

[BUUCTF]zip伪加密

原创

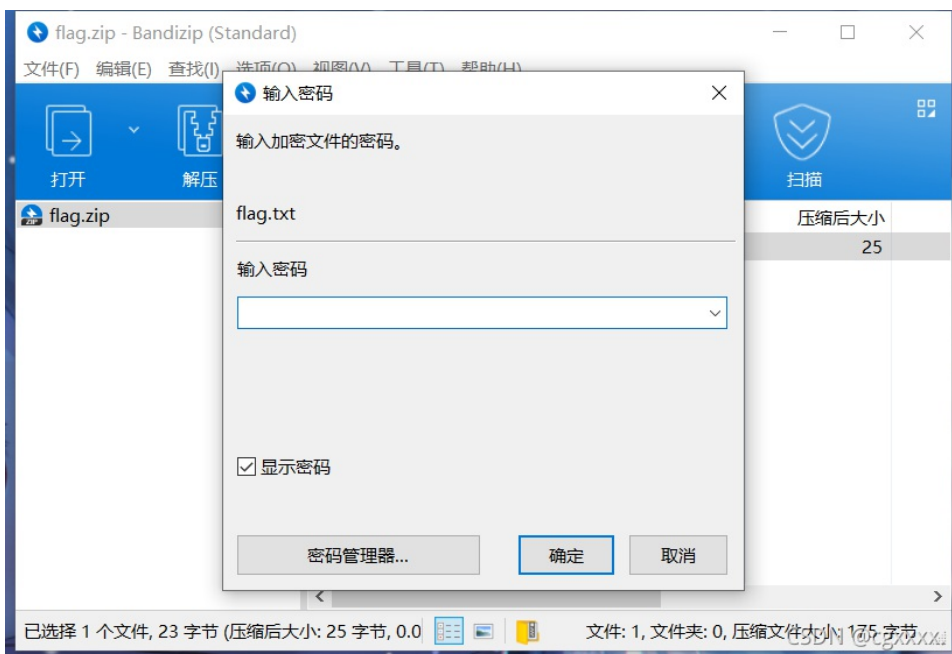
cgxxxx 于 2021-11-05 10:41:25 发布 135 收藏 1

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。

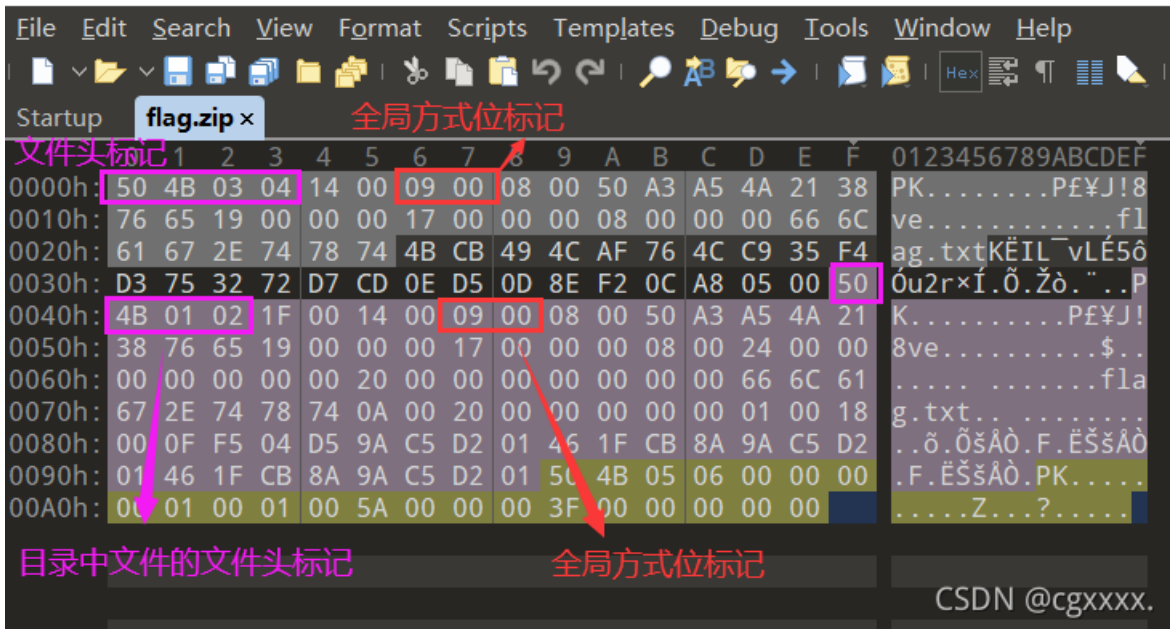
本文链接: https://blog.csdn.net/m0_61996125/article/details/121156937

版权



打开压缩文件发现需要密码, 结合题目知道这是伪加密

zip伪加密是在文件头的加密标记位做修改, 进而再打开文件时识被别为加密压缩包



未加密:

文件头中的全局方式位标记为00 00

目录中源文件的全局方式位标记为00 00

伪加密:

文件头中的全局方式位标记为00 00

目录中源文件的全局方式位标记为09 00

真加密:

文件头中的全局方式位标记为09 00

目录中源文件的全局方式位标记为09 00

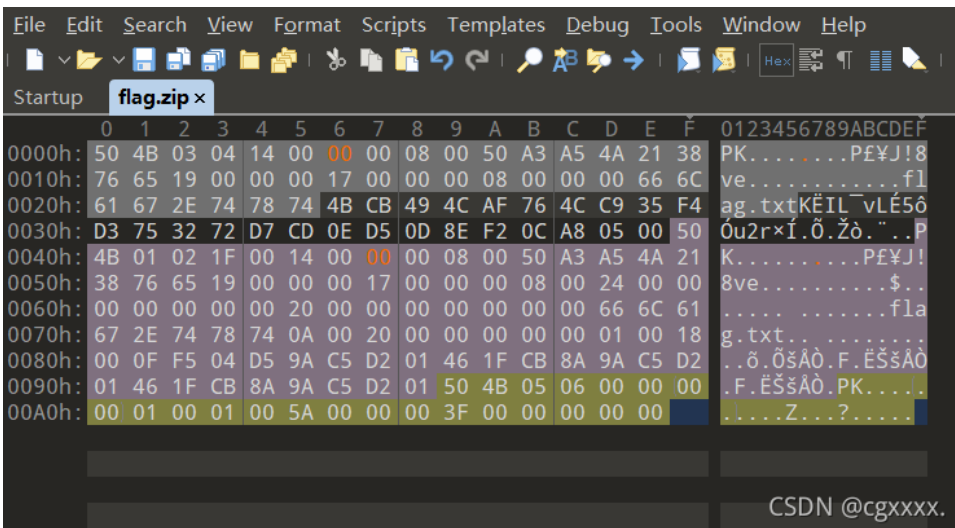
ps:也不一定要09 00或00 00, 只要是奇数都视为加密, 而偶数则视为未加密

但是这道题全是09 00, 因此我的第一想法是真加密, 并通过Ziperello破解

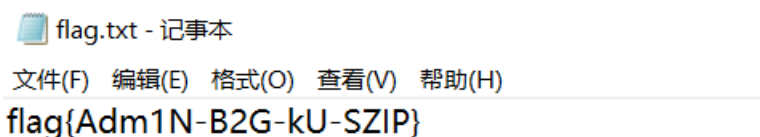


但是发现破解很久都不出结果，因为题目也提示了是伪加密，本来就没密码，肯定破解不出来。

因此按伪加密处理，把两个地方的全局方式位标记都改为00 00，接着保存，这样处理后文件就属于未加密了



再次尝试打开，发现flag



CSDN @cgxxxx.

这道题以假乱真，用两个09 00完全迷惑了我们，通过这道题、我们不能一上来就破解，也可能和这题一样 破解是得不出结果的，因此首先尝试修改全局方式位标记，不行在尝试破解。