攻防世界 - MISC - 11 - base64stego

原创

古月浪子 于 2019-10-03 18:28:38 发布 4941 收藏 5

分类专栏： 攻防世界CTF新手练习区 文章标签： 攻防世界 XCTF CTF WP writeup

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/tqydyqt/article/details/102002577

版权


攻防世界CTF新手练习区 专栏收录该内容

11 篇文章 7 订阅

订阅专栏

攻防世界 - MISC - 11 - base64stego

审题

思路

结合题目、题干和上一题，初步推断这一题跟base64是过不去了

知识点

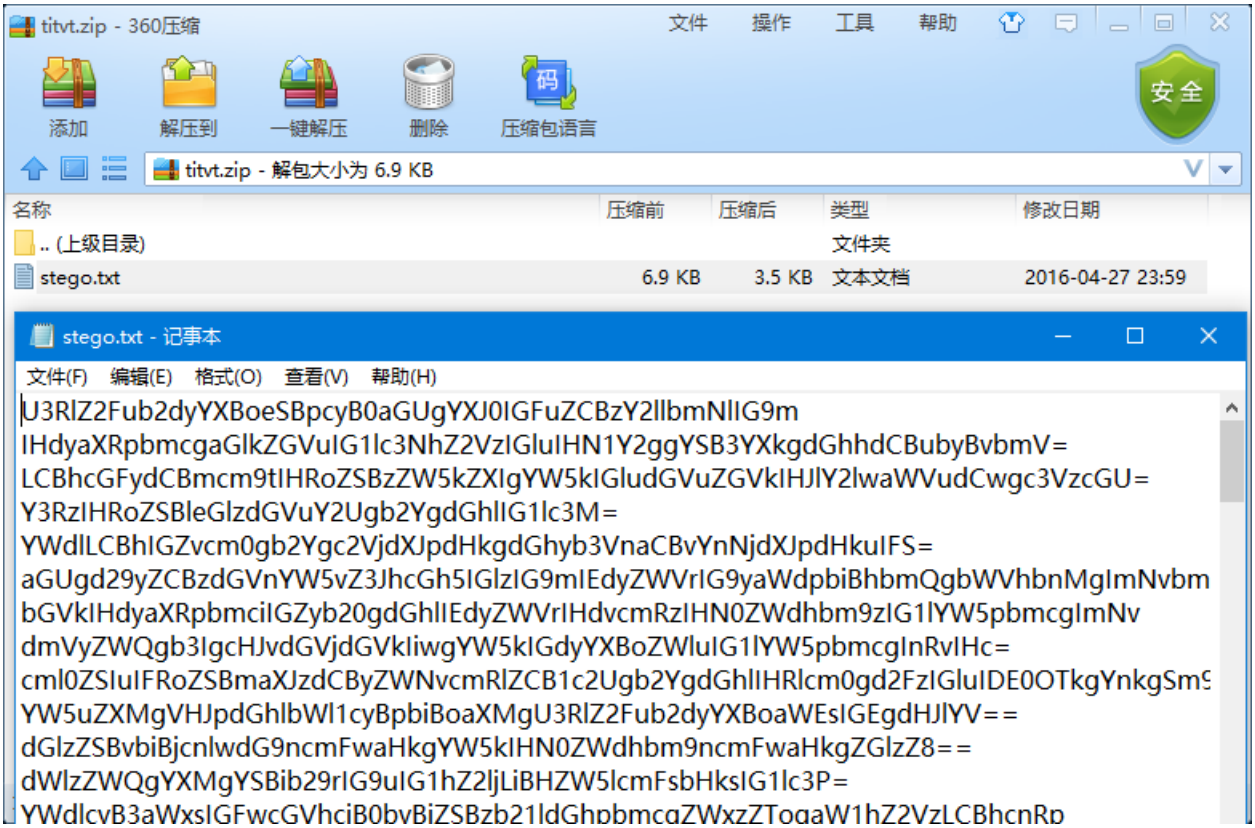
考查选手对base64隐写的理解

所需工具

无

解题

用360压缩打开附件，发现其中的stego.txt里有许多base64编码后的字符串



强行base64解密会得到一堆毫无用处的数据，显然flag被隐写在了文本的某处
我们知道，base64是6bit编为1个字符，而1个字节是8bit，因此base64可能会出现3种情况：刚好能编完（例如3个字节的字符串base64加密后有4个字符）、剩余2bit（例如2个字节的字符串base64加密后第3个字符只编码了4bit，此时使用=补充6bit）、剩余4bit（例如1个字节的字符串base64加密后第2个字符只编码了2bit，此时使用==补充12bit），由于第3/2个字符只编码了4/2bit，所以只有前面被编码的bit是有效的，而后面的bit则在正常情况下默认填0，因此可以将想隐写的数据隐藏在后面的bit中，即：1个=可以隐藏2个bit
我们将这些bit读出来，拼在一起转换为字符串即可获得flag

flag

flag{Base_sixty_four_point_five}

反思与心得

这个题的解密脚本有点难写，而且隐写的思路也很新奇，给1★感觉有点低了