2017NJCTF get flag writeup

原创

szuaurora 于 2017-03-12 23:14:05 发布 1036 收藏
分类专栏： writeup 文章标签： NJCTF CTF 信息安全 writeup web

题目网址：*http://218.2.197.235:23725/*

打开题目是一个输入框，是输入文件名来搜索图片的功能。随便输入*aaa*跳转到了另一个页面，是一张读不出来的图片。查看源代码可看到

<imgsrc="">

查了一下是基于*RFC2397*的一种*URL*格式，可以直接嵌入网页显示的一种数据显示方式。*base64*后面是*base64*编码的语句，解密一下就看到是*cat:images/aaa: No such file or directory*，也就是说里面是调用了*linux*的*cat*指令来进行执行的。于是想到了能否使用通配符解决问题。但是输入*和-后，出现*Too young too simple*的字样，也就是说是被禁掉了。<也被禁了，排除*xss*。后来发现*&*没有被禁掉，于是用*ls*指令查看目录下的文件，发现在当前目录下有一个*flag.txt*文件，还以为这么快就找到答案了，但是答案格式不对，输入进去后也不是正确答案。于是再一级一级网上找，后来在*../../../*目录下发现一个*9iZM2qTEmq67SOdJp%!oJm2%M4!nhS_thi5_flag*的文件，这个多半就是*flag*了。这就可以用*cat*打开了。于是*payload*是：

../../../9iZM2qTEmq67SOdJp%!oJm2%M4!nhS_thi5_flag。

另外通配符?也没有禁掉，也是可以用来找*flag*的，不过会麻烦一些。