

Web:

1.Are you from Europe?

这道题目是我最先解出来的题目 F12 发现源代码然后发现

```
function getCard(num) {  
    var SSR = 0.0000001;  
    var SR = 0.15;
```

这怕不是假的吧。

我就复制黏贴到我的 pycharm 改成 100 在本地浏览器打开，就弹出来了=。=奇奇怪怪的方法

2.Special number

这道题是 PHP 的弱类型，看到了正则表达式学习了正则表达式，一开始我还以为是绕过正则表达式，然后上网查了什么 MD5 加密绕过发现差不多，0e00000000 也符合正则表达式要求了，就试一试然后就拿到了 flag，主要的就是转为数组的时候别的字符串都会变为 NULL 然后就不匹配，而 0e000000 会变成 0，那个字符串也会变成 0 然后就匹配



```
hgame{pHp_w34k_typing_s000_e4sy}
```

```
include_once("flag.php");  
if(isset($_GET['key'])){
```

3.Can you find me?

这道题的提示是 robot 然后我就想起来有个协议就是主目录下有个 robot.txt 来决定爬虫是怎么爬，然后进入 robot.txt，里面有提示

Disallow: /flaaaaaaaaag.php

进入之后改一下 admin 为 1 就好了

4.Tell me what you want

先提交会发现他要求是 post，然后 F12 改一下提交为 post，之后就是要本地，上网查了一下，就是请求头里面有一个 X-Forwarded-For 这个是伪造 IP 请求，发现这道题就是改请求头的，之后就是 user-agent 改为 IceFox 56.0，按照要求改下去就可以拿到 flag 了我使用 bp 的不难

5.我们不一样

这个又是 php 的弱口令上网查了一下空数组可以绕过，写了一个 python 的 post 请求就拿到了

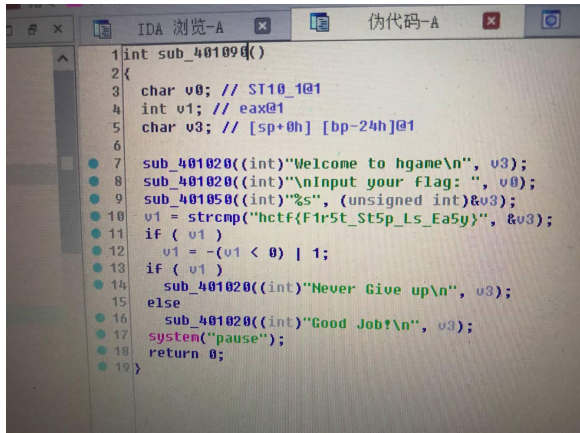
```
import requests  
  
url='http://118.25.18.223:10002/'  
data={'str1':'0',  
      'str2[]':''}  
req=requests.post(url,data=data)  
print(req.text)
```

"C:\Program Files\Python36\python.exe" C:/Users/ass
flag is:hgame(g3t_f14g_is_so0000_ez)

Re

太垃圾=。=re 只解了两道题

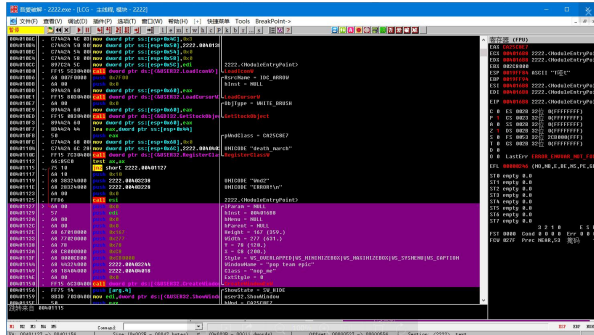
1.Re0



里面有一个 strcmp 函数自带答案=。

2. Nop_pop

提示是用 WinRAR 去广告窗没有用过。。我是一步一步用 o1lydbg 调出来然后把关键的语句去了好



就是标注的那一段

Misc

1.白菜2

想吐槽白菜1 是假的 LSB 吧，我用 stegsolve 看的眼睛都瞎了都没找出来，图片下载下载用 binwalk 知道了里面还有 rar 文件，然后打开里面就有 flag.txt

2.Pacp1

用 wireshark 打开之后。。里面就有找一找，随便打开，刚好是。。

557	17.532392	192.168.110.1	192.168.110.128	HTTP	432 GET /flag.php HTTP/1.1
558	17.532672	192.168.110.128	192.168.110.1	TCP	60 80 → 30616 [ACK] Seq=174530 Ack=6153 Win=51584 Len=0
559	17.535130	192.168.110.128	192.168.110.1	HTTP	359 HTTP/1.1 200 OK (text/html)
560	17.576299	192.168.110.1	192.168.110.128	TCP	54 30616 → 80 [ACK] Seq=6153 Ack=174835 Win=64512 Len=0
561	18.732523	192.168.110.1	192.168.110.128	TCP	55 [TCP Keep-Alive] 30617 → 80 [ACK] Seq=1003 Ack=78337 Win=65536 Len=0
562	18.733129	192.168.110.128	192.168.110.1	TCP	66 [TCP Keep-Alive ACK] 80 → 30617 [ACK] Seq=78337 Ack=1004 Win=31232 Len=0
563	18.764502	192.168.110.1	192.168.110.128	TCP	55 [TCP Keep-Alive] 30620 → 80 [ACK] Seq=668 Ack=048 Win=64512 Len=0
[Calculated window size: 51584]					
[Window size scaling factor: 128]					
Checksum: 0x7a00 [unverified]					
[Checksum Status: Unverified]					
Urgent pointer: 0					
▷ [SEQ/ACK analysis]					
TCP payload (305 bytes)					
▷ Hypertext Transfer Protocol					
◀ Line-based text data: text/html					
hgame{bfebcf95972871907c89893aa3096ec6}					
0000	01101000	01100111	01100001	01101101	01100101
0008	01100101	01100010	01100011	01100110	00111001
0016	00110010	00111000	00110111	00110001	00111001
0024	00111000	00111001	00111000	00111001	00110011
0032	00110000	00111001	00110110	01100011	01111101

Crypto

1.Easy Caesar

用在线解密解了一下密结果发现不对 hgame{The_qu8ck_br7wn_lx_jUmps_ovEr_a_La9y_dOg}
 然后说要看语义，看了一下原文是 the quick brown fox jumps over a lazy dog
 改了一下数字。。。真鸡儿坑 hgame{The_qu1ck_br0wn_4x_jUmps_ovEr_a_La2y_dOg}

2.Polybius

轮盘加密
 学习了一下，那个j的地方是 ij 都可以的，答案是 i，我都试了一下=。=，反正就出来了

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

hgame{fritz_nebel_invented_it}