WhaleCTF Web部分writeup

原创

MozhuCY 于 2018-02-04 00:16:42 发布 3146 收藏 1
分类专栏： CTF入门 文章标签： web

Web部分writeup（真的是部分wp

二进制小白兼web盲来记录下今天做的几道题。。。

0x00

> 签到题直接f12查看源码即可

0x01 http呀

> **这里提供两种思路**
> 做web肯定少不了burpsuit啦，网页中给了提示，Do you know what happend just now?！（•∀•)突然想起南邮CTF平台上的两道题，考虑是不是flag在中间页面里，在点击时来了一次非常快的跳转呢？
> 抓了一次包发现啥都没有…后来尝试了几次发现，打开index.php的页面时，会跳到index.html。这就好办了，抓包拿flag，同时，同为二进制手的Cossack9989因为burpsuit过期了，想到了用wireshark来抓取流量，也是很顺利的拿到了flag
> (偷偷宣传一波W8Cloud战队和Cossack9989的博客

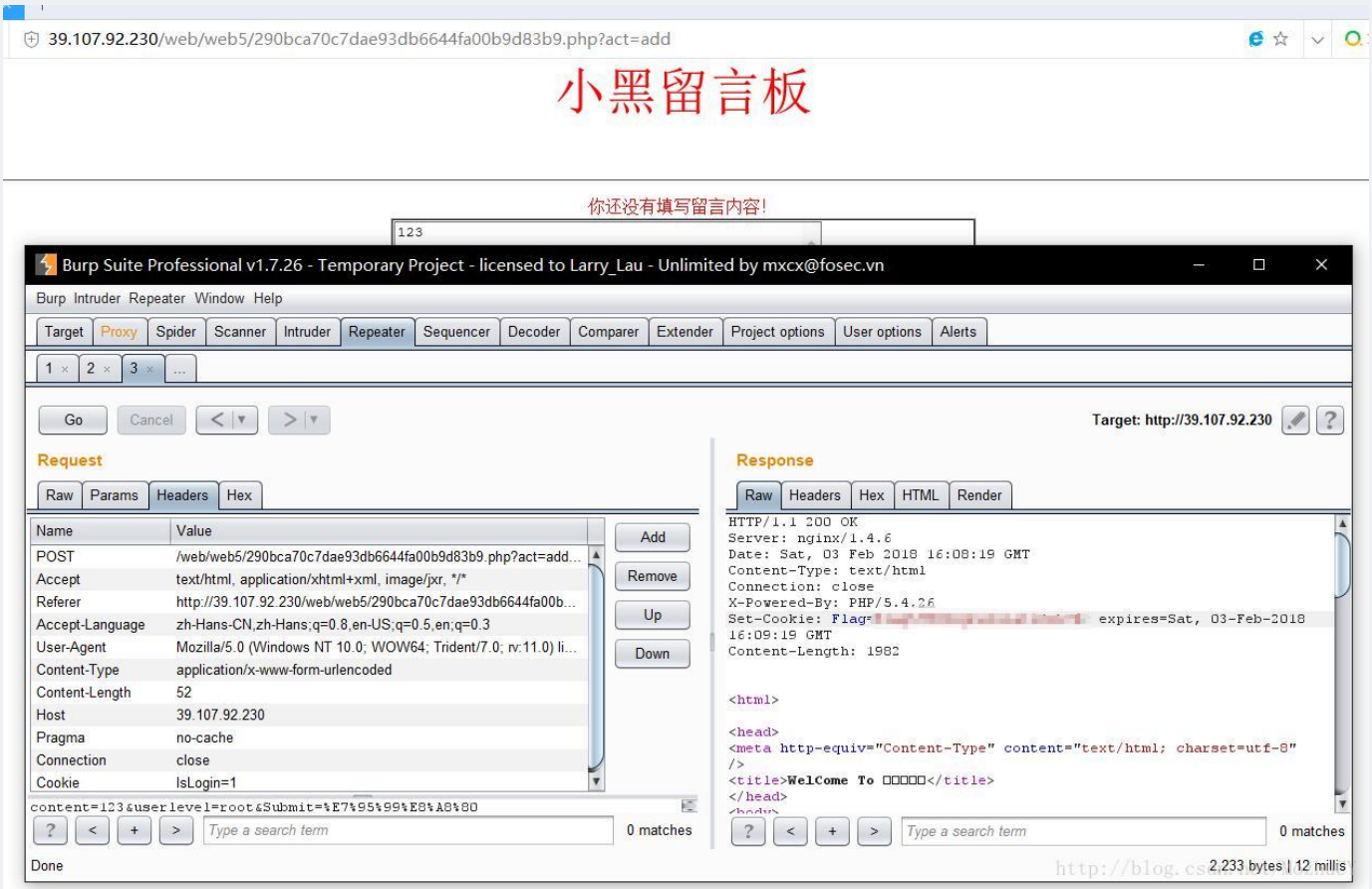
0x02 本地登录

> 本地登录，听名字大概就是伪造ip地址然后post过去吧，抓包加X-Forwarded-For: 127.0.0.1 成功拿到flag

0x03密码泄露

web的最后一题了，果然坑不少，是一个登陆样子的界面，查看源码发现有一个小提示“password.txt”，好的直接找到了密码表，来一发爆破吧，发现“Nsf0cuS”对应的返回包略大一点，查看Respone，有一个newpage，把对应的字符串base64解码居然到了一个新的网页w(°Д°)w来继续分析吧

去网上查了一波关于留言板的wp，莫非是xss，那么高深的东西也做不了啊。。后来和学长交流了一下，发现居然做法还是抓包。。。我来随便留一段文字，改了一下userlevel=root，发现居然还不对，原来是忘记改了IsLogin,0改1，拿到flag



sql注入对我这个web盲还是太高深了（；´д｀）ゞ学习一下再来补sql的wp吧....