# BUUCTF记录 Misc

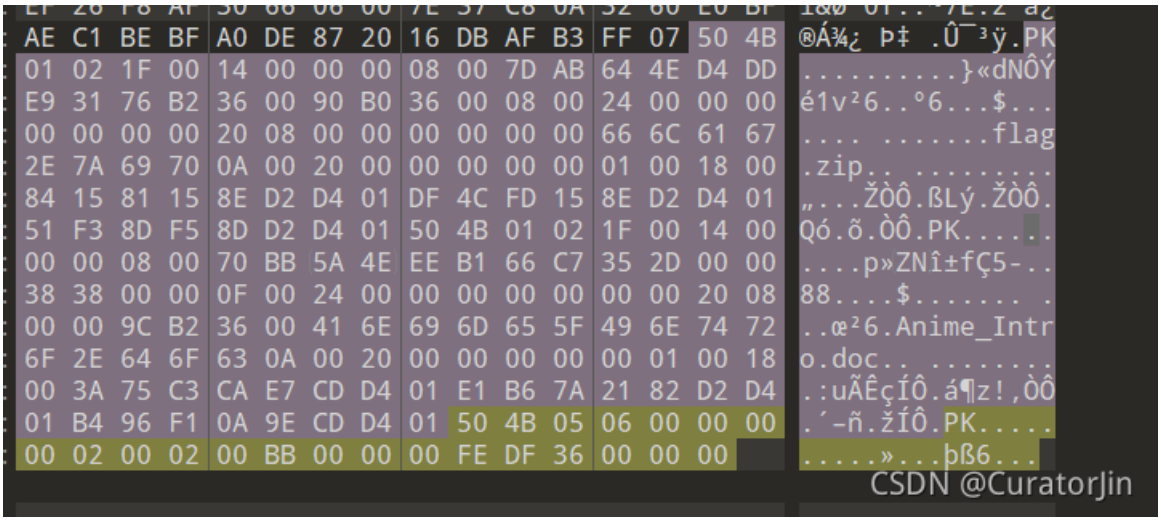
原创

CuratorJin 于 2021-10-11 22:10:00 发布 20 收藏 1
文章标签： html html5

本文链接：https://blog.csdn.net/CuratorJin/article/details/120430463


## [*CTF2019]otaku

下载得到attachment.zip




通过010editor发现其中flag.zip为伪加密，修改加密位后解压文件

flag.zip中last words.txt提示用明文攻击

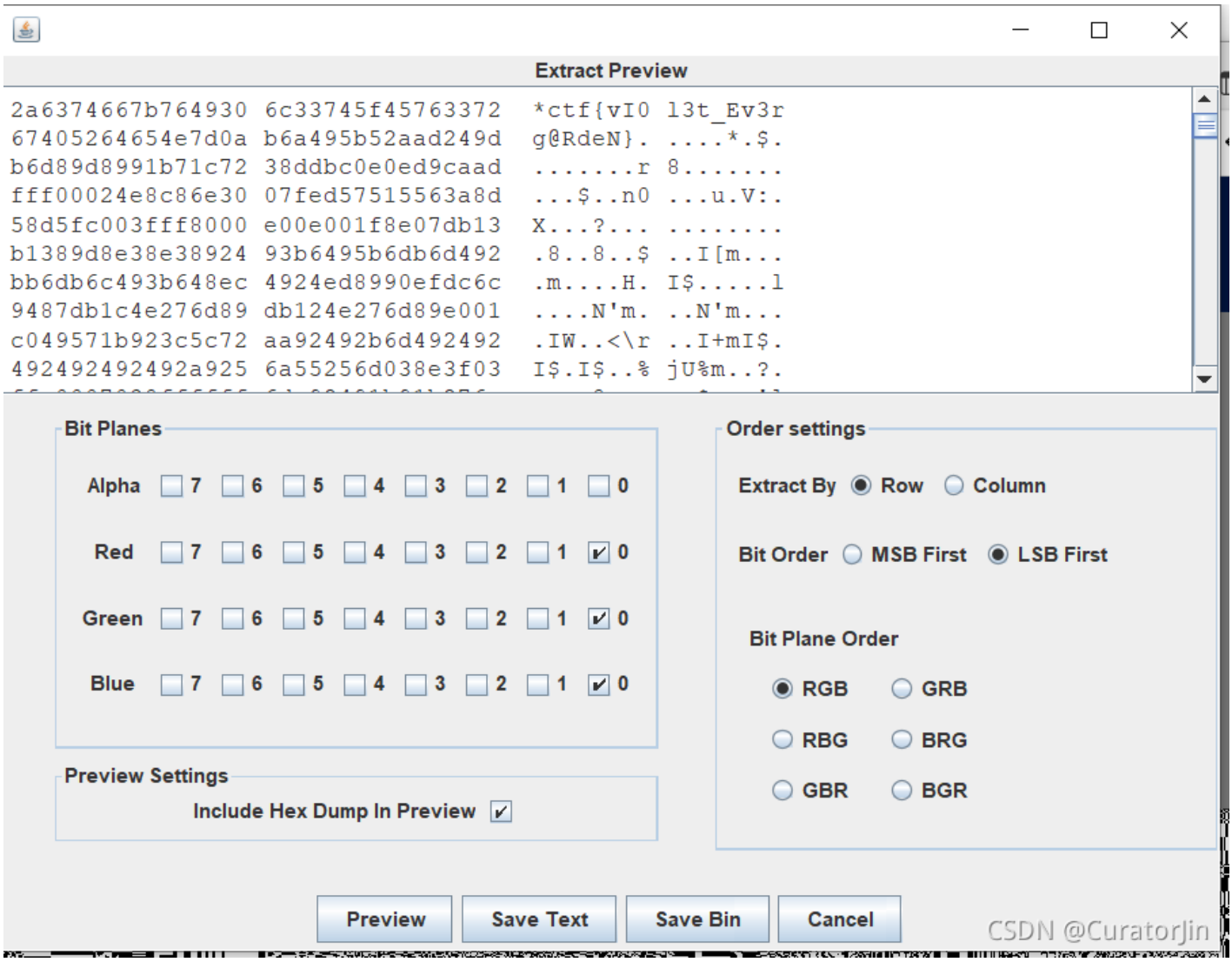
打开另一个doc文件，发现文字间格式不一样，可推测其中有坑

其中隐藏的文字即破解压缩包所需的last word.txt

这里面还有个坑就是需要将last word.txt中编码转为gbk编码，否则所得到的CRC32值不一样，无法进行爆破

爆破后得到flag.png

最后还得通过lsb隐写才能得到flag




## [湖南省赛2019]Findme

可以看看大佬的wp，写的很详细

(3条消息) BuuCTF难题详解| Misc | [湖南省赛2019]Findme_pone2233的博客-CSDN博客
https://blog.csdn.net/pone2233/article/details/107990787我爬了

## [INSHack2018]Self Congratulation

下载得到附件


观察左上方有一小块奇怪的东西

以白块为0，黑块为1，对图片尝试解码：
00110001001
10010001100
11001101000
01101010011
01100011011
10011100000

发现01串长度为66，为6的倍数，考虑base64解码

```
table=['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T',
a='00110001001100100011001100110100001101010011011000110111001100000'
str=''
tmp=''
for i in range(len(a)):
    tmp+=a[i]
    if i%6==5:
        str+=table[int(tmp,2)]
        tmp=''
print(str)
print(base64.b64decode('MTIzNDU2Nzg='))
```

得到flag{12345678}(好简单的flag)