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

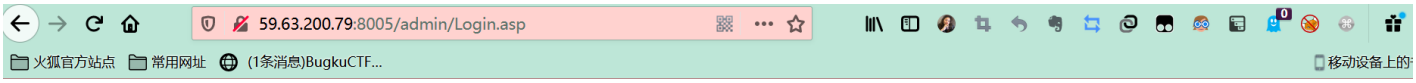
本文链接：https://blog.csdn.net/weixin_43965597/article/details/107137982


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

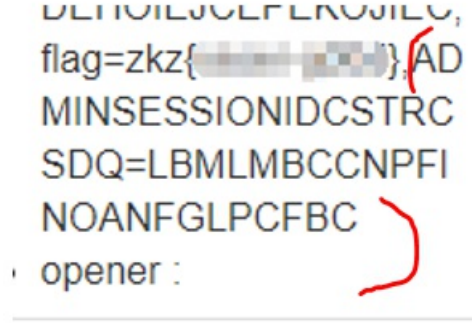
> Tips:
> 1、通过修改Cookie登录后台（没用重打） 2、上传SHELL！3、Flag在web根目录（flag.php） 3.上传图片时建议上传小文件，我建议用QQ表情

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



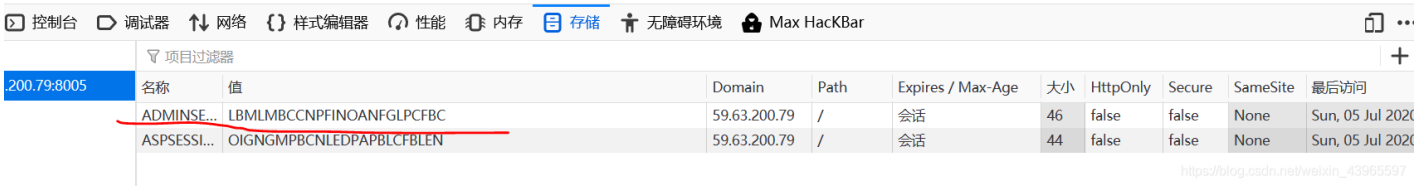
修改为管理员cookie后请直接访问管理页面 准备好了吗？

上一题得到的数据如下



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



方法二：用ModHeader

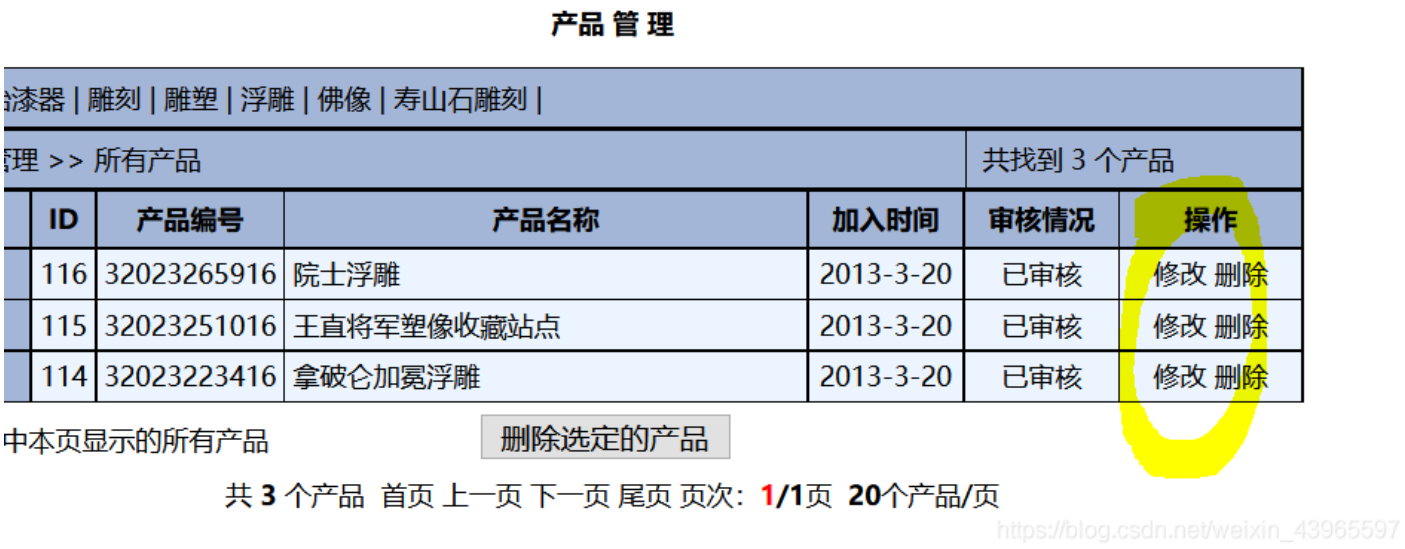
点击“准备好了”即可进入登录后台

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

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



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

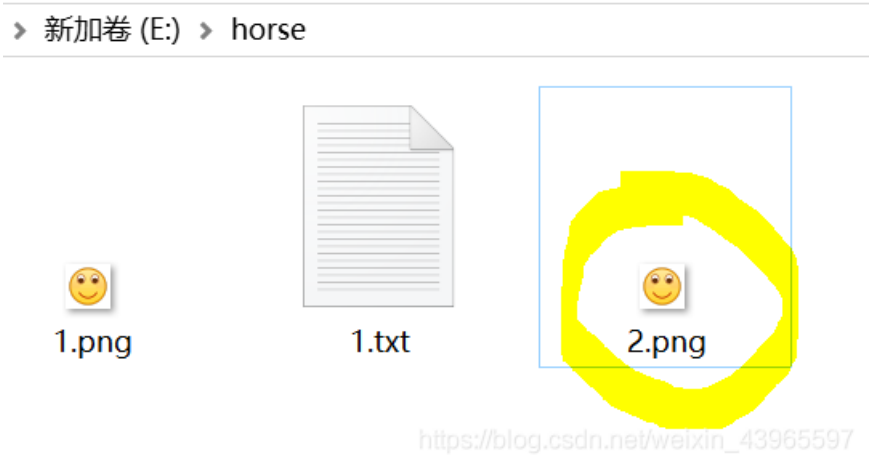
因为单独的txt文件一般不让传，只让上传如下类型的

合成的方法见下列博客

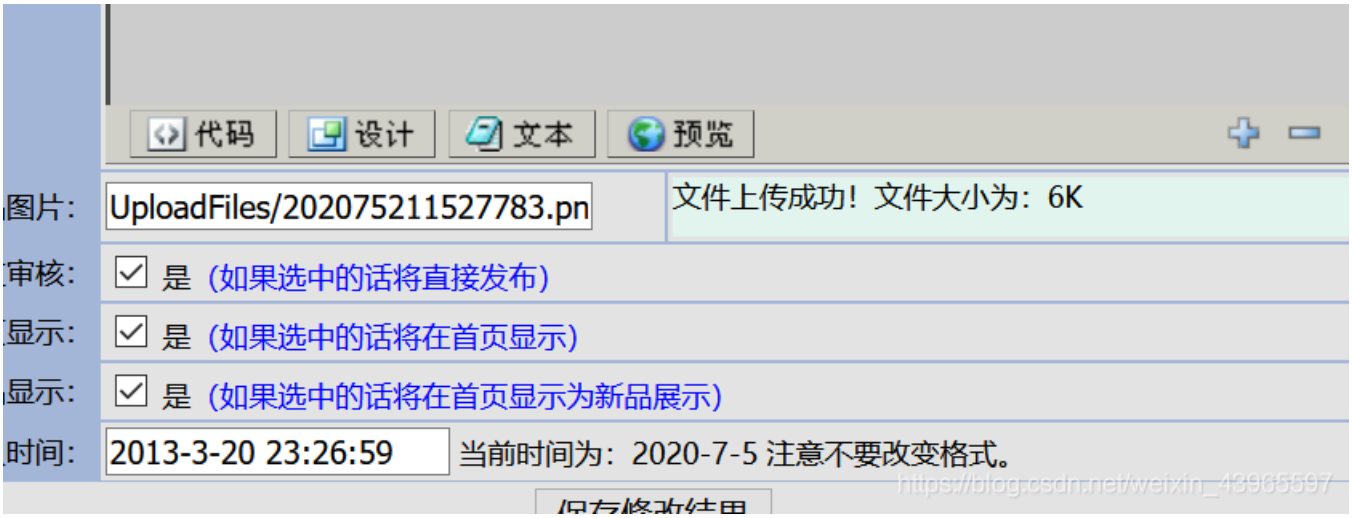
图片马的合成

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

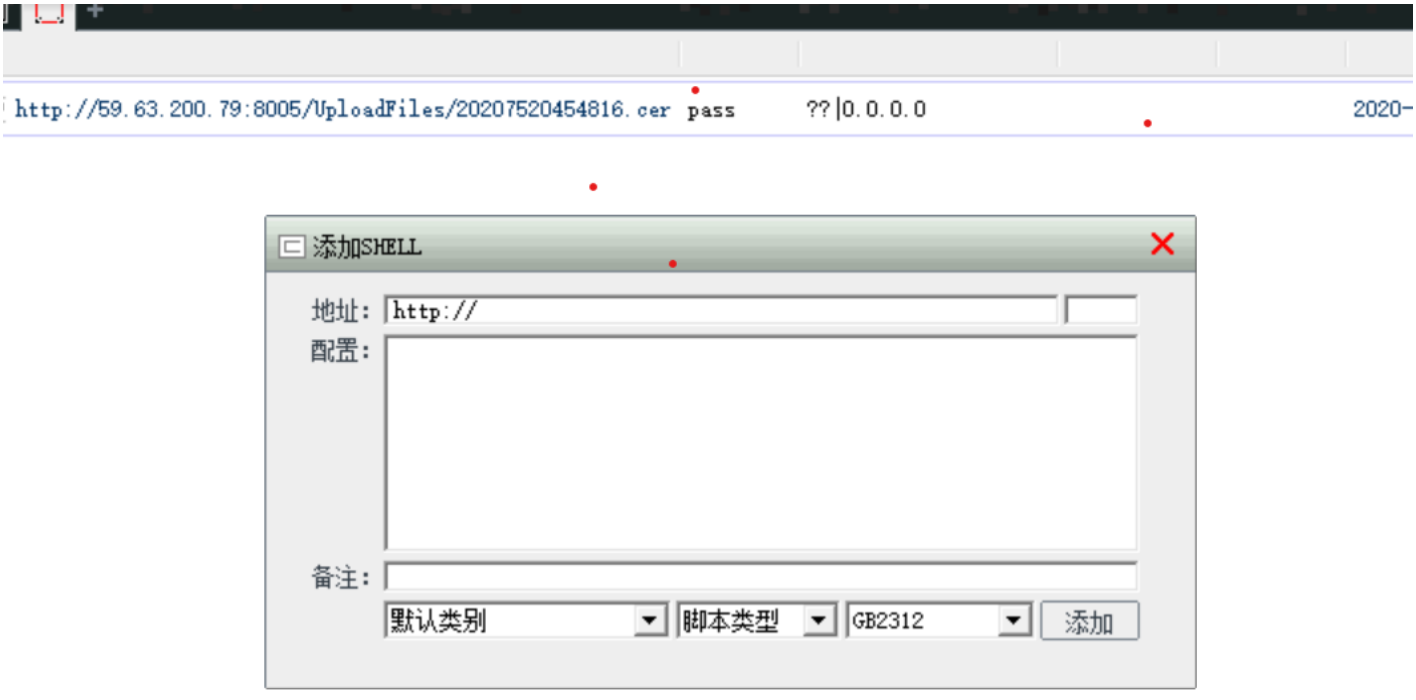
合成好如下



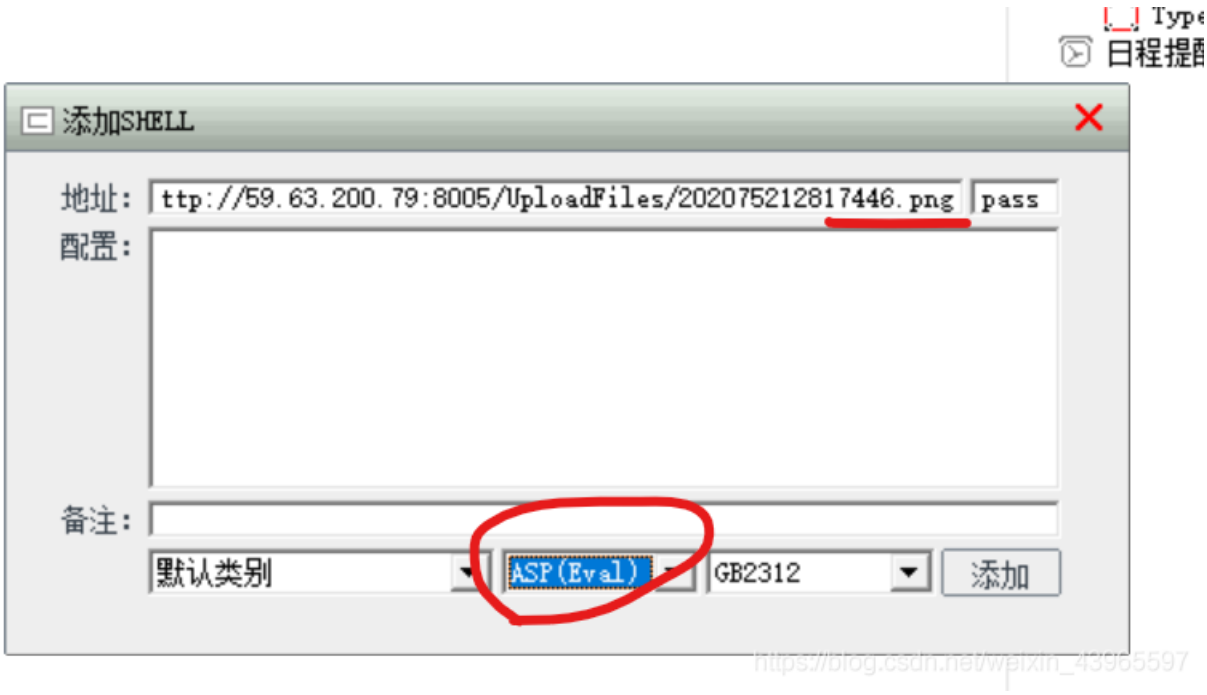
返回网站上传，显示上传成功



打开caidao，在空白处右键添加



地址填写网页的url加上UploadFiles啥啥啥，密码随便吧



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。

然后把图片马名字改为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。