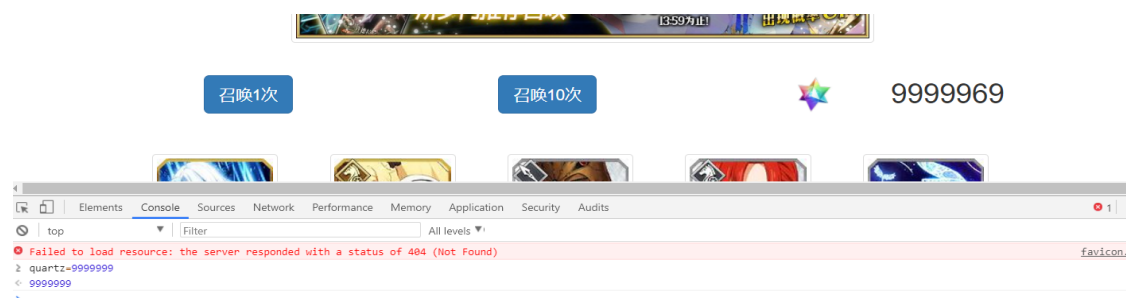


# ZclusLLoye \_Writeup\_week1

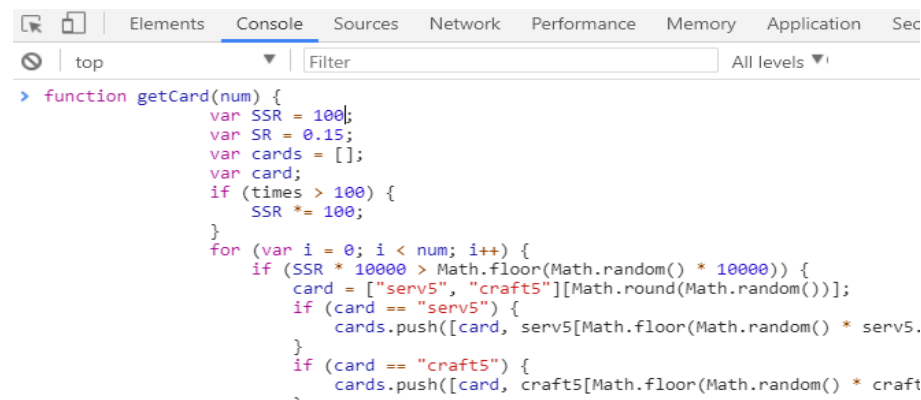
## WEB

### 1. Are you from Europe?

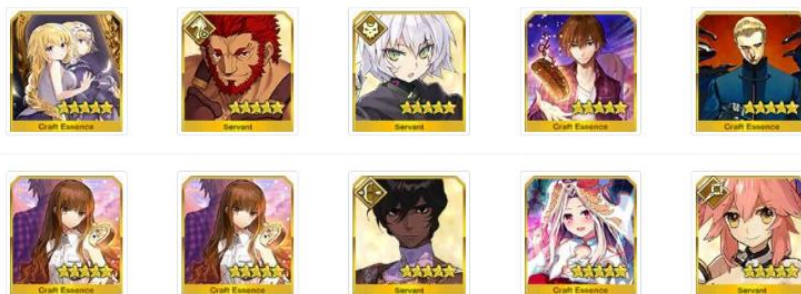
第一次做的时候以为只要不断抽卡就可以拿到 flag, so....通过查看源代码发现了 quartz 这个变量控制了。。圣晶石？然后用 chrome 的 console 把 quartz 改成 999999, 不断抽卡获得 flag。  
(抽了几十次出来的。。难道我是欧洲人吗。= =！)



后来第二次做的时候好像概率下调？（第一次没注意。。）想到能不能调一下，就把整个 function getcard() 拿到 console 里把 SSR 的概率给调了。。后来想想把网页放在本地直接改下概率好像更直接一点。。



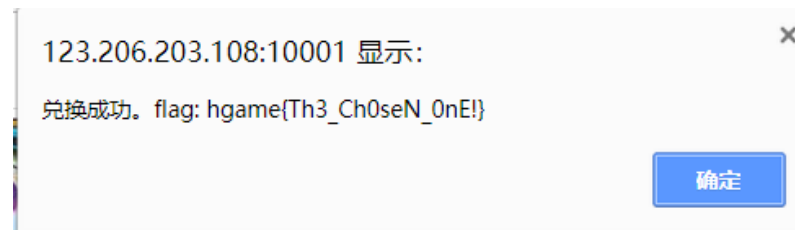
然后召唤一次窗口就弹出来了。（ps.全是 SSR 很舒服。。下次抽崩崩崩吧。。）



还想到一种方法就是在 console 里输入

```
> quartz=9999999999;
var i=0;
while(i<5000){
  getTen();
  i++;
}
```

来实现自动抽卡 50000 次（比用按键精灵脚本快多了。。。），基本上都会抽到吧。。。获得 flag。



hgame{Th3\_Ch0seN\_0Ne!}

## 2.Special number

```
include_once("flag.php");
if(isset($_GET['key'])){
    $pattern = '/^(?=[0-9].*)(?=[a-zA-Z].*).{7,}$/';
    $key = $_GET['key'];
    if(preg_match($pattern, $key)==0){
        echo "格式错误";
    }else{
        $lock="*****";
        $b = json_decode($key);
        if($b==$lock){
            echo $flag;
        }else{
            echo "this is no special number";
        }
    }
}
```

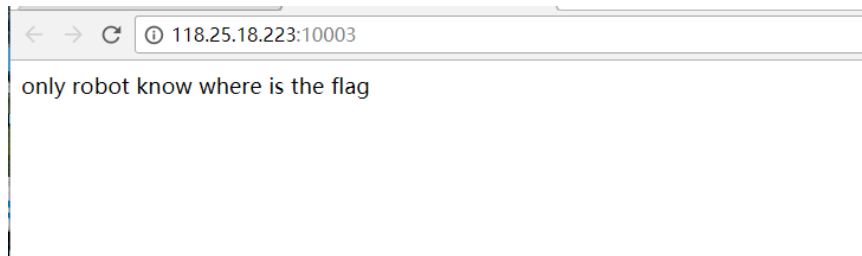
审阅代码可知，要 get 一个 key 值，其中这个 key 值满足数字加字母必须是 7 位以上。查阅 PHP 手册可知，0 == “string”，且 0e 开头的字符串都认为是科学记数法，所以只需是 key 的值为 0 即可，而 key 值又必须含有字母，所以构造 0e 开头的 key 值。Get 一下，获得 flag。



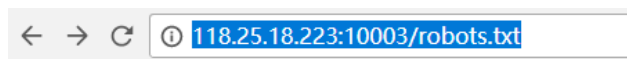
hgame{pHp\_w34k\_typing\_s000\_e4sy}

hgame{pHp\_w34k\_typing\_s000\_e4sy}

### 3.Can u find me?

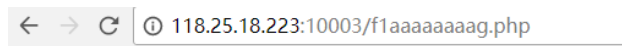


刚开始拿到题目想到了 robot 文件，输入/robot 和 robot.txt 都不对。。。网上一查才知道原来是 robots.txt。。。然后。。。



User-agent: \*  
Disallow: /f1aaaaaaaaag.php

接着进入 f1aaaaaaaaag.php。

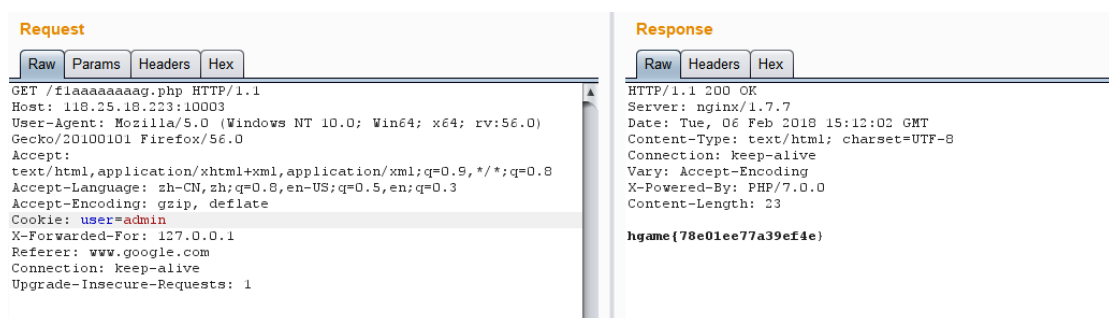


only admin can get flag

查看了一下 header 信息

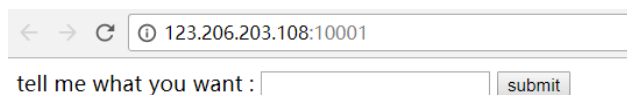
▼ Request Headers view source  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Cache-Control: max-age=0  
Connection: keep-alive  
Cookie: user=guest  
Host: 118.25.18.223:10003  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36

发现 cookie 为 user = guest。。。用火狐插件或者 BurpSuite 改一下 cookie 为 user=admin 获得 flag。

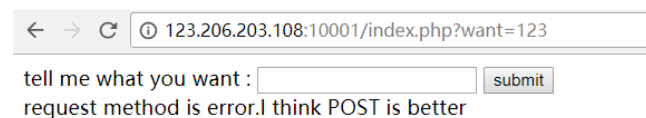


hgame{78e01ee77a39ef4e}

### 4.Tell me what you want



在输入框输入发现需要使用 post 方法提交 want 的值。



改用 post 方法提交后逐步出现了几句话。

only localhost can get flag

please use Icefox/57.0

the requests should referer from www.google.com

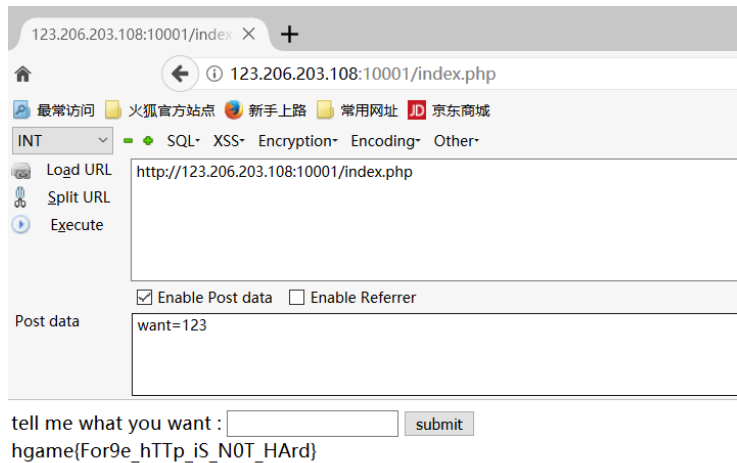
you are not admin

需要分别修改 X-Forwarded-For 为 127.0.0.1, User-agent 为 Mozilla/5.0 (Windows NT 6.1; rv,2.0.1) Gecko/20100101 Icefox/57.0, Referer 为 [www.google.com](http://www.google.com), 还有 cookie 为 isadmin=1。使用火狐插件修改并提交（刚开始直接把 user-agent 改成 icefox 发现不行，后来把 firefox 的 ua 中的 fire 改成 ice 就好了。。。。）。或者写个简单的脚本跑一下。。获得 flag 一枚。

```
1 import requests
2 import re
3 url = 'http://123.206.203.108:10001/'
4 data = {
5     'want': '123'
6 }
7 headers = {
8     'X-Forwarded-For': '127.0.0.1',
9     'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; rv,2.0.1) Gecko/20100101 Icefox/57.0',
10    'Referer': 'www.google.com',
11    'Cookie': 'isadmin=1'
12 }
13 html = requests.post(url, data=data, headers=headers)
14 flag = re.findall('hgame{(.*)}', html.text)[0]
15 print(flag)
16
17
18
```

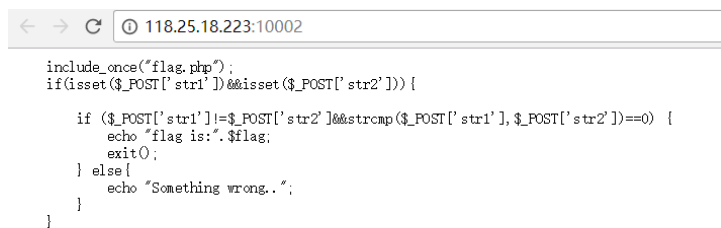
问题 输出 调试控制台 终端

For9e\_hTTP\_iS\_N0T\_HARd

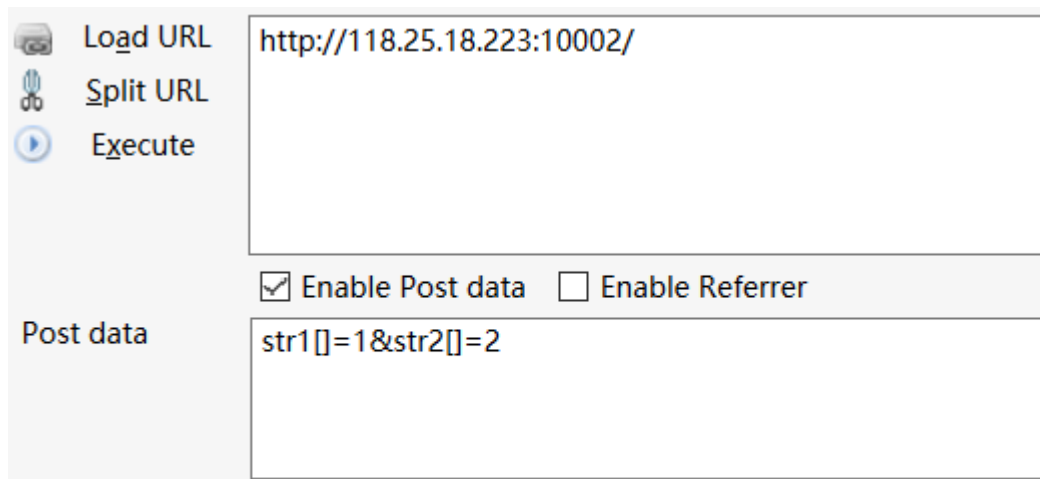


hgame{For9e\_hTTP\_iS\_N0T\_HArD}

## 5.我们不一样



和第二题类似，都是 PHP 弱类型。题意为需要 post 两个值 str1 和 str2，str1 不等于 str2，但是 strcmp(str1,str2)需要为真，查阅资料知，当 strcmp 函数的参数为数组类型时，函数返回真。Post 提交获得 flag。



flag is:hgame{g3t\_f14g\_is\_so0000\_ez}

hgame{g3t\_f14g\_is\_so0000\_ez}

# RE

## 1. re0

用 OD 打开先搜索一下字符串，果然发现 flag 一个。

01291096	-	A1 00302901	mov eax,dword ptr ds:[0x1293000]	
01291098	-	33C5	xor eax,ebp	
0129109D	-	8945 FC	mov [local.1],eax	
012910A0	-	68 24212901	push re0.01292124	Welcome to hgame\n
012910A5	-	E8 76FFFFFF	call re0.01291020	
012910AA	-	68 38212901	push re0.01292138	\nInput your flag:
012910AF	-	E8 6CFFFFFF	call re0.01291020	
012910B4	-	6A 20	push 0x20	
012910B6	-	8D45 DC	lea eax,[local.9]	
012910B9	-	50	push eax	
012910BA	-	68 4C212901	push re0.0129214C	%s
012910BF	-	E8 8CFFFFFF	call re0.01291050	
012910C4	-	83C4 14	add esp,0x14	
012910C7	-	8D45 DC	lea eax,[local.9]	
012910CA	-	B9 08212901	mov ecx,re0.01292108	hctf{F1r5t_St5p_Ls_Ea5y}
012910CF	-	90	nop	
012910D0	>	8A11	mov dl,byte ptr ds:[ecx]	
012910D2	-	3A10	cmp dl,byte ptr ds:[eax]	
012910D4	~	75 1A	jnz short re0.012910F0	
012910D6	-	84D2	test dl,dl	
012910D8	~	74 12	jg short re0.012910EC	
012910DA	-	8B51 01	mov dl,byte ptr ds:[ecx+0x11]	

hctf{F1r5t\_St5p\_Ls\_Ea5y}

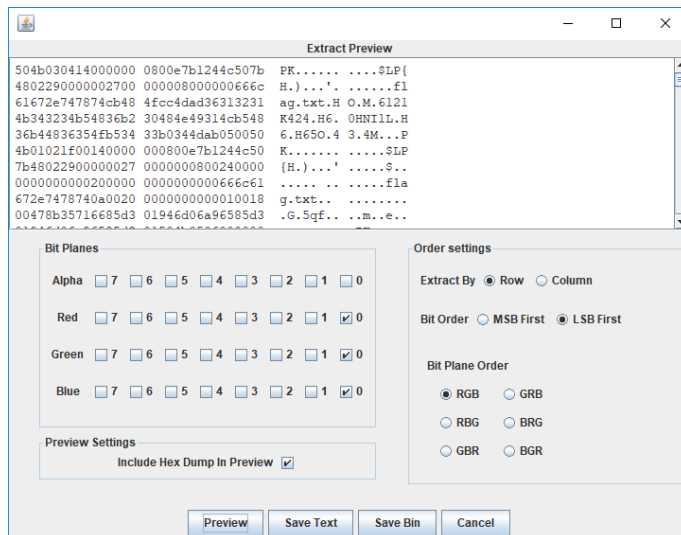
# MISC

## 1. 白菜 1

习惯先用 binwalk 跑一下，没发现什么。

root@kali:~# binwalk flag.png		
视频	图片	文档
下载	音乐	桌面
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 1080 x 1920, 8-bit/color RGB, non-interlaced
41	0x29	Zlib compressed data, default compression

用 winhex 打开也没发现什么异常。。感觉应该是 LSB 最低位隐写。用神器 StegSolve 看下 0 通道下的数据。



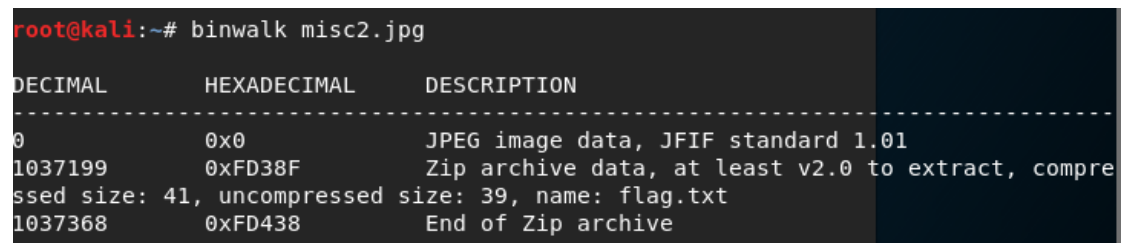
发现 PK 开头的压缩包，保存为 flag.zip。打开发现了一个 flag.txt，打开，获得 flag.



hgame{4246a2158c280cdd1e8c18c57e96095f}

## 2. 白菜 2

还是先用 binwalk 看看。



里面有个压缩包，用 foremost 或者 binwalk -e 分离一下。。

```

root@kali:~# foremost misc2.jpg
Processing: misc2.jpg
|foundat=flag.txt0H00M0NL3JL000L402L5NIM322313100NM50JI0
*|
root@kali:~# binwalk -e misc2.jpg

```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
1037199	0xFD38F	Zip archive data, at least v2.0 to extract, compressed size: 41, uncompressed size: 39, name: flag.txt
1037368	0xFD438	End of Zip archive

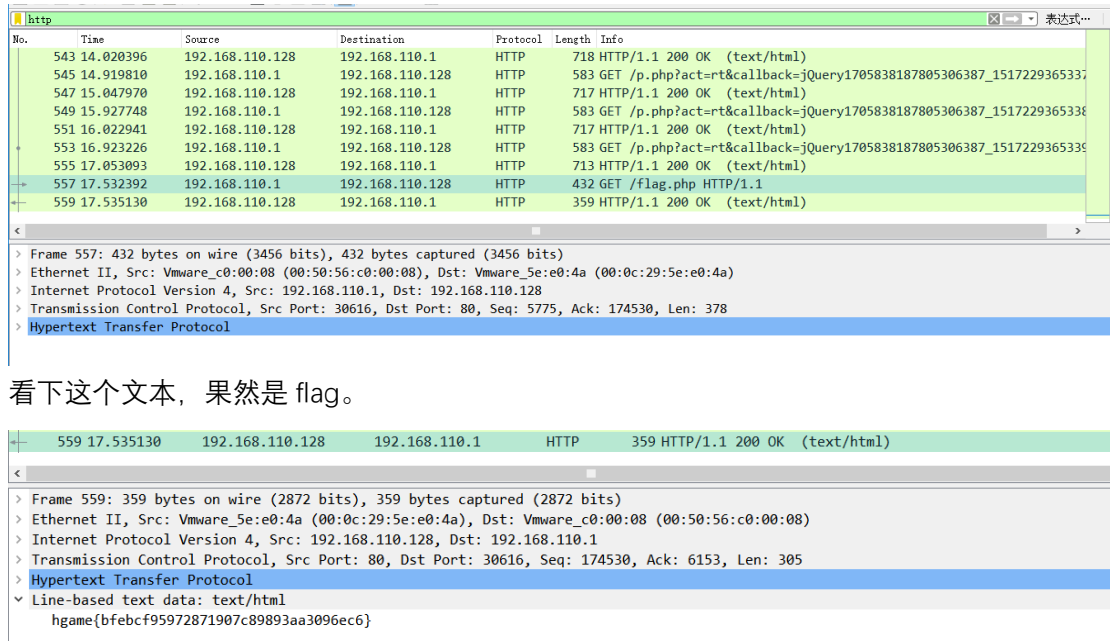
打开压缩包，依旧是 flag.txt。获得 flag。(ps.我比较喜欢直接把图片的后缀改成 zip。。。)



hgame{af2ab981a021e3def22646407cee7bdc}

### 3. pacp1

用 wireshark 打开文件，过滤一下 tcp，发现 GET 了 /flag.php，并且服务器返回了一个文本。



看下这个文本，果然是 flag。

hgame{bfebcf95972871907c89893aa3096ec6}



# Crypto

## 1. easy Caesar

描述

相信你们都知道啥是凯撒加密的，so Ciphertext: vuoa{Hvs\_ei8qy\_pf7kb\_1l\_xladg\_cjSf\_o\_Zo9m\_rCu}

话不多说，先把这个字符串凯撒解密一下。

ROT12                      hgame{The\_qu8ck\_br7wn\_1x\_jUmps\_ovEr\_a\_La9y\_dOg}

提交发现 flag 错误。。想想是不是数字也经过凯撒加密了。。因为 key 是 12，就把每个数字通过 0123456789 的顺序凯撒解密了一下，拿到 flag。（ps.通过句意也可以把数字改正确。）

hgame{The\_qu1ck\_br0wn\_4x\_jUmps\_ovEr\_a\_La2y\_dOg}

## 2. Polybius

描述

其实这个和凯撒差不多 Ciphertext: hgame{FDXGDADDG\_FXXFAAXFAG\_GDFXFFXFXADXFDA\_GDAD}

Wiki 上看了一下，似乎是通过一个方阵来进行加密，网上找到了原始的方阵。

	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	j	c	u	x
X	m	r	e	w	y

注意 i 和 j 是在同一个格子，得根据句意来判断是 i 还是 j。每两位对应拿到 flag。

hgame{fritz\_nebel\_invented\_it}

### 3. Hill

描述

Not hard key: 9 17 6 5 Ciphertext: phnfetzhzzwz 解出来之后手动加上hgame{

希尔密码，通过线性代数的方法来加密。本想用 matlab 解一下，无意间发现有个在线解密网站，填入数据，得到 flag。

Plaintext

overthehillx

key = 9 17 6 5

v Encrypt v

 $\wedge$  Decrypt  $\wedge$ 

Ciphertext

phnfetzhzzwz

# hgame{overthehillx}

#### 4. confusion

描述

[illegible]

一串摩斯电码，先解密一下。得到一串大写英文字符串。

MRLTK6KXNVZXQWBSNA2FSU2GGBSW45BSLAZFU6SVJBNDASRHU6Q

想到 base32 只有大写英文和数字 234567，所以用 base32 解码一下。后面加上 4 个等号，python 解码得到

dW5yWmsxX2h4YSF0ent2X2ZzUHZ0fQ==

然后就是熟悉的 base64 解码，接着解码，得到：

unrZk1\_hxa!tz{v\_fsPvt}

看到括号在后面，想到应该是栅栏加密，而且因为 flag 的格式为 hgame 开头，所以应该也经过了凯撒加密。先凯撒解密一下，且第一位应该是 h，所以得到

haeMx1\_ukn!gm{i\_sfCig}

再来进行栅栏解密，分两栏，得到 flag

# hgame{Mix\_1s\_fuCking!}