小白首次打CTF，思路详解记录

原创

雾十 于 2019-10-11 15:30:31 发布 956 收藏 3

文章标签： CTF Brup

本文链接：https://blog.csdn.net/weixin_37990514/article/details/102502233

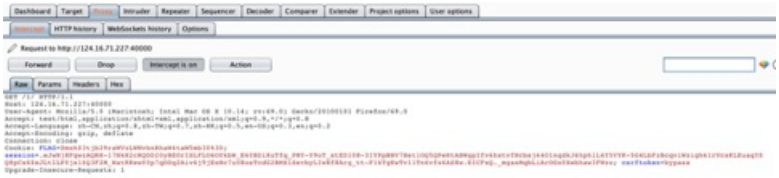
引言

小编第一次接触CTF，有点儿刺激啊/捂脸 一脸懵逼的那种刺激，但是在好心人的帮助下终于完美解决了三个问题！

正文

题一：

访问http://124.16.71.227:40000/1/，看到题目“找flag”，用brup查看报文



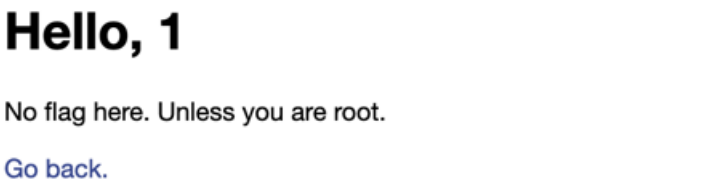
可以看到cookie项包含FLAG信息：

=ZmxhZ3tjb29raWVzLWNvbnRhaW4taW5mb30%3D

这是一串base64编码的加密信息，先用url解码，将末尾的%3D转换为=，再用base64解码刚刚url解码得到的字符串，找到了flag。

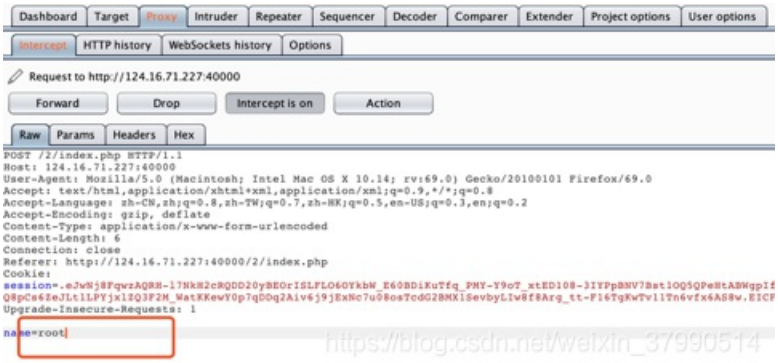
题二：

访问http://124.16.71.227:40000/2/，看到页面中有登录输入框，于是随便输入用户名1，点击login，看到：



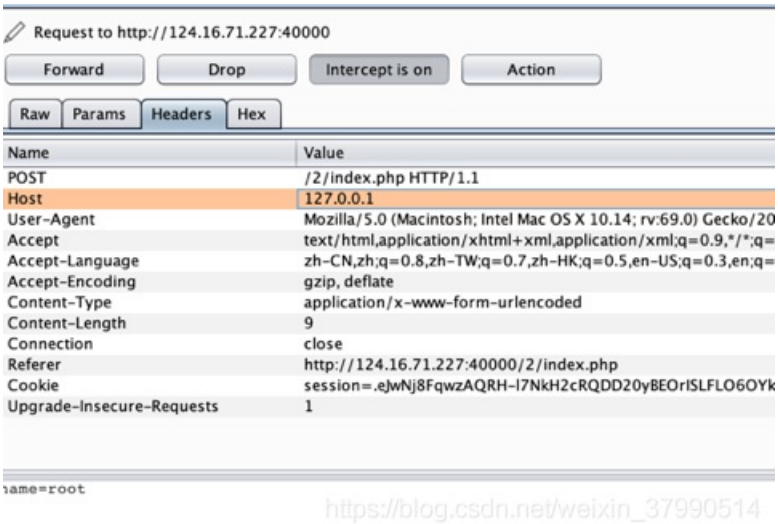
于是换成root登录，发现仍然不合法，

于是再次使用用户名1登录，使用brup拦截请求报文，手动将请求报文中的登录名改为root，



再次尝试发现仍然存在错误，提示host名不对，

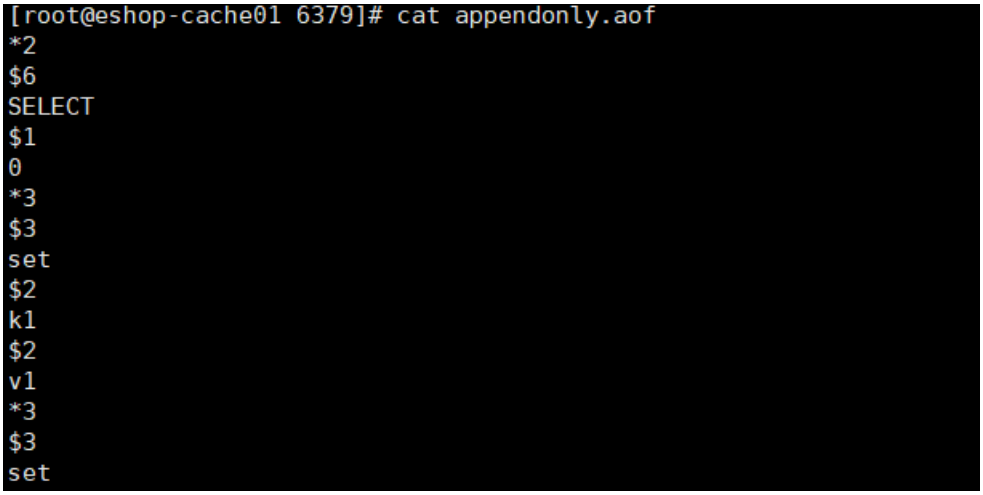
于是手动将请求报文中的name改为root, host改为127.0.0.1，



最终得到了flag。

题三：
访问http://124.16.71.227:40001/csrf，题目是说下面表单被django csrf中间件保护，尝试点击get flag按钮，发现：

没有思路，于是查看源代码，发现了注释信息：



```
$2
k2
$2
v2
```

于是将请求报文中的csrfmiddlewarewtoken的值改成bypass，点击get flag按钮，发现禁止访问，

通过阅读禁止信息，发现，csrftoken值缺失或者不正确，因为之前修改了csrfmiddlewarewtoken的值，猜测这两个值应该一样，于是手动将请求报文中的csrftoken改为bypass，

发送报文，得到了flag。