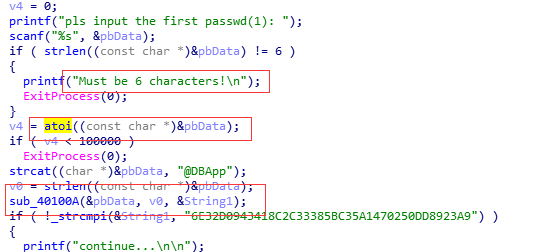
# 题目分析

程序让输入两个password，先看第一个。



先让输入6个字符，然后发现atoi函数，这个函数是把字符串转化为整型数的一个函数。所以可以判断输入password1是六个数字字符。接着又在password1字符串后加上了”@DBApp”。

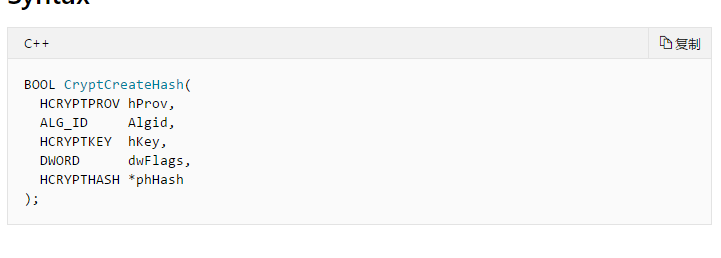
然后我们看sub\_40100A函数。

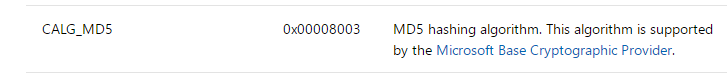
搜索后发现是进行了哈希加密，根据0x8004判断是sha加密。



<https://docs.microsoft.com/zh-cn/windows/win32/api/wincrypt/nf-wincrypt-cryptcreatehash?redirectedfrom=MSDN>

https://docs.microsoft.com/zh-cn/windows/win32/seccrypto/alg-id?redirectedfrom=MSDN



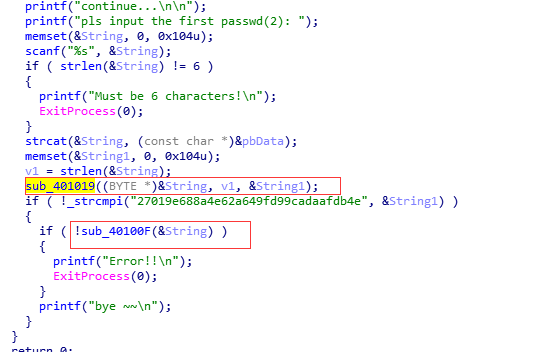


然后password1可写脚本进行爆破得到。

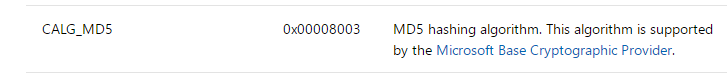
import hashlib  
password1 = ""  
arr = ['0', '1', '2', '3', '4', '5', '6', '7', '8', '9']  
for i1 in arr:  
 for i2 in arr:  
 for i3 in arr:  
 for i4 in arr:  
 for i5 in arr:  
 for i6 in arr:  
 password1 = i1 + i2 + i3 + i4 + i5 + i6 + "@DBApp"  
 if(hashlib.sha1(password1).hexdigest().upper() == "6E32D0943418C2C33385BC35A1470250DD8923A9"):  
 print password1  
 break

可以得到password1为“123321”。

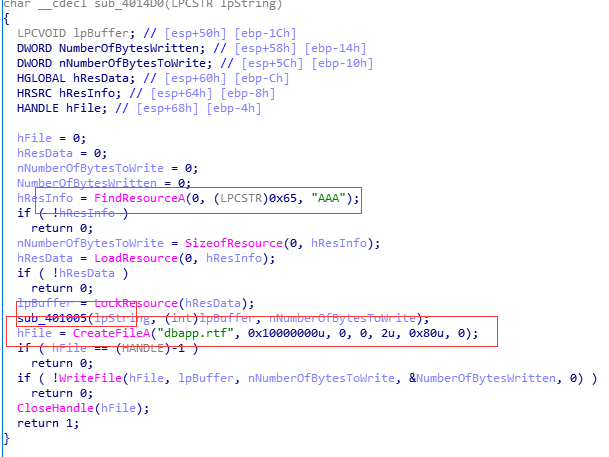
然后是password2 。



根据CryptCreateHash函数的第二个参数进行可以判断出是对6个字符进行了md5加密。



然后进行了对比，如果直接爆破的话花时间回很久，我们先看sub\_40100F函数。

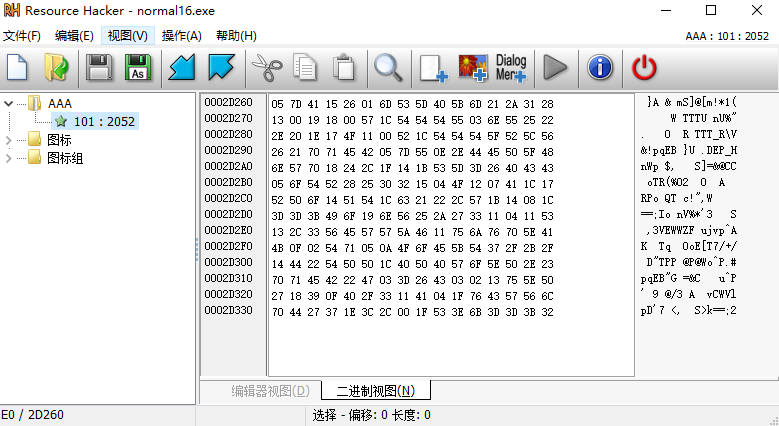


首先查找名为“AAA”的资源并取出数据，接着进入sub\_401005发现是取出的数据跟

输入的密码2+输入的密码1+“@DBApp”进行了异或，最后生成了.rtf文件，最后的flag应该就在.rtf文件里。

由于密码2是最前面先异或的数据，我们又能查找到“AAA”资源的数据，然后我们还可以搜索到.rtf的数据格式得到前面几个的固定的数据，所以可以写脚本得到密码2 。

使用ResourceHacker软件查看资源，得到前六个数据为0x5,0x7D,0x41,0x15,0x26,0x1。



然后我们搜索rtf文件格式，可以得到前六个字符为“{\rtf1”。

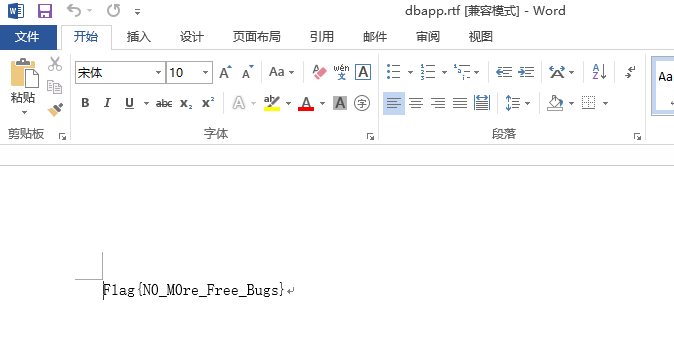


然后写出脚本得到password2 。

arr = [0x05,0x7D,0x41,0x15,0x26,0x01]  
str = "{\\rtf1"  
password2 = ""  
for i in range(6):  
 password2 += chr(arr[i] ^ ord(str[i]))  
print password2

password2为“~!3a@0”。

然后我们输入这两个password，会生成一个rtf文件，打开后文件内容即是flag。



## Flag{N0\_M0re\_Free\_Bugs}