封神台-第三章 爆破管理员账户登录后台

原创

ploto_cs 于 2020-09-26 18:52:42 发布 1646 收藏 7

分类专栏： # 封神台 文章标签： 信息安全

本文链接：https://blog.csdn.net/ploto_cs/article/details/108815525

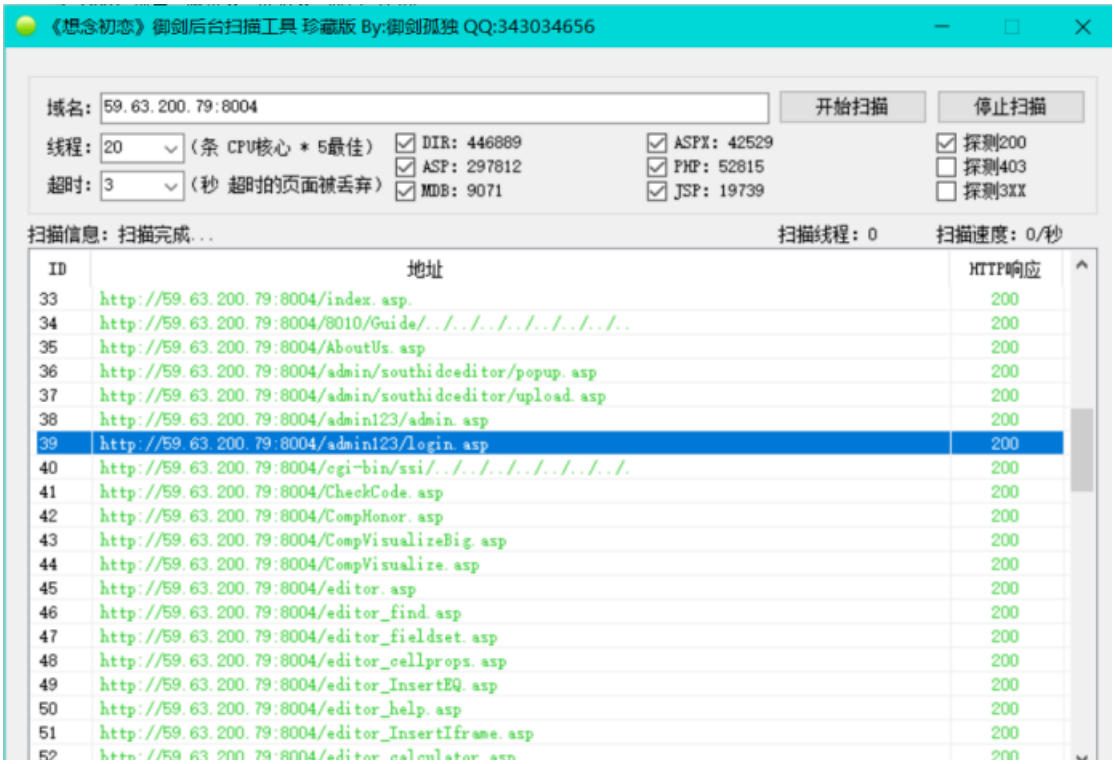
封神台-第三章 爆破管理员账户登录后台

1.探测真实登录网址

第二关拿到密码后，虽然在admin路径中成功登录后台，但那竟然是一个假后台!
不过没关系，尤里也遇到过不少假后台，他决定换个思路入手，通过信息收集..... 它找到了女神的另一个购物网站，尤里决定从这个网站入手.....
(注：字典加助教领取)
传送门

有题目可知，8004端口下admin是假后台，故使用御剑探测8004端口

2.探测可得，admin123才是真后台

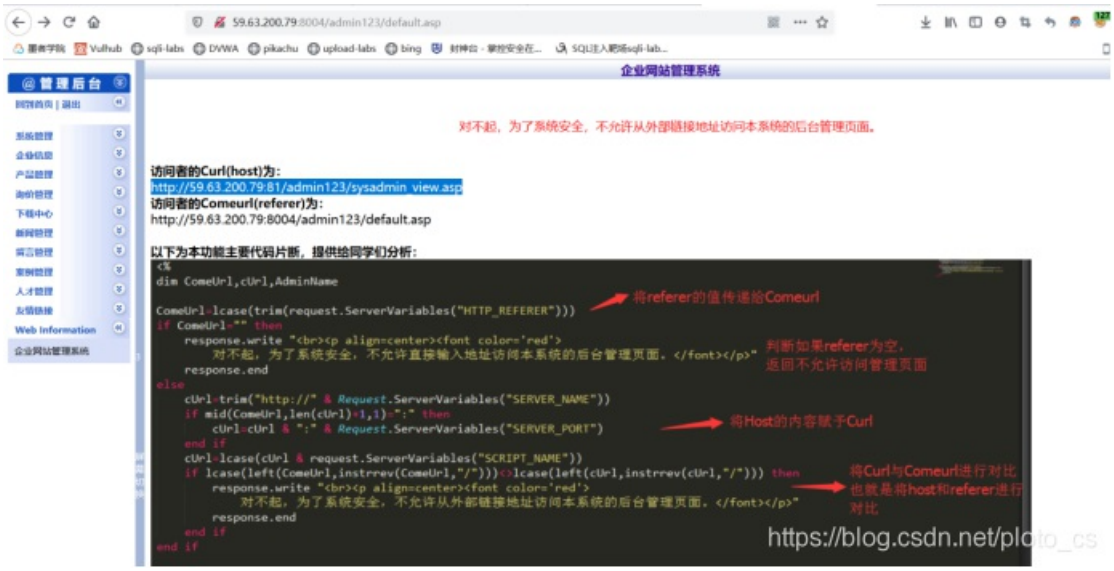


3.使用上一章节爆破出的密码继续登录

账户：admin

密码：welcome

成功登录后可得



4.分析代码

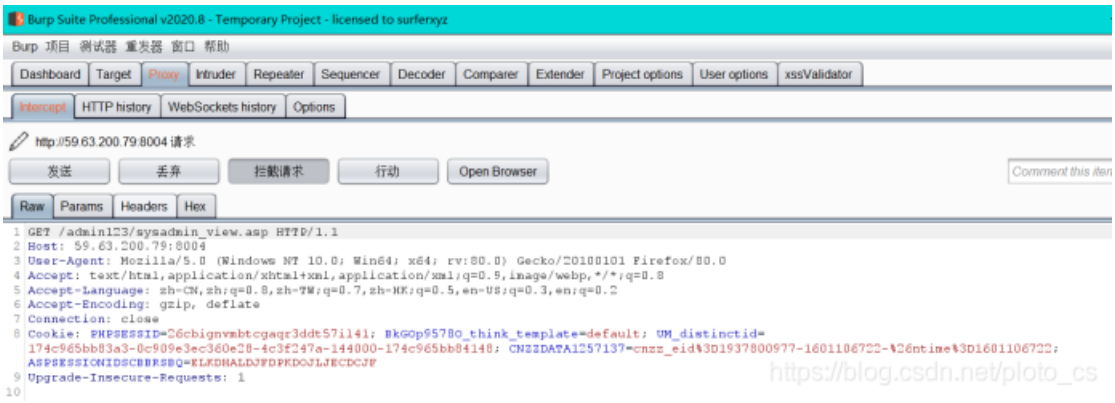
① 从请求头中拿到Referer，并赋值给ComeUrl。

② 判断ComeUrl是否为空，若是空，则表明是直接输入地址访问。本题不允许

③ ComeUrl不为空， 读取Host，并在前面拼接 http:// 赋值给cUrl，如果ComeUrl有 " : ",表明有端口号，在为cUrl 加上端口号。

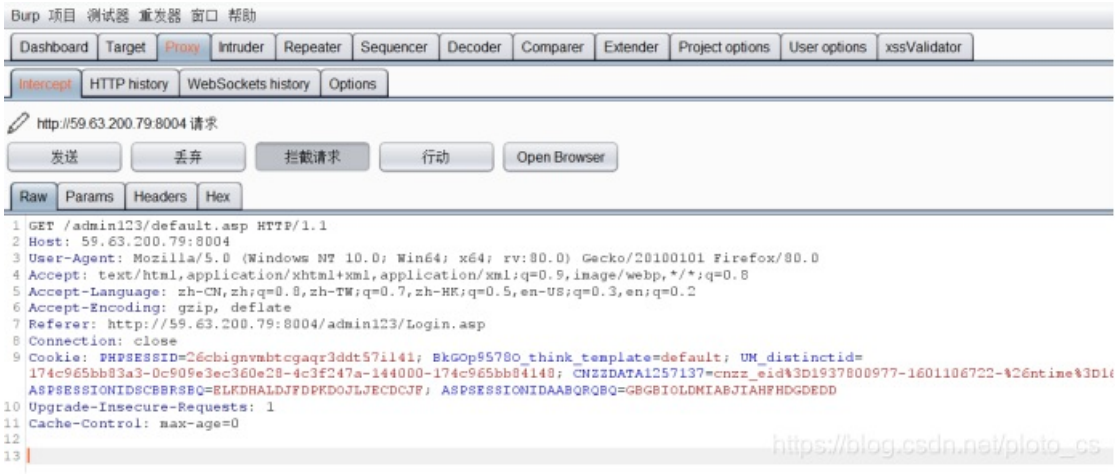
> 参考链接：https://blog.csdn.net/x_yhy/article/details/96430600

5.在url中输入http://59.63.200.79:8004/admin123/sysadmin_view.asp，并使用Bp抓包



这样抓包没有出现Referer字段

在url中输入http://59.63.200.79:8004/admin123/default.asp，并使用Bp抓包

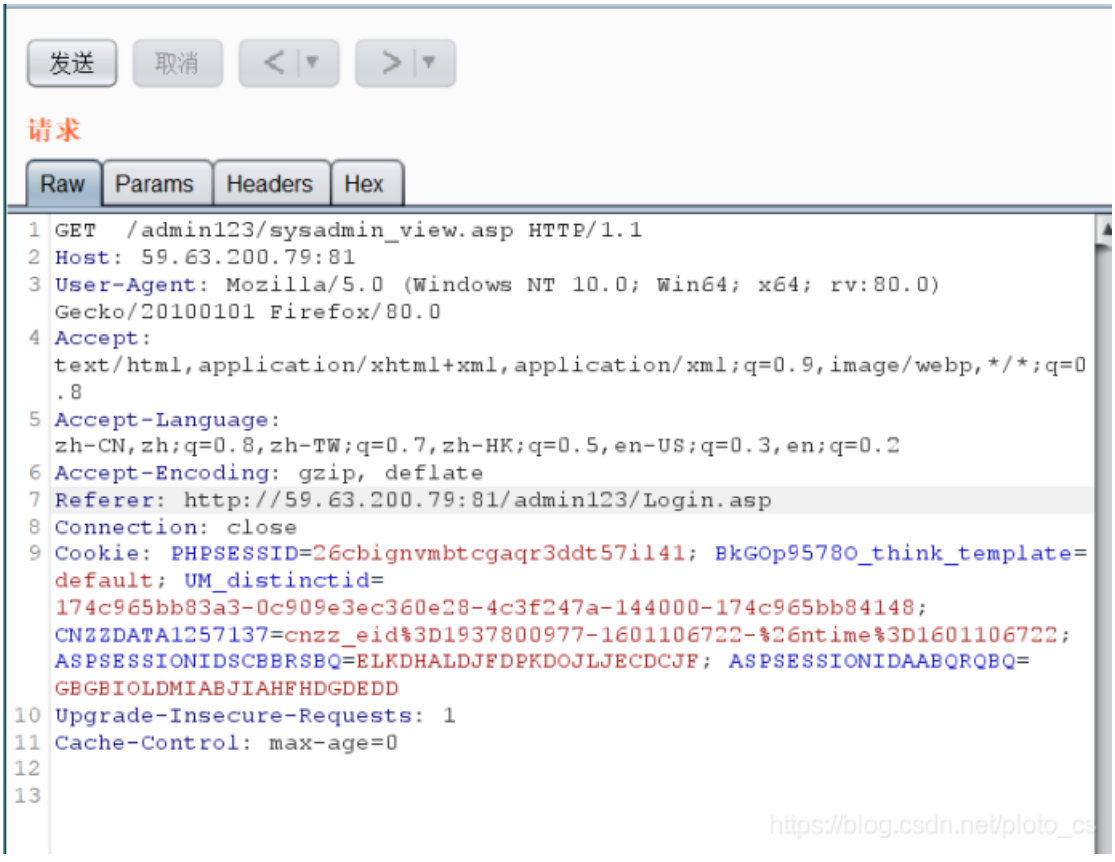


6.修改信息

将get后的/admin123/default.asp 换成 /admin123/sysadmin_view.asp

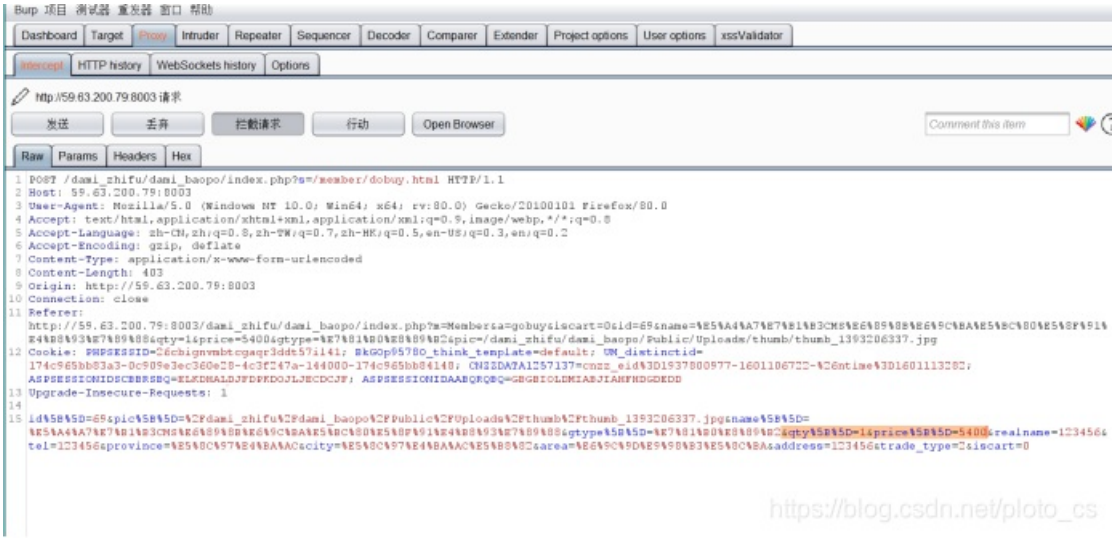
以及Host端口号和Referer的端口号都改为81

发送到重发器可以看到



又是突发奇想，这个还可以通过抓包更改购物信息

抓包 更改价格数量



发送到重发器，测试

哈哈哈哈哈哈

网络信息安全-ploto