




JarvisOJ basic部分WriteUp

原创

Magic1an  于 2017-08-25 00:12:18 发布  2211  收藏

分类专栏: [ctf](#) 文章标签: [ctf](#)

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/Magic1an/article/details/77543978>

版权



[ctf 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

0x0 前言

由于开学后会有个省赛, 作为一个好久没做过除re以外ctf题的小白, 不得不抽出时间来刷一刷题...通过做JarvisOJ的basic部分确实学到了不少东西, 感谢~

0x1 base64?

1.题目描述

GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXGYZTGNLGGY3DGNBWMU3WI===

2.解题过程

base64?应该是base家族的, 写个脚本decode一下。

```
import base64
str1='GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXGYZTGNLGGY3DGNBWMU3WI==='
try:
    print base64.b64decode(str1)
except:
    try:
        print base64.b32decode(str1)
    except:
        print base64.b16decode(str1)
```

得到结果504354467b4a7573745f743373745f683476335f66346e7d, 很明显, 十六进制转字符就可以了~

```
flag=''
key='504354467b4a7573745f743373745f683476335f66346e7d'
for i in range(0,len(key),2):
    flag+=chr(int(key[i:i+2],16))
print flag
```

得到flag:PCTF{Just_t3st_h4v3_f4n}

0x2 关于USS Lab.

题目描述

USS的英文全称是什么，请全部小写并使用下划线连接_，并在外面加上PCTF{}之后提交

解题过程

百度uss lab可以搜到

[USS Lab. - Ubiquitous System Security Lab.](#)

查看此网页的中文翻译，请点击 [翻译此页](#)

Ubiquitous System Security Lab. Welcome to USS(Ubiquitouse System Security) Lab. US

Lab. belongs to Electrical Engineering College in Zhejiang University...

www.usslab.org/ - [百度快照](#) <http://blog.csdn.net/Magiclan>

OK,flag得到了。

0x3 veryeasy

题目描述

使用基本命令获取flag

解题过程

使用strings得到flag.

```
myubuntu@ubuntu:~/Desktop$ strings veryeasy
__PAGEZERO
__TEXT
__text
__TEXT
__unwind_info
__TEXT
__DATA
__data
__DATA
__LINKEDIT
/usr/lib/dyld
/usr/lib/libSystem.B.dylib
PCTF{strings_is_3asy_isnt_i7}
__mh_execute_header
$main
__mh_execute_header
__main
dyld_stub_binder
```

0x4 段子

题目描述

程序猿圈子里有个非常著名的段子：

手持两把锃斤拷，口中疾呼烫烫烫。

请提交其中“锃斤拷”的十六进制编码。(大写)

FLAG: PCTF{你的答案}

解题过程

对于不会的东西需要百度...

Unicode和老编码体系的转化过程中，肯定有一些字，用Unicode是没法表示的，Unicode官方用了一个占位符来表示这些文字，这就是：U+FFFD REPLACEMENT CHARACTER。

那么U+FFFD的UTF-8编码出来，恰好是 '\xef\xbf\xbd'。如果这个'\xef\xbf\xbd'，重复多次，例如 '\xef\xbf\xbd\xef\xbf\xbd'，然后放到GBK/CP936/GB2312/GB18030的环境中显示的话，一个汉字2个字节，最终的结果就是：锒斤拷——锒(0xEFBF)，斤(0xBDEF)，拷(0xBFBD) ^[1]。



好了，将三个字拼起来就得到了flag: PCTF{EFBFBDEFBFBFD}

0x5 手贱

题目描述

某天A君的网站被日，管理员密码被改，死活登不上，去数据库一看，啥，这密码md5不是和原来一样吗？为啥登不上咧？

d78b6f302l25cdc811adfe8d4e7c9fd34

请提交PCTF{原来的管理员密码}

解题过程

在上面不容易看出，复制到别的地方还是可以轻松的发现上面md5比正确的值多了一位l。去掉l后得到d78b6f30225cdc811adfe8d4e7c9fd34，进行md5解密后即可。

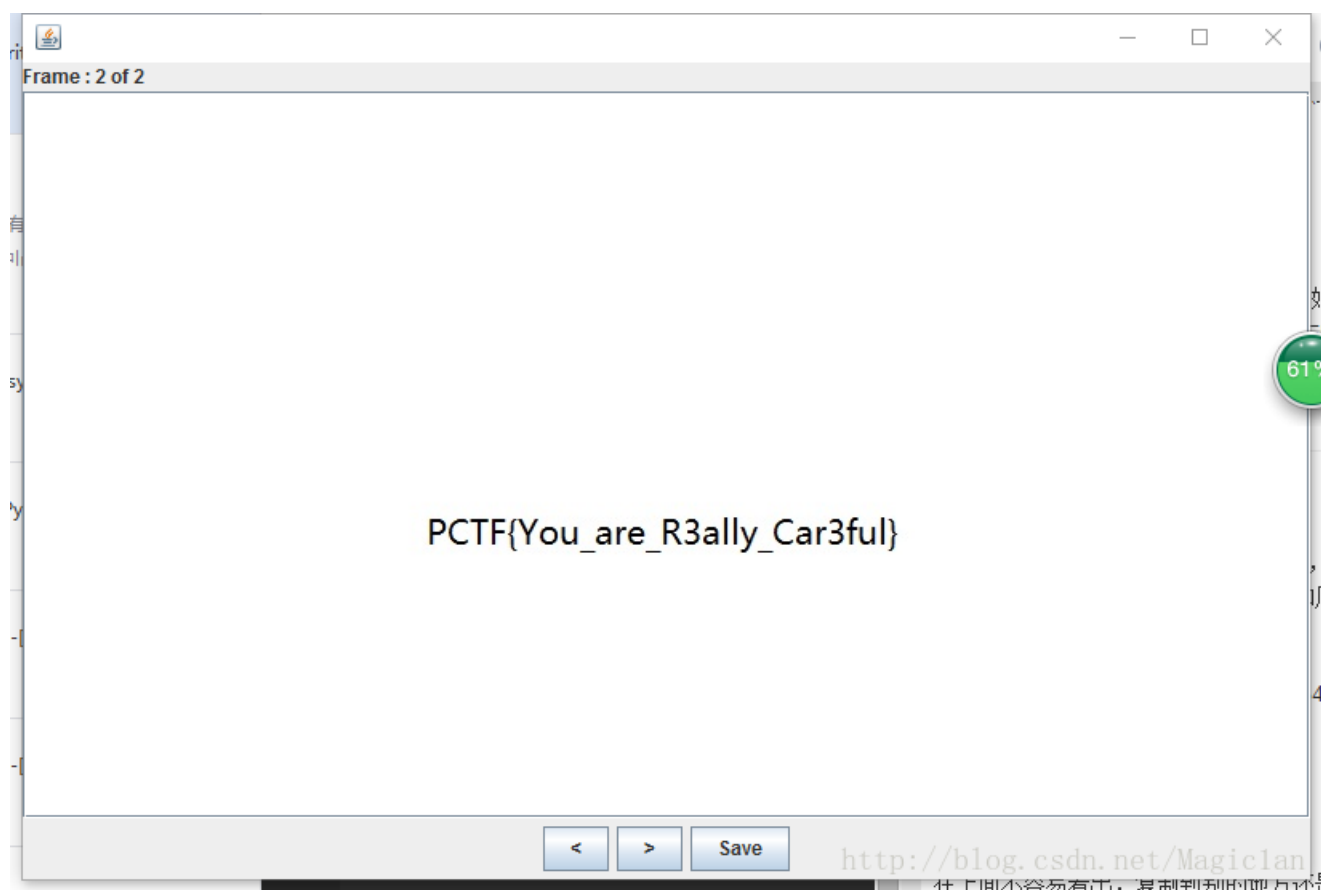
0x6 美丽的实验室logo

题目描述

出题人丢下个logo就走了，大家自己看着办吧

解题过程

运用StegSolve的Frame Brower功能可以在第二帧中得到flag。



0x7 veryeasyRSA

题目描述

已知RSA公钥生成参数:

$p = 3487583947589437589237958723892346254777$ $q = 8767867843568934765983476584376578389$

$e = 65537$

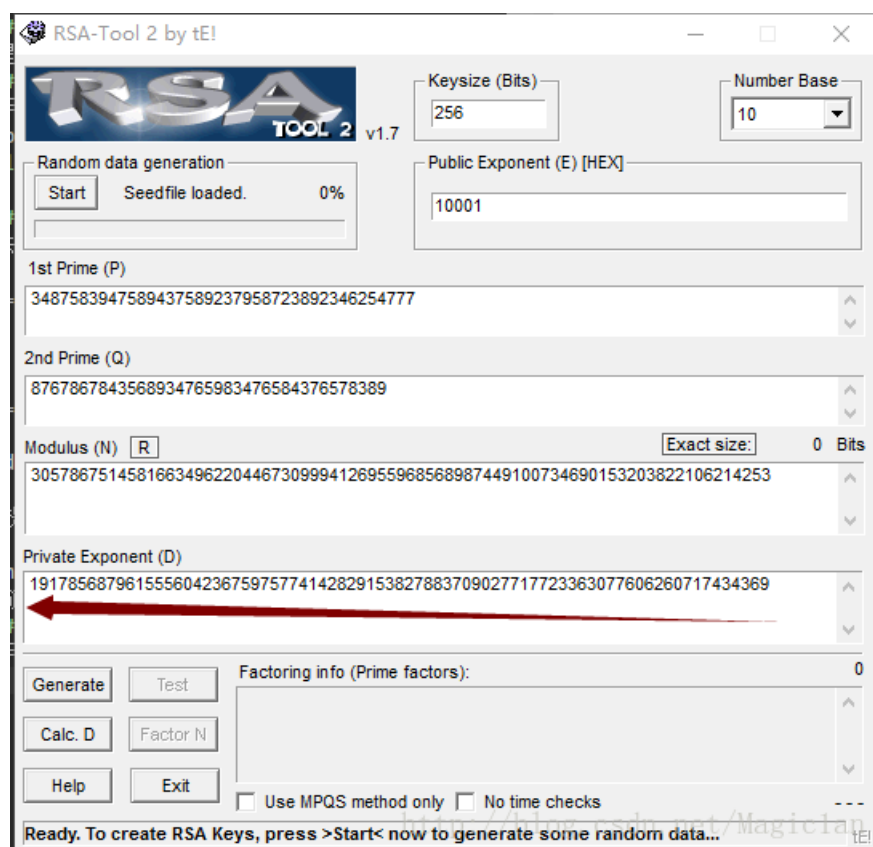
求 $d =$

请提交 PCTF{d}

Hint1: 有好多小伙伴问d提交什么格式的, 现在明确一下, 提交十进制的d

解题过程

运用RSA Tool计算出d.



0x8 神秘的文件

题目描述

出题人太懒，还是就丢了个文件就走了，你能发现里面的秘密吗？

解题过程

利用linux的file得知所给文件为磁盘文件。

将磁盘文件挂载

```
mkdir ffffile &&sudo mount haha ffffile
```

挂载后可以查看文件中的内容

我们发现里面是253个只包含一个字符的文件

猜测可以把这些字符拼接起来得到flag.

```
flag=''
for i in range(254):
    file=open('fffffile/'+str(i))

    flag+=file.read()
    file.close()
print flag
```

```
myubuntu@ubuntu:~/Desktop$ python kkkkk.py
Haha ext2 file system is easy, and I know you can easily decompress of it and find the content in it. But the content is spilted in pieces can you make the pieces together. Now this is the flag PCTF{P13c3_7oghter i7}. The rest is up to you.
Cheer up, boy.
```

<http://blog.csdn.net/Magiclan>

0x9 公倍数

题目描述

请计算1000000000以内3或5的倍数之和。

如：10以内这样的数有3,5,6,9，和是23

请提交PCTF{你的答案}

解题过程

```
sum=0
for i in xrange(1000000000):
    if i%3==0 or i%5==0:
        sum+=i
print sum
```

一个简单的小脚本得到flag,这里注意一定要用xrange,不要用range!

0x10

题目描述

都说逆向挺难的，但是这题挺容易的，反正我不会，大家来挑战一下吧~~:)

解题过程

载入IDA，很容易就能找到关键代码

```

*(_WORD *)v5 = 0xDDABu;
v5[2] = 0x33;
v5[3] = 0x54;
v5[4] = 0x35;
v5[5] = 0xEFu;
printf((unsigned __int64)"Input your password:");
_isoc99_scanf((__int64)"%s", v6, *(_QWORD *)v5);
if ( strlen(v6) == 26 )
{
    v3 = 0LL;
    if ( (v6[0] ^ 0xAB) == list1 )
    {
        while ( ((unsigned __int8)v6[v3 + 1] ^ (unsigned __int8)v5[(signed __int64)(((signed int)v3 + 1)
        {
            if ( ++v3 == 25 )
            {
                printf((unsigned __int64)"Congratulations!");
                return 0;
            }
        }
    }
}
printf((unsigned __int64)"Password Wrong!! Please try again.");
return 0;
}

```

逆一下代码写脚本得到flag.

```

v5=[0xAB,0xDD,0x33,0x54,0x35,0xEF]
lists = [0xfb,0x9e,0x67,0x12,0x4e,
         0x9d,0x98,0xab,0x00,0x06,
         0x46,0x8a,0xf4,0xb4,0x06,
         0x0b,0x43,0xdc,0xd9,0xa4,
         0x6c,0x31,0x74,0x9c,0xd2,
         0xa0]
flag=chr(v5[0]^lists[0])
for i in xrange(1,len(lists)):
    flag+=chr(v5[i%6]^lists[i])
print flag

```

得到flag:

PCTF{r3v3Rse_i5_v3ry_eAsy}

0x11 Secret

题目描述

传说中的签到题

题目入口: <http://web.jarvisoj.com:32776/>

Hint1: 提交格式PCTF{你发现的秘密}

解题过程

查看响应头，可以找到疑似flag的字符串..



请求网址: http://web.jarvisoj.com:32776/
请求方法: GET
远程地址: 120.26.131.152:32776
状态码: ● 200 OK [详细了解] 编辑和重发 原始头
版本: HTTP/1.1

过滤消息头

响应头 (321 字节)

- Date: "Wed, 23 Aug 2017 11:24:34 GMT" [详细了解]
- Server: "Apache/2.4.18 (Unix) OpenSSL/..._perl/2.0.8-dev Perl/v5.16.3" [详细了解]
- X-Powered-By: "PHP/5.6.21"
- Secret: "Welcome_to_phrackCTF_2016" [详细了解]
- Content-Length: "26" [详细了解]
- Keep-Alive: "timeout=5, max=100" [详细了解]
- Connection: "Keep-Alive" [详细了解]
- Content-Type: "text/html; charset=UTF-8" [详细了解]

请求头 (432 字节) http://blog.csdn.net/Magiclan

提交上去没想到竟然是对的。

0x12 爱吃培根的出题人

题目描述

听说你也喜欢吃培根？那让我们一起来欣赏一段培根的介绍吧：

bacon is one of aMeriCa'S sWEethEartS. it's A dARlinG, SuCCulEnt fOoD tHAT PaIRs FlawLE

什么，不知道要干什么？上面这段巨丑无比的文字，为什么会有大小写呢？你能发现其中的玄机吗？

提交格式：PCTF{你发现的玄机}

解题过程

提示培根加密，直接用脚本，不过脚本得到的flag多了一个字母...不知道哪儿出了问题。


```

#coding:utf-8
import string
letters=string.uppercase
a="bacoN is one of aMerICa'S sWEethEartS. it's A dARlInG, SuCCuLEnt fOoD tHAT PaIRs FlawLE"
str1=''
str2=''
key1={"A":"aaaaa","B":"aaaab","C":"aaaba","D":"aaabb","E":"aabaa","F":"aabab","G":"aabba","H":"aabbb",
      "T":"baabb",
      "U":"babaa",
      'V':'babab',
      'W':'babba',
      'X':'babbb',
      'Y':'bbaaa',
      'Z':'bbaab'}
key2={'a':'AAAAA','g':'AABBA','n':'ABBAA','t':'BAABA',
      'b':'AAAAB','h':'AABBB','o':'ABBAB','u':'BAABB','v':'BAABB',
      'c':'AAABA','i':'ABAAA','j':'ABAAA','p':'ABBBA','w':'BABAA',
      'd':'AAABB','k':'ABAAB','q':'ABBBB','x':'BABAB',
      'e':'AABAA','l':'ABABA','r':'BAAAA','y':'BABBA',
      'f':'AABAB','m':'ABABB','s':'BAAAB','z':'BABBB'}
list1=[]
list2=[]
temp1=''
temp2=''
num=0
for i in a:
    if i.isupper():
        temp1+='b'
        temp2+='B'
        num+=1
        if num%5==0:
            list1.append(temp1)
            list2.append(temp2)
            temp1=''
            temp2=''
    elif i.islower():
        temp1+='a'
        temp2+='A'
        num+=1
        if num%5==0:
            list1.append(temp1)
            list2.append(temp2)
            temp1=''
            temp2=''
#
for i in list1:
    for j,k in key1.items():
        if i==k:
            str1+=j
print "第一种:"
print str1+'\n'
for i in list2:
    for j,k in key2.items():
        if i==k:
            str2+=j
print "第二种:"
print str2

```

0x13 Easy RSA

题目描述

还记得veryeasy RSA吗？是不是不难？那继续来看看这题吧，这题也不难。

已知一段RSA加密的信息为：0xdc2eeeb2782c且已知加密所用的公钥：

($N=322831561921859$ $e = 23$)

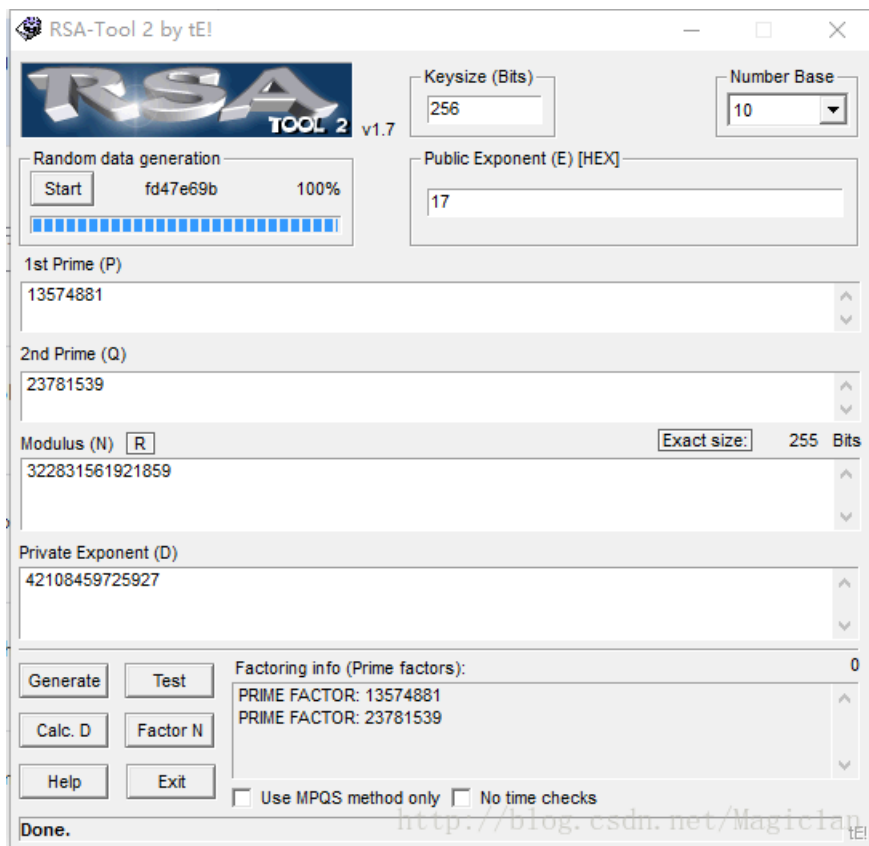
请解密出明文，提交时请将数字转化为ascii码提交

比如你解出的明文是0x6162，那么请提交字符串ab

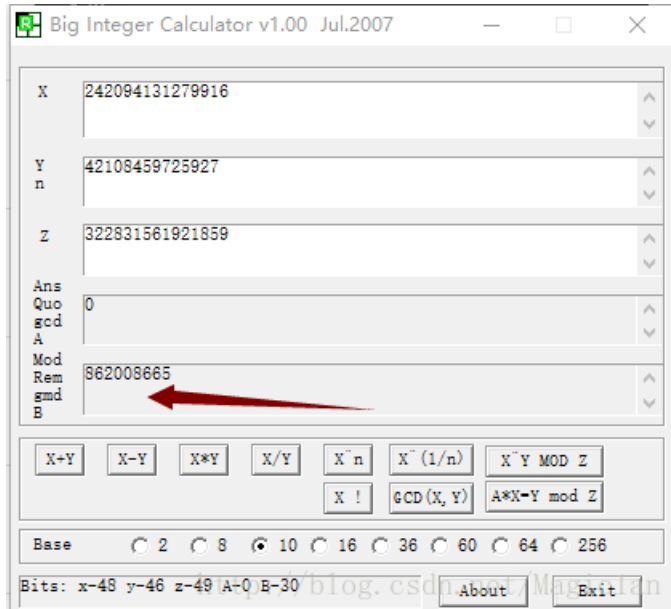
提交格式:PCTF{明文字符串}

解题过程

已知N、e可以计算出d，这里仍然可以用RSA Tool。



然后再利用 $\text{密文} = \text{明文}^d \bmod N$ 的公式计算出密文，最后将密文转化为ascii就好了。



最后得到flag为PCTF{3a5Y}

0x14 ROPGadget

题目描述

都说学好汇编是学习PWN的基础，以下有一段ROPGadget的汇编指令序列，请提交其十六进制机器码(大写，不要有空格)

```
XCHG EAX,ESP
```

```
RET
MOV ECX,[EAX]
MOV [EDX],ECX
POP EBX
RET
```

提交格式: PCTF{你的答案}

解题过程

一开始我试图用pwntools的asm函数去求flag,不过不幸的是失败了。然后又想到利用od去求,幸好这次成功了。

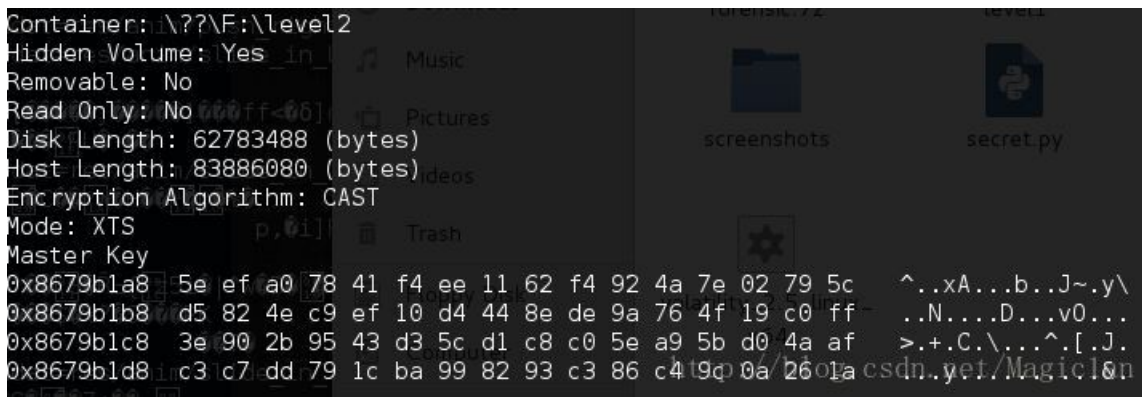
```
94 xchg eax,esp
C3 retn
8B88 mov ecx,dword ptr ds:[eax]
890A mov dword ptr ds:[edx],ecx
5B pop ebx
C3 retn
```

将十六进制拼接起来既是flag。

0x15 取证

题目描述

有一款取证神器如下图所示,可以从内存dump里分析出TureCrypt的密钥,你能找出这款软件的名字吗?名称请全部小写。



解题过程

以前没接触过只好百度了,不过得到好多结果,最后试出flag为PCTF{volatility}

0x16 熟悉的声音

题目描述

两种不同的元素,如果是声音的话,听起来是不是很熟悉呢,据说前不久神盾局某位特工领便当了大家都很惋惜哦

XYYY YXXX XYXX XXY XYY X XYY YX YXXX

请提交PCTF{你的答案}

解题过程

先将上面字符串转化为-组成的字符串

```
def getMorse(s):
    morse=''
    for i in range(len(s)):
        if s[i]=='X':
            morse+='.'
        elif s[i]=='Y':
            morse+='-'
        else:
            morse+=s[i]
    return morse
s='XYYY YXXX YXXX XXY XYY X XYY YX YXXX'
print getMorse(s)
```

得到-... .- -.- -.. -.-.- -.-

然后找一个摩斯密码解密的网站得到JBLUWEWNZ。本来以为到这就完了，结果提交上去并不对..需要凯撒解密才可以得到flag~

```
#http://rot13.de/index.php

s="JBLUWEWNZ"
for j in xrange(26):
    flag=''
    print str(j)+':',
    for i in s:
        if(i>='A' and i<='Z'):
            temp = ord(i) + j
            if temp>ord('Z'):
                temp = temp - 26
            flag +=chr(temp)

        elif i>='a' and i<='z':
            temp = ord(i) + j
            if temp>ord('z'):
                temp = temp -26
            flag +=chr(temp)

    else:
        flag +=i
    print flag
```

0x16 Baby's Crack

题目描述

既然是逆向题，我废话就不多说了，自己看着办吧。

解题过程

载入IDA找到关键代码

```
while ( feof(*(_QWORD *)&argc, argv, v8, v16) == 0 )
{
    v17 = fgetc(*(_QWORD *)&argc, argv, v9, v16);
    if ( v17 != -1 && v17 )
    {
        if ( v17 > 47 && v17 <= 96 )
        {
            v17 += 53;
        }
        else if ( v17 <= 46 )
        {
            v17 += v17 % 11;
        }
        else
        {
            v17 -= v17 % 61;
        }
        fputc(*(_QWORD *)&argc, argv, v15, (unsigned int)v17);
    }
}
```

<http://blog.csdn.net/Magiclan>

我这采用了爆破的方法解密文件.

最后将解密的十六进制转为字符即可得到flag.

```
file=open('flag.enc','r')
s=file.read()
flag=''
for i in range(len(s)):
    for j in range(128):
        if j>47 and j<=96:
            k=j+53
            if k==ord(s[i]):
                flag+=chr(j)
                break
        elif j<=46:
            k=j+j%11
            if k==ord(s[i]):
                flag+=chr(j)
                break
        else:
            k=j-j%61
            if k==ord(s[i]):
                flag+=chr(j)
                break
    print flag
file.close()
key=''
for i in range(0,len(flag),2):
    key+=chr(int(flag[i:i+2],16))
print key
```

0x17 Help!!

题目描述

出题人硬盘上找到一个神秘的压缩包，里面有个word文档，可是好像加密了呢~让我们一起分析一下吧！

解题过程

解题过程

啥也不说，直接摩斯密码解密得到flag.

0x21 德军的密码

题目描述

已知将一个flag以一种加密形式为使用密钥进行加密，使用密钥WELCOMETOCFF加密后密文为00010111000011000100000010100000001 请分析出flag。Flag为12位大写字母

解题过程

一种名为费纳姆密码的加密方式，解密脚本如下

```
# coding=utf-8
#--author:Magician--
miwen='000000000000000000000000000000000000000000000000000000000000000010111000011000100000010100000001'
passdict={'A':'100001','B':'100010','C':'100011','D':'1000100','E':'1000101','F':'1000110','G':
password='WELCOMETOCFF'
li=[]
for i in password:
    li.append(passdict[i])
flag=''
for i in range(0,len(miwen),7):
    test=miwen[i:i+7]
    test=int(test,2)
    test^=int(li[i/7],2)
    for i,j in passdict.items():
        if test==int(j,2):
            flag+=i
print '解密/加密结果为:%s'%flag
```

0x22 握手包

题目描述

给你握手包，flag是Flag_is_here这个AP的密码，自己看着办吧。

解题过程

以前没接触过，百度得知可以用linux自带的aircrack-ng进行暴力破解。

```
aircrack-ng -a2 -w password.txt wifi.cap
```