

封神台——菜刀初体验——一句话木马

原创

Zichel77 于 2020-07-05 13:59:37 发布 272 收藏

分类专栏: [web学习](#) [封神台](#) 文章标签: [图片木马制作教程](#) [shell](#) [web](#)

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/weixin_43965597/article/details/107137982

版权



[web学习](#) 同时被 2 个专栏收录

65 篇文章 5 订阅

订阅专栏



[封神台](#)

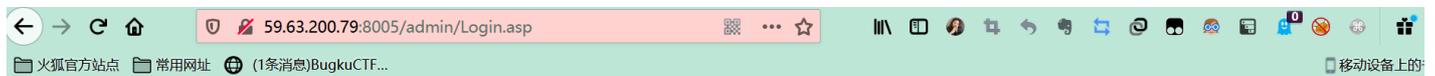
5 篇文章 0 订阅

订阅专栏

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

看题意就是和上一题相关的, 上一题在Cookie中找到了flag, 这一题就要利用上一题中的数据修改Cookie, 从而绕过登陆密码登入后台



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/weixin_43965597

上一题得到的数据如下

```
DELTOIEJUEFEROJIEC,  
flag=z{kz{[REDACTED]},AD  
MINSESSIONIDCSTRC  
SDQ=LBMLMBCCNPF  
NOANFGLPCFBC  
opener :
```

把Name修改为等号前的内容, Value修改为等号后的内容

方法一: 检查元素->存储

名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问
ADMINSE...	LBMLMBCCNPFINOANFLPCFBC	59.63.200.79	/	会话	46	false	false	None	Sun, 05 Jul 2020
ASPSSESI...	OIGNGMPCNLEDPAAPBLCFBLEN	59.63.200.79	/	会话	44	false	false	None	Sun, 05 Jul 2020

https://blog.csdn.net/weixin_43965597

方法二：用ModHeader

点击“准备好了”即可进入登录后台

企业网站管理系统

管理快捷方式

快速功能链接	管理员管理
--------	-------

系统信息

用户名: admin	IP: 183.131.113.142
身份过期: 30 分钟	现在时间: 2020年7月5日21:5
上线次数: 549	上线时间: 2018-3-30 18:27:39
服务器域名: 59.63.200.79 / 59.63.200.79:8005	脚本解释引擎: VBScript/5.6.8832
服务器软件的名称: Microsoft-IIS/6.0	浏览器版本: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
FSO文本读写: <input checked="" type="checkbox"/>	数据库使用: <input checked="" type="checkbox"/>
Jmail组件支持: <input checked="" type="checkbox"/>	CDONTS组件支持: <input checked="" type="checkbox"/>

https://blog.csdn.net/weixin_43965597

根据提示我们需要上传Shell

那么就要先找到能够上传文件的界面

我先是找到了添加产品

英文产品说明:

产品图片:

已通过审核: 是 (如果选中的话将直接发布)

首页显示: 是 (如果选中的话将在首页显示)

首页新品显示: 是 (如果选中的话将在首页显示为新品展示)

录入时间: 2020-7-5 21:08:17 当前时间为: 2020-7-5 注意不要改变格式。

https://blog.csdn.net/weixin_43965597

但是提交的时候会要求填名字啊内容啊这些必填的东西，弄起来很麻烦，于是就找一个现成的产品做修改

产品管理

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

中本页显示的所有产品

删除选定的产品

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

https://blog.csdn.net/weixin_43965597

点击修改，即可直接上传文件

首先根据如下步骤合成一个图片马

因为单独的txt文件一般不让传，只让上传如下类型的



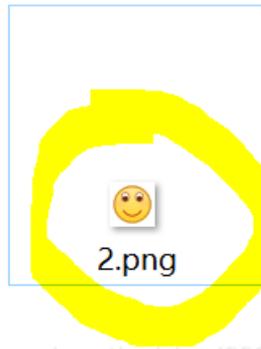
合成的方法见下列博客

[图片马的合成](#)

创建快捷方式的步骤可以省略，只需要将图片文件和一句话放在同一个文件夹，在该文件夹的路径下直接输入'cmd'即可，然后输入合成命令

合成好如下

› 新加卷 (E:) › horse

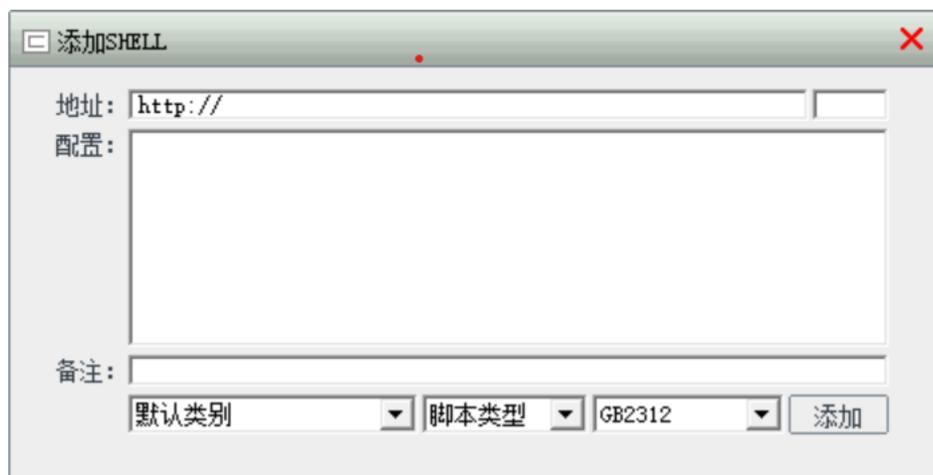


https://blog.csdn.net/weixin_43965597

返回网站上传，显示上传成功

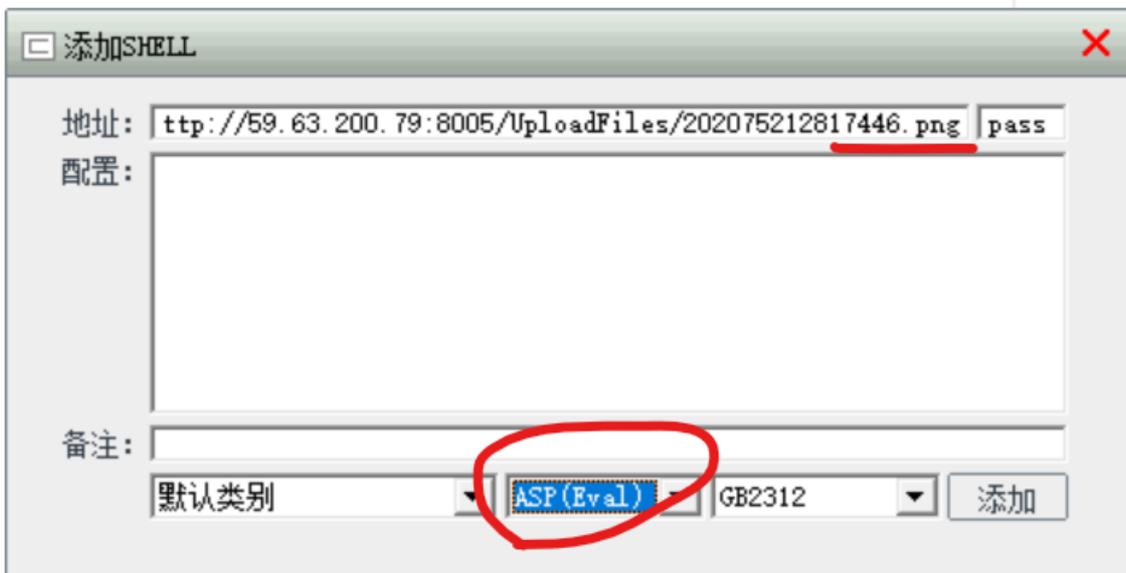


打开caidao，在空白处右键添加



https://blog.csdn.net/weixin_43965597

地址填写网页的url加上UploadFiles啥啥啥，密码随便吧



https://blog.csdn.net/wpxin_43965597

然后保存修改

双击地址会出现405的问题，

因为jpg文件不解析，因为你的后缀是图片格式，所以服务器会当做一张图片去读取，而不是代码。

就和你把一个图片后缀改为TXT然后打开里面的东西都会当文本读取而不是图片。

报错信息里面写了iis6.0的中间件。百度下iis6.0的解析漏洞，就能发现上传cer文件，iis6.0会解且执行。

然后把图片名字改为cer上传，成功上传，然后菜刀连接，成功进入，然后滚轮划一下就能看到flag! .txt，然后双击打开就是flag了。

D:\05\

9.63.200.79 目录(11),文件(177)

名称	时间	大小
editor_selcolor.asp	2013-04-07 18:15:00	4086
editor_SelectUpFile.asp	2013-04-07 18:15:00	8003
editor_tableprops.asp	2013-04-07 18:15:00	10095
editor_tsfh.htm	2013-04-07 18:15:00	37020
editor_ubbhelp.asp	2013-04-07 18:15:00	5564
Error.ASP	2013-04-07 18:15:00	3313
Feedback.asp	2019-04-10 15:58:08	9656
FeedbackMember.asp	2013-04-07 18:15:00	10372
FeedbackSave.asp	2013-04-07 18:15:00	2282
FeedbackView.asp	2019-04-10 15:58:08	9259
FLAG!.txt	2018-03-30 19:26:00	24
Foot.asp	2013-04-07 18:15:00	1129
GetPassword.asp	2013-04-07 18:15:00	9990
Head.asp	2013-04-07 18:15:00	5041
Help.asp	2013-04-07 18:15:00	2025
History.asp	2013-04-07 18:15:00	4576
home.asp	2013-04-07 18:15:00	359
HomeMarket.asp	2013-04-07 18:15:00	5124
HrDemand.asp	2019-04-10 15:58:08	9904
HrDemandAccept.asp	2019-04-10 15:58:08	23523

C:
 D:
 05
 06
 admin
 Databases
 flash
 Images
 Img
 imgbly
 imgbyw
 Inc
 Menu
 UploadFiles
 E

2014/12/13@4b4a956b9c7dc734f339fa05e4c2a990

https://blog.csdn.net/weixin_43965597