CTF Misc -- base64隐写

原创

Cer0 于 2019-10-20 22:43:14 发布 1913 收藏 9
分类专栏： CTF 文章标签： CTF

昨天参加比赛，打酱油的同时学到不少新知识，可能是由于自己知识面比较窄的原因，学到一个新的隐写方法--base64隐写，base64编码经常见到，但是利用base64来隐藏一些信息还是第一次遇到，网上搜了一下，文章还挺多，引用一下大神们的成果吧。

首先是base64编码解码原理

base64编码原理

字符对应ASCII转换成八位二进制

base64的基础单位是 3*8bit的二进制，若是不够3*8bit则在后面添加0字节（padding）直至满足

3*8bit的二进制转换成4*6bit的二进制

4*6bit的二进制转换成十进制

对照base64表把十进制转换成字符

base64解码原理

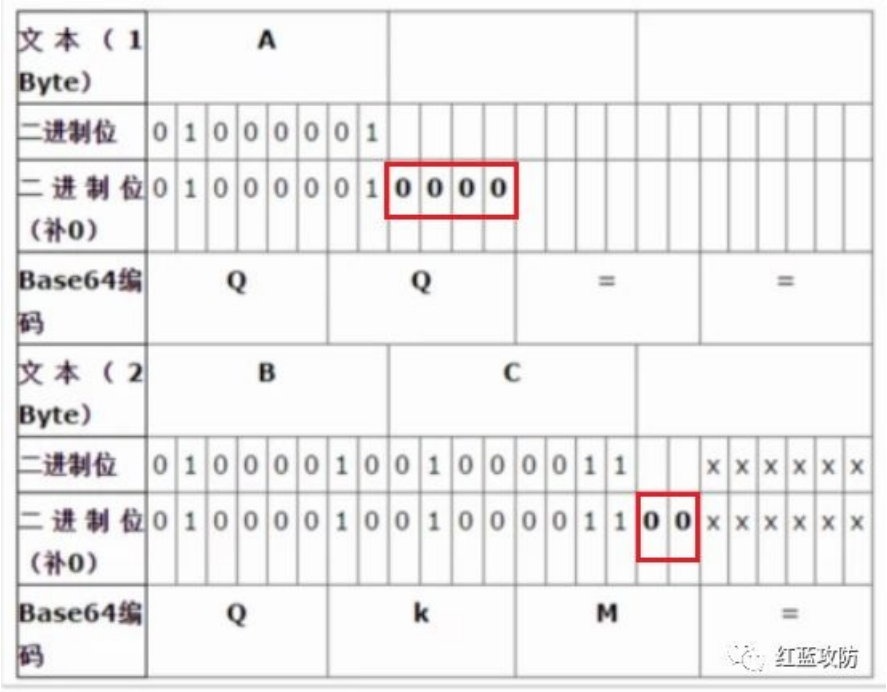
检查base64编码后面有几个等于号

把字符串按照base64表转换成4*6的倍数位数二进制

删除等于号的个数*8的bit

按照6个bit一组转成字符

下图为base64编码的过程



base64隐写原理

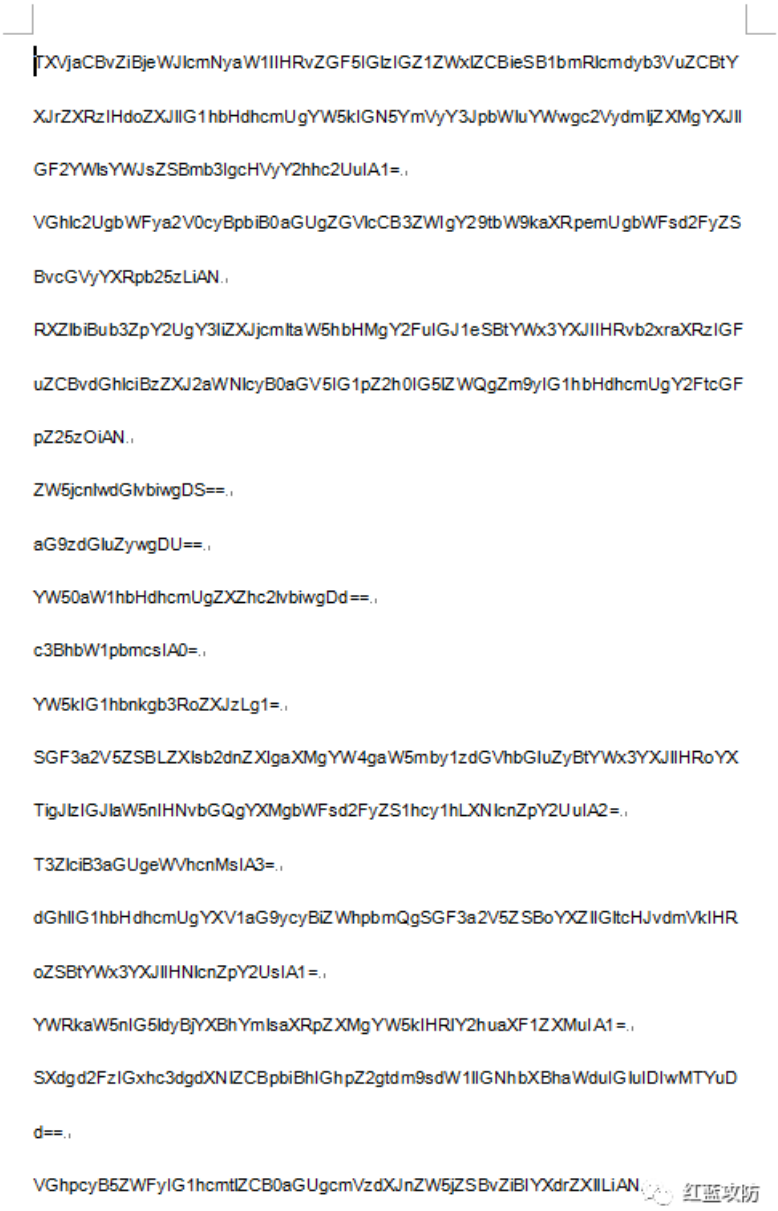
解码的时候，会删除等号的个数*8的bit，而且只用6个bit表示一个等于号(000000)，那么，可以控制等号*2bit的字符(上图中加粗的0)，用于隐藏关键信息，并且不影解码的内容。

附上大神的base64隐写及解码脚本：

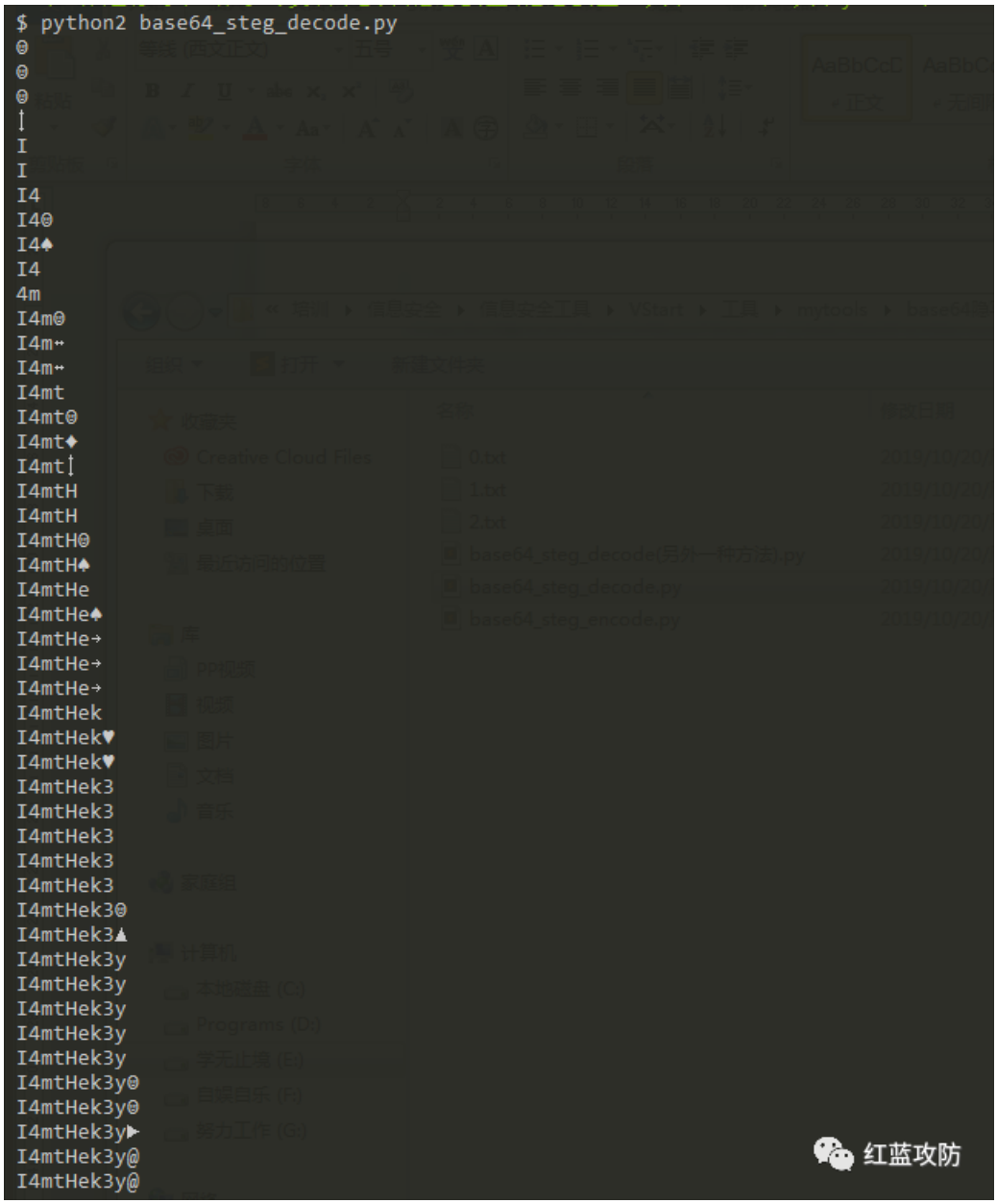
```
# -*- coding: utf8 -*-
#base64隐写加密脚本，python2 运行
import base64


#flag需要隐写的字符串
flag = 'Cer0{Base64_steg_1s_s0_F4n}'
bin_str = ''.join([bin(ord(c)).replace('0b', '').zfill(8) for c in flag])
base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'


#'0.txt'是明文, '1.txt'用于存放隐写后的 base64
with open('0.txt', 'rb') as f0, open('1.txt', 'wb') as f1:
    for line in f0.readlines():
        rowstr = base64.b64encode(line.replace('\n', ''))
        equalnum = rowstr.count('=')
        if equalnum and len(bin_str):
            offset = int('0b'+bin_str[:equalnum * 2], 2)
            char = rowstr[len(rowstr) - equalnum - 1]
            rowstr = rowstr.replace(char, base64chars[base64chars.index(char) + offset])
            bin_str = bin_str[equalnum*2:]
        f1.write(rowstr + '\n')
```

```
# -*- coding: utf-8 -*-
#base64解码脚本，Python2 运行

b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'

# 2.txt为需要解码的文件
with open('2.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = ''.join(line.split())
        rowb64 =  ''.join(stegb64.decode('base64').encode('base64').split())
        offset = abs(b64chars.index(stegb64.replace('=','')[-1])-b64chars.index(rowb64.replace('=','')[-1])
        equalnum = stegb64.count('=') #no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
        print ''.join([chr(int(bin_str[i:i + 8], 2)) for i in xrange(0, len(bin_str), 8)]) #8位一组
```

举个栗子：昨天的比赛有个Misc题(题目文件见附件)，解题过程得到一个word文件，打开之后得到很多base64编码的字符串，像这样：



大神们一看应该就知道这是在考察base64隐写，直接解码就行，将字符串复制到2.txt文件中，运行上面的解码脚本。



得到隐藏在文件中的关键字符串。要将指定内容进行隐写，直接运行加密脚本即可。

参考文章： https://www.tuicool.com/articles/RRr2miE

更多资料： https://www.tr0y.wang/2017/06/14/Base64steg/

https://www.jianshu.com/p/48fe4dd3e5ce

附件下载地址：

链接：https://pan.baidu.com/s/10lt0rCb7Dtblo8onJN0c0g&shfl=sharepset

提取码：bzor
