

# Isc2016 writeup

转载

[weixin\\_30651273](#) 于 2017-02-15 21:42:00 发布 79 收藏

原文链接: <http://www.cnblogs.com/hua198/p/6403519.html>

版权

第一题: (仿射变换源码略)

已知仿射加密变换为  $c = (11m + 8) \bmod 26$ , 试对密文 `sjoyuxzr` 解密

```
Flag
16
FangsheMima [Java Application] C:\Program Files\Java\jre1.8.0_9
请输入两个密钥: http://blog.csdn.net/
11 8
请选择: 1、加密; 2、解密; 3、退出
2
请输入密文:
sjoyuxzr
明文: itksuzlp
请选择: 1、加密; 2、解密; 3、退出
Flag: itksuzlp
```

第二题:

好长的字符串

50

725 solves

```
Vm0wd2QyVkhVWGHVYmxKV1YwZDRXRmxVUm5kVIJscHpXa2M1
VjFKdGVGWIZNbmhQWVd4YWMxZHViRmROYWxaeVdWZDRZV01
4WkhGU2JlQk9VbTVdZVZkV1pEUlRNazE0Vkc1T2FWSnVRaziWY
WtwdlZWWmtWMMWt6YUZSTIZUVkpWbTEwYzJGV1NuVIJiR2hYWW
xSV1JGcFdXbXRXTVZwMFpFWINUbFp1UWpaV2Fra3hVakZaZVZO
cmJGSmlWR3hXVm01d1lyUldjRmhsUjBacVZtczFNVmt3WkRSVkJER
kZWbXBXVjFKc2NGaFdh3BIVTBaYWRWSnNTbGRTTTTAwMQ==
```

Base64 连续多次解码

```
ZmxhZzpnbn29kbHVja21zY2M=
```

编码

解码

Base64编

```
flag:goodluckiscc
```

解答错误, 去掉“flag:”试试, 正确。



# 心灵鸡汤

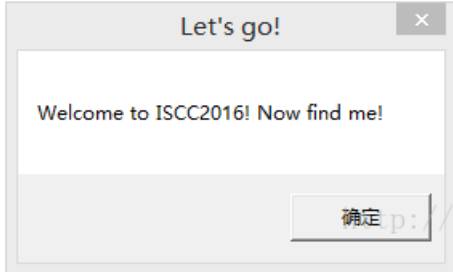
100

276 solves

本程序中暗藏了一句加密的心灵鸡汤，找到它并对其进行解密。

[附件下载](#)

打开附件并执行



IDA 打开 .exe 文件，搜索 ISCC2016，在上方找到 Unicode

```
0 Caption: ; DATA XREF: sub_401000+1770
0 unicode 0, <Congratulations! You need remember:>,0
3 ; const WCHAR Text
3 Text: ; DATA XREF: sub_401000+1C70
3 unicode 0, <DEath IS JUST A PaRT oF LIFE,sOMeTHInG wE>
3 dw 27h
3 unicode 0, <RE aLL dESTInED TO dO.>,0
3 align 4
3 ; const WCHAR aLetSGo
3 aLetSGo: ; DATA XREF: sub_401000:loc_40103470
3 unicode 0, <Let>
3 dw 27h
3 unicode 0, <s go!>,0
0 ; const WCHAR aWelcomeToIscc2
0 aWelcomeToIscc2: ; DATA XREF: sub_401000+3970
0 unicode 0 <Welcome to ISCC2016! Now find me!> 0
```

DEath IS JUST A PaRT oF IIFE,sOMeTHInG wERE aLL dESTInED TO dO.Lets Go!

DEath ISJUS TAPaR ToFII FEsOM eTHInG wERE aLL dESTInED TO dO.Lets go!

解密错误，继续解密

经查找为培根解密：

DEath ISJUS TAPaR ToFII FEsOM eTHInG wERE aLL dESTInED TOdO.Lets go!

AABBB AAAAA AAABA ABABA AABAA BAAAB ABAAA BAABA AAABA AAABA

Flag: HACKERISCC

第五题：

小伟将自己神秘网站的密码保存在了附件中，并进行了他自认为保险的加密方法，请破解它吧。

## 附件下载



解压无法找到 flag 中的文件夹，于是使用命令行，进入 `Thumbs.ms`

```
C:\Basic-8\flag>dir/a
驱动器 C 中的卷没有标签。
卷的序列号是 5E69-A650

C:\Basic-8\flag 的目录

2015/08/13  20:38  <DIR>          .
2015/08/13  20:38  <DIR>          ..
2015/08/13  13:47                76 desktop.ini
2015/08/13  20:24  <DIR>          Thumbs.ms
                1 个文件           76 字节
                3 个目录 162,582,089,728 可用字节

C:\Basic-8\flag>cd Thumbs.ms
```

进入后看到 `desktop.ini` 文件，被设置成了隐藏属性，删除。  
用 `attrib` 命令清除它的只读、存档、系统、隐藏属性，删除。

```
C:\Basic-8\flag\Thumbs.ms>dir/a
驱动器 C 中的卷没有标签。
卷的序列号是 5E69-A650

C:\Basic-8\flag\Thumbs.ms 的目录

2015/08/13  20:24  <DIR>          .
2015/08/13  20:24  <DIR>          ..
2015/08/13  13:47                65 desktop.ini
2015/08/13  20:24  <DIR>          _com1.<d3e34b21-9d75-4
                1 个文件           65 字节
                3 个目录 162,582,056,960 可用字节

C:\Basic-8\flag\Thumbs.ms>del desktop.ini
找不到 C:\Basic-8\flag\Thumbs.ms\desktop.ini

C:\Basic-8\flag\Thumbs.ms>attrib -r -a -s -h desktop.ini
http://blog.csdn.net/
C:\Basic-8\flag\Thumbs.ms>del desktop.ini
```

用 `dir/x` 看到短文件名，将其修改

```
C:\Basic-8\flag\Thumbs.ms>dir/x
驱动器 C 中的卷没有标签。
卷的序列号是 5E69-A650

C:\Basic-8\flag\Thumbs.ms 的目录

2015/08/13  20:24  <DIR>          _COM1~1.<D3  _com1.<d3e34b21-9d75-101a-8
00aa001a1652>
                0 个文件           0 字节
                1 个目录 162,565,165,056 可用字节
```

```

C:\Basic-8\flag\Thumbs.ms>ren _COM1~1.<D3 1
C:\Basic-8\flag\Thumbs.ms>ed 1
'ed' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
C:\Basic-8\flag\Thumbs.ms>cd 1
C:\Basic-8\flag\Thumbs.ms\1>dir/x
驱动器 C 中的卷没有标签。
卷的序列号是 5E69-A650

C:\Basic-8\flag\Thumbs.ms\1 的目录

2015/08/13  20:24    <DIR>          .
2015/08/13  20:24    <DIR>          ..
2015/08/13  20:24    <DIR>          ΔΔ  ~1      ΔΔ  ̂
           0 个文件             0 字节
           3 个目录 162,564,730,880 可用字节

```

这个文件夹的名称是以小数点结尾的，而文件名是不可以用小数点结尾的。  
改名，用 `ren " + Tab` 输入。

```

C:\Basic-8\flag\Thumbs.ms\1>ren "ΔΔ  ~1" 1
C:\Basic-8\flag\Thumbs.ms\1>cd 1
C:\Basic-8\flag\Thumbs.ms\1\1>dir
驱动器 C 中的卷没有标签。
卷的序列号是 5E69-A650

C:\Basic-8\flag\Thumbs.ms\1\1 的目录

2015/08/13  20:24    <DIR>          .
2015/08/13  20:24    <DIR>          ..
2015/08/13  20:24    <DIR>          LastF
2015/08/13  13:47                1,756 System.db
           1 个文件             1,756 字节
           3 个目录 162,550,042,624 可用字节

```

进入最后的文件夹，发现名为 `text.bmp` 的文件，无法显示，于是修改后缀为 `.txt` 试试，`flag` 出现了。

```

C:\Basic-8\flag\Thumbs.ms\1\1\LastF 的目录

2015/08/13  20:24    <DIR>          .
2015/08/13  20:24    <DIR>          ..
2015/08/13  20:33                40 text.bmp
           1 个文件             40 字节
           2 个目录 162,550,034,432 可用字节

C:\Basic-8\flag\Thumbs.ms\1\1\LastF>cd text.bmp
目录名称无效。

C:\Basic-8\flag\Thumbs.ms\1\1\LastF>text.bmp
C:\Basic-8\flag\Thumbs.ms\1\1\LastF>ren text.bmp text.txt
C:\Basic-8\flag\Thumbs.ms\1\1\LastF>text.txt
C:\Basic-8\flag\Thumbs.ms\1\1\LastF>

```

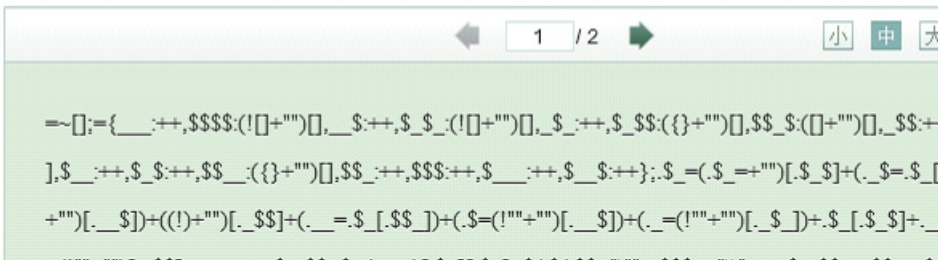
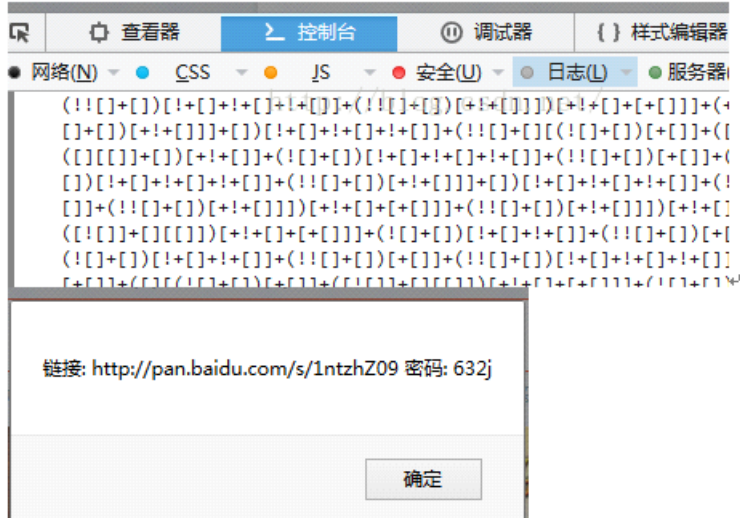
能看出单词顺序有误，变位加密，重新组合，[InformationSecurityTechnology](http://www.InformationSecurityTechnology.com/)

第六题：

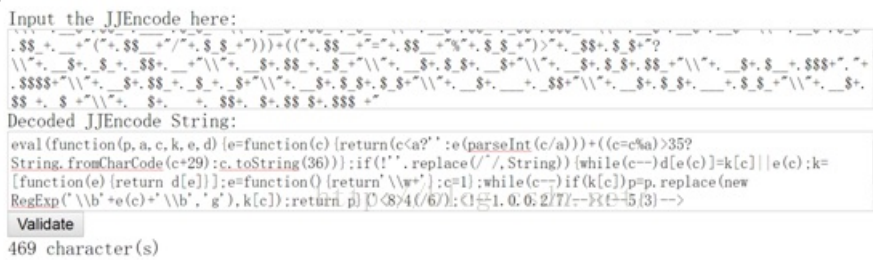
从一段不明所以的符号中，你能得到flag吗？

附件下载

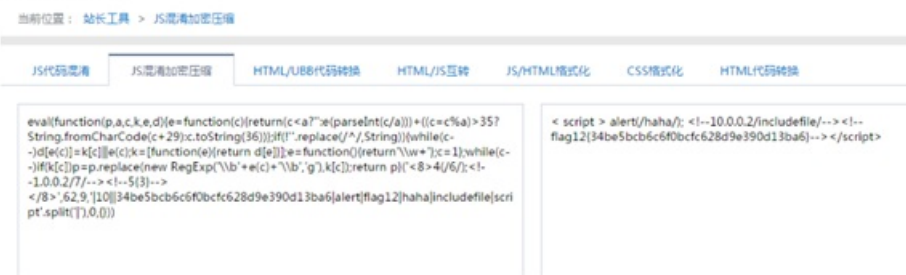
打开附件发现



经查找为 JJencode，解密



JS 混淆解密



Flag: 34be5bcb6c6f0bcfc628d9e390d13ba6