BJDCTF 2nd writeup(二)

原创

abtgu 于 2020-03-29 08:49:35 发布 1918 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43790779/article/details/105173161

文章目录

Misc

[BJDCTF 2nd]A_Beautiful_Picture

[BJDCTF 2nd]小姐姐-y1ng

[BJDCTF 2nd]TARGZ-y1ng

[BJDCTF 2nd]Imagin - 开场曲

Crypto

[BJDCTF 2nd]cat_flag

[BJDCTF 2nd]燕言燕语

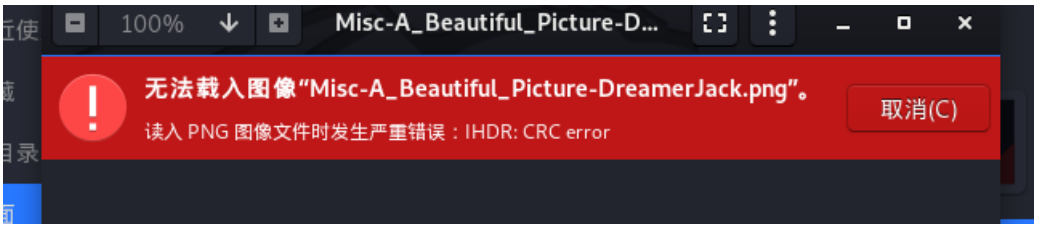
[BJDCTF 2nd]Y1nglish

Misc

[BJDCTF 2nd]A_Beautiful_Picture

题目： 得到的 flag 建议用 flag{} 包上提交。

解题思路： 将图片放到kali中，发现报crc错误



直接上脚本爆破，脚本如下

```
import zlib
import struct

filename = 'Misc-A_Beautiful_Picture-DreamerJack.png'
with open(filename, 'rb') as f:
    all_b = f.read()
    crc32key = int(all_b[29:33].hex(),16)
  ![2](C:\Users\daiqi\Desktop\writeupImages\2.PNG)  data = bytearray(all_b[12:29])
    n = 4095
    for w in range(n):          #高和宽一起爆破
        width = bytearray(struct.pack('>i', w))
        for h in range(n):
            height = bytearray(struct.pack('>i', h))
            for x in range(4):
                data[x+4] = width[x]
                data[x+8] = height[x]
            crc32result = zlib.crc32(data)
            if crc32result == crc32key:
                print("宽为：",end="")
                print(width)
                print("高为：",end="")
                print(height)
                exit(0)
```

得宽高为：

```
-------
宽为：bytearray(b'\x00\x00\x03\xe8')
高为：bytearray(b'\x00\x00\x03\xe8')
>>>
```

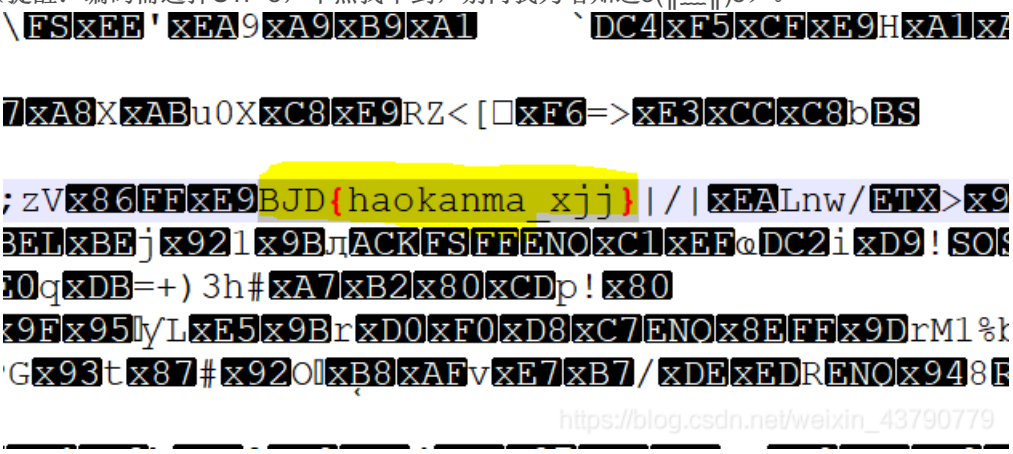
修改高度，得到flag

BJD{PnG_He1ghT_1s_WR0ng}

[BJDCTF 2nd]小姐姐-y1ng

题目： 你就是馋她身子，得到的 flag 建议用 flag{} 包上提交。

解题思路： 仔细观察图片，图片出现了错位，猜测中间被插入flag，用notepad++打开图片，搜索ctf，未找到flag，在搜索BJD，发现flag。（提醒：编码需选择UTF-8，不然找不到，别问我为啥知道o(╥﹏╥)o）。



[BJDCTF 2nd]TARGZ-y1ng

题目： 哎？ 我的tar zxvf怎么不好使了？解压密码不需要爆破，得到的 flag 建议用 flag{} 包上提交。

解题思路： kali中打开，发现报错，用file命令查看文件类型，发现是zip，修改后缀名，题中提示密码不需爆破，尝试文件名，解压成功，发现其中还是压缩文件，典型的套娃，写脚本爆破即可。

```
import zipfile,os
def unzip(zipname):
    while True:
        passwd = zipname.split('.')[0]
        zf = zipfile.ZipFile(zipname,'r')
        zf.extractall(pwd=passwd.encode())
        os.remove(zipname)
        zipname = zf.namelist()[0]
        zf.close()
unzip("OKMIlLVft.tar.gz")
```

得到flag，BJD{wow_you_can_rea11y_dance}。

[BJDCTF 2nd]Imagin - 开场曲

Crypto

[BJDCTF 2nd]cat_flag

题目： 得到的 flag 建议用 flag{} 包上提交。

解题思路： 图中每行有8只猫，总共有两种猫，猜测为二进制ASCII码，二进制转换成字符串即可。BJD{M!a0~}。

[BJDCTF 2nd]燕言燕语

题目： 小燕子，穿花衣，年年春天来这里，我问燕子你为啥来，燕子说:

79616E7A69205A4A517B78696C7A765F6971737375686F635F73757A6A677D20

解题思路： 明显是16进制数据，转字符，得yanzi ZJQ{xilzv_iqssuhoc_suzjg}，猜测是维吉尼亚密码，yanzi是密钥解密，得到flag。BJD{yanzi_jiushige_shabi}

[BJDCTF 2nd]Y1nglish

题目： Y1ng根据English居然独自发明了一门语言，就叫Y1nglish。明文都是可读的英文单词，flag如果提交失败，自己读一下，把错误的单词修正，再提交(某个地方的u和i不需要调换顺序，错误点不在那里)。得到的 flag 建议用 flag{} 包上提交。

解题思路： 明显需要用到cryptogram solver，用quipqiup破解

地址：https://www.quipqiup.com/

得到BJD{pyth0n_Brut3_f0rc3_oR_quipquip_AI_Cr4cy}，根据提示将Cr4cy改成Cr4ck即可。