【wp】i春秋百度杯CTF比赛2016年12月场writeup

转载

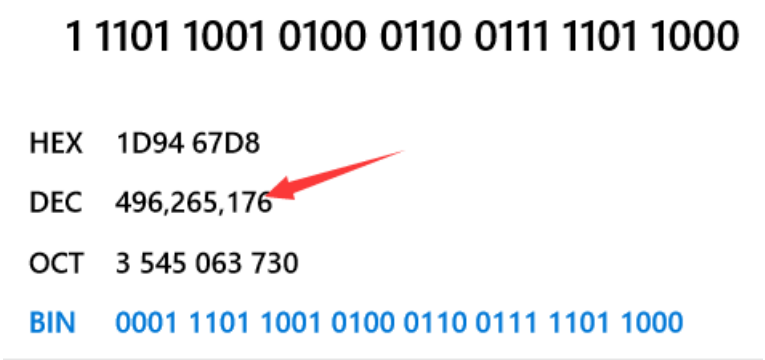
普通网友 于 2017-06-27 00:21:00 发布 329 收藏
文章标签： 密码学 python markdown
原文链接：http://www.cnblogs.com/findneo/p/7083078.html
版权

第一场

传说中的签到题·进阶篇

> 题目：
> 没那么简单~
> 11101100101000110011111011000
> tips1：big num
> tips2： 496265176

1. 二进制转十进制刚好和提示一样，



2. 搜索群号码，在群公告看到疑似base64编码的字符串

Python解码得到flag

```
flag{b159028c-95ff-4f71-ad7b-cef510a22d00}
```

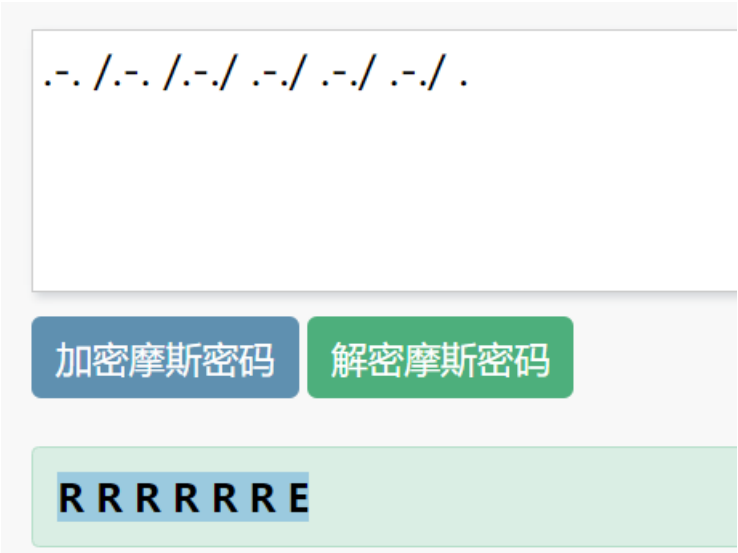
```
>python
Python 2.7.12 (
Type "help", "copyright", credits" or "license" for more information
.
>>> import base64
>>> base64.b64decode('ZmxhZ3tiMTU5MDI4Yy05NWZmLTRmNzEtYWQ3Yi1jZWY1MTB
hMjJkMDB9')
'flag{b159028c-95ff-4f71-ad7b-cef510a22d00}'
>>>
```

福尔摩斯

> 题目：
> 贝克街旁的圆形广场
> -.-. -.-. -.-. -.-. -.-. -.-. .
> flag格式：flag{*********}

可以想到是摩斯电码，把'_'换成'-'，手动添加分隔符，在线解密即可得到flag内容

> flag{RRRRRRE}

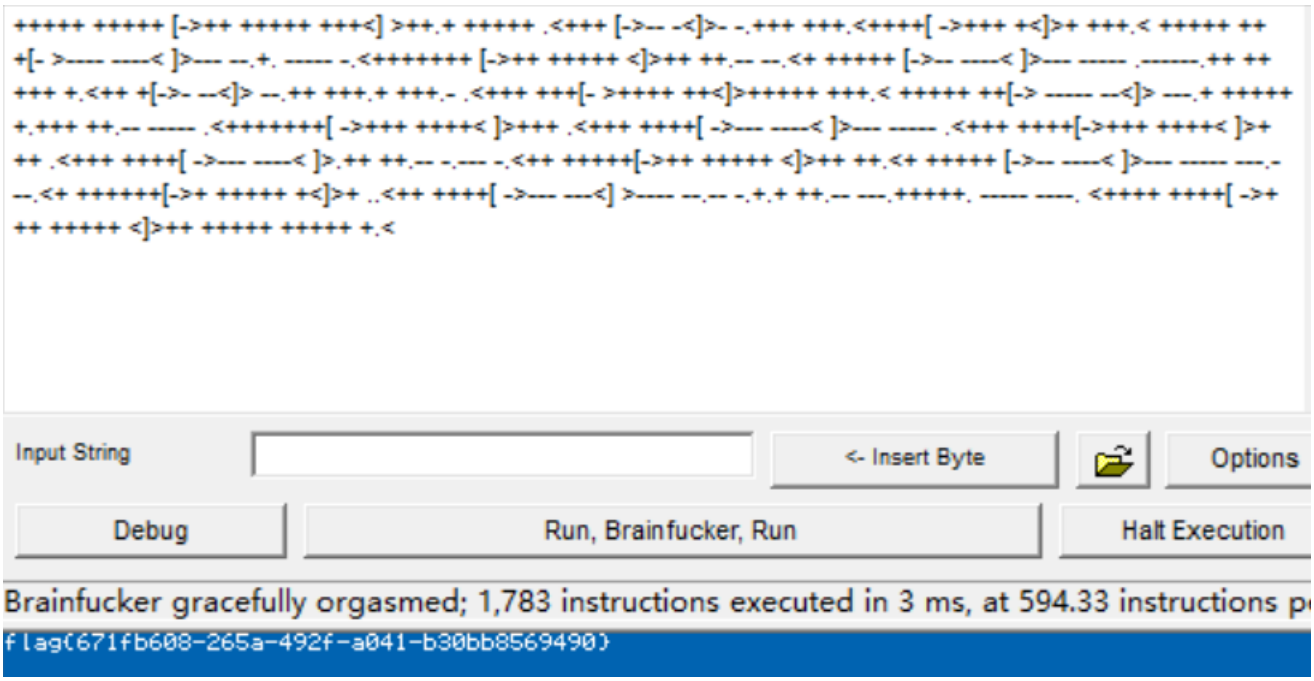


+ —— +

```
+++++ +++++ [->++ +++++ +++<] >++.+ +++++ .<+++ [->-- -<]>- -.+++ +++.<
++++[ ->+++ +<]>+ +++.< +++++ +++[- >---- ----< ]>--- --.+. ----- -.<++
+++++ [->++ +++++ <]>++ ++.-- --.<+ +++++ [->-- ----< ]>--- ----- .----
--.++ +++++ +.<++ +[->- --<]> --.++ +++.+ +++.- .<+++ +++[- >++++ ++<]>
+++++ +++.< +++++ ++[-> ----- --<]> ---.+ +++++ +.+++ ++.-- ----- .<+++
++++[ ->+++ ++++< ]>+++ .<+++ ++++[ ->--- ----< ]>--- ----- .<+++ ++++[
->+++ ++++< ]>+++ .<+++ ++++[ ->--- ----< ]>.++ ++.-- -.--- -.<++ +++++
[->++ +++++ <]>++ ++.<+ +++++ [->-- ----< ]>--- ----- ---.- --.<+ +++++
+[->+ +++++ +<]>+ ..<++ ++++[ ->--- ---<] >---- --.-- -.+.+ ++.-- ---.+
++++. ----- ----. <++++ ++++[ ->+++ +++++ <]>++ +++++ +++++ +.<
```

是Esolang的一种，brainfuck,写的程序，用解释器/或者在线工具运行一下得到flag

```
flag{671fb608-265a-492f-a041-b30bb8569490}
```



第二场

一个十六岁的少年

```
题目：
有一天，表姐的好朋友贝丝远房的表亲，一个16岁的少年
给表姐递了一封情书，表姐看不懂，你能帮忙翻译下吗？
666C61677B65633862326565302D336165392D346332312D613031322D303861613566613762653637D
```

贝丝、十六岁，容易猜想是base16编码，Python解码得到flag

> flag{ec8b2ee0-3ae9-4c21-a012-08aa5fa7be67}

```
>>> base64.b16decode('666C61677B656338623265653302D336165392D346332312
D613031322D303861613566613762653637377D')
'flag{ec8b2ee0-3ae9-4c21-a012-08aa5fa7be67}'
>>>
```

藏在邮件头里的秘密

> flag{ichunqiu_=E6=8A=80=E6=9C=AF=E6=9C=89=E6=B8=A9=E5=BA=A6}

曾接触过类似特征的编码，判断为可打印字符编码(Quoted_Printable),在线解码即得到flag

> flag{ichunqiu_技术有温度}

另外：

> 在所有邮件处理的各式各样的编码中，很多编码的目的都是通过编码手段使 得七位字符的邮件协议体系可以传送八位的二进制文件、双字节语言文字等等。 Quoted-Printable也是这样一些编码中的一个， 它的目的同样是帮助非ASCII 编码的信件传输通过 SMTP。Quoted-Printable 编码是字符对应的编码，每个未 编码的二进制字符被编码成三个字符，即一个等号和一个十六进制的数字，如“=A8”。
> Quoted-Printable编码的源码样式如下: =D4=DA=CB=F9=D3=D0=D3=CA=BC=FE=B4=A6=C0=ED.....

吃货

> 麻辣烫的标配
> flag{abbab_babbb_baaaa_aaabb}

根据提示猜想是培根密码
解密得到两种可能，逐一尝试得正确flag

> flag{N_X_Q_D}

```
       *******Bacon Encode_Decode System*******
input should be lowercase,cipher just include a b
1.encode
2.decode
3.exit
please input number to choose
2
please input string to decode:
abbabbabbbbaaaaaaabb
first decode method result is:
nxqd
second decode method result is:
ozrd
```

第三场

misc1

话不多说，看图片

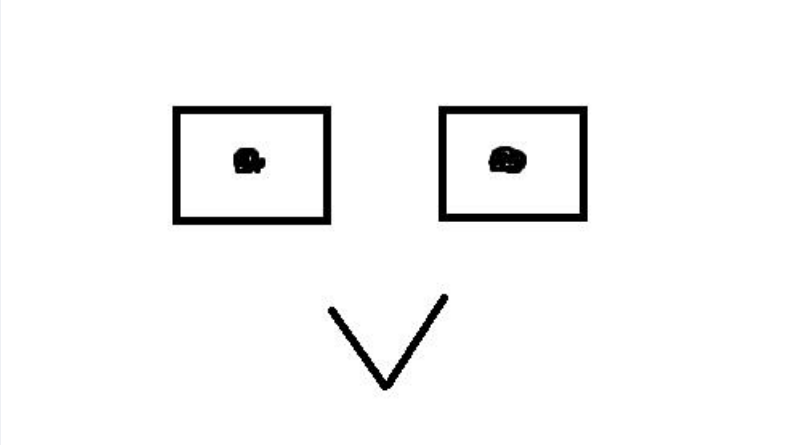
大概是隐写吧，先用winhex打开看看，拖到最后直接可以看到flag

flag{stego_is_s0_bor1ing}

misc1.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000062C0	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
000062D0	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
000062E0	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
000062F0	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00006300	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00006310	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00006320	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00006330	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00006340	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00006350	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00006360	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00006370	40	05	14	51	40	05	14	51	40	1F	FF	D9	2D	2D	2D	A1	@ Q@ Q@ ÿÙ---¡
00006380	B7	66	6C	61	67	20	49	53	20	66	6C	61	67	7B	73	74	·flag IS flag{st
00006390	65	67	6F	5F	69	73	5F	73	30	5F	62	6F	72	31	69	6E	ego_is_s0_borlin
000063A0	67	7D															g}

misc2



很明显是猪圈密码，对照密码表手工解密得到flag

> flag{NSN}

misc3

> 哒哒哒哒，你知道什么是键盘坐标密码吗？
> 11 21 31 18 27 33 34
> flag格式：flag{*****}

谷歌了键盘坐标密码，很浅显。看到出现数字7/8，判断数字应该是（行，列）组合，试了下qazijcv，不行，改大写即可。

> flag{QAZIJCV}

第四场

misc1-纵横四海

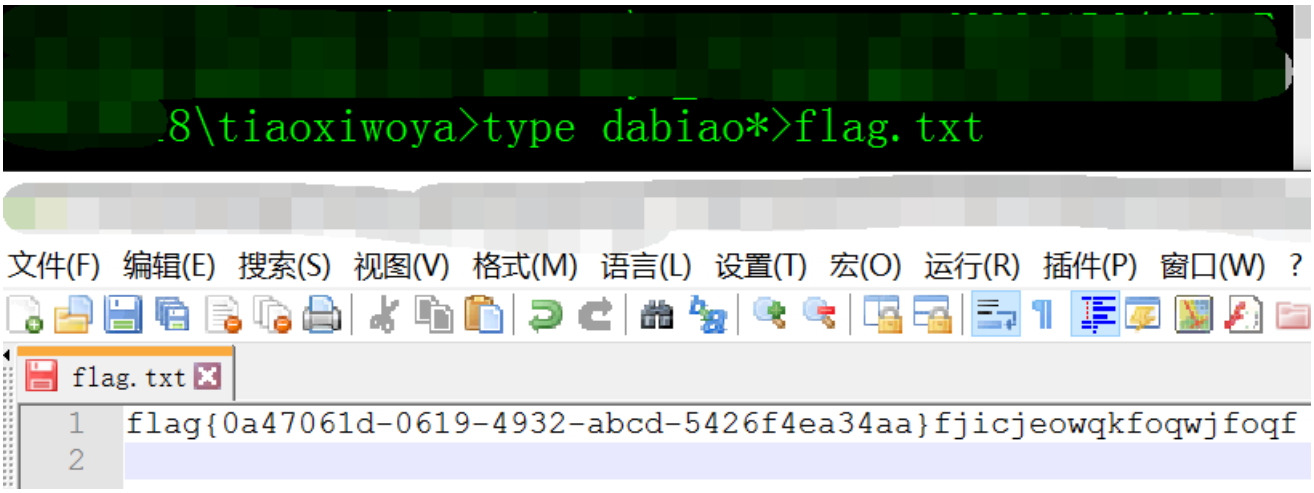
> 题目：
> 有句话说的好
> （大表姐最美）
> 。
> 。
> 。
> 。
> 。
> 天下分久必合，合久必分
> 附件下载

附件是一个压缩包，解压。按文件名称正序排列后打开前几个文件看到每个文件里有一个字符，诸如‘f’,‘l’,‘a’...云云，于是会心一笑。。。

```
//windows下命令行
**> cd tiaoxiwoya
**> type dabiaojie* >>flag.txt
```

然后去掉换行符就得到flag

> flag{0a47061d-0619-4932-abcd-5426f4ea34aa}



misc2-对错

> 题目：
> 如果说1代表对，0代表错，那么-1代表？
> 附件下载

点开链接，跳转到一个静态页面，上面只有一个二进制串

> 01100110011011000110000101100111011110110111101001101000010001010110001100111001001100000011(

直接binary->ascii即可得到flag

> flag{zhEc9034jodsjfosko}

misc3-枯竭

> 讲真的，才华已经枯竭
> 大家好好答题
> 也许这道题一点都不坑
> 也许。。。。。
> 附件下载

是一个加密的压缩包，用Ziperello爆破得到密码“12345”
解压后得到flag

> flag{319b7f63-e17d-4ac5-8428-c2476c7ecce3}

总结

1. 只会做misc。。。
2. misc考点依次大概是base64,摩斯,brainfuck,base16,Quoted-Printable,bacon,简单隐写,pigpen cipher,键盘坐标密码，观察力，编码，zip爆破
3. 为了写writup学了markdown,还找到一个厉害的图床 sm.ms

---

by findneo

转载于:https://www.cnblogs.com/findneo/p/7083078.html