刷题之旅第12站,CTFshow misc签到题

原创

圆圈勾勒成指纹 于 2020-02-15 09:42:10 发布 2127 收藏 6

分类专栏： 刷题之旅100站

本文链接：https://blog.csdn.net/weixin_45940434/article/details/104323401

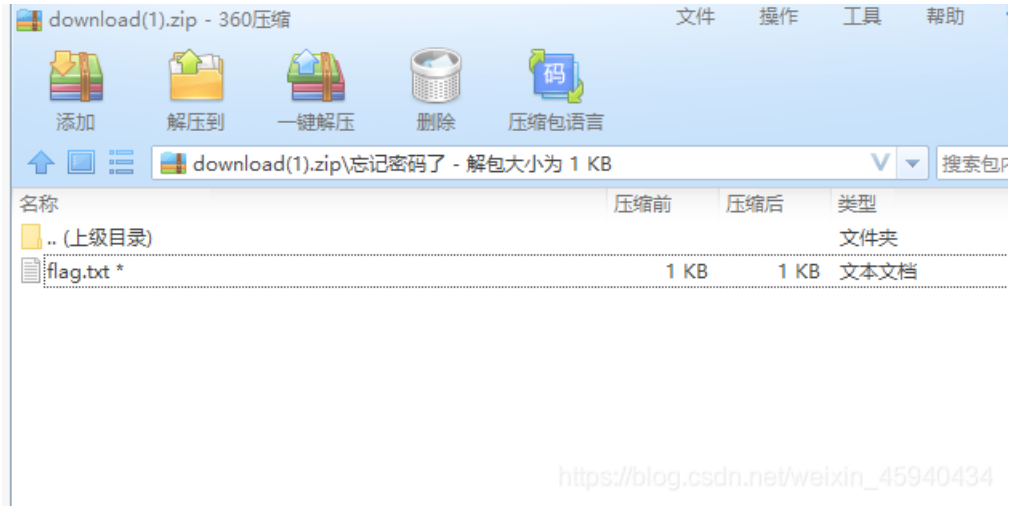
刷题之旅100站 专栏收录该内容

49 篇文章 11 订阅

订阅专栏

感谢CTF show平台提供题目

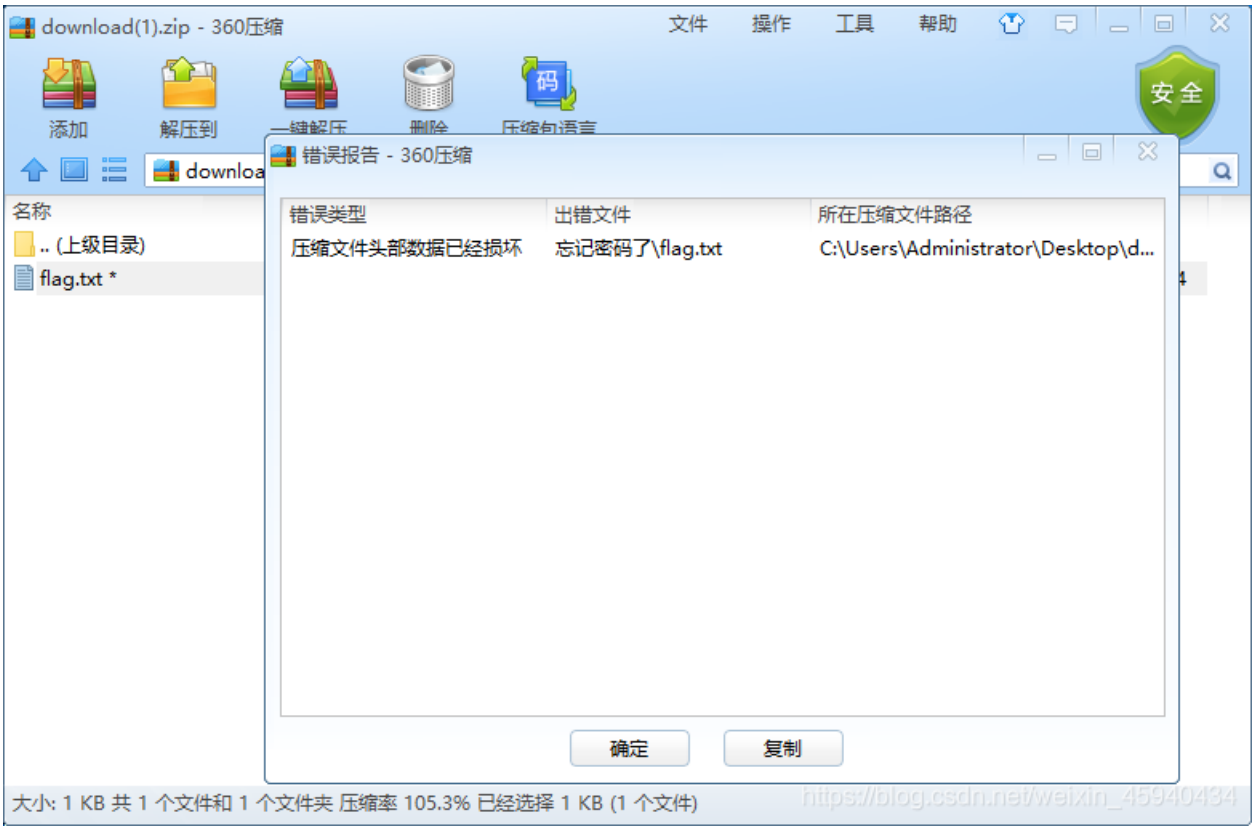
下载得到文件后，思路很明确，破解压缩包密码。



先讲一下，我做压缩包密码题目时的思路。

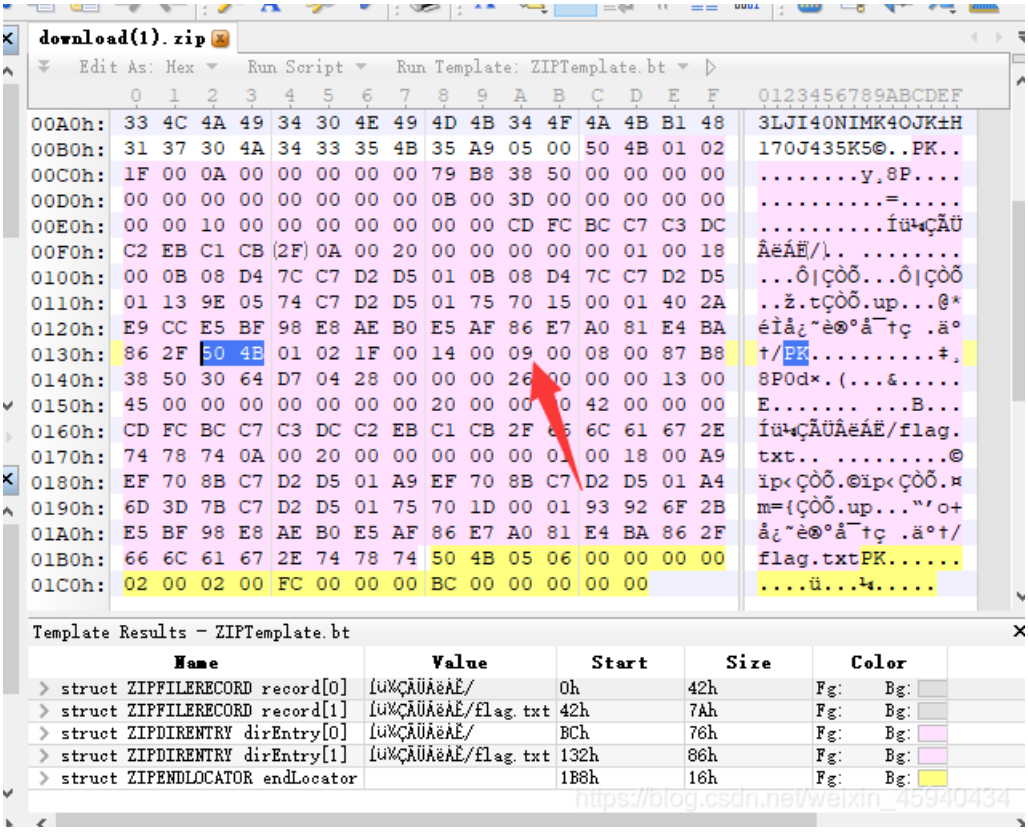
1、右键属性查看文件信息
2、 010 查看压缩包尾部是否有隐藏信息
3、 伪加密
4、 以上都不行的话，直接爆破

言归正传，当我们尝试解压文件的时候，提示错误。

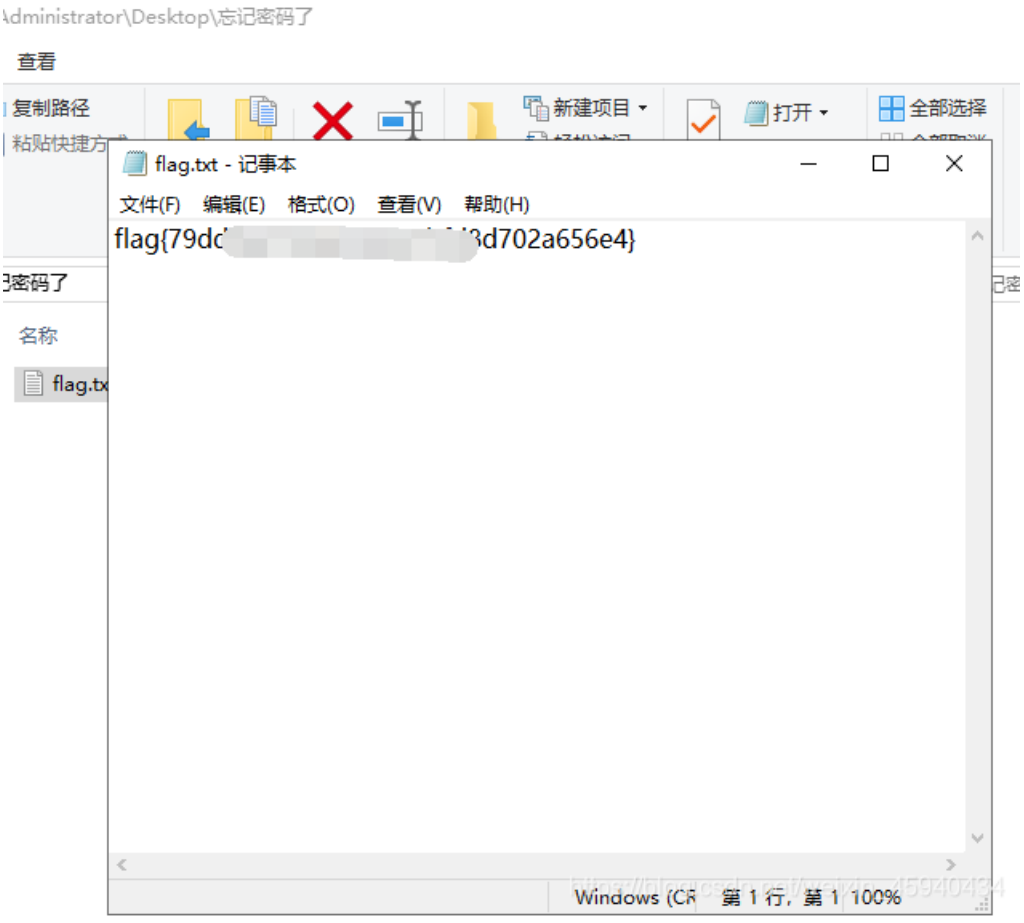


那么，我猜测可能是出题人进行的伪加密，导致文件结构损坏。

打开010 editor，搜索50 4B，在这里发现了异常。



修改09为00，保存文件，成功进行了解压。



zip伪加密原理：

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） 头文件标记后2bytes

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，伪加密的关键） 目录文件标记后4bytes

> https://blog.csdn.net/qq_26187985/article/details/83654197

原创文章不易，点个赞再走吧。