zip伪加密-Write Up

原创

do you best 于 2021-11-21 00:24:43 发布 4574 收藏 3

分类专栏： ctf 文章标签： 安全 web安全 安全

本文链接：https://blog.csdn.net/qq_46202048/article/details/121448247

ctf 专栏收录该内容

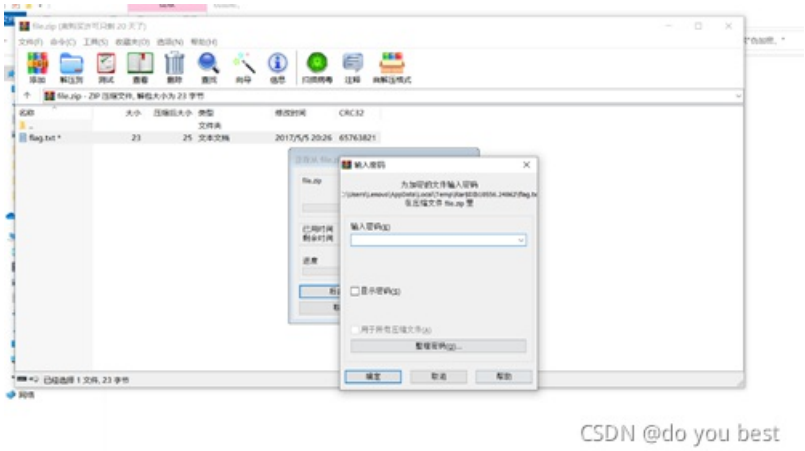
4 篇文章 0 订阅

订阅专栏

zip伪加密WriteUp

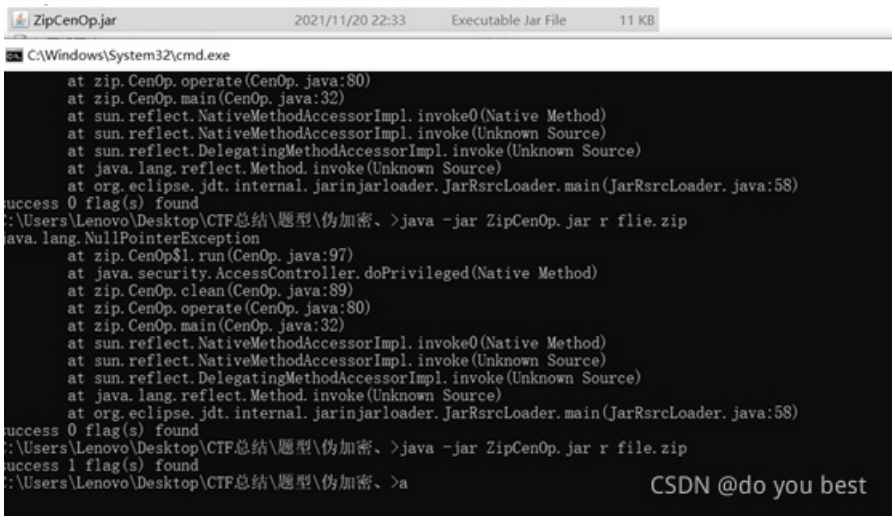
#题目源于bugku-zip伪加密

正常打开题目的压缩包提示是需要输入解压密码进行解压



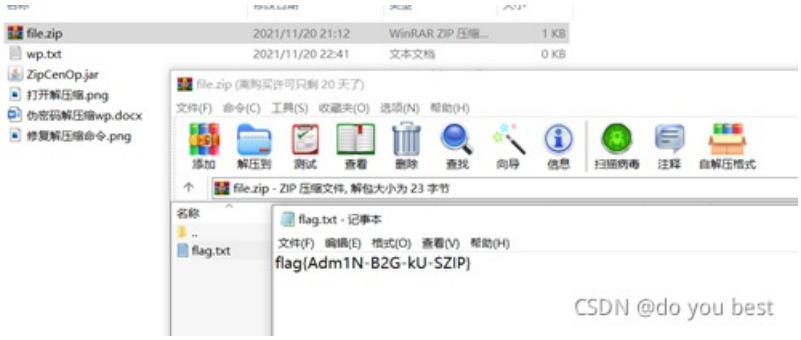
我这里讲两个破解压缩包伪加密的方法：

1、 下载一个ZipCenOp.jar专门修复压缩包的工具，该工具需要在java环境下调试使用。（方便快捷）



在此路径下cmd一下输入修复命令：java -jar ZipCenOp.jar r filezip

提示success 1 flag(s) found则修复成功！



打开原本提示需要密码的压缩包已经不需要密码了，成功获取flag！

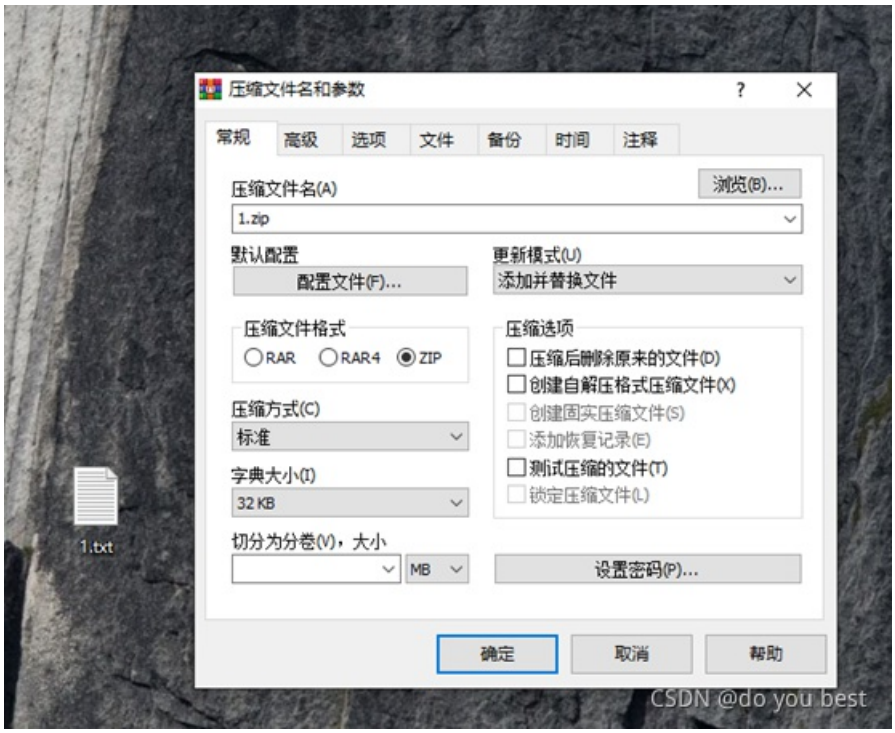
flag{Adm1N-B2G-kU-SZlP}

2、 还有一种思路修改标识符进行压缩包修复破解，我这里使用反推思路进行讲解和演示，如何破解就不演示了。使用winhex可以修改压缩包标识符的软件进行修改标识符破解，首先了解一下伪压缩包加密的知识：

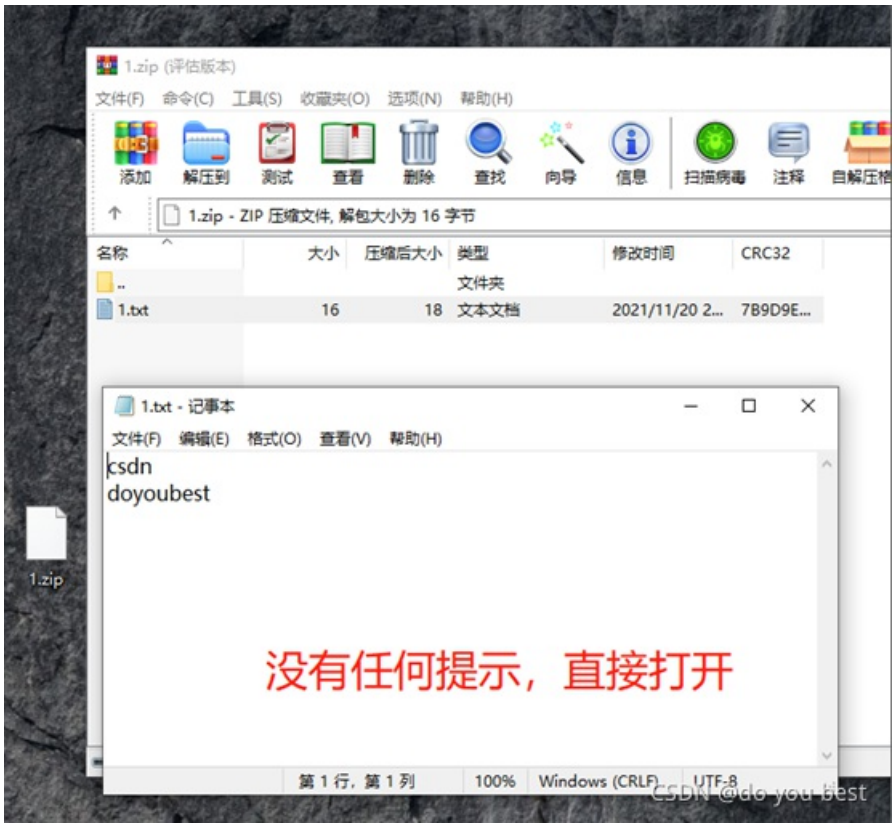
什么是伪加密？

就拿题干中的文件来讲，zip文件是一种压缩文件，可进行加密，也可不加密。而伪加密是在未加密的zip文件基础上修改了它的压缩源文件目录区里的全局方式位标记的比特值，使得压缩软件打开它的时候识别为加密文件，提示输入密码， 而在这个时候，不管你用什么软件对其进行密码破解，都无法打开它，因为本身并没有加密，而是一种伪装。

第一步创建一个txt的测试文档用来进行伪加密：

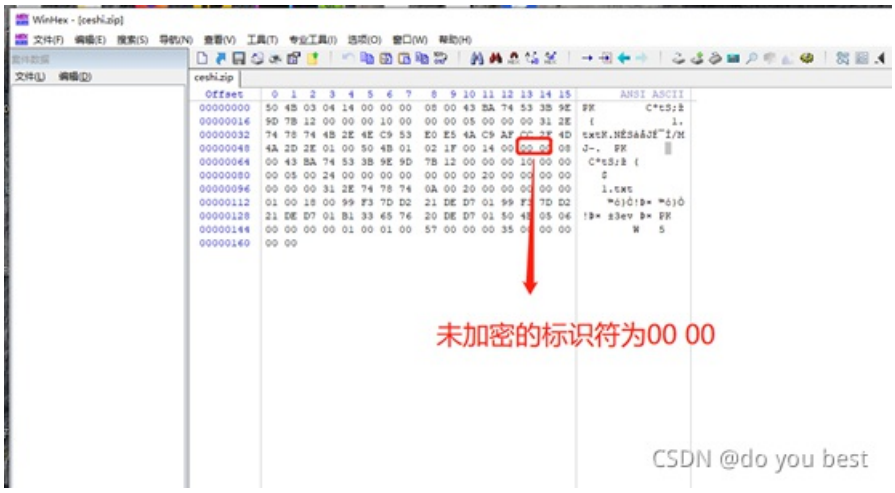


这里我们不设置密码，压缩伪zip结尾的普通压缩包，打开压缩包内容，没有密码提示

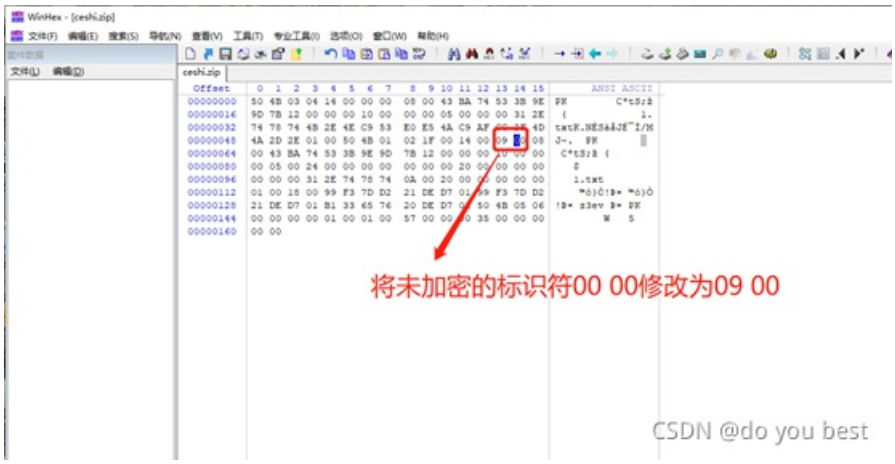


第二步使用winhex把没有密码的压缩包进行伪加密

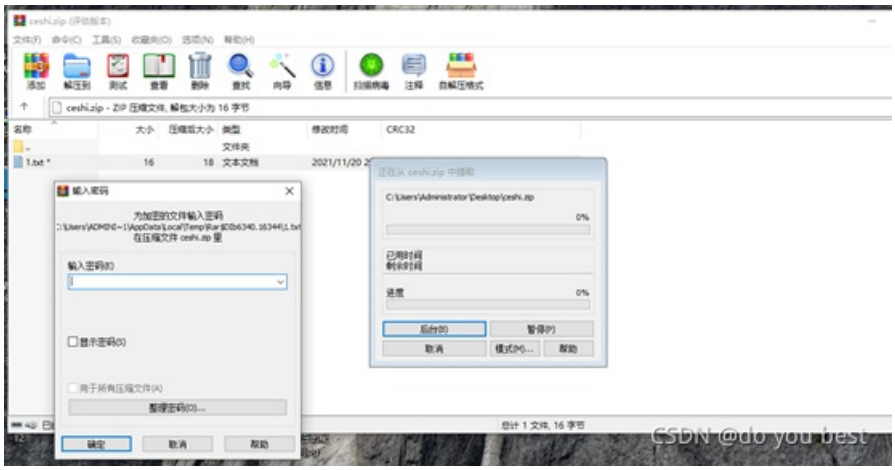
打开没有加密的压缩包：



修改加密位00 00 为09 00



保存后打开原来没有加密的压缩包文件：



打开压缩包提示有密码，成功进行压缩包伪加密！

压缩包的一些标识符解如下，请各位师傅食用

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）

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

压缩源文件目录区：
50 4B 01 02：目录中文件头标记
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，这个更改这里进行伪加密，改为09 00打开就会提示有密码了）
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
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：ZIP 文件注释长度

#CTF#网络安全安全爱好者