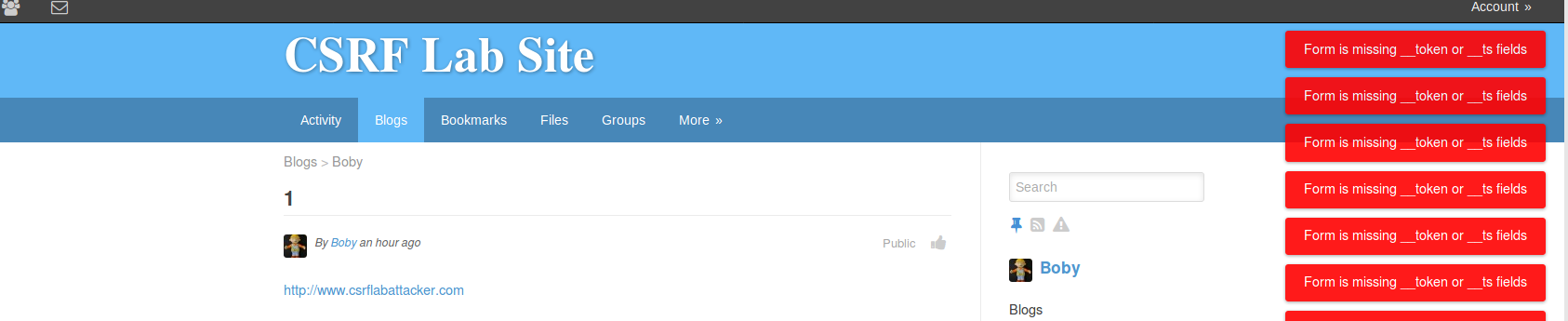


Task4:

修改的ActionsService.php，如图



之后再次点击Boby博客中的链接，进入[www.csrfattacker.com](http://www.csrfattacker.com)后不断自动刷新，退出后发现右侧提示错误：没有修改签名的权限。



查看签名，发现并没有被修改，说明防御手段起到了作用，因为攻击者网站的代码里没有\_\_elgg\_ts和\_\_elgg\_token两个字段的正确值。

