

BUUCTF zip伪加密

原创

Outsider213 于 2021-11-07 21:23:28 发布 51 收藏

分类专栏: [CTF MISC](#) 文章标签: [网络安全](#)

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/qq_54551352/article/details/121193461

版权



[CTF 同时被 2 个专栏收录](#)

1 篇文章 0 订阅

订阅专栏

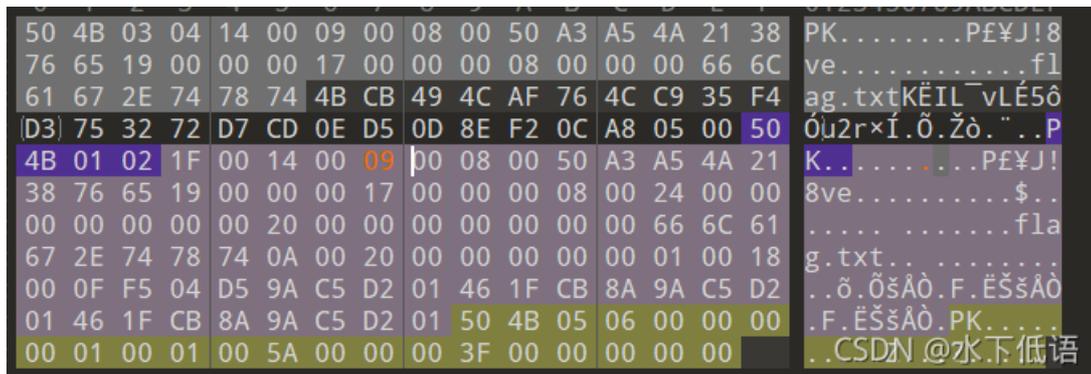


[MISC](#)

1 篇文章 0 订阅

订阅专栏

先把压缩文件用010打开看看



翻阅一些资料我们可以知道, zip文件格式分为三个部分

1.压缩源文件数据区

50 4B 03 04是源文件数据区文件头的标识

14 00: 解压文件所需 pkware 版本 (这个在这道题用不到)

09 00: 全局方式位标记

2.压缩源文件目录区

50 4B 01 02是源文件目录区文件头的标识

14 00: 解压文件所需 pkware 版本

00 09: 全局方式位标记 (由此决定是否加密显示, 偶数无加密显示, 奇数有加密显示)

3.源文件目录结束区

50 4B 05 06是目录结束标记

我们这道题只需要改源文件目录区的这个全局方式位标记为偶数即可

所以我们只要把这里的00 09改成任意的偶数即可, 譬如00 00

```
50 4B 03 04 14 00 09 00 08 00 50 A3 A5 4A 21 38 PK.....PŸ¥J!8
76 65 19 00 00 00 17 00 00 00 08 00 00 00 66 6C ve.....fl
61 67 2E 74 78 74 4B CB 49 4C AF 76 4C C9 35 F4 ag.txtKĒIL vLÉ5ô
D3 75 32 72 D7 CD 0E D5 0D 8E F2 0C A8 05 00 50 ōu2r×Ī.Ō.Žò."..P
4B 01 02 1F 00 14 00 00 00 08 00 50 A3 A5 4A 21 K.....PŸ¥J!
38 76 65 19 00 00 00 17 00 00 00 08 00 24 00 00 8ve.....$.
00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C 61 .....fla
67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 18 g.txt.....
00 0F F5 04 D5 9A C5 D2 01 46 1F CB 8A 9A C5 D2 ..ō.ŌšÅÒ.F.ĚŠšÅÒ
01 46 1F CB 8A 9A C5 D2 01 50 4B 05 06 00 00 00 .F.ĚŠšÅÒ.PK....
00 01 00 01 00 5A 00 00 00 3F 00 00 00 00 00 ..CSDN.@水下低语
```

最终是这样，直接打开得到flag

```
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 视图(V) 帮助(H)
flag{Adm1N-B2G-kU-SZIP}
CSDN @水下低语
```