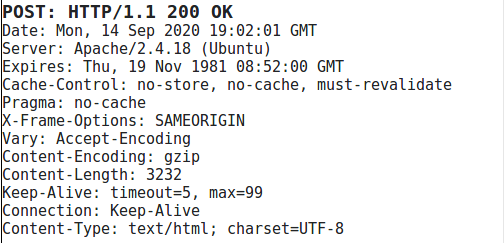
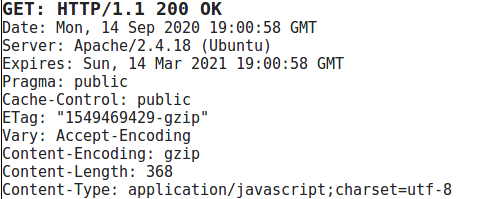
**Lab4-report**

**57118132 吴嘉琪**

**Task1: Observing HTTP Request**

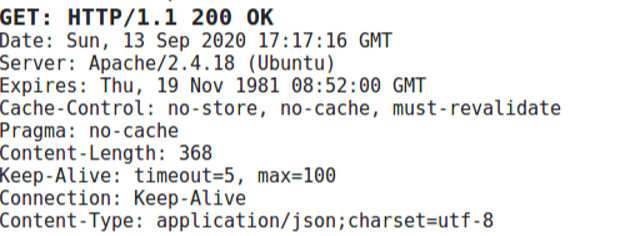
获取到的 GET 请求和 POST 请求如下：



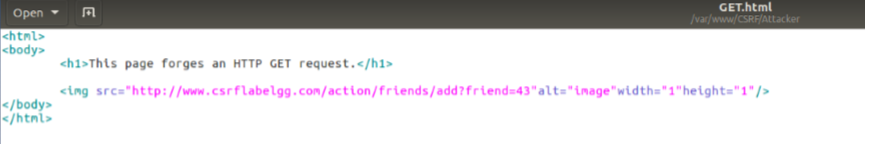


**Task2: CSRF Attack using GETR equest**

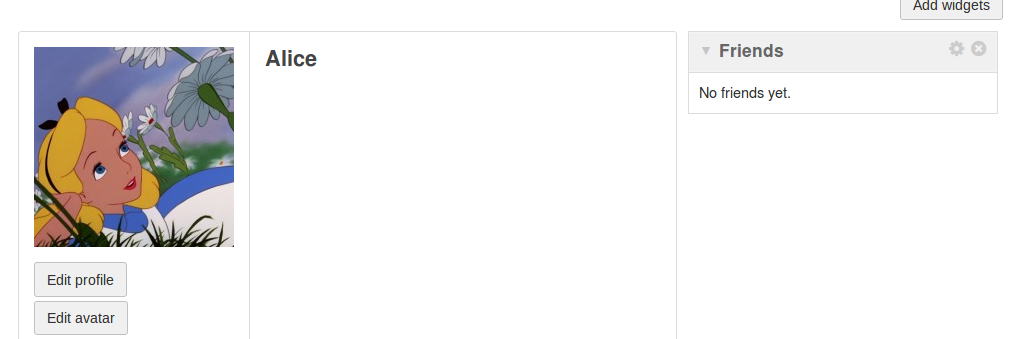
使用 HTTP HEADER LIVE 获取到添加好友的 GET 请求：



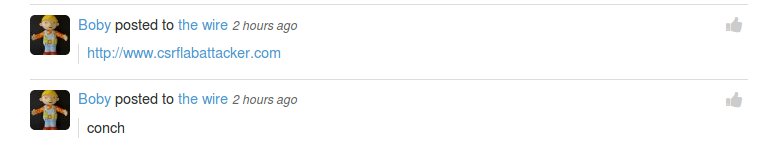
在目录/var/www/CSRF/Attacker/下添加 index.html，代码如图：



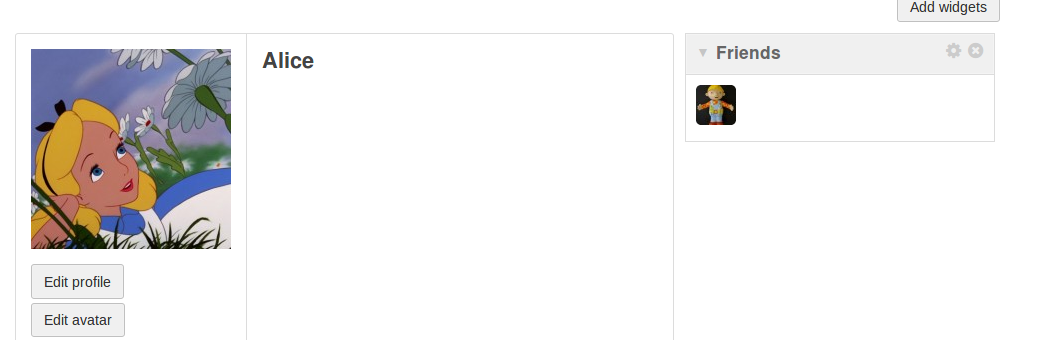
首先可以看到 Alice 没有好友。



接着使用 Boby 账号发出攻击链接的 blog

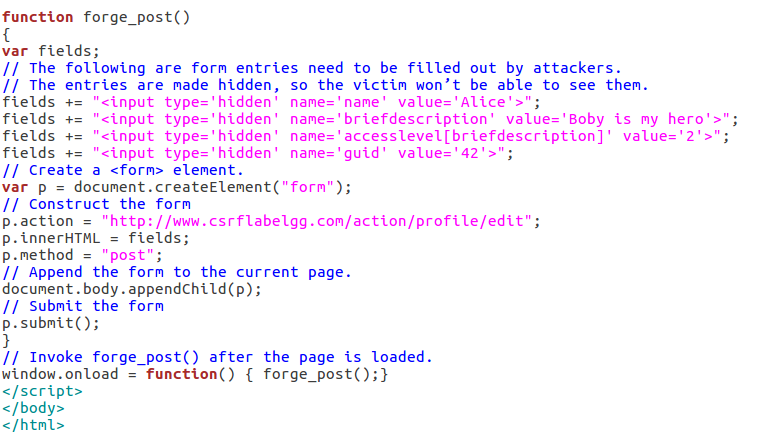


接着使用 Alice 的账号进入网站点击链接，回到 Alice 账户下，可以发现已经添加了好友Boby。

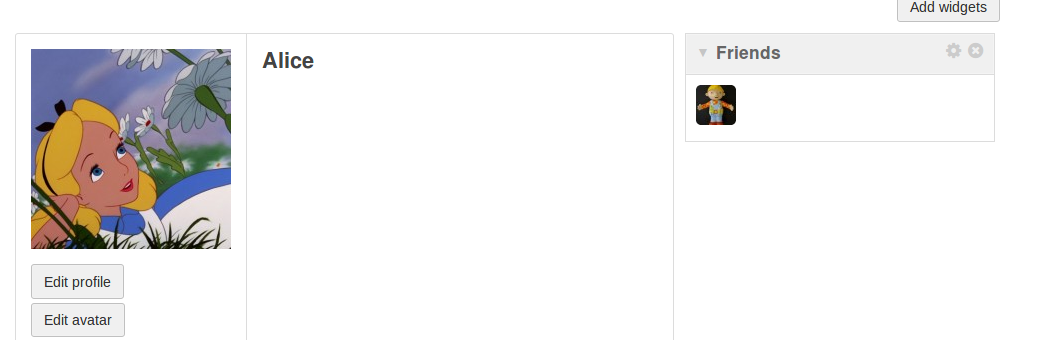


**Task3: CSRF Attack using POST Request**

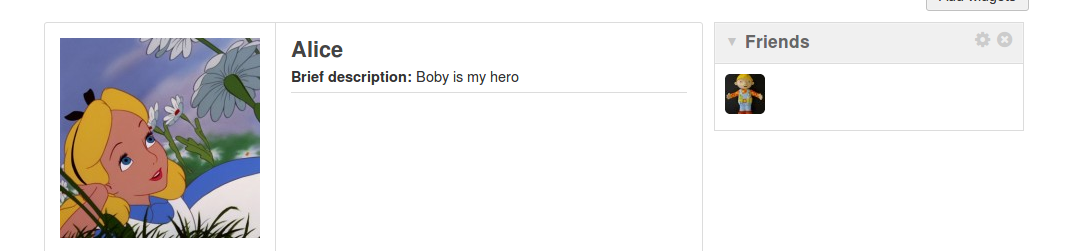
所以攻击代码如下：



首先来到 Alice 的首页，可以看到是空白的：

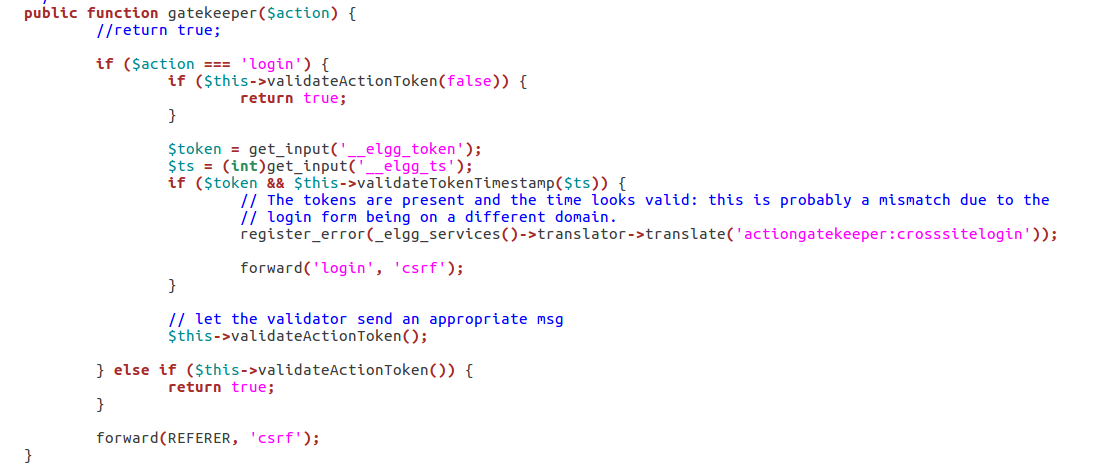


点击 Boby 发的博客，自动跳转回 Alice 首页，可以看到 Alice 的个人主页已经被修改，发了条动态。

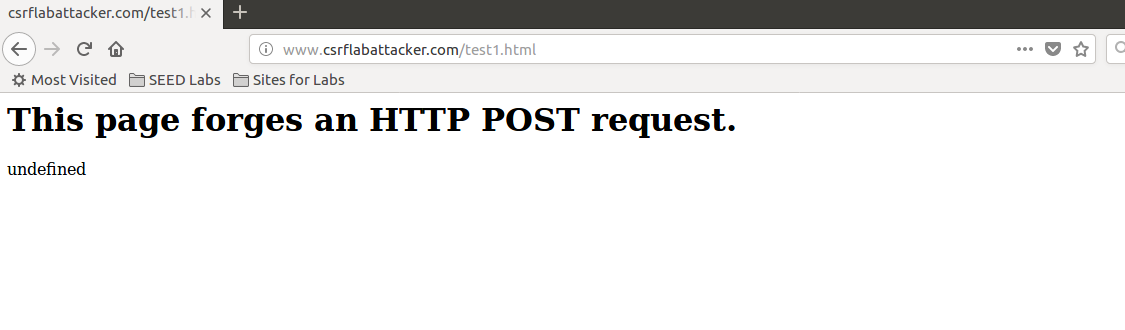


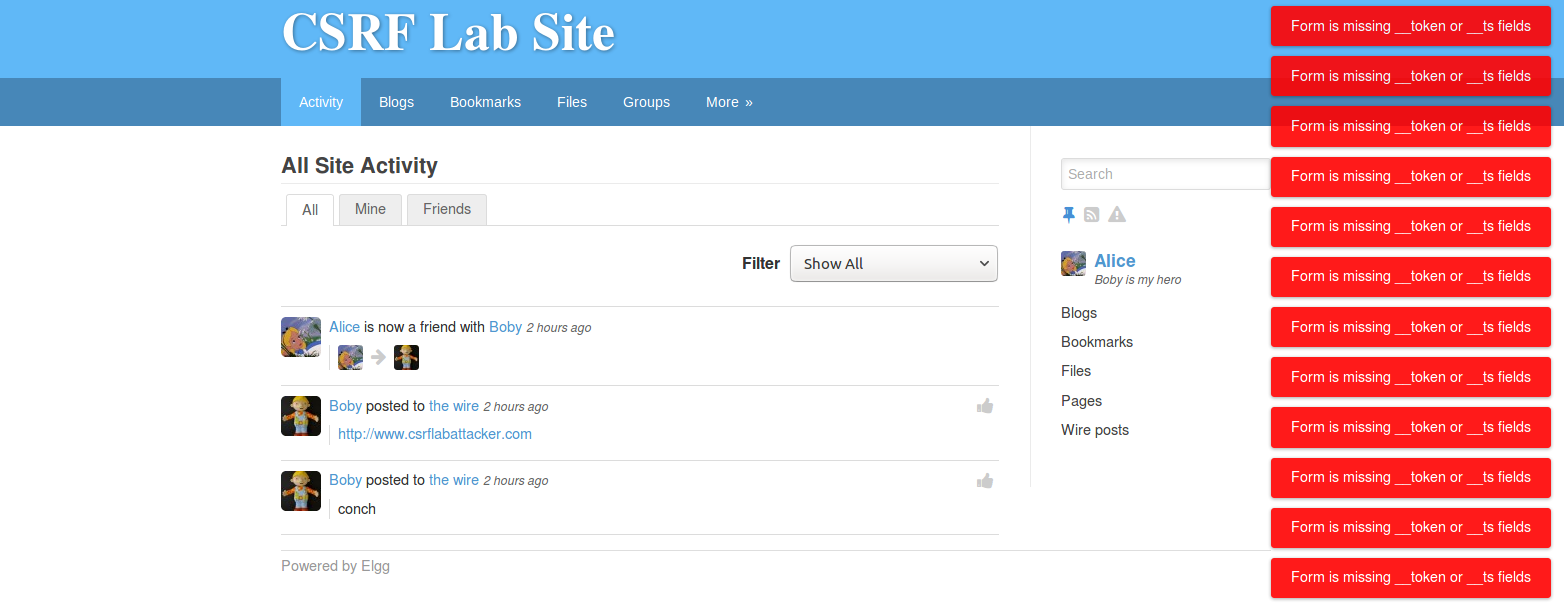
**Task4: Implementing a counter measure for Elgg**

将对策开启之后的代码：



Alice再次尝试攻击链接：





发现攻击失败，原因是攻击者代码中没有\_\_elgg\_ts 和\_\_elgg\_token 两个字段的正确值。