

# BugkuCTF\_杂项004

原创

FAFU小宋 于 2020-11-04 22:49:48 发布 75 收藏

分类专栏: [BugkuCTF](#) 文章标签: [安全](#)

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/FAFUxiaosong/article/details/109400979>

版权



[BugkuCTF 专栏收录该内容](#)

6 篇文章 0 订阅

订阅专栏

## BugkuCTF\_杂项

[猫片\(安恒\)](#)

[多彩](#)

[旋转跳跃](#)

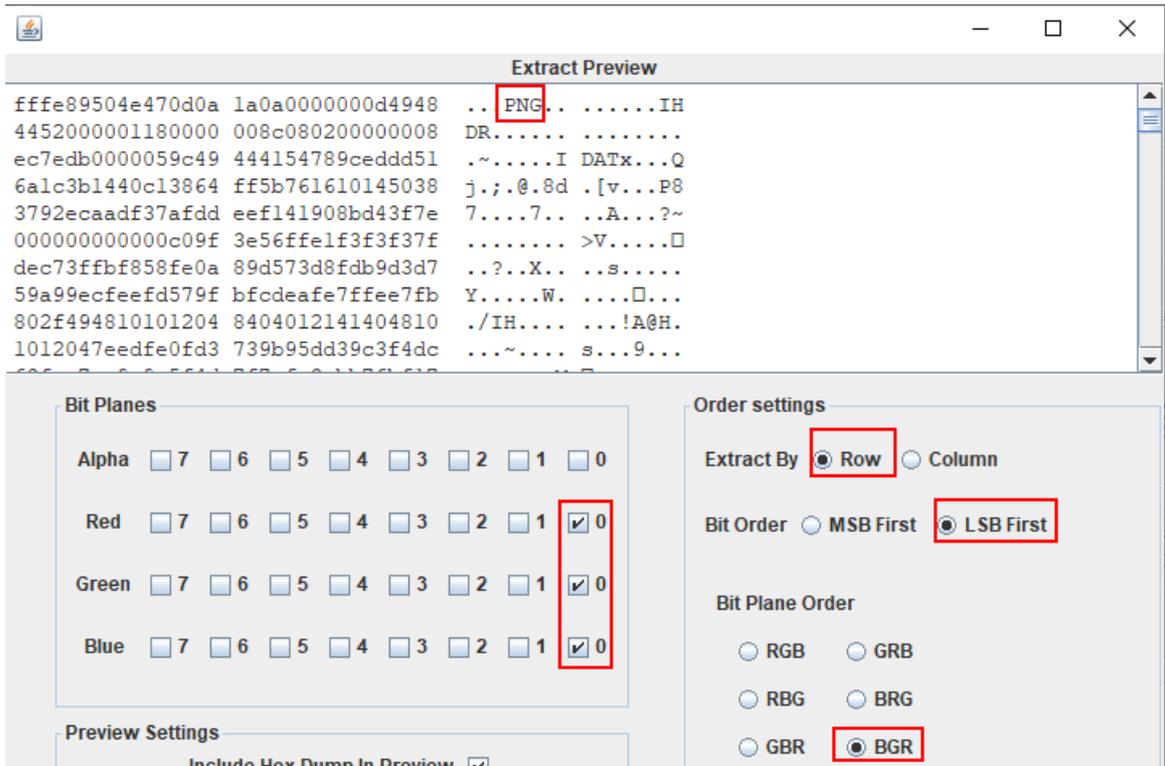
[普通的二维码](#)

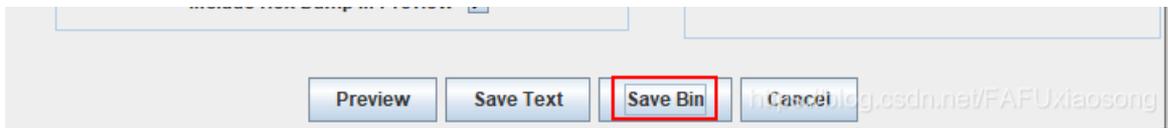
## 猫片(安恒)

(1) 将下载的文件后缀名改为png (注: png正常文件头: 89 50 4E 47)

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	44	52	PNG.....IHDR
00000010	00	00	02	80	00	00	02	80	08	02	00	00	00	83	af	5e	...€...€.....儻^D

(2) 根据提示LSB和BGR, 用stegsolve工具打开, 发现一张png图片





(2) 将其保存下来，并修改后缀名为.png，但无法打开。用notepad++打开，发现文件头错误

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	ff	fe	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	错PNG.....IHDR
00000010	44	52	00	00	01	18	00	00	00	8c	08	02	00	00	00	08	DR.....?.....

(3) 将前面的ff fe删掉并保存，打开图片，是半张二维码



(4) 修改图片高度试试，改为和长度一样。

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	44	52	错PNG.....IHDR
00000010	00	00	01	18	00	00	00	8c	08	02	00	00	00	08	ec	7e	.....?.....
00000020	db	00	00	05	9c	49	44	41	54	78	9c	ed	dd	51	6a	1c	?..浪DATx濞鞞j.00

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	44	52	错PNG.....IHDR
00000010	00	00	01	18	00	00	01	18	08	02	00	00	00	08	ec	7e	.....
00000020	db	00	00	05	9c	49	44	41	54	78	9c	ed	dd	51	6a	1c	?..浪DATx濞鞞j.00

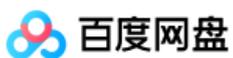


(5) 看到了完整的二维码，但和正常的有些不一样，中间的正方形应为黑色。用画图工具反色一下（新建->粘贴来源->右键-反色->裁剪）





(6) 扫描器扫描，得到一个网址，是一个百度云链接



网盘

分享

一刻相册

更多

SVIP新人礼! 最低仅12元

flag.rar

保存到网盘

下载(766B)

保存到手机

举报

2017-12-06 07:23 失效时间: 永久有效

赞(5)



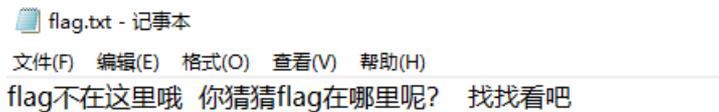
文件大小:766B

<https://blog.csdn.net/FAFUxiaosong>

(7) 下载下来后，是一个rar压缩包，但解压时出现了问题，可以用WinRAR打开



(8) 不过依然得到一个flag.txt文件

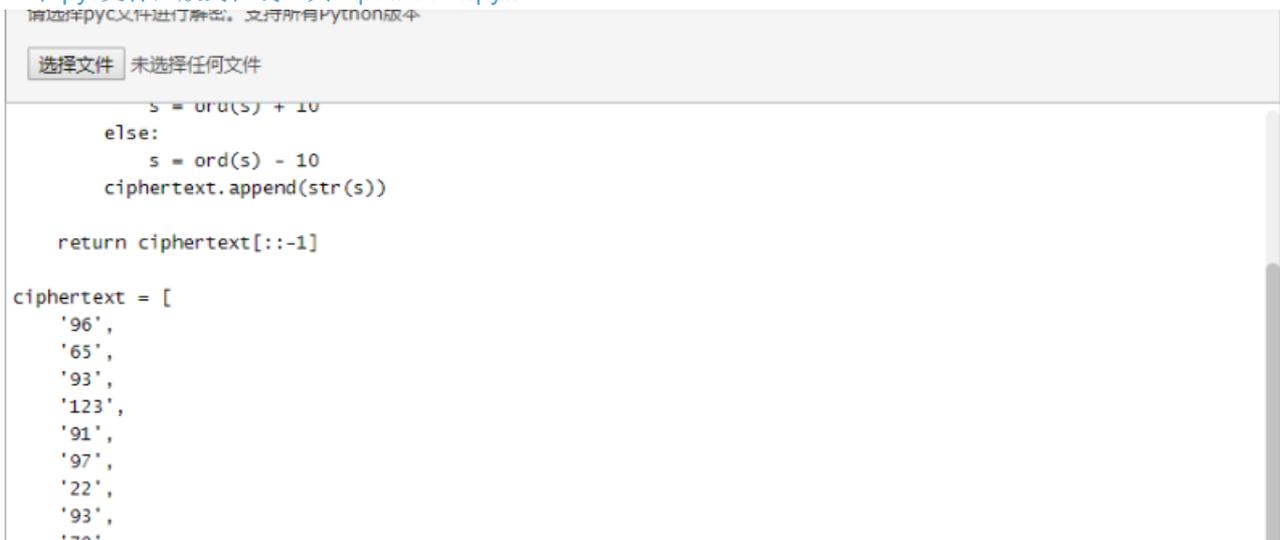


(9) 根据hint里的提示“NTFS”,用NtfsStreamsEditor查看数据流，然后导出。

#flag.rar这个压缩文件一定要用winrar来解压才能找得到数据流。



(10) 一个.pyc文件，放到在线工具<https://tool.lu/pyc/>



```
'102',  
'94',  
'132',  
'46',  
'112',  
'64',  
'97',  
'88'
```

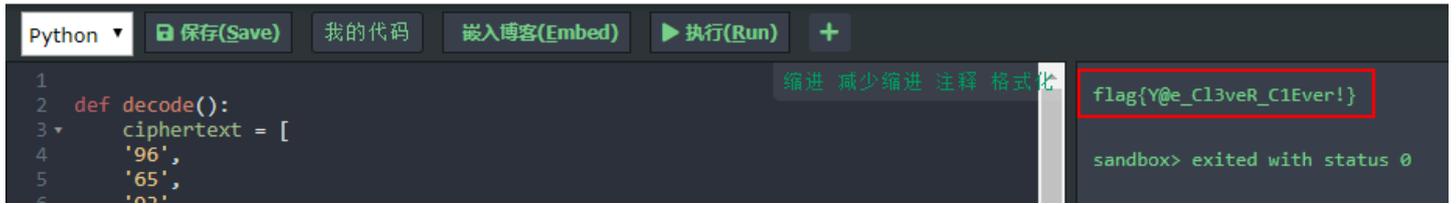
<https://blog.csdn.net/FAFUxiaosong>

(11) 根据这个加密脚本，再写一个解密脚本

```
def decode():  
    ciphertext = [  
        '96',  
        '65',  
        '93',  
        '123',  
        '91',  
        '97',  
        '22',  
        '93',  
        '70',  
        '102',  
        '94',  
        '132',  
        '46',  
        '112',  
        '64',  
        '97',  
        '88',  
        '80',  
        '82',  
        '137',  
        '90',  
        '109',  
        '99',  
        '112']  
    ciphertext.reverse()  
    flag = ''  
    for i in range(len(ciphertext)):  
        if i % 2 == 0:  
            s = int(ciphertext[i]) - 10  
        else:  
            s = int(ciphertext[i]) + 10  
        s=chr(i^s)  
        flag += s  
    return flag  
  
def main():  
    flag = decode()  
    print(flag)  
  
if __name__ == '__main__':  
    main()
```

(12) 用代码在线工具执行一下<https://tool.lu/coderunner/>

## 在线工具



The screenshot shows an online code runner interface. At the top, there is a language selector set to 'Python', a '保存(Save)' button, a '我的代码' button, an '嵌入博客(Embed)' button, a '执行(Run)' button, and a '+' button. Below the toolbar, the code editor contains the following Python code:

```
1
2 def decode():
3     ciphertext = [
4         '96',
5         '65',
6         '02']
```

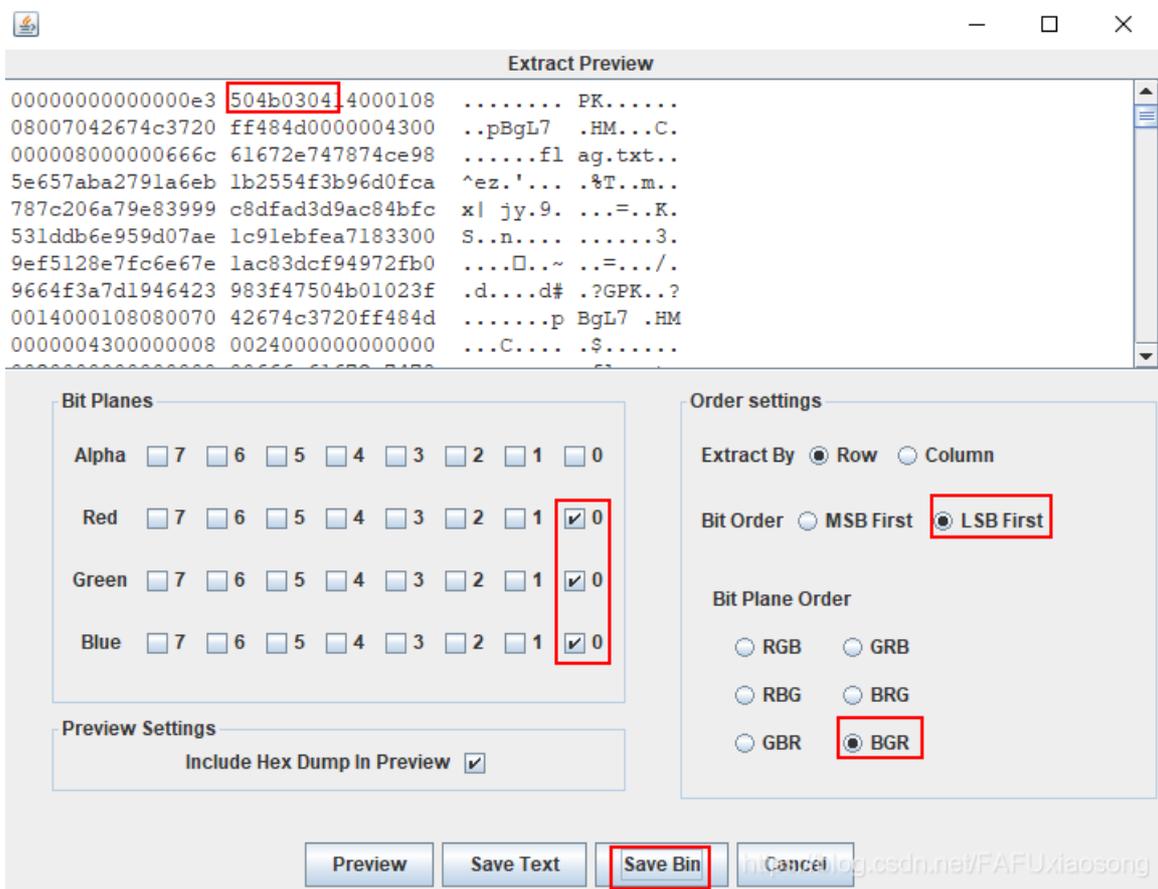
On the right side, the execution output is displayed in a terminal window. The first line is `flag{Y@e_C13veR_C1Ever!}`, which is highlighted with a red box. The second line is `sandbox> exited with status 0`. Above the terminal output, there are buttons for '缩进', '减少缩进', '注释', and '格式化'.

多彩

(1) 得到一张.png的图片,在notepad++里没有发现有用信息



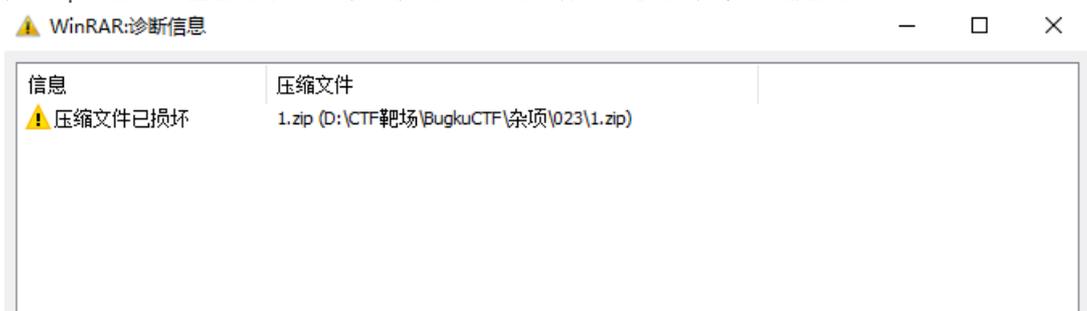
(2) 放到stegsolve里分析,发现了图片中隐藏的数据,是一个压缩包,将其抽取出来



(3) 先用notepad++打开这个压缩包,删掉文件头前面的东西,然后保存

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	00	00	00	00	00	00	00	e3	50	4b	03	04	14	00	01	08	..... K.....
00000010	08	00	70	42	67	4c	37	20	ff	48	4d	00	00	00	43	00	..pBgL7 HM...C.
00000020	00	00	08	00	00	00	66	6c	61	67	2e	74	78	74	ce	98	.....flaq.txt?[]

(4) 把后缀名改为zip,解压,但出错了,后缀名改为.rar也是这样(不执行第3步也会出错)



(5) 看了一些大佬的writeup,压缩文件是加密的,需要用到图片中的色号。但我这里直接显示出错,没让我输入密码。后面就不会做了。(呜呜)

1,27,59,11,23,7,57,1,1,76,222,1,1,50,214,6,77,50,53,214,6

## 旋转跳跃

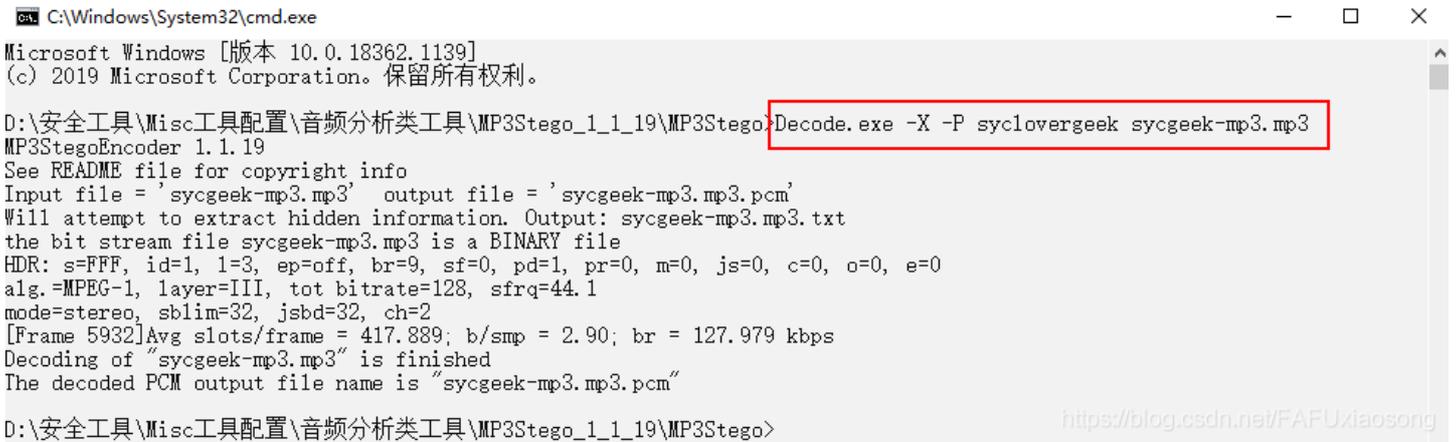
100

熟悉的声音中貌似又隐藏着啥 **key: syclovergeek**

题目来源: 第七季极客大挑战 <https://blog.csdn.net/FAFUxiaosong>

(1) 附件是一个音频文件, 使用工具MP3Stego来对音频进行解码。将该音频文件拷贝到MP3Stego目录下, 在目录栏里输入cmd打开运行窗口。输入如下命令解码

```
Decode.exe -X -P syclovergeek sycgeek-mp3.mp3 // -P后面即为题目提示的密码
```

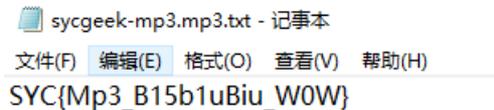


```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.18362.1139]
(c) 2019 Microsoft Corporation。保留所有权利。

D:\安全工具\Misc工具配置\音频分析类工具\MP3Stego_1_1_19\MP3Stego>Decode.exe -X -P syclovergeek sycgeek-mp3.mp3
MP3StegoEncoder 1.1.19
See README file for copyright info
Input file = 'sycgeek-mp3.mp3' output file = 'sycgeek-mp3.mp3.pcm'
Will attempt to extract hidden information. Output: sycgeek-mp3.mp3.txt
the bit stream file sycgeek-mp3.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 5932]Avg slots/frame = 417.889; b/smp = 2.90; br = 127.979 kbps
Decoding of "sycgeek-mp3.mp3" is finished
The decoded PCM output file name is "sycgeek-mp3.mp3.pcm"

D:\安全工具\Misc工具配置\音频分析类工具\MP3Stego_1_1_19\MP3Stego>
```

(2) 解码完后, 在MP3Stego目录下多了一个sycgeek-mp3.mp3.txt文件, 打开即可看到flag。



```
sycgeek-mp3.mp3.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
SYC{Mp3_B15b1uBiu_W0W}
```

## 普通的二维码

(1) 下载附件，得到一张二维码，扫描后没有flag。用notepad++打开看看



(2) 在最后发现一串数字，想到ASCII码，146作为八进制时对应的是f。然后把这串数字转换成对应的字符，得到flag。

### Ascii Encoding

Text

```
flag{Have_y0U_Py_script_Otc_To_Ten_Ascii!}
```

Bin

```
1100110 1101100 1100001 1100111 1111011 1001000 1100001 1110110 1100101 1011111 1111001 110000 1010101
1011111 1010000 1111001 1011111 1110011 1100011 1110010 1101001 1110000 1110100 1011111 1001111
1110100 1100011 1011111 1010100 1101111 1011111 1010100 1100101 1101110 1011111 1000001 1110011
```

Oct

```
146 154 141 147 173 110 141 166 145 137 171 60 125 137 120 171 137 163 143 162 151 160 164 137 117 164 143 137
124 157 137 124 145 156 137 101 163 143 151 151 41 175
```

Dec

```
102 108 97 103 123 72 97 118 101 95 121 48 85 95 80 121 95 115 99 114 105 112 116 95 79 116 99 95 84 111 95 84 101
110 95 65 115 99 105 105 33 125
```

Hex

```
66 6c 61 67 7b 48 61 76 65 5f 79 30 55 5f 50 79 5f 73 63 72 69 70 74 5f 4f 74 63 5f 54 6f 5f 54 65 6e 5f 41 73 63 69 69 21
7d
```

<https://blog.csdn.net/FAFUxiaosong>