xctf攻防世界 MISC高手进阶区 János-the-Ripper

原创

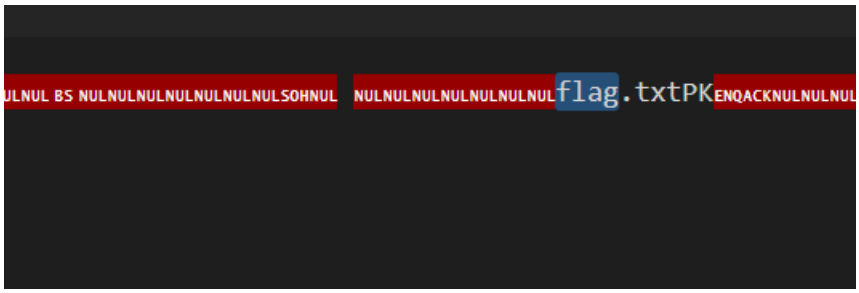
l8947943 于 2022-01-13 15:58:13 发布 190 收藏

分类专栏： 攻防世界misc之路 文章标签： 安全 misc

本文链接：https://blog.csdn.net/l8947943/article/details/122475798

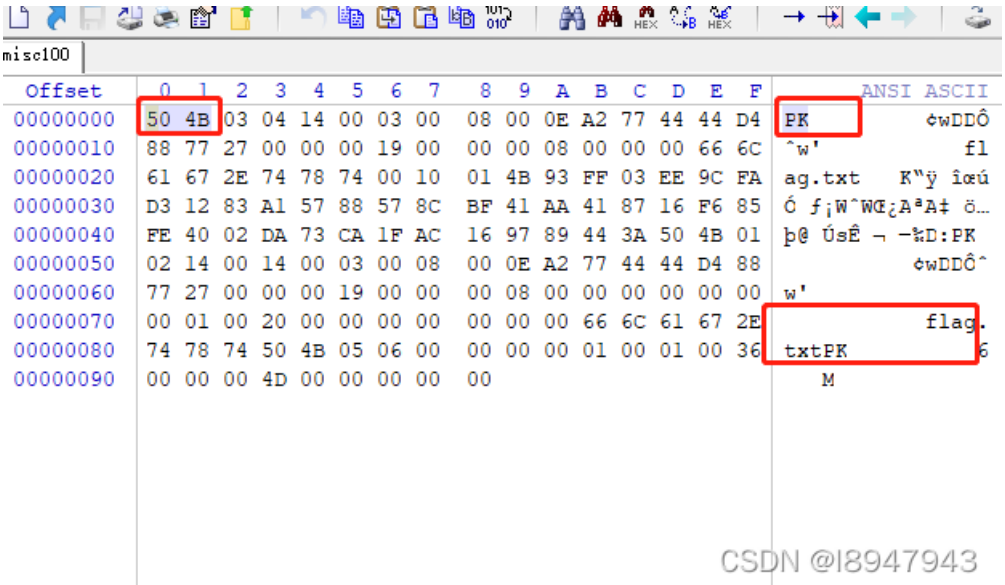
1. 打开环境，下载附件

是一个misc100无后缀的文件，用vscode打开后发现是一堆乱码，但其中包含flag.txt，如图：



2. 问题分析

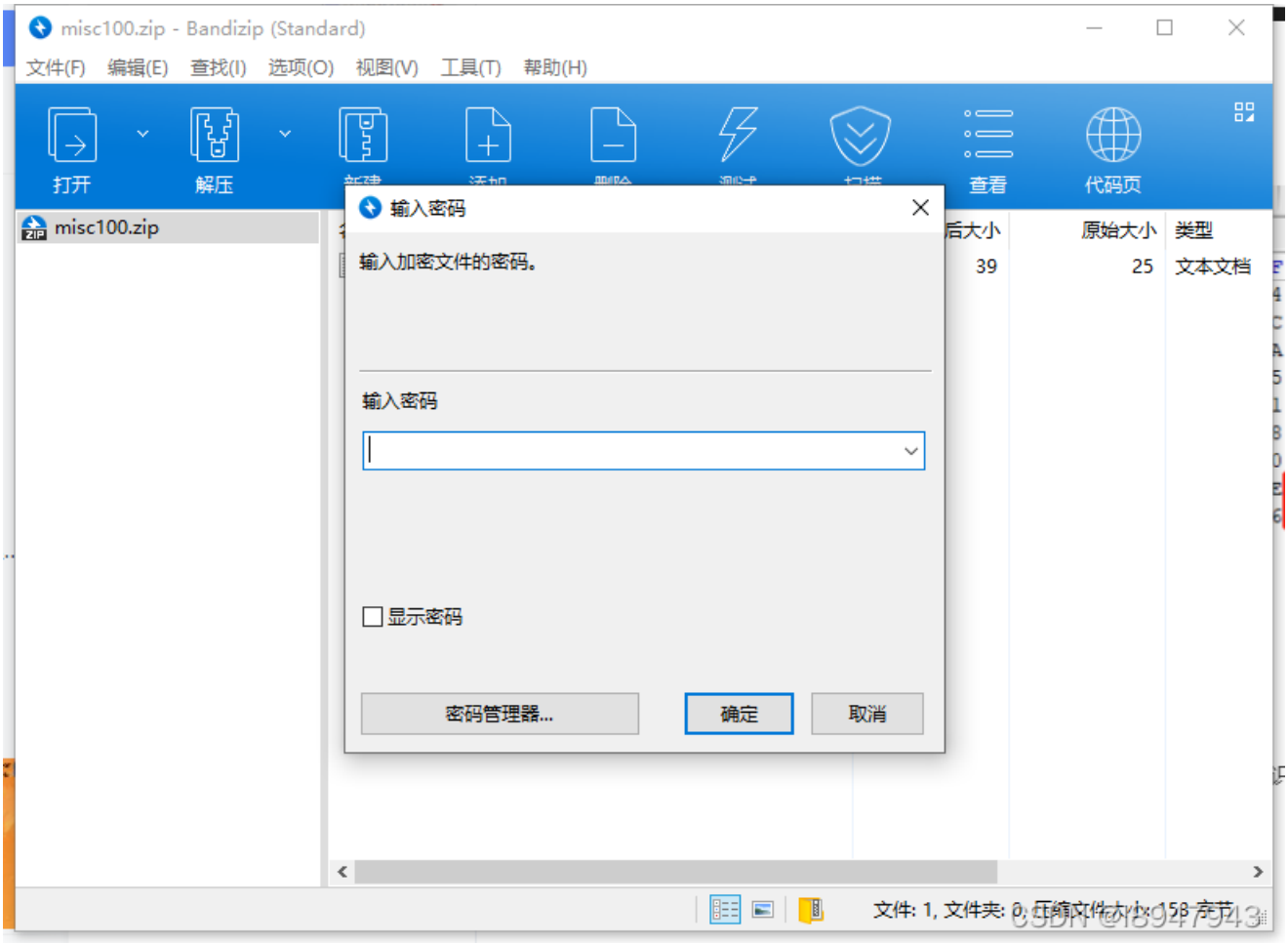
1. 使用winhex打开文件



我们可以看到文件的开头为`504B，PK开头的文件`，我们知道这个开头的标识是zip文件，详见：**各类文件的文件头标志**

改为zip文件

我们将文件修改成zip结尾的，发现需要解压密码，如图：



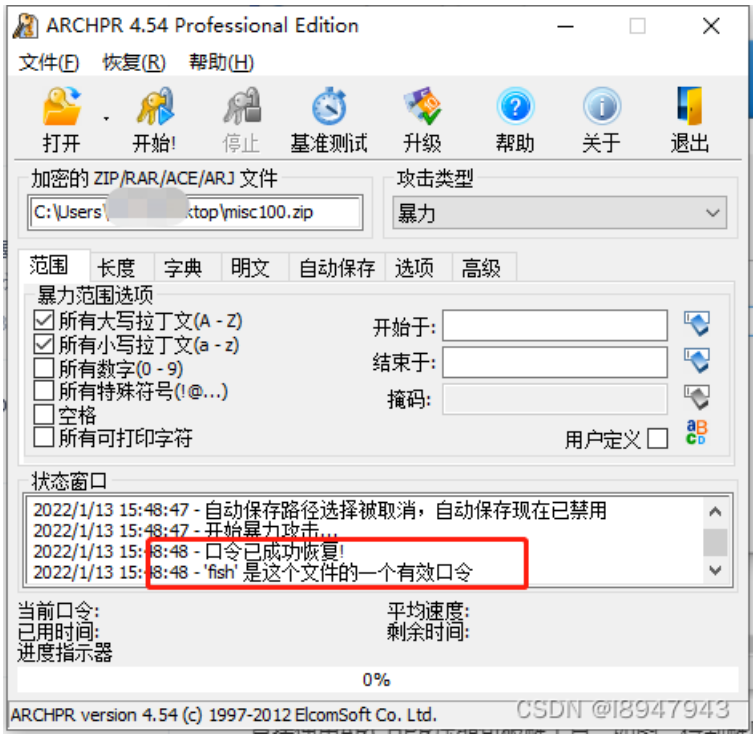
winhex中并没有伪加密，说明需要我们进行暴力破解。

掏出ARCHPR

附带工具下载链接：**https://zhangfa.lanzouw.com/iQmy8yq3tuh**

或者GitHub上下载：**https://github.com/cnsuhao/Advanced-Archive-Password-Recovery-Professional-Edition**

直接使用ARCHPR压缩包破解工具，如图，得到解压码'fish'，如图：



我们将zip解压，得到flag.txt。最终的答案为：`flag{ev3n::y0u::bru7us?!}`