口令攻击实验V2.0

原创

AKalone 于 2019-10-21 01:42:24 发布 1689 收藏 3

分类专栏： 网络攻防 文章标签： 口令攻击 网络攻防

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/shidonghang/article/details/102656486

版权

网络攻防 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

口令攻击实验V2.0

实验目标

解开flag.rar的口令，获得解压缩文件中的Flag。

实验初始线索

打开nnn.docm，其中会有下一步指示。

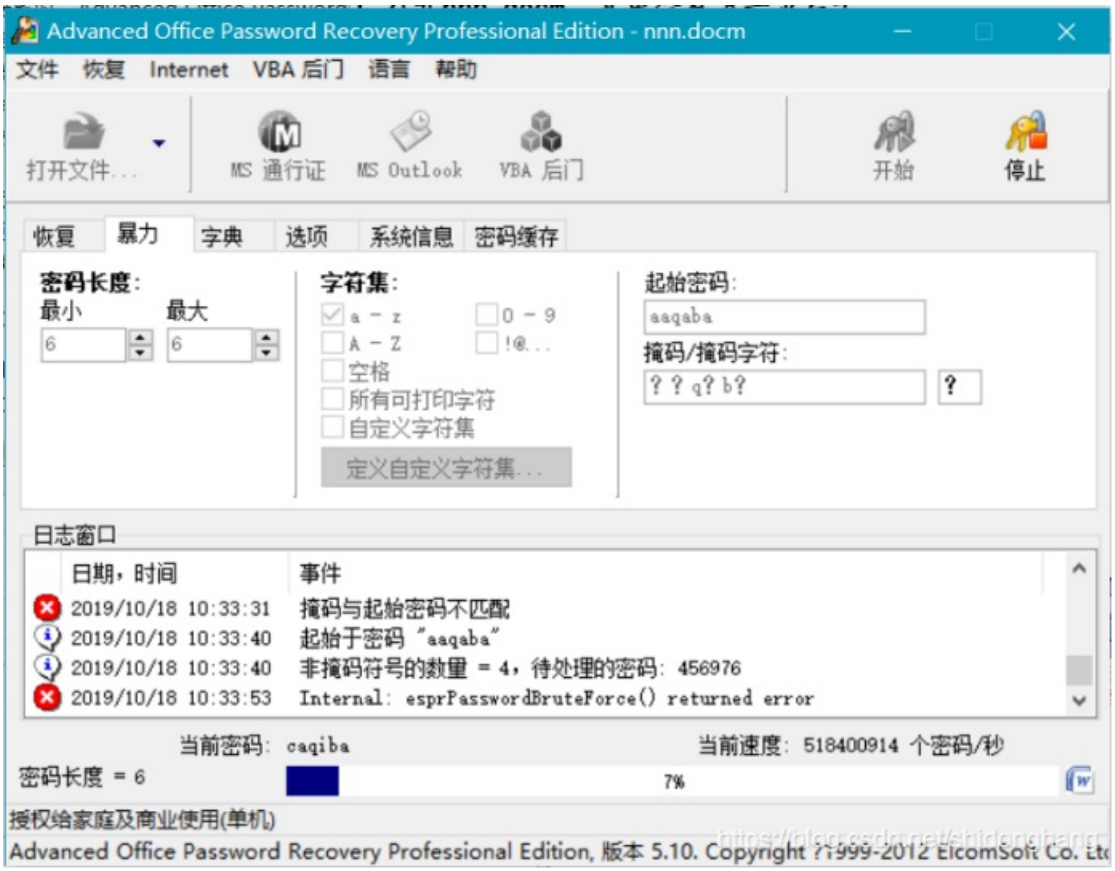
提示：文档nnn.docm的打开口令由6位小写英文字母构成，其中第3位为"q",倒数第2位为“b”。

实验步骤

一、破解nnn.docm文档打开密码。

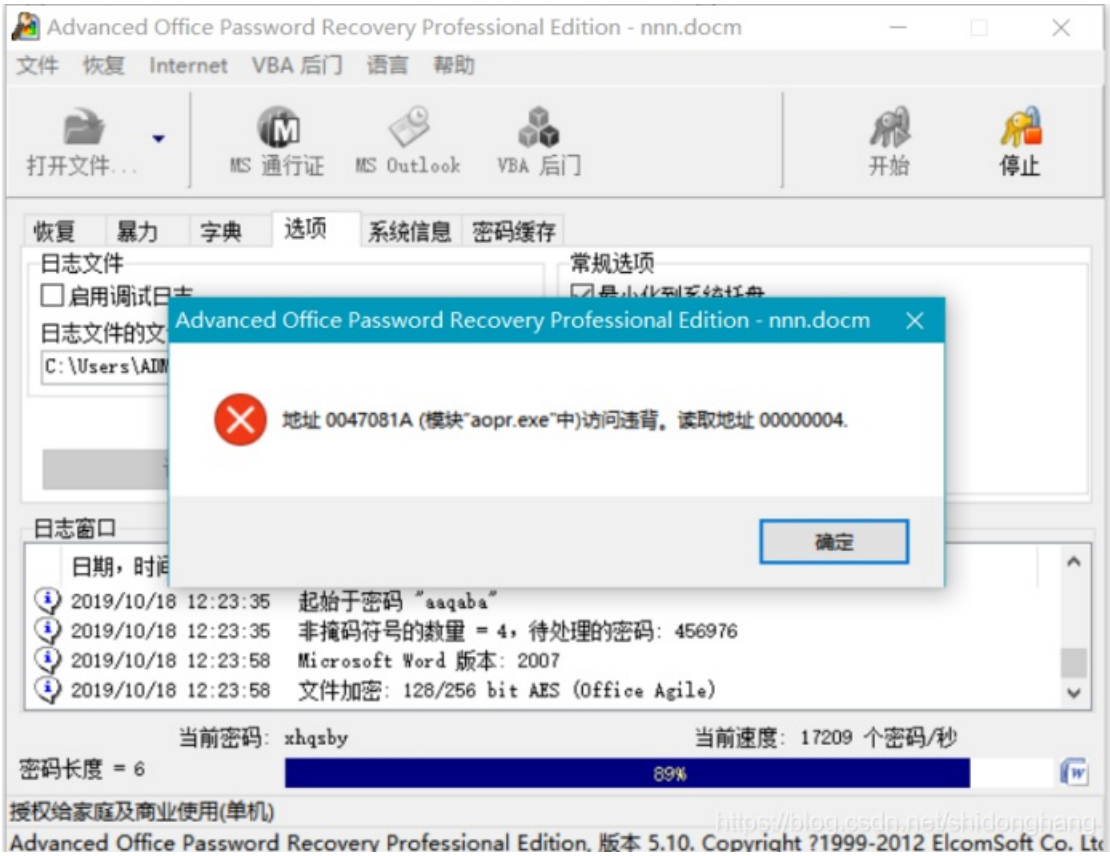
1.使用AOPR，配置并进行带掩码的暴力破解。


恢复
暴力
字典
选项
系统信息
密码缓存
日志文件
启用调试日志
日志文件的文件夹:
C:\Users\AIMINI~1\AppData\Local\Temp\Adv
设备管理器
常规选项
最小化到系统托盘
如果方案被更改则提示
初步暴力破解
初步字典破解
密码缓存初步破解

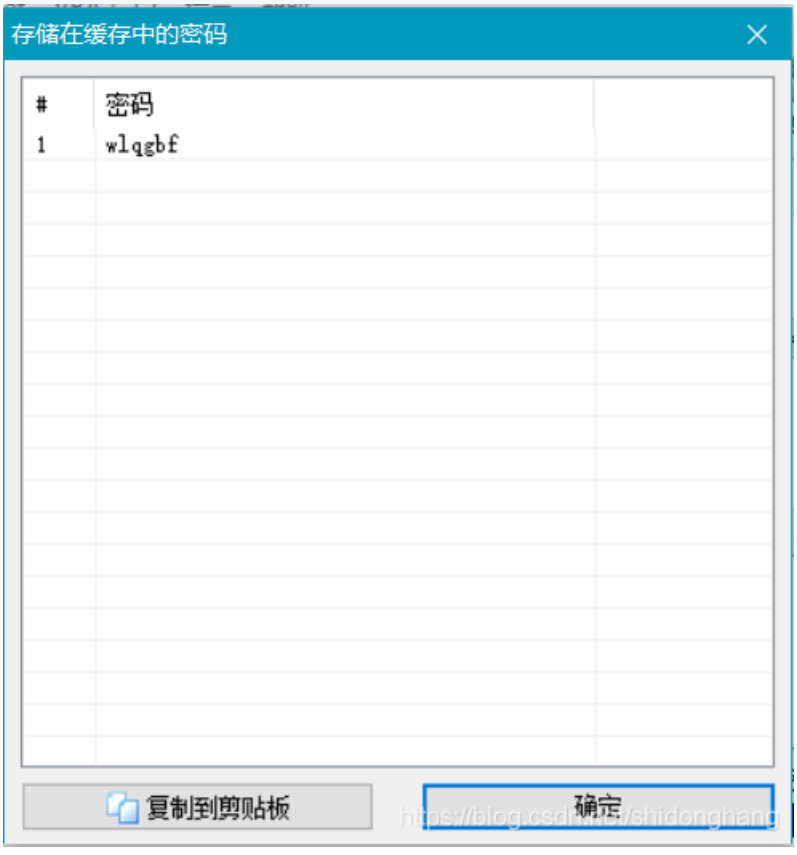

Advanced Office Password Recovery Professional Edition - nnn.docm
文件
恢复
Internet
VBA 后门
语言
帮助
打开文件...
MS 通行证
MS Outlook
VBA 后门
开始
停止
恢复
暴力
字典
选项
系统信息
密码缓存
密码长度:
最小
最大
6
6
字符集:
a - z
A - Z
空格
所有可打印字符
自定义字符集
0 - 9
!@...
定义自定义字符集...
起始密码:
aaqaba
掩码/掩码字符:
? ? q? b?
?
日志窗口
日期，时间
事件
2019/10/18 10:33:31
掩码与起始密码不匹配
2019/10/18 10:33:40
起始于密码 "aaqaba"
2019/10/18 10:33:40
非掩码符号的数量 = 4，待处理的密码: 456976
2019/10/18 10:33:53
Internal: esprPasswordBruteForce() returned error
当前密码: caqiba
当前速度: 518400914 个密码/秒
密码长度 = 6
7%
授权给家庭及商业使用(单机)
Advanced Office Password Recovery Professional Edition, 版本 5.10. Copyright ?1999-2012 ElcomSoft Co. Lt

2.在该处突然中断，弹框。

原本以为是我配置有误，再次使用，直接中断，于是，我重新下载该软件，依旧无法实现100%破解，搞了一节多课，后来，才知道密码已经得到，放在了缓存内。



3.打开密码缓存，得到密码。



二、绕宏取线索。

1.打开nnn.docm，出现如下窗口。

点击取消后，看到如下文字：

本任务终极目标是：将给定的 rar 包解开，提取文档中的 flag。

1. 线索需要由本文档中的宏运行给出，因此不要禁用宏。
2. Rar 密码为复杂型，长度为 13 位，包含了字母、数字和符号。
3. 宏口令为 8 位，包括 5 位小写字母和 3 个数字。

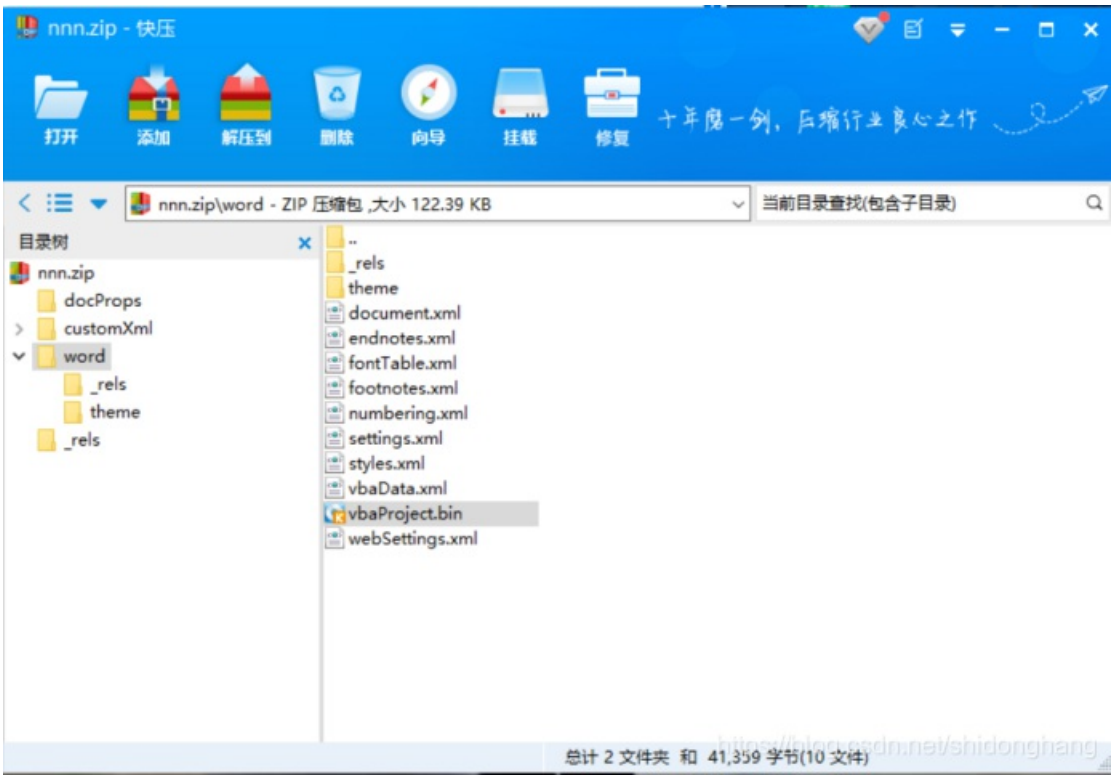
https://blog.csdn.net/shidonghang

可知，文档给出的线索不足，需要破解出宏口令，而宏口令有8位，5位小写字母，3位数字，直接求解宏口令难以实现，所以需要绕宏。

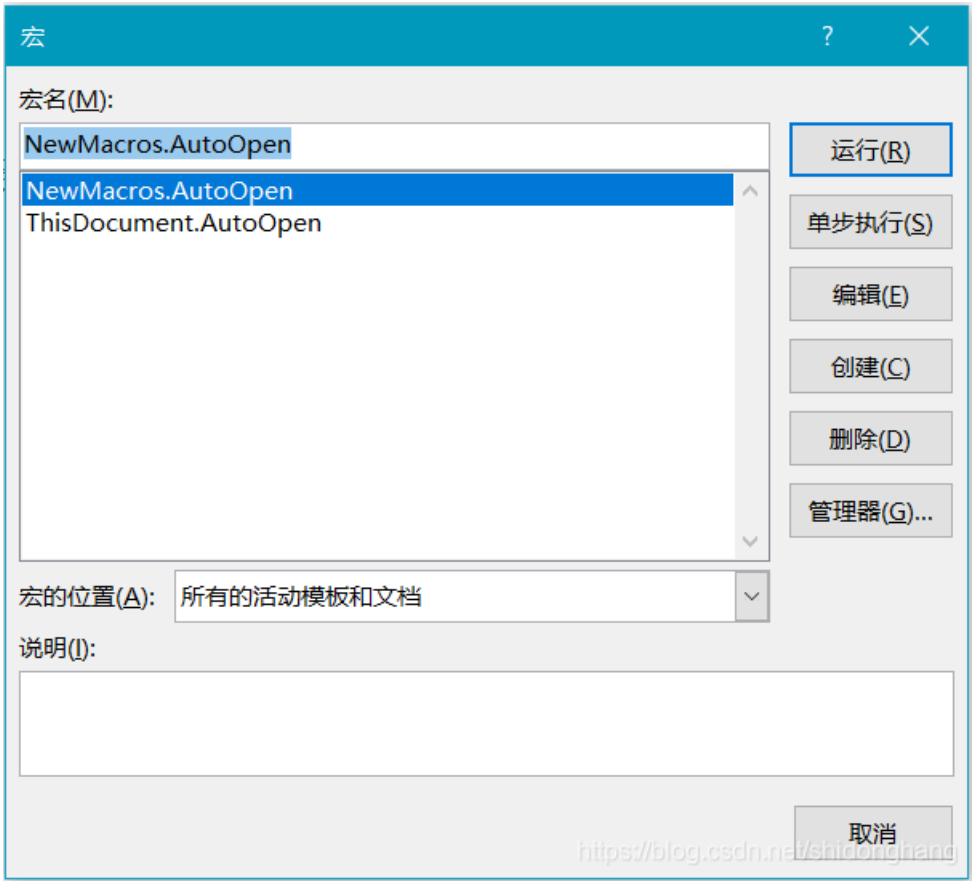
2.绕宏看VB代码

先将nnn.docm文件重命名为zip格式，然后将其中的vbaProject.bin先拖到桌面，用UltraEdit软件把文中DPB改为DPX，保存后拖

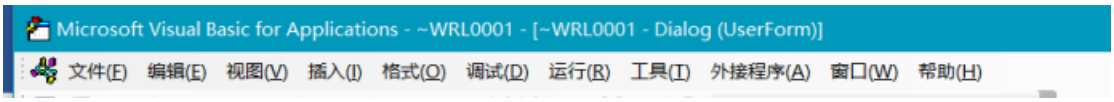
先将nnn.docm文件重命名为zip格式，然后将其中的vbaProject.bin先拖到桌面，用UltraEdit软件把文件DPB改为DPX，保存后拖回nnn.zip，最后改回nnn.docm。

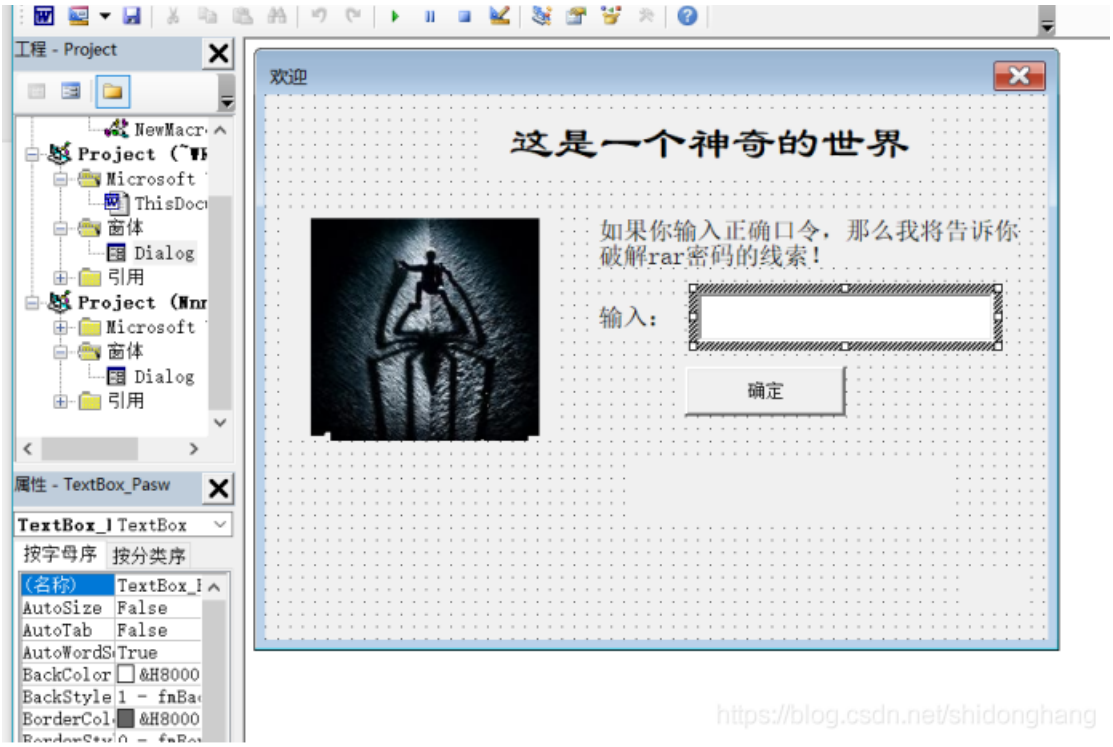


再次打开nnn.docm，弹框点“是”，然后查看宏，进入编辑。



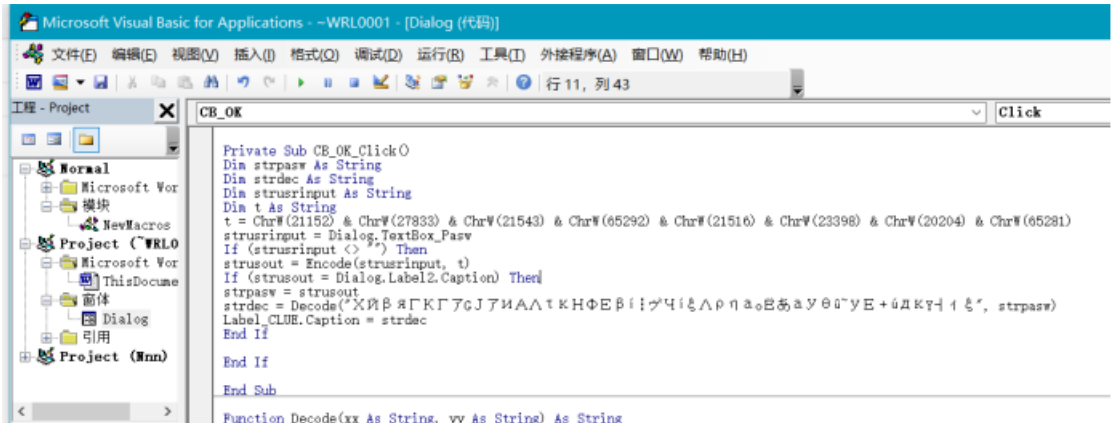
发现查看该项目不再需要密码，但是点击输入框和确定框时会弹出错误提示，错误为40230。

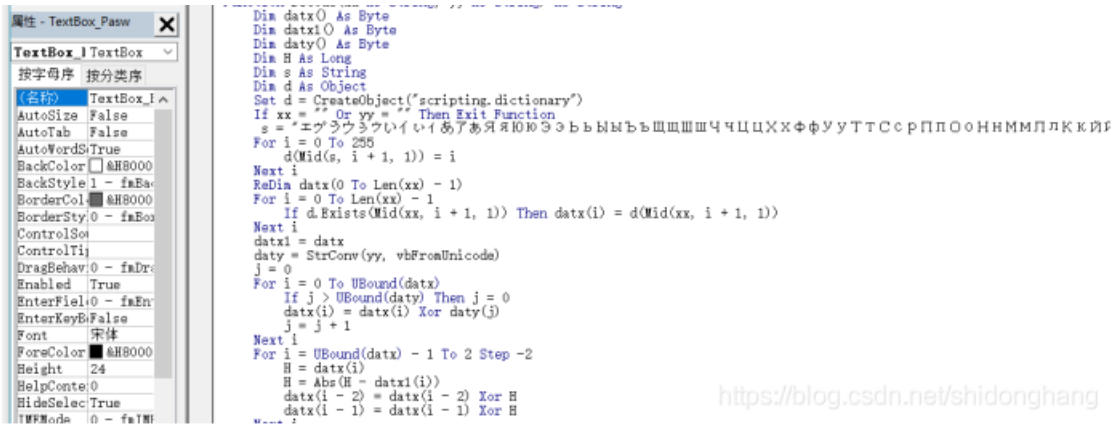




经过百度，在工具->Project-工程属性，设置如下：

确认后即可查看VB代码。





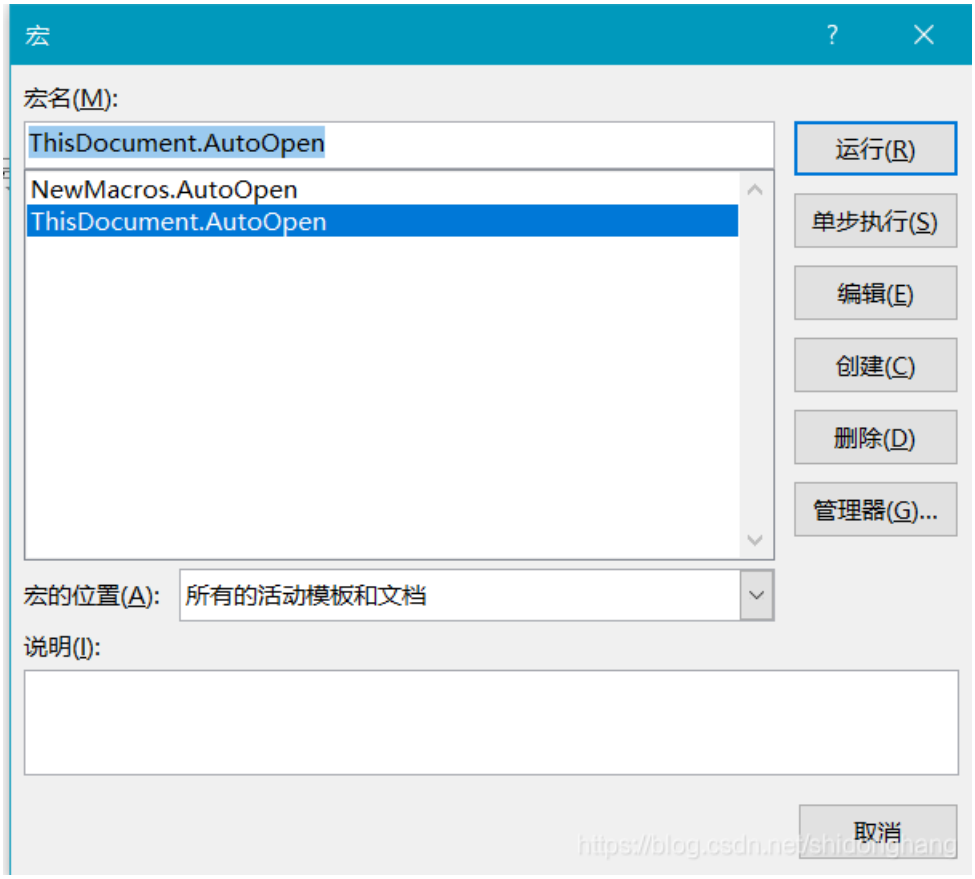
将其中一段代码，改为如下：

```
Private Sub CB_OK_Click()
Dim strpasw As String
Dim strdec As String
Dim strusrinput As String
Dim t As String
t = ChrW(21152) & ChrW(27833) & ChrW(21543)
strusrinput = Dialog.TextBox_Pasw
If (strusrinput <> "") Then
strusout = Encode(strusrinput, t)
If (4052017050#) Then
strusout = Dialog.Label2.Caption
strpasw = strusout
strdec = Decode("ХЙβЯГКГ了GJ了ИΑΛτ
Label_CLUE.Caption = strdec
End If

End If

End Sub
```

运行如图选中宏：



弹出该窗口，输入自己设置的4052017050，即我的学号，得到提示。

三、破解flag.rar密码。

现在我们已有的线索如下：

1.Rar密码为复杂型，长度为13位，包含了字母、数字和符号。
2.还记得我们练过的大字吗？亭台六七座，八九十枝花。

思考如下：

一看到这诗句，我立马想到了“娉娉袅袅十三余，豆蔻梢头二月初。”这个CSDN年度最佳密码，这个rar密码一定大同小异。
密码为13位，而“亭台六七座，八九十枝花。”中若把六七八九十写为数字，则十可以变为10，长度加一。
又因为密码包含符号，起初我以为要把“花”理解为*，么没有考虑标点符号，如此，密码长度不足，而除“十”占两位外，其余各一位，刚好能凑齐13位密码。
如此分配，可得到“tt67z,8910zh.”，我激动尝试，失败了，我很难过。
我反复看这两条线索，甚至读了起来，一读起来，这“大字”就很别扭了，我就觉得要大写字母吧，试了一下，还不行？？？
我产生了自暴自弃的想法，用字典生成器生成出所有的大小写搭配字典，然后暴力破解。嗯！是的，我已经开始下载了，还真是琳琅满目。

心累的我，打开了计蒜客网页，做了做ACM编程题，正巧遇到了“;”与“；”傻傻分不清的编写错误。
这个错误提醒了我，回头一看，我的密码是开了英文输入的，标点符号是英文的，因为密码没设置可见，之前也没有注意，然后，这次改用中文标点符号，输入密码“TT67Z，8910ZH。”,Boom!!!这个让我熬到深夜的flag.txt文档就打开了。

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖