攻防世界-MISC:base64stego

原创

LY613313 于 2021-11-25 17:48:14 发布 197 收藏

分类专栏： 攻防世界 文章标签： 安全

本文链接：https://blog.csdn.net/m0_56161093/article/details/121524866

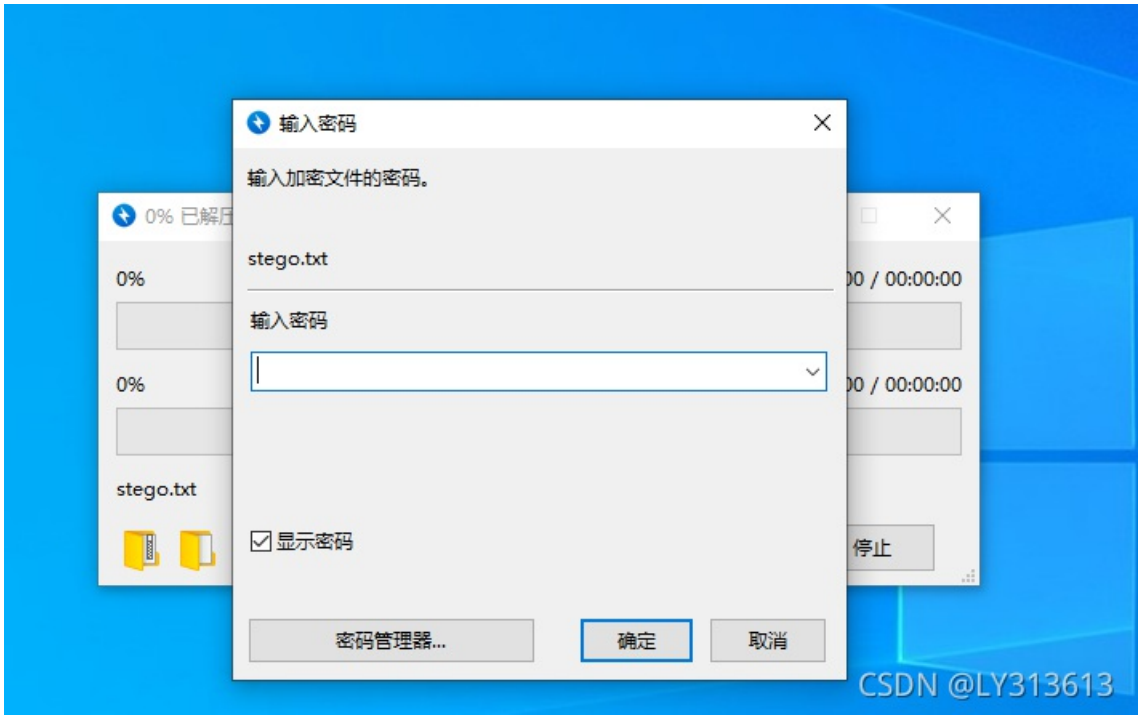

攻防世界 专栏收录该内容

21 篇文章 1 订阅

订阅专栏

这是攻防世界新手练习区的第十一题，题目如下：

点击下载附件一，发现是一个压缩包，点击解压，发现是需要密码才能解密



先用UltraEdit打开这个压缩包，这里需要知道zip压缩包的组成部分，包括压缩源文件数据区、压缩源文件目录区、压缩源文件目录结束区，具体组成如下：

压缩源文件数据区(组成/长度)	
文件头标记	4 bytes(0x04034b50)
解压文件所需的 pkware 版本	2 bytes
全局方式位标记(判断真伪加密)	2 bytes
压缩方式	2 bytes
最后修改文件时间	2 bytes
最后修改文件日期	2 bytes
CRC-32 校验	4 bytes
压缩后尺寸	4 bytes
未压缩尺寸	4 bytes
文件名长度	2 bytes
扩展记录长度	2 bytes
文件名	不定长度
扩展字段	不定长度

压缩源文件目录区(组成/长度)	
目录中文件的文件头标记	4 bytes(0x02014b50)
压缩使用的 pkware 版本	2 bytes
解压缩所需的 pkware 版本	2 bytes
全局方式位标记(判断真伪加密)	2 bytes
压缩方式	2 bytes
最后修改文件时间	2 bytes
最后修改文件日期	2 bytes
CRC-32 校验	4 bytes
压缩后尺寸	4 bytes
未压缩尺寸	4 bytes
文件名长度	2 bytes
扩张字段长度	2 bytes
文件注释长度	2 bytes
磁盘开始号	2 bytes
内部文件属性	2 bytes
外部文件属性	4 bytes
局部文件偏移量	4 bytes
文件名	不定长度
扩展字段	不定长度
文件注释	不定长度

压缩源文件目录结束标志(组成/长度)	
目录结束标记	4 bytes(0x06054b50)
当前磁盘编号	2 bytes
目录区开始磁盘编号	2 bytes
本磁盘上记录总数	2 bytes
目录区中记录总数	2 bytes
目录区尺寸大小	4 bytes
目录区对第一张磁盘的偏移量	4 bytes
ZIP 文件注释长度	2 bytes
ZIP 文件注释	不定长度

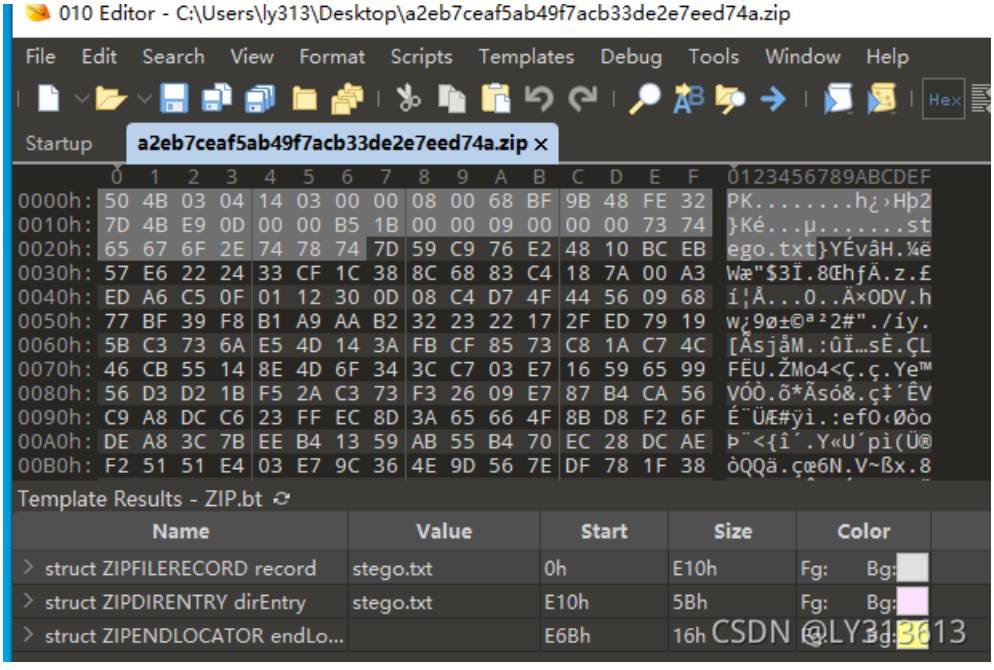
压缩包是否为伪加密的判断

> 1、无加密：
> （1）压缩源文件数据区的全局加密标志应当为00 00
> （2）且压缩源文件目录区的全局方式位标记应当为00 00

> 2、伪加密：
> （1）压缩源文件数据区的全局加密标志应当为00 00
> （2）且压缩源文件目录区的全局方式位标记应当为**09 00**

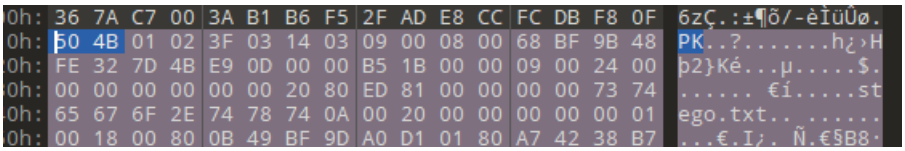
> 3、真加密
> （1）压缩源文件数据区的全局加密标志应当为09 00
> （2）且压缩源文件目录区的全局方式位标记应当为09 00

现在看一下这道题，该压缩包的压缩源文件的数据区如下



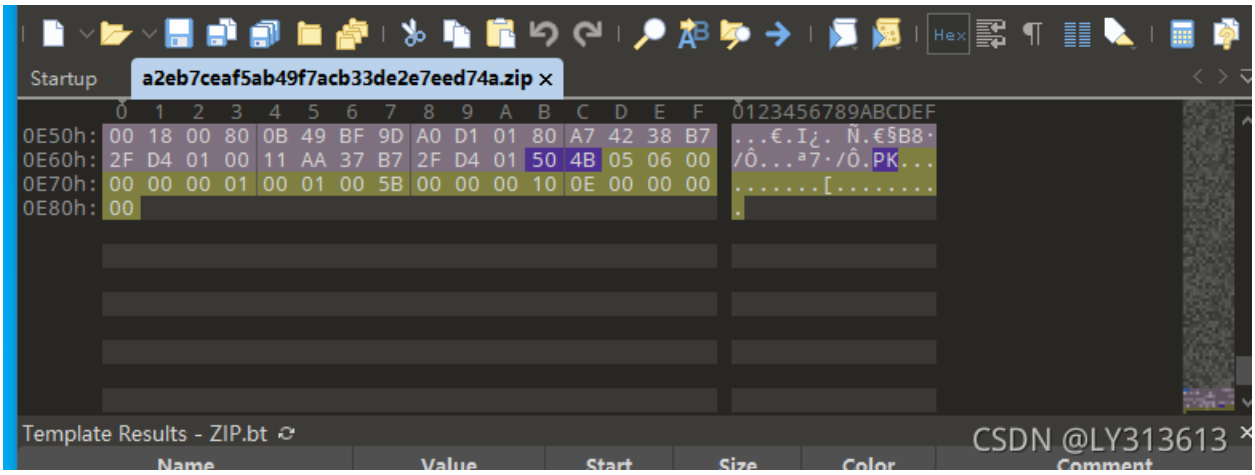
50 4B 03 04：文件头标记（0x04034B50）
14 03：解压文件所需 pkware 版本
00 00：全局方式位标记（判断真伪加密的重要标志）
08 00：压缩方式
68 BF：最后修改文件时间
9B 48：最后修改文件日期
FE 32 7D 4B：CRC-32校验
E9 0D 00 00：压缩后尺寸
B5 1B 00 00：未压缩尺寸
09 00：文件名长度
00 00：扩展记录长度

该压缩包的压缩源文件的目录区如下：



50 4B 01 02：目录中文件文件头标记(0x02014B50)
3F 03：压缩使用的 pkware 版本
14 03：解压文件所需 pkware 版本
09 00：全局方式位标记（数据区的加密标志为00 00，所以判断这是伪加密，将09 00 改为00 00即可）
08 00：压缩方式
68 BF：最后修改文件时间
9B 48：最后修改文件日期
FE 32 7D 4B：CRC-32校验（1480B516）
E9 0D 00 00：压缩后尺寸（25）
B5 1B 00 00：未压缩尺寸（23）
09 00：文件名长度
24 00：扩展字段长度
00 00：文件注释长度
00 00：磁盘开始号
00 00：内部文件属性
20 80 ED 81：外部文件属性
00 00 00 00：局部头部偏移量

该压缩包源文件目录结束标志如下：

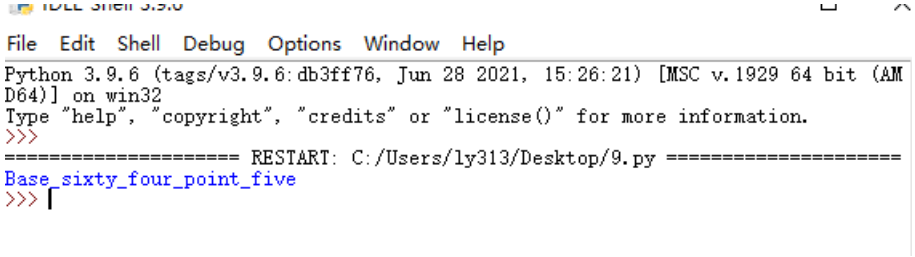


> 50 4B 05 06：目录结束的标记（0x06054B50）
> 00 00：当前磁盘编号
> 00 00：目录区开始磁盘编号
> 01 00：本磁盘上纪录总数
> 01 00：目录区中纪录总数
> 5B 00 00 00：目录区尺寸大小
> 10 0E 00 00：目录区对第一张磁盘的偏移量
> 00 00：ZIP 文件注释长度

所以，我们只要将该压缩包的压缩源文件的全局方式位标记由09 00 改为00 00即可解压该文件，
通过解压文件我们可以得到一个文本文档。打开后可以看到是一些base64字符，我们写个脚本跑一下

```
import base64
bin_str=''
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('stego.txt','r') as f:  # 这里要改成你的文件路径
 for line in f.readlines():
  s64="".join(line.split())
  r64="".join(str(base64.b64encode(base64.b64decode(s64)),'utf-8').split())
  offset=abs(b64chars.index(s64.replace('=','')[-1])-b64chars.index(r64.replace('=', '')[-1]))
  equal=line.count('=')
  if equal:
   bin_str += bin(offset)[2:].zfill(equal * 2)
 print(''.join([chr(int(bin_str[i:i + 8], 2)) for i in range(0,len(bin_str),8)]))
```

代码运行结果如下：



所以这道题的flag如下：

```
flag{Base_sixty_four_point_five}
```

以上就是我对这道题的解法。因本人菜鸡一只，如果有什么不对的地方，实属正常。还请各位大佬予以指正，谢谢！