



# BUUCTF ZIP伪加密

原创

宁嘉  于 2020-05-01 15:55:23 发布  2043  收藏 15

分类专栏: [BUUCTF Crypto](#) 文章标签: [加密解密](#)

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/MikeCoke/article/details/105877451>

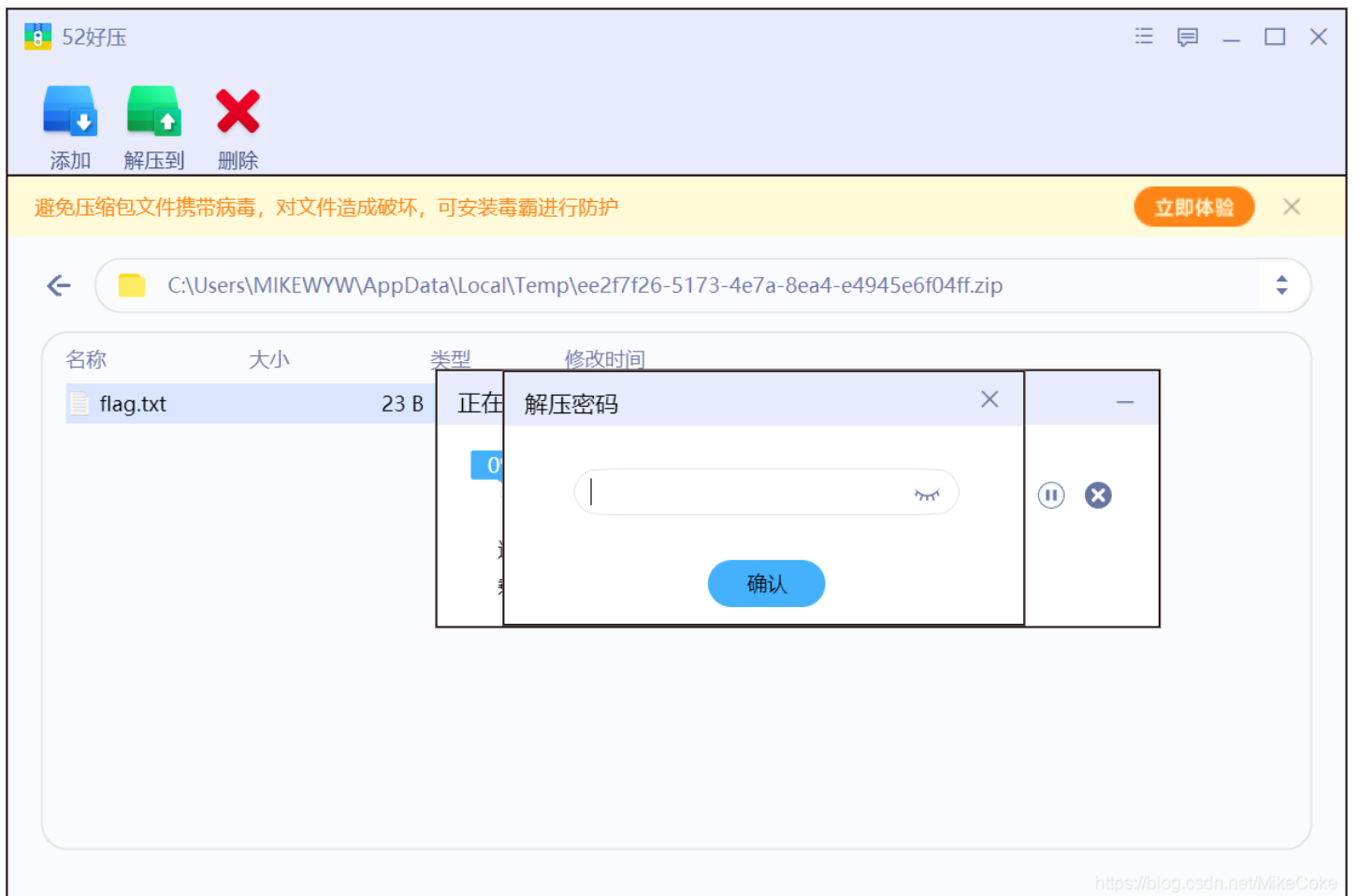
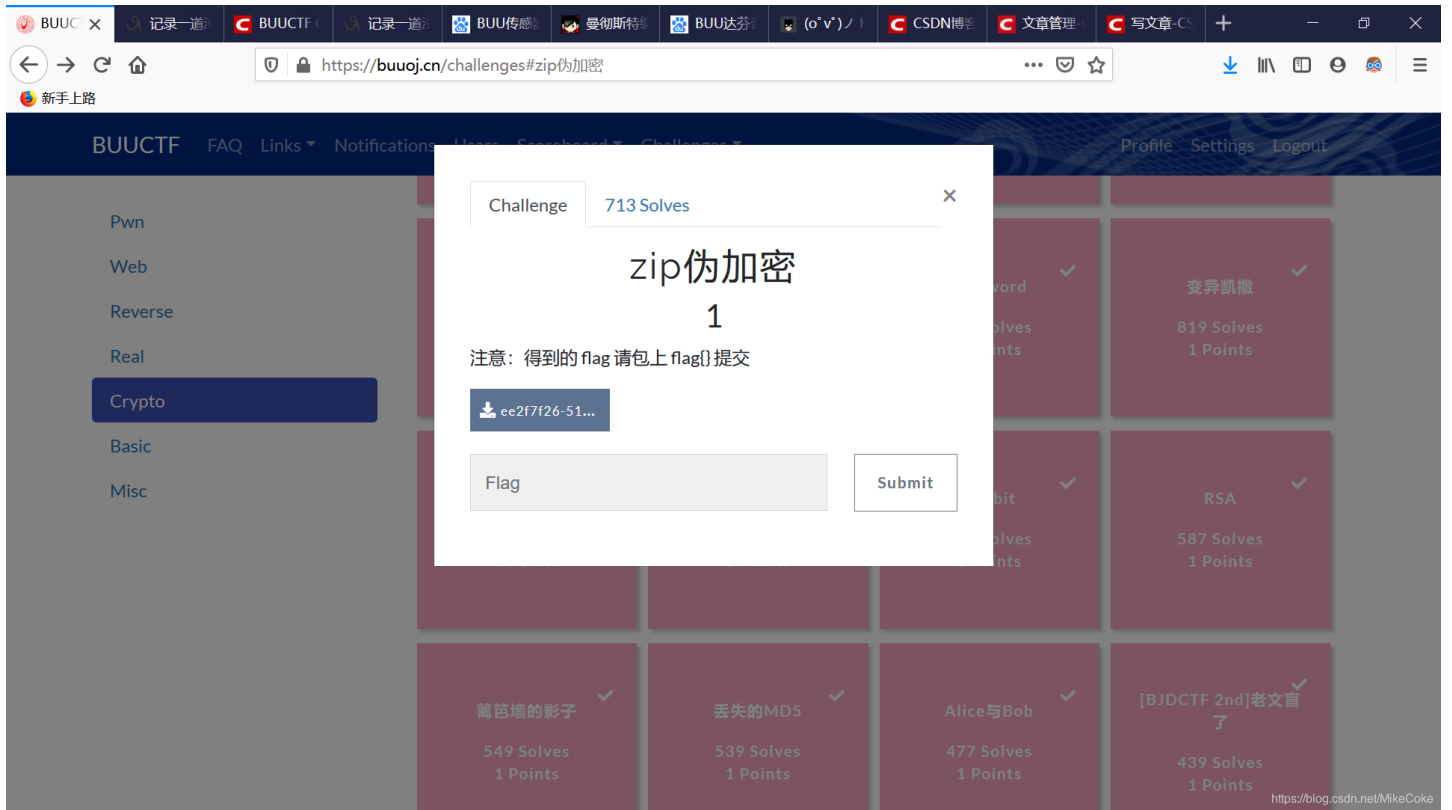
版权



[BUUCTF Crypto](#) 专栏收录该内容

34 篇文章 2 订阅

订阅专栏



发现压缩包无法解压

方法1（不一定每次都有用）：将压缩包直接发送给QQ好友，然后在手机上就能成功查看文件内容了。

钰杰 14:25  
对方已成功接收了你发送的离线

我的Android手机 14:23  
[图片]

开启消息漫游，可查看在其他设备产生的聊天记录。

2020/4/22 15:40:16

发起了屏幕分享

14:24:53

ee2f7f26-5173-4e...ff.zip (175.00B)  
已转发该文件

打开 打开文件夹 转发

对方已成功接收了你发送的离线文件“ee2f7f26-5173-4e7a-8ea4-e4945e6f04ff.zip” (175.00B)。

https://blog.csdn.net/MikeCoke

<https://ctf.bugku.com/challenges#%E4%B8%80%E6%AE%B5Base64>

04-22 15:28

%windir%\System32\SlideToShutDown.exe

星期六 11:27

已取消，点击重拨

对方未接听

14:24

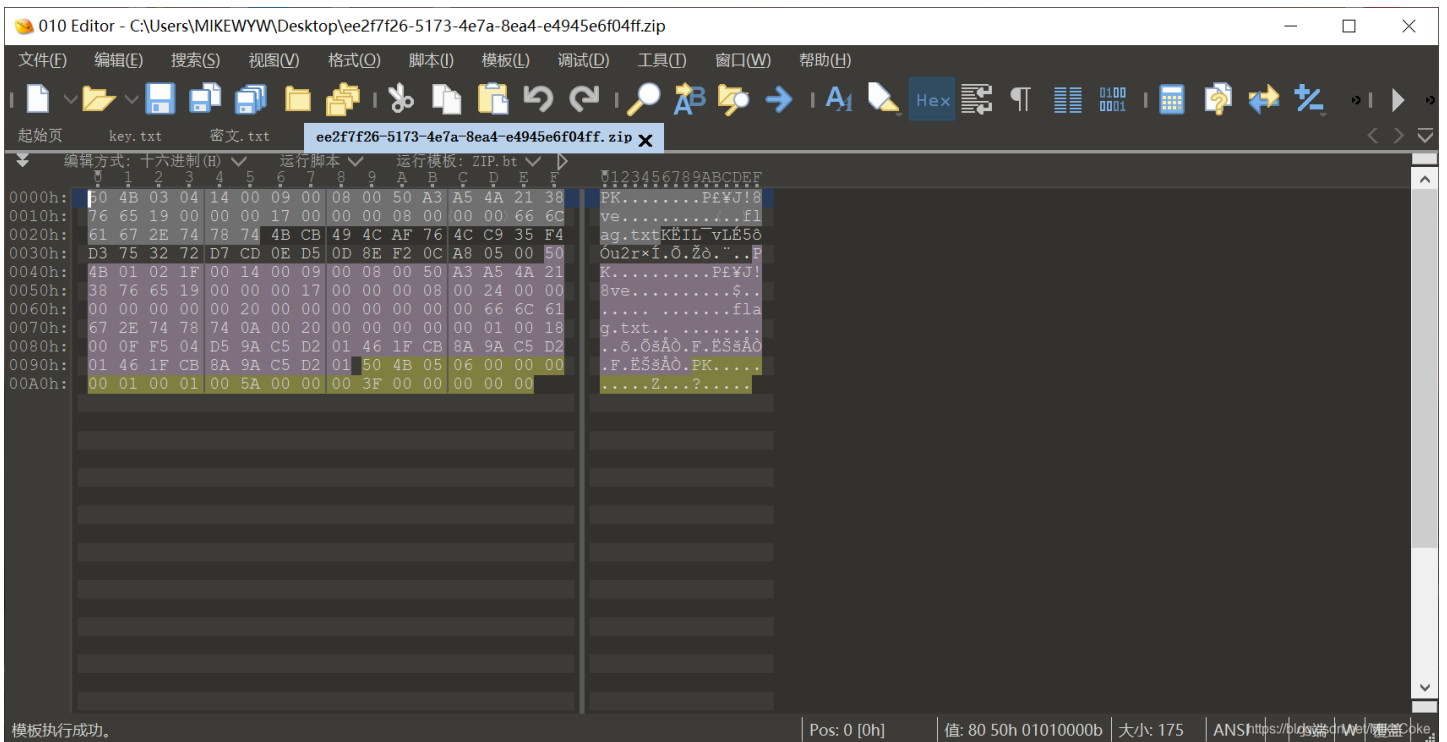
ee2f7f26-5173-4e7a-8ea4...ff(2).zip  
175B / 已发送

https://blog.csdn.net/MikeCoke



方法2:

这种伪加密的题目，[直接用010Editor打开](#) [下载地址](#)



来了解一下ZIP文件的组成

一个 ZIP 文件由三个部分组成:

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标志

a. 压缩源文件数据区:

50 4B 03 04: 这是头文件标记 (0x04034b50)

14 00: 解压文件所需 pkware 版本

00 00: 全局方式位标记 (有无加密, 奇数加密, 偶数无加密)

08 00: 压缩方式

5A 7E: 最后修改文件时间

F7 46: 最后修改文件日期

16 B5 80 14: CRC-32校验 (1480B516)

19 00 00 00: 压缩后尺寸 (25)

17 00 00 00: 未压缩尺寸 (23)

07 00: 文件名长度

00 00: 扩展记录长度

6B65792E7478740BCECC750E71ABCE48CDC9C95728CECC2DC849AD284DAD0500

#### b. 压缩源文件目录区:

50 4B 01 02: 目录中文件文件头标记(0x02014b50)

3F 00: 压缩使用的 pkware 版本

14 00: 解压文件所需 pkware 版本

00 00: 全局方式位标记 (有无加密, 奇数加密, 偶数无加密)

08 00: 压缩方式

5A 7E: 最后修改文件时间

F7 46: 最后修改文件日期

16 B5 80 14: CRC-32校验 (1480B516)

19 00 00 00: 压缩后尺寸 (25)

17 00 00 00: 未压缩尺寸 (23)

07 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 00 00 00: 外部文件属性

00 00 00 00: 局部头部偏移量

6B65792E7478740A002000000000000010018006558F04A1CC5D001BDEBDD3B1CC5D001BDEBDD3B1CC5D001

#### c. 压缩源文件目录结束标志:

50 4B 05 06: 目录结束标记

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

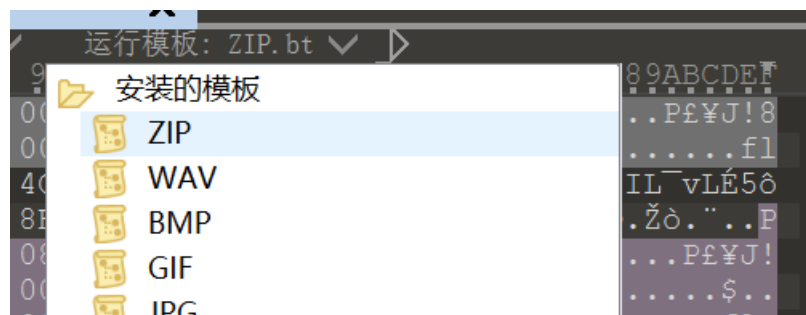
01 00: 目录区中纪录总数

59 00 00 00: 目录区尺寸大小

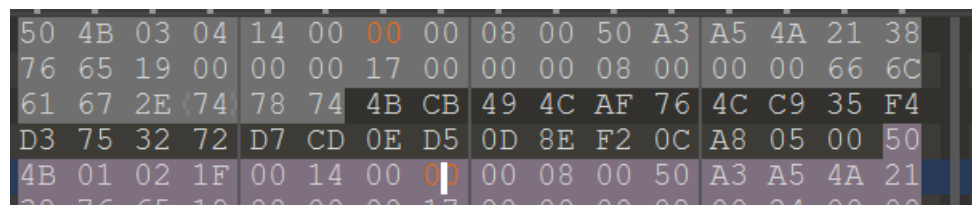
3E 00 00 00: 目录区对第一张磁盘的偏移量

00 00 1A: ZIP 文件注释长度

运行一下ZIP模板:



对两个加密点的数据都尝试修改一下, 改为偶数, 不同的解压软件识别的加密点不一样。有的是前面一个, 有的是后面一个。



修改保存后重新打开压缩包就行了

