封神台----尤里的复仇I-第三章：这个后台能识别登录者...

原创

向那风 于 2019-07-18 15:20:31 发布 1575 收藏 3

分类专栏： 渗透学习 靶场练习

本文链接：https://blog.csdn.net/x_yhy/article/details/96430600

渗透学习 同时被 2 个专栏收录

10 篇文章 0 订阅

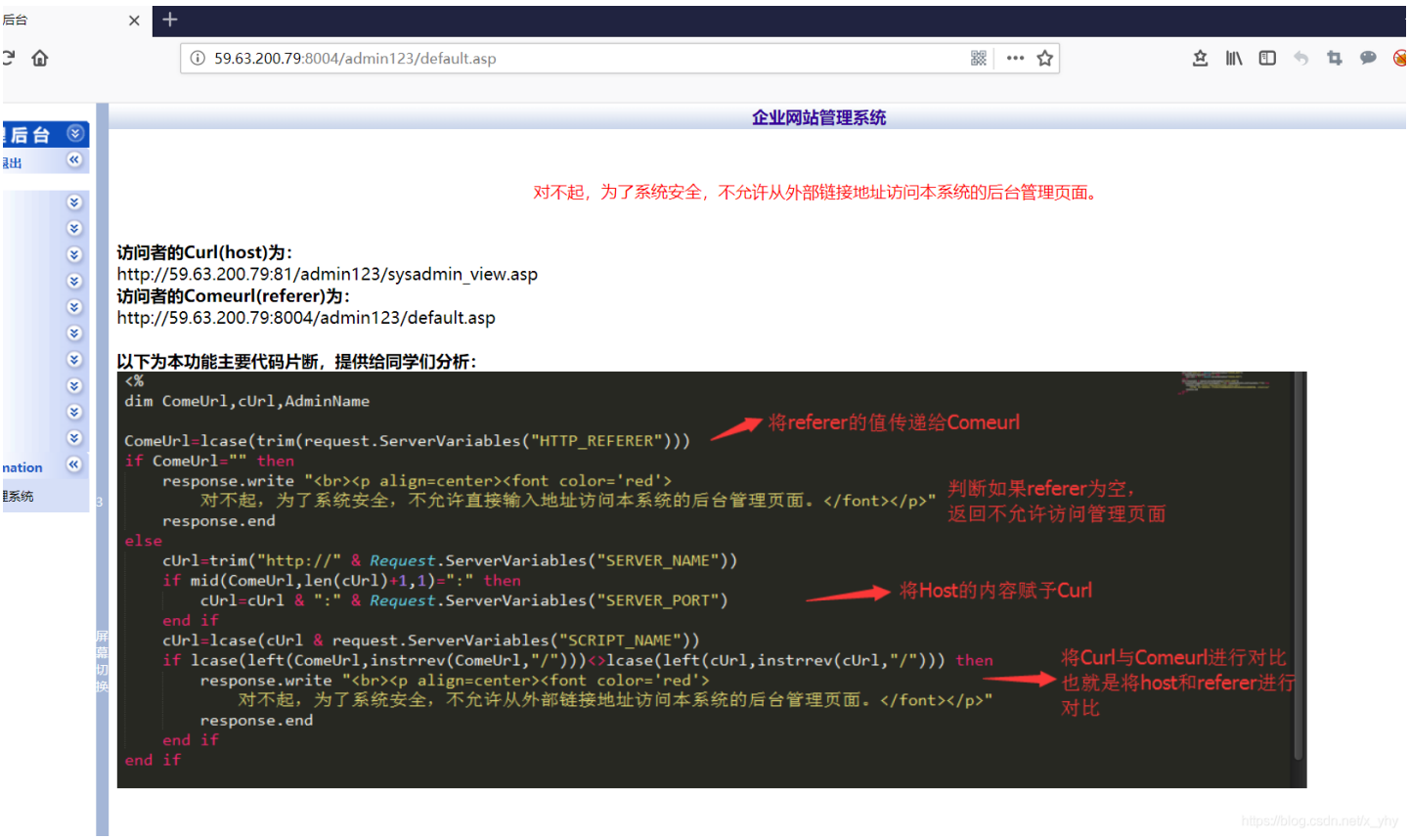
订阅专栏

靶场练习

7 篇文章 0 订阅

订阅专栏

根据提示，真正的后台地址为admin123，输入上一关的账号、密码进去。



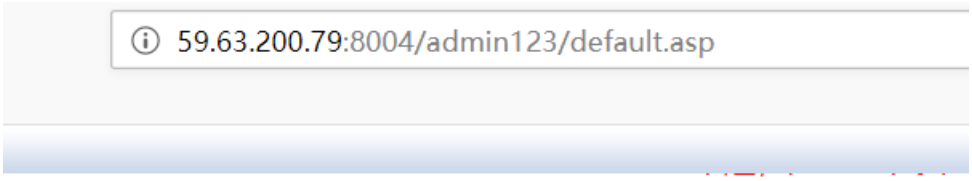
分析代码：

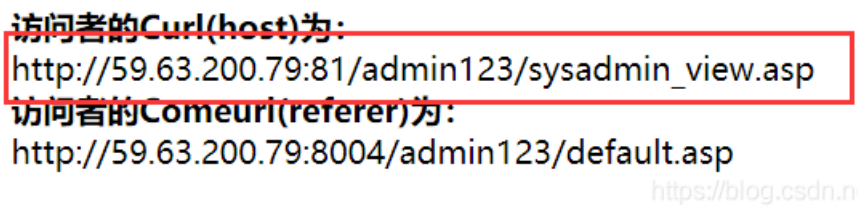
1. 从请求头中拿到Referer，并赋值给ComeUrl。
2. 判断ComeUrl是否为空，若是空，则表明是直接输入地址访问。本题不允许
3. ComeUrl不为空， 读取Host，并在前面拼接 http:// 赋值给cUrl，如果ComeUrl有 " : ",表明有端口号，在为cUrl 加上端口号。
4. 最后判断cUrl和ComeUrl中从右边看，第一次出现"/"的位置，返回的是从左数的下标。比如：

```
str="123456.78.9.txt"
response.write(InstrRev(str,"."))              #输出：12
```

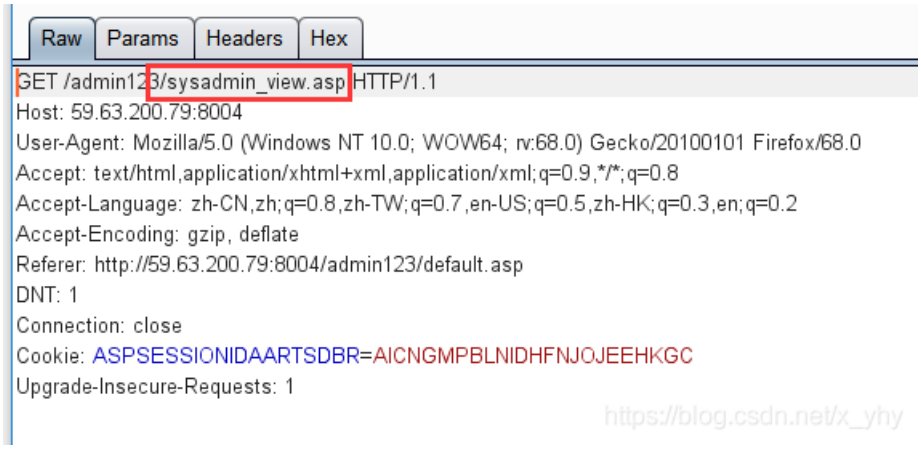
5. 就是说Referer的ip、port和host的ip、port必须一样。

从给出的信息中可以猜测，我们实际要访问的是sysadmin_view.asp





刷新，当出现



时，Host端口号和Referer的端口号改为81，或者都删去。