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

本文链接：https://blog.csdn.net/FAFUxiaosong/article/details/109400979

BugkuCTF_杂项

猫片(安恒)

多彩

旋转跳跃

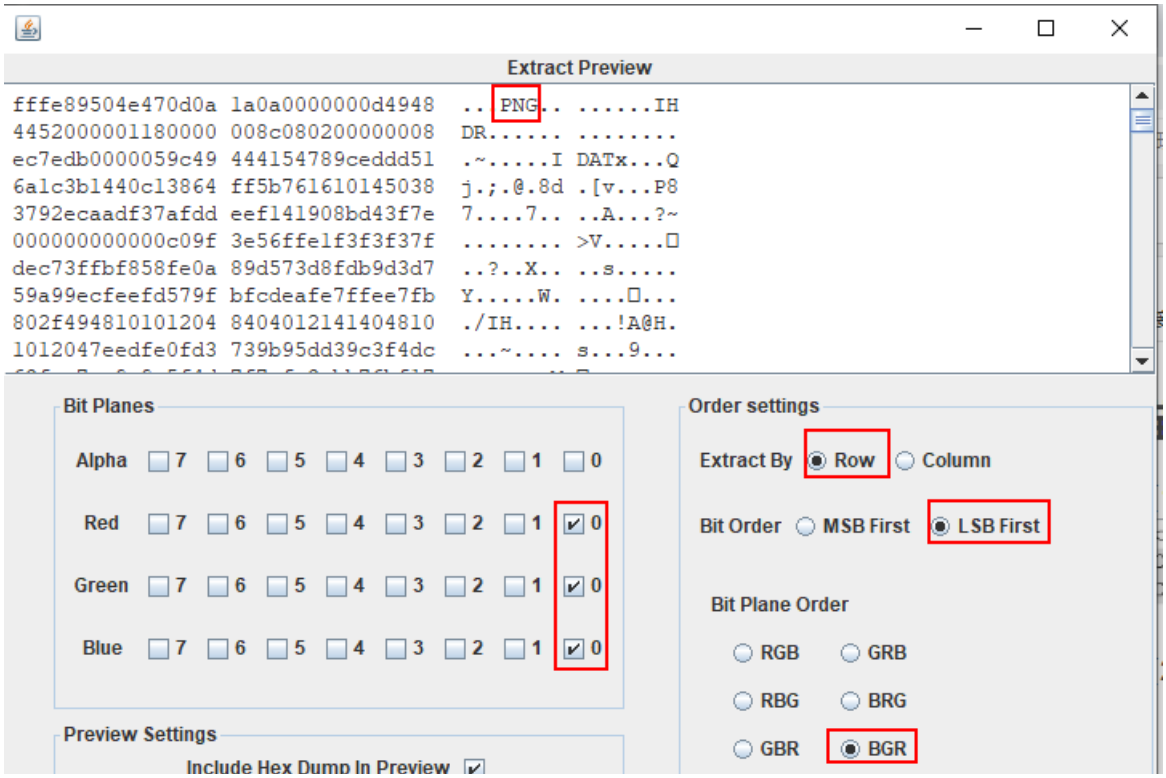
普通的二维码

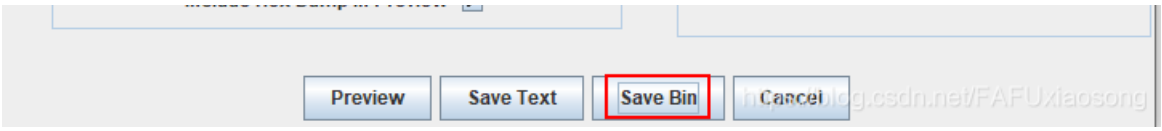
猫片(安恒)

（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	塒NG.....IHDR
00000010	00	00	02	80	00	00	02	80	08	02	00	00	00	83	af	5e	...€...€.....^

（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	镩PNG.....IH
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。

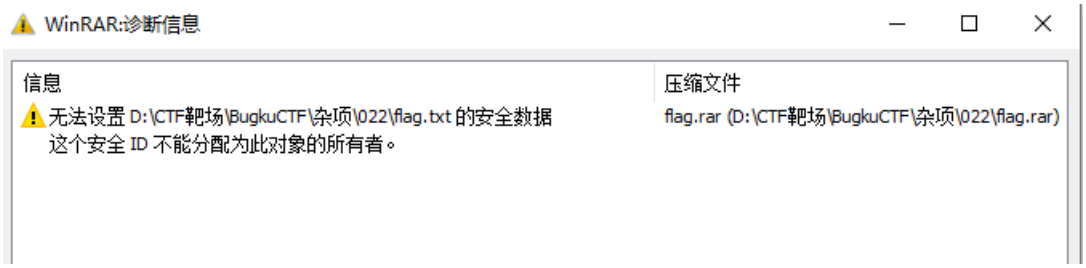
Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	44	52	塒NG.....IHDR[
00000010	00	00	01	18	00	00	00	8c	08	02	00	00	00	08	ec	7e	.....?.....靭□[
00000020	db	00	00	05	9c	49	44	41	54	78	9c	ed	dd	51	6a	1c	?..涙DATx澀輗j.□[

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	塒NG.....IHDR[
00000010	00	00	01	18	00	00	01	18	08	02	00	00	00	08	ec	7e	.....靭□[
00000020	db	00	00	05	9c	49	44	41	54	78	9c	ed	dd	51	6a	1c	?..涙DATx澀輗j.□[

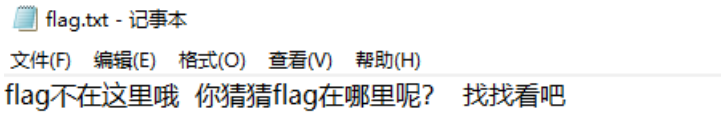
（5）看到了完整的二维码，但和正常的有些不一样，中间的正方形应为黑色。用画图工具反色一下（新建–>粘贴来源–>右键–反色–>裁剪）

（6）扫描器扫描，得到一个网址，是一个百度云链接

（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



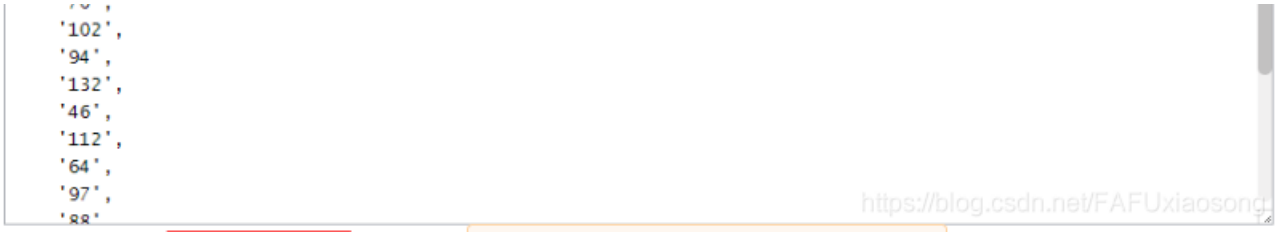
（8）不过依然得到一个flag.txt文件



（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/



（11）根据这个加密脚本，再写一个解密脚本

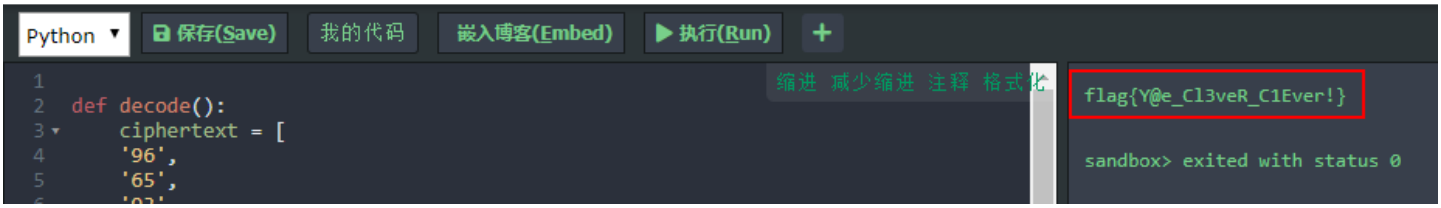
```
def decode():
    ciphertext = [
    '96',
    '65',
    '93',
    '123',
    '91',
    '97',
    '22',
    '93',
    '70',
    '102',
    '94',
    '132',
    '46',
    '112',
    '64',
    '97',
    '88',
    '80',
    '82',
    '137',
    '90',
    '109',
    '99',
    '112']
    ciphertext.reverse()
    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/

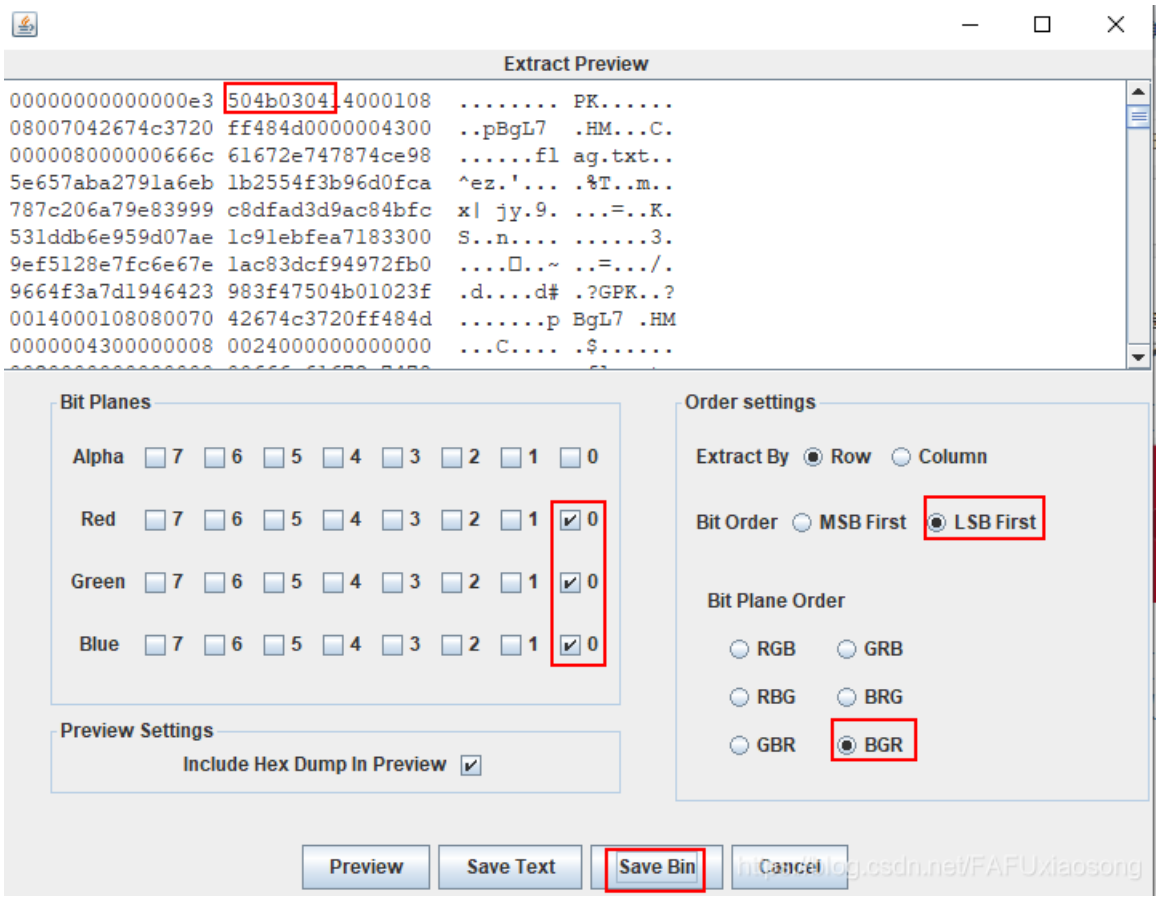
在线工具



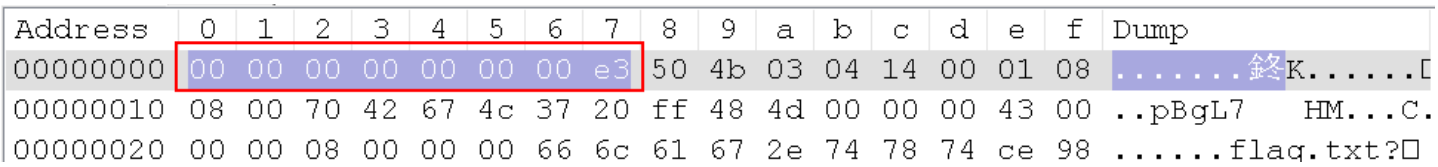
多彩

（1）得到一张.png的图片,在notepad++里没有发现有用信息

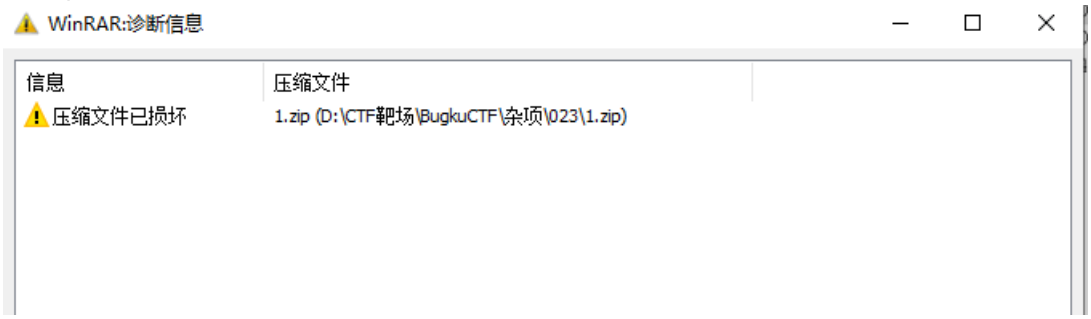
（2）放到stegsolve里分析，发现了图片中隐藏的数据，是一个压缩包，将其抽取出来



（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



（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）



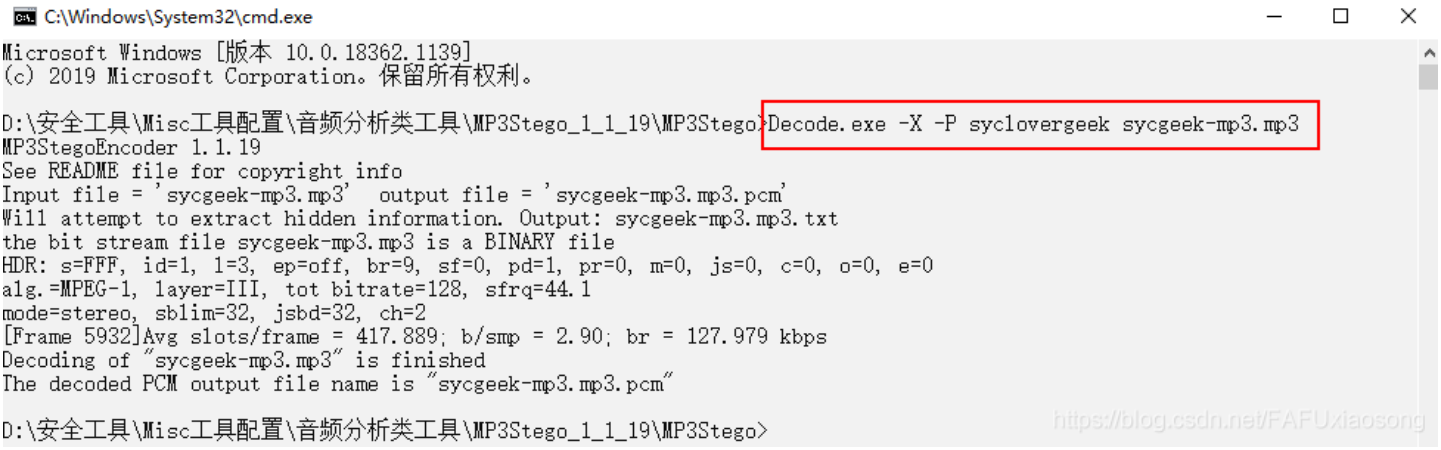
（5）看了一些大佬的writeup，压缩文件是加密的，需要用到图片中的色号。但我这里直接显示出错，没让我输入密码。后面就不会做了。（嘤嘤嘤）

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

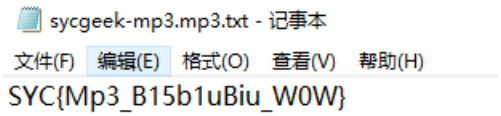
旋转跳跃

（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
```

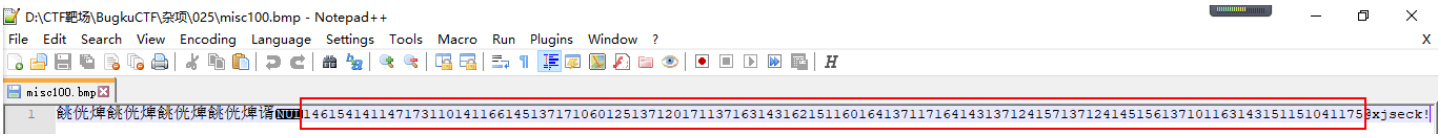


（2）解码完后，在MP3Stego目录下多了一个sycgeek-mp3.mp3.txt文件，打开即可看到flag。



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。