# 不简单的压缩包 BugkuCTF-杂项-MISC

原创

旭日X8022 于 2019-10-25 12:46:10 发布 5466 收藏 4

分类专栏： CTF Bugku 文章标签： CTF Bugku



本文链接：https://blog.csdn.net/qq_33184105/article/details/102736802



CTF 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏

Bugku

2 篇文章 0 订阅

订阅专栏

**不简单的压缩包 Bugku **

1.emm。。。。看上去我是第一个写此题攻略的菜鸡，先声明，我只是个菜鸡。

2.我做不出来自闭的时候也想找writeup，发现网上没有，于是更自闭了。。。

3.攻略里有不严谨的地方，欢迎各位大佬在评论提意见，我保证不会改的

4.卑微求赞


完整思路

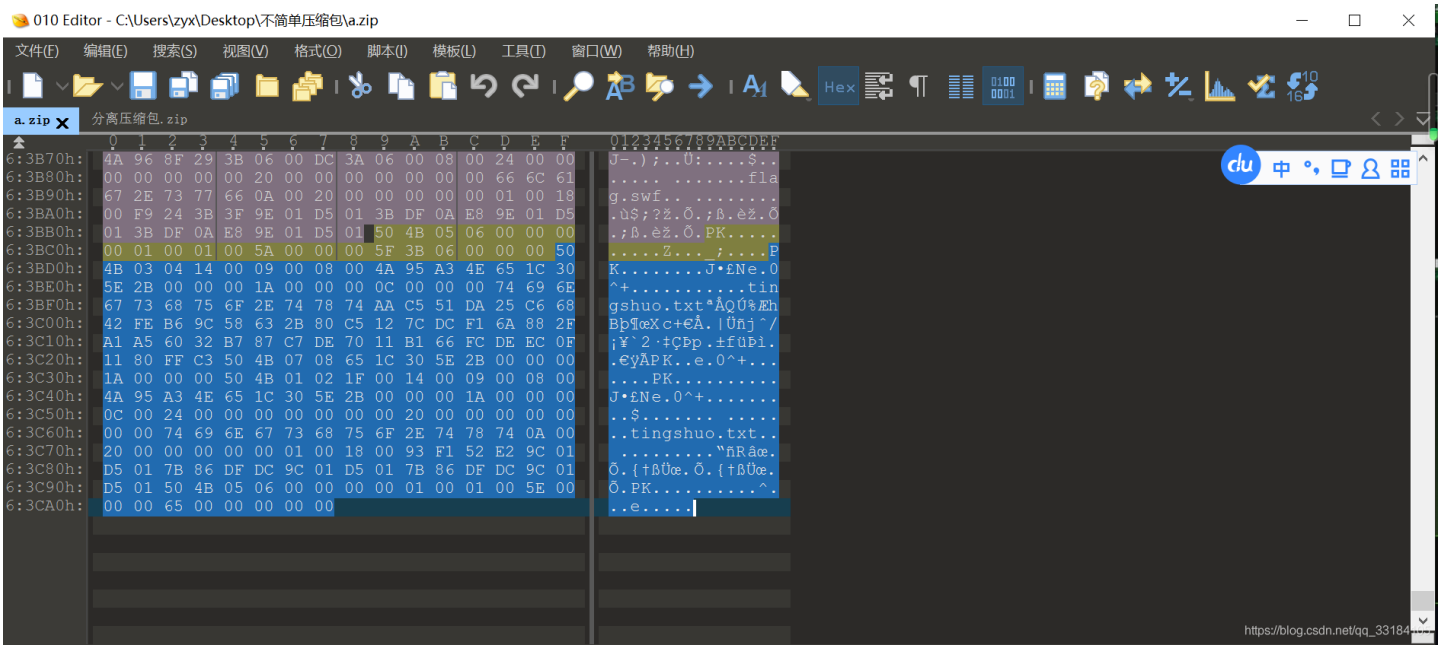
下载过来先改名a.zip（提前说一下，不能用rar压缩这个软件打开压缩包，看到的文件数不完整，后来我用的是360压缩，大概是因为两个软件算法不一致吧）

360压缩直接打开，提示有密码

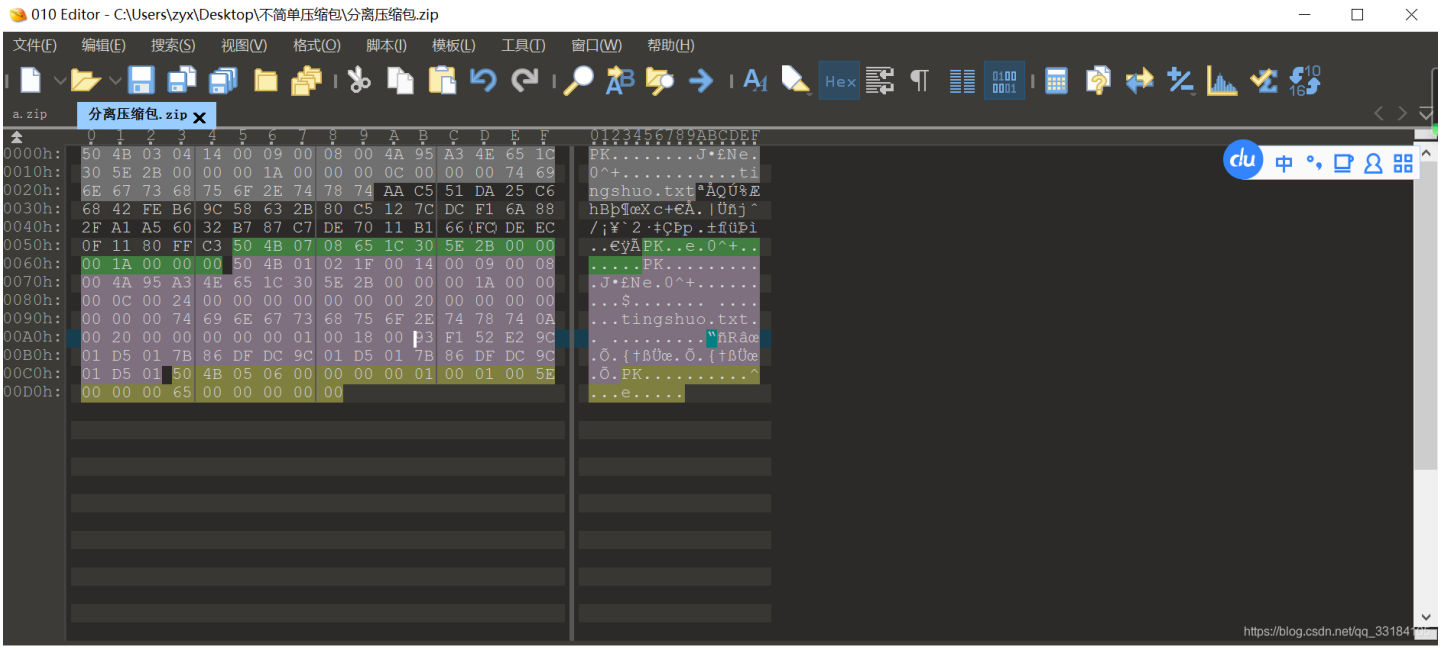
打开010

在末尾发现第二个压缩包

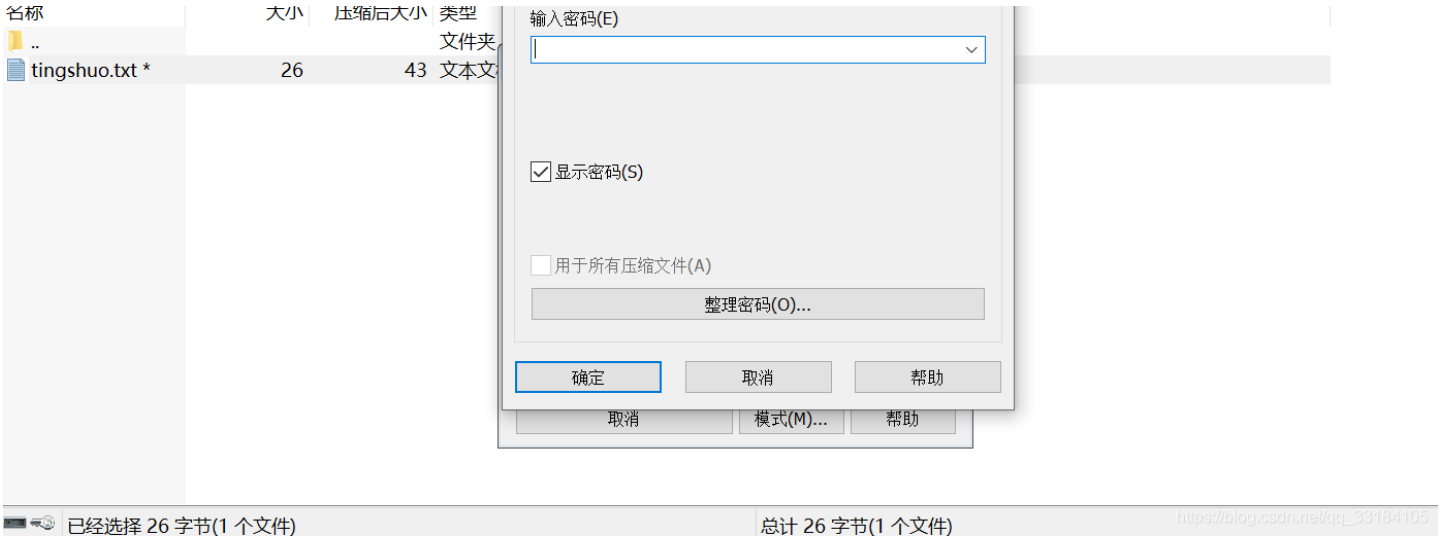
zip文件头是504B0304，文件尾504B



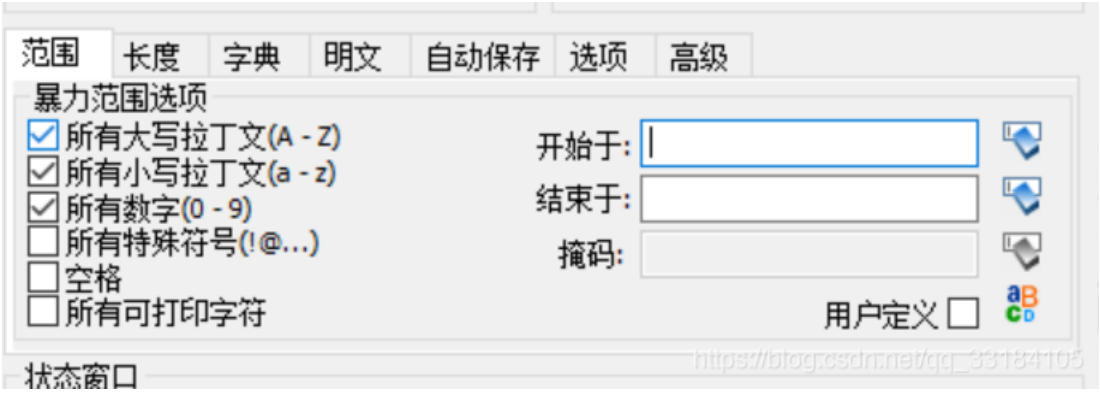

手动分离出去（之前用binwalk扫描过这个压缩包，发现存在swf文件，txt文件和另一个压缩包，我的binwalk只能检测，不能分离文件，可能是因为binwalk组件丢失了，但是我不会修复）

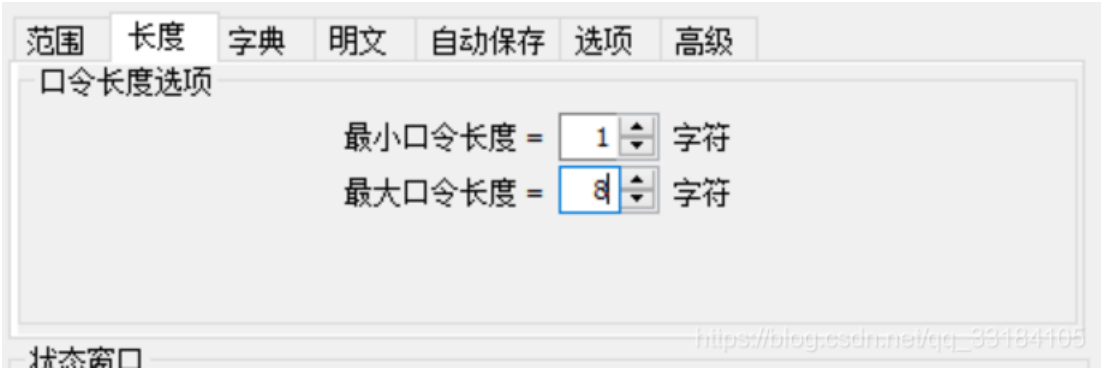


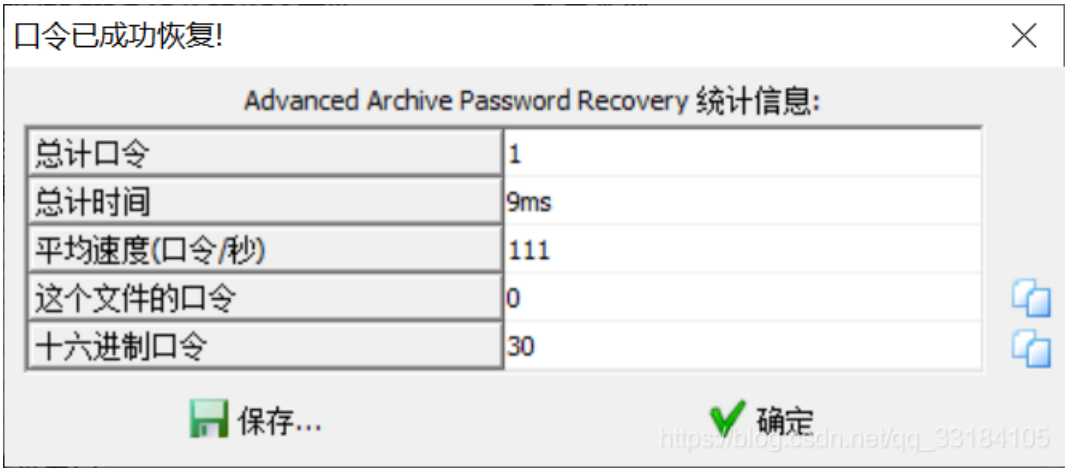
另存为第二个zip




打开，有密码，以为是伪加密，把140009改成140000，进压缩包，提示解压文件损坏。我懵C了。
那行吧，不是伪加密，只能放ARCHPR暴力破解，说不定破解几个小时就出来了。。。
然鹅。。。。。事情并不是这样

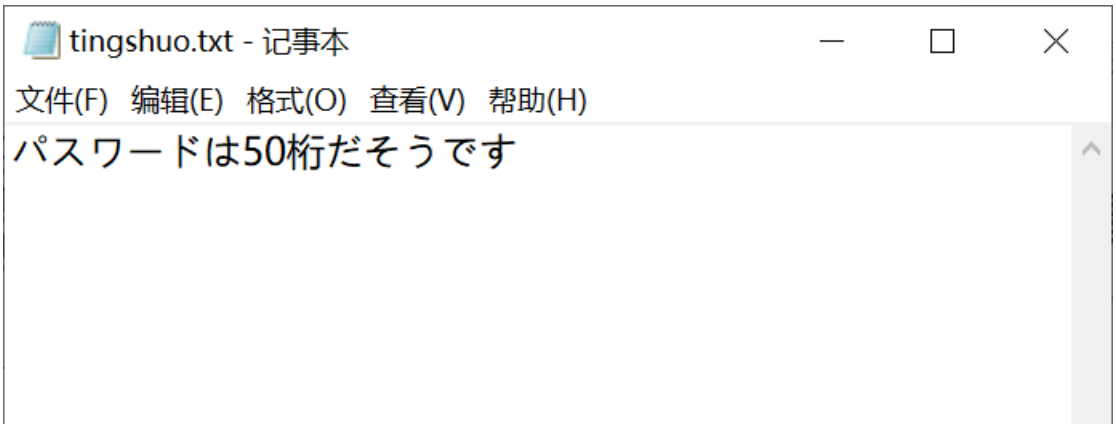


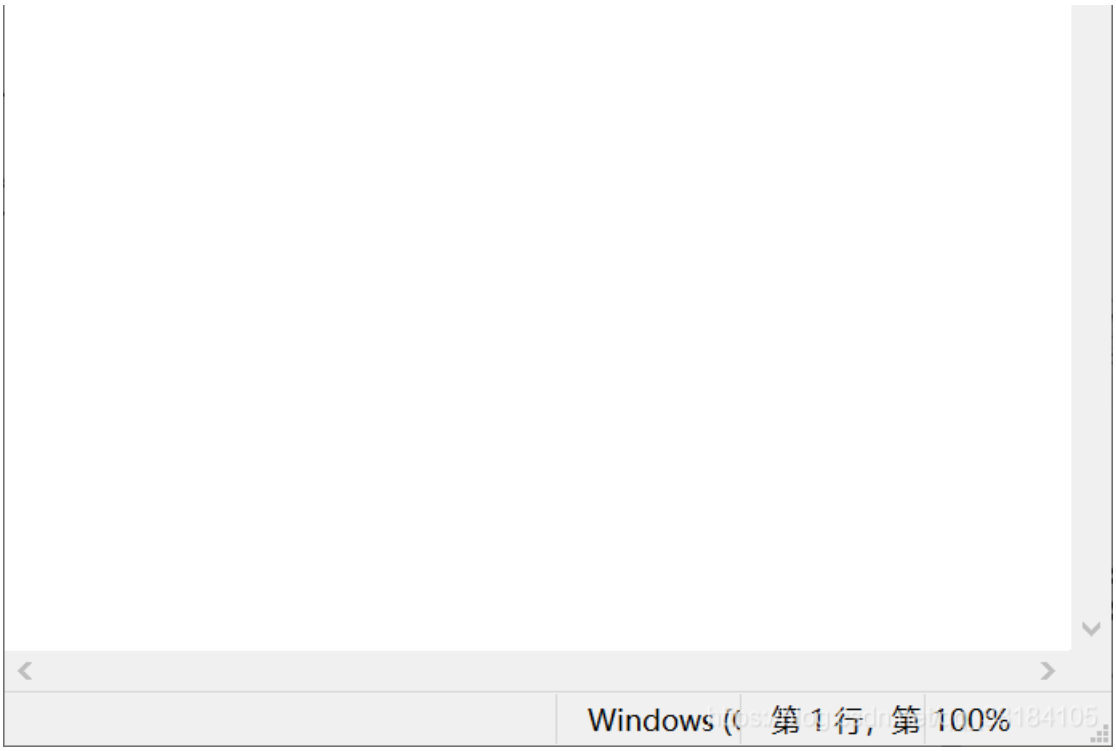



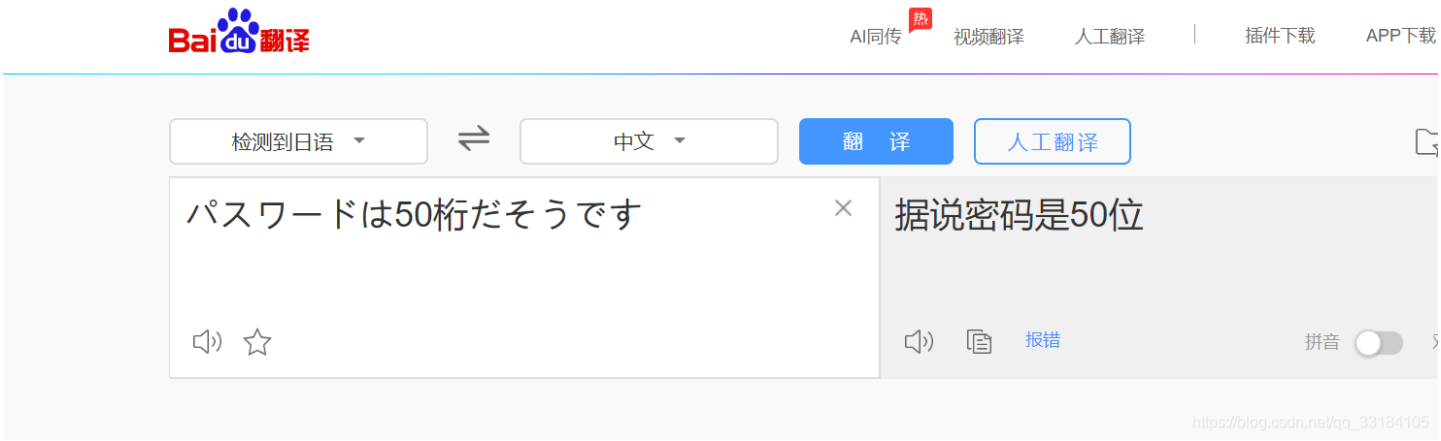

？！居然一运行就跑出了密码，密码是0，很皮啊。

接下来，你们懂的，解压出tingshuo.txt，发现一段谜之日语

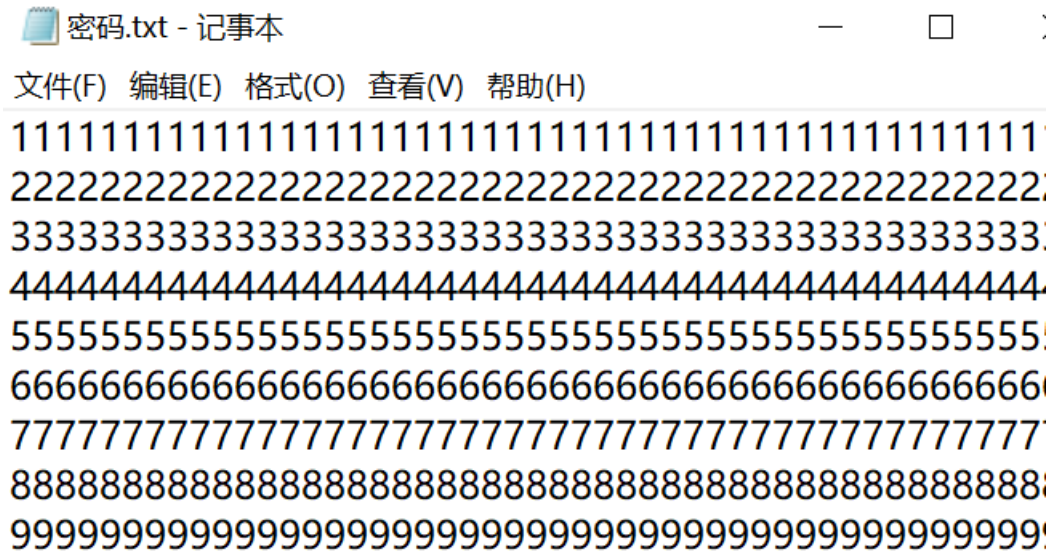


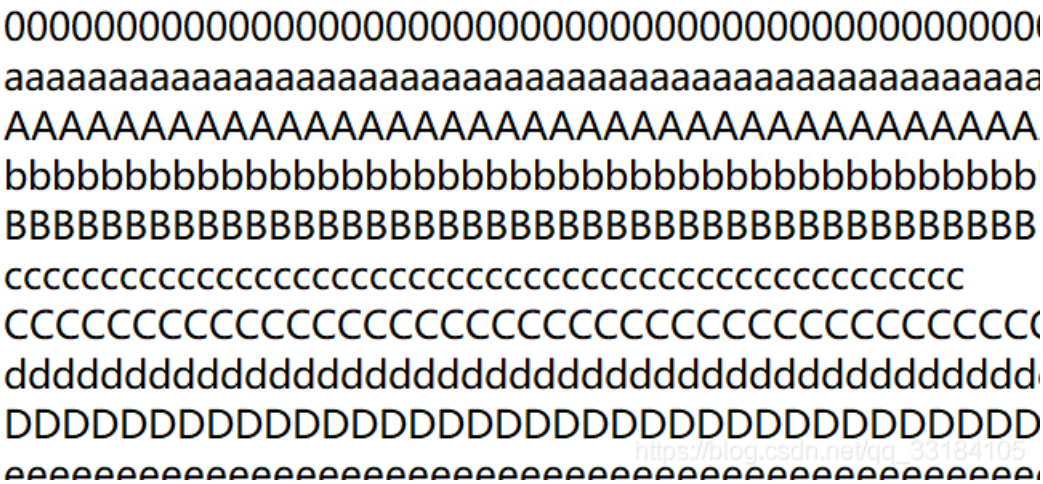



翻译一下



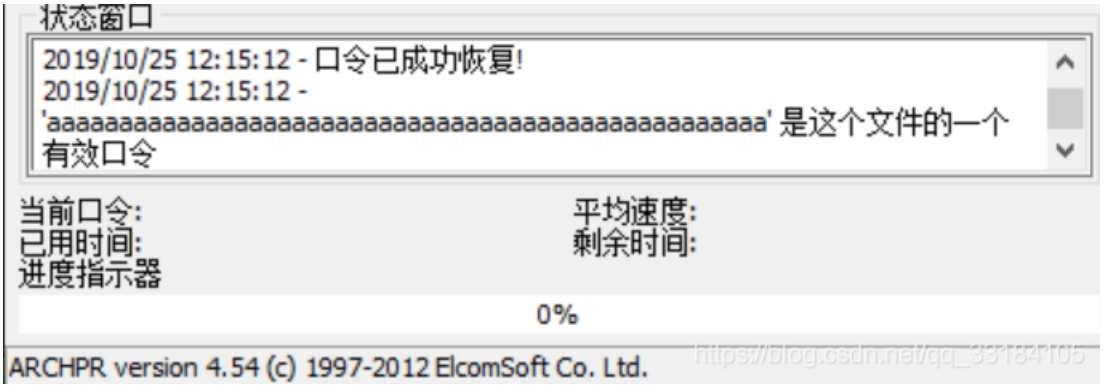

密码50位，对应的应该是a.zip的，但是密码它有50位？？？暴力破解能解到地老天荒，密码会不会在属性里？看了一下属性好像没什么问题（之前还试过流隐写破解，还是没什么发现）
那，猜猜密码？？50位密码，如果混合组合，肯定没法解开，要不然试试相同符号密码？于是我做了一个这样的字典





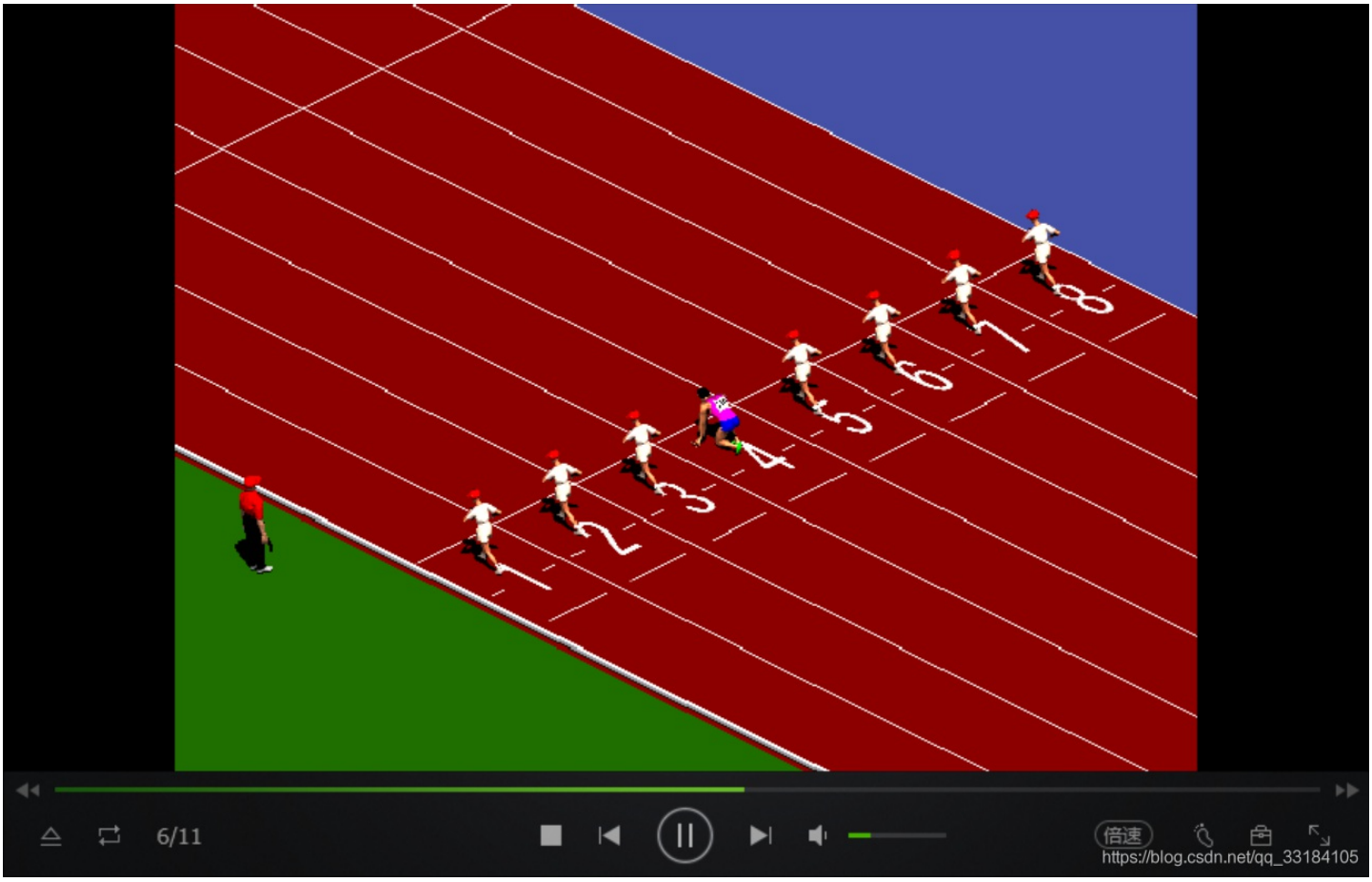

每行50个相同字符

打开ARCHPR，跑一下字典




？！又解开了？？？密码50个a

好了，打开a.zip，输入密码，解压出flag.swf文件
点开，




一个谜之游戏，我试了好几次，通不了关，可能是我太菜了吧
我想着。。。。是一个游戏，通关之后可能会有flag，试试改存档？
但是并没有存档文件出现在文件夹里。。。

调整一下思路
在百度搜索.swf

Baidu百科 .swf 进入词条

目录



## 基本信息

编辑

SWF是一种基于矢量的Flash动画文件，一般用FLASH软件创作并生成SWF文件格式，也可以通过相应软件将PDF等类型转换为SWF格式。SWF格式文件广泛用于创建吸引人的应用程序，它们包含丰富的视频、声音、图形和动画。可以在Flash中创建原始内容或者从其它Adobe应用程序（如Photoshop或Illustrator）导入它们，快速设计简单的动画，以及使用Adobe AcitonScript 3.0开发高级的交互式项目。设计人员和开发人员可使用它来创建演示文稿、应用程序和其它允许用户交互的内容。Flash可以包含简单的动画、视频内容、复杂演示文稿和应用程序以及介于它们之间的任何内容。通常，使用Flash创作的各个内容单元称为应用程序，即使它们可能只是很简单的动画。您也可以通过添加图片、声音、视频和特殊效果，构建包含丰富媒体的Flash应用程序。

**如何播放SWF：**

可以利用FLASH控件实现播放FLASH的SWF文件，常用的第三方软件（如：实用Flash播放器、超级Flash播放器 [1] 、SWF Flash Player）可以直接在主流下载站下载后并安装，即可使用。

## 文件结构

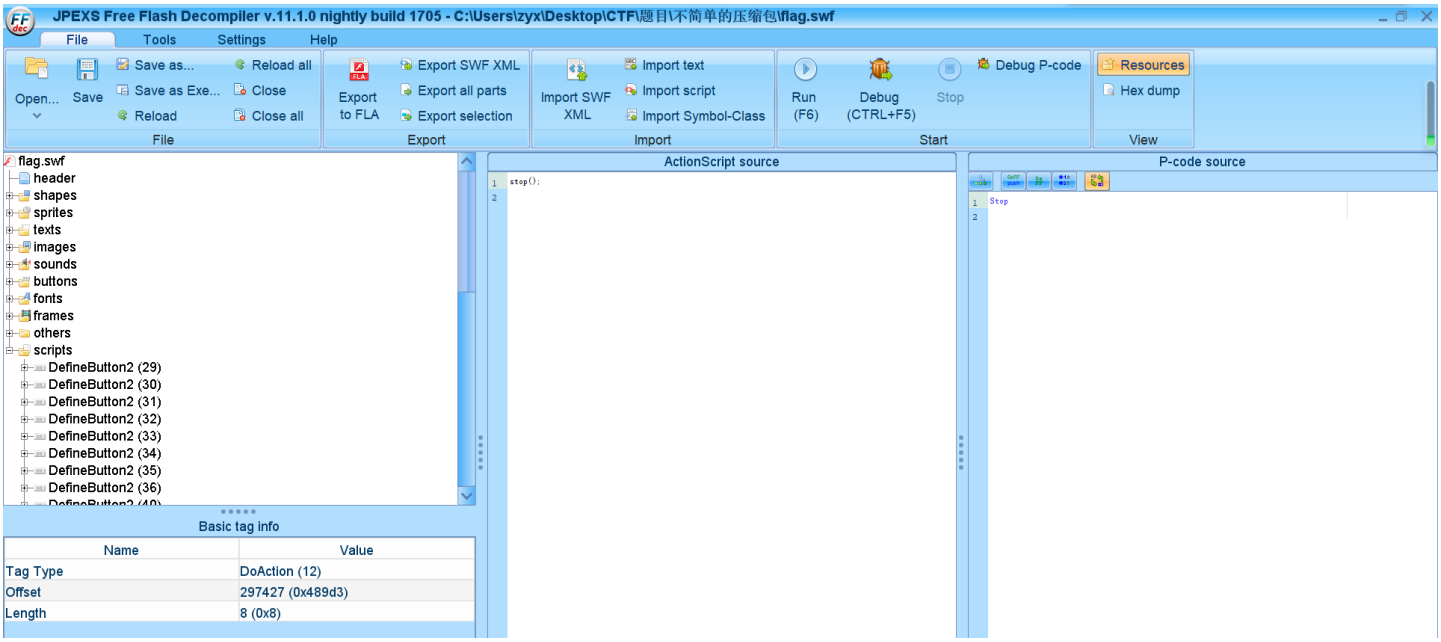
编辑

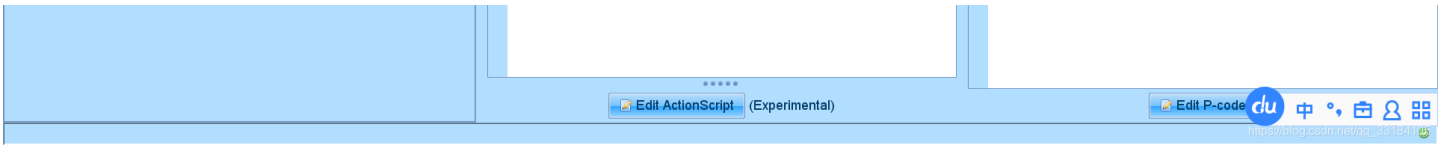


SWF格式文件广泛用于创建吸引人的应用程序，

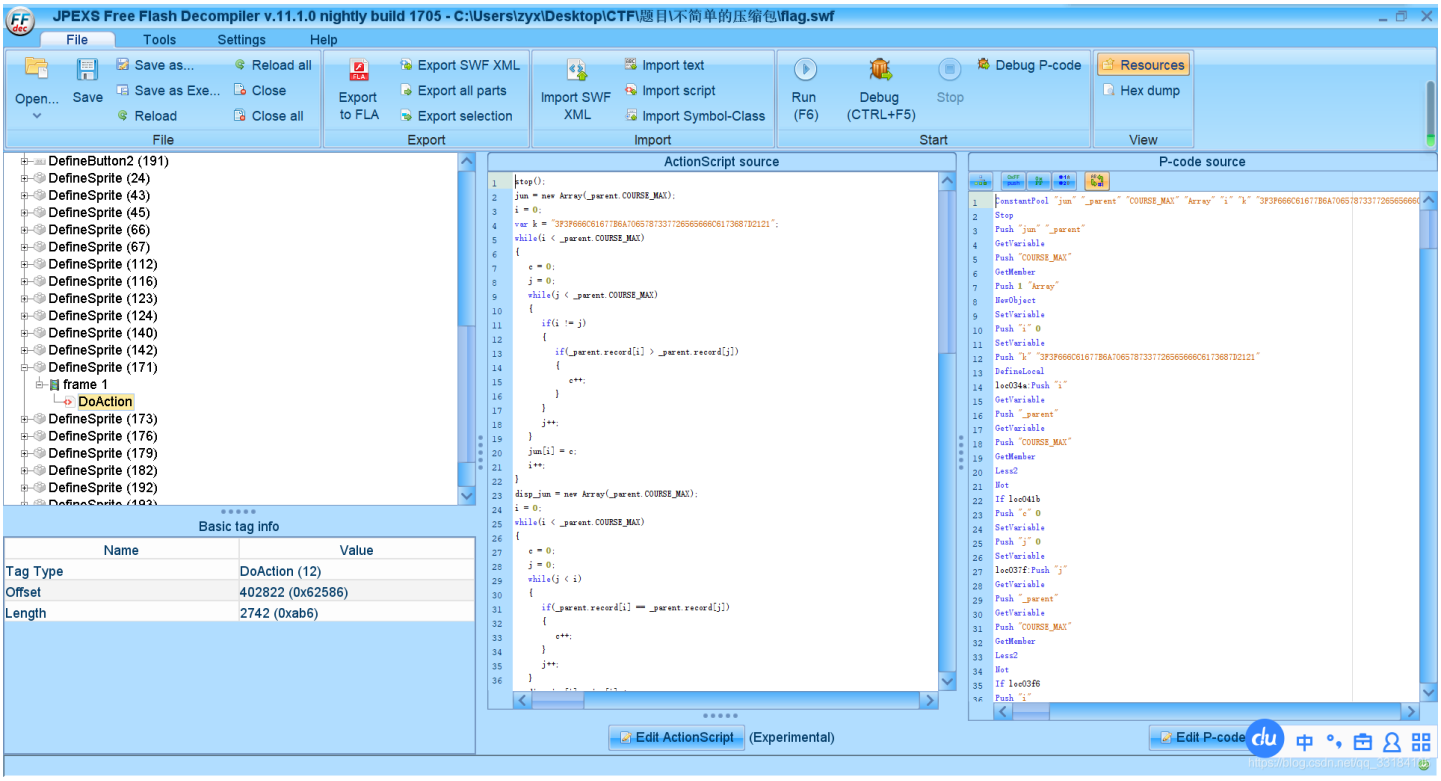
既然是应用程序那就试试反编译看源码喽，也许修改能直接通关吧。
然后，我在网上找到一个名叫JPEXS Free Flash Decompiler的软件

用它打开flag.swf



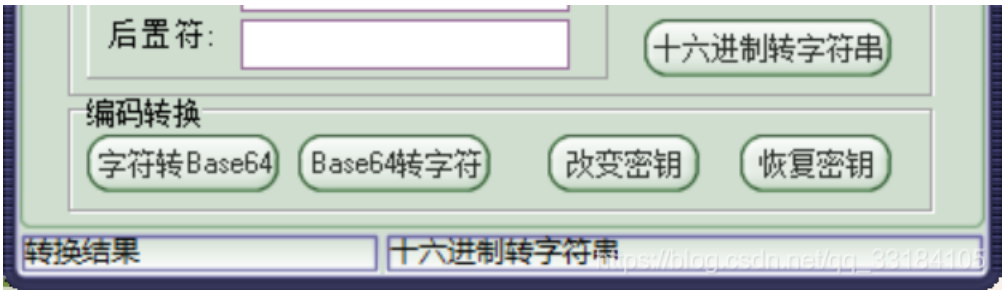



一个一个看源码，在scripts中有一个名叫DefineSprite (171)的项目，点开之后发现一段奇怪的字符串




```
Push "k" "3F3F666C61677B6A7065787337726565666C6173687D2121"
```

看上去像是16进制，转换一下试试，




密码居然！！！wtf！！在这里
填进flag，居然通过了！！！！


over，我只是个碰巧找到答案的菜鸡，
36号。
…再次卑微求赞…