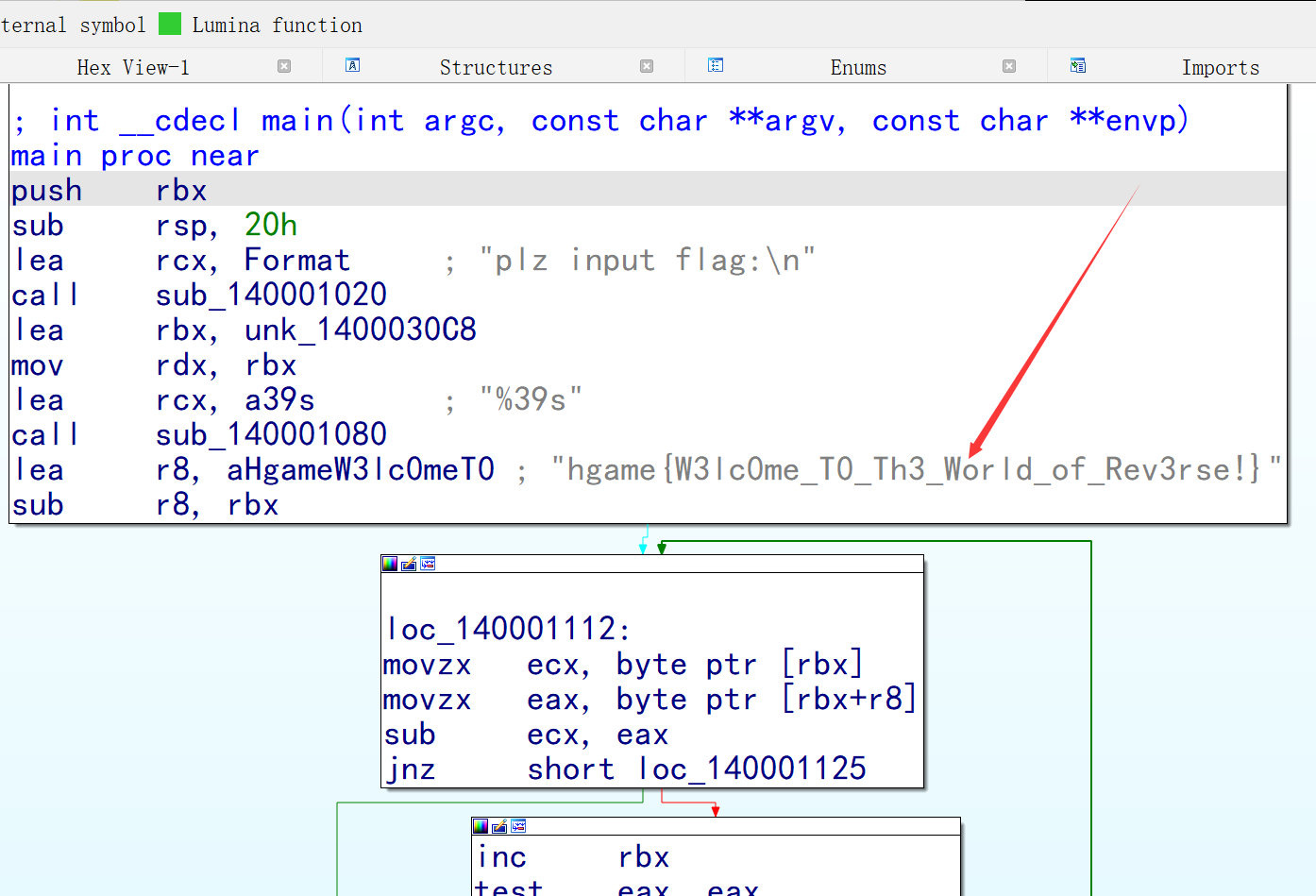
**HGAME比赛第一周WP**

**题目一：ezIDA**

**解题过程：先查壳，64位，无壳，拖入ida中**

****

**Flag：如图所示**

**题目二：ezASM**

**解题过程：打开txt文件，是一堆汇编代码，分析一下只需要将数据与0x22进行异或即可得到flag，关键代码如下：**

**section .data**

**c db 74, 69, 67, 79, 71, 89, 99, 113, 111, 125, 107, 81, 125, 107, 79, 82, 18, 80, 86, 22, 76, 86, 125, 22, 125, 112, 71, 84, 17, 80, 81, 17, 95, 34**

**flag db 33 dup(0)**

**format db "plz input your flag: ", 0**

**success db "Congratulations!", 0**

**failure db "Sry, plz try again", 0**

**; Check flag**

**xor esi, esi**

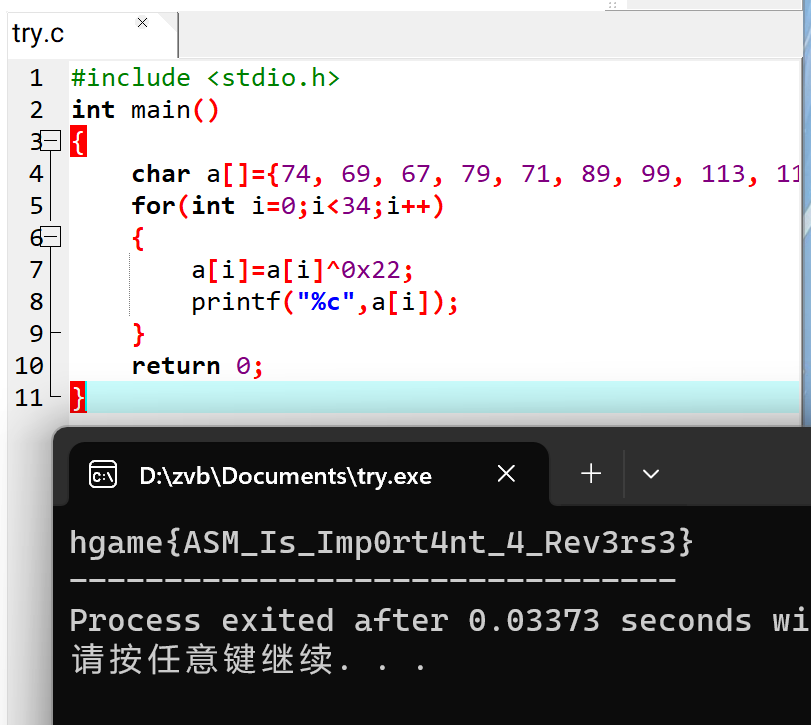
**check\_flag:**

**mov al, byte [flag + esi]**

**xor al, 0x22**

**cmp al, byte [c + esi]**

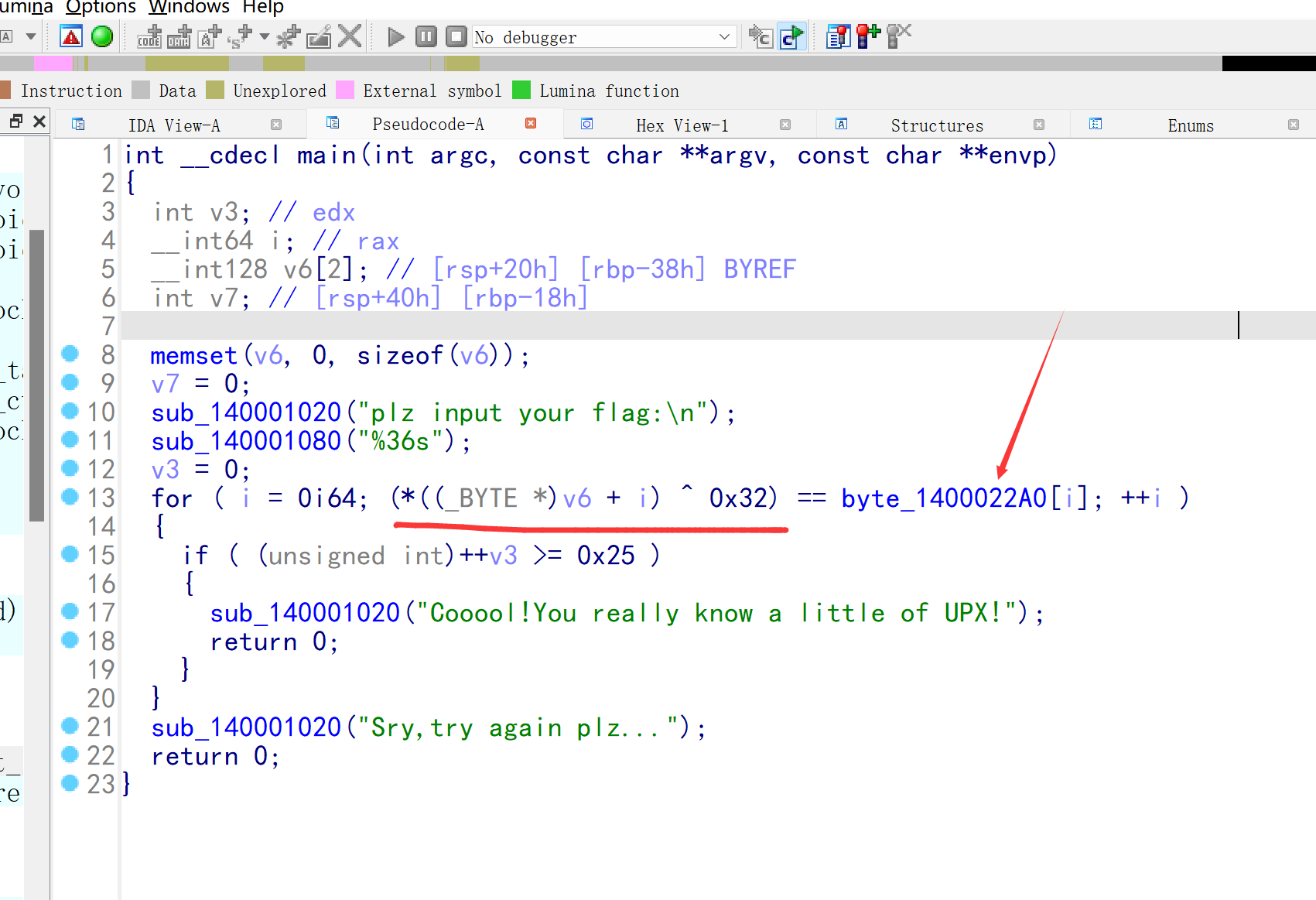
**jne failure\_check**

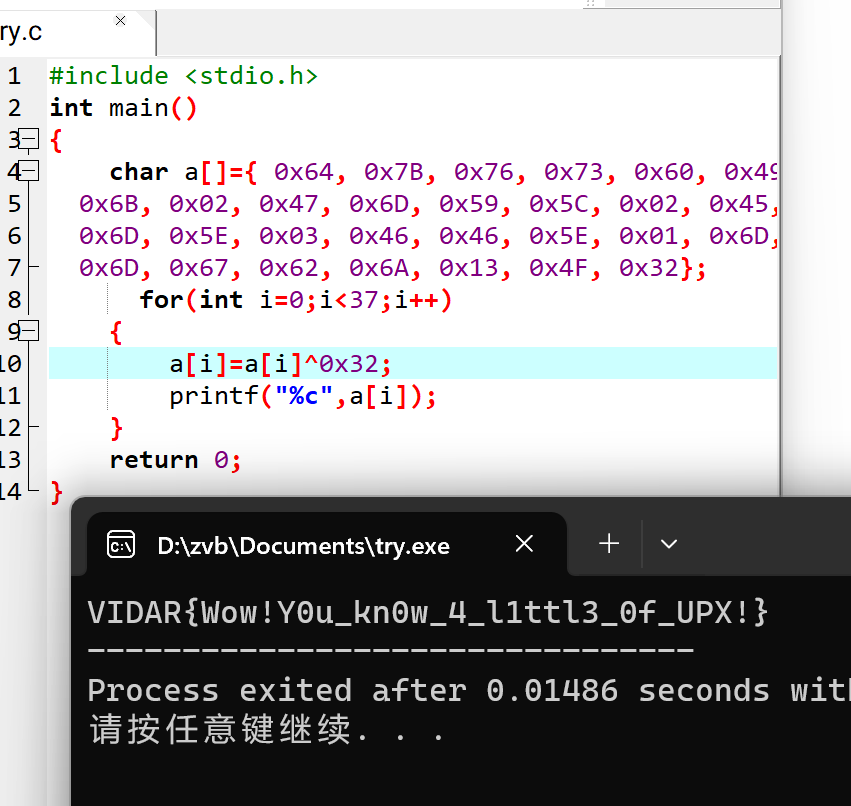
****

**Flag：hgame{ASM\_Is\_Imp0rt4nt\_4\_Rev3rs3}**

**题目三：ezUPX**

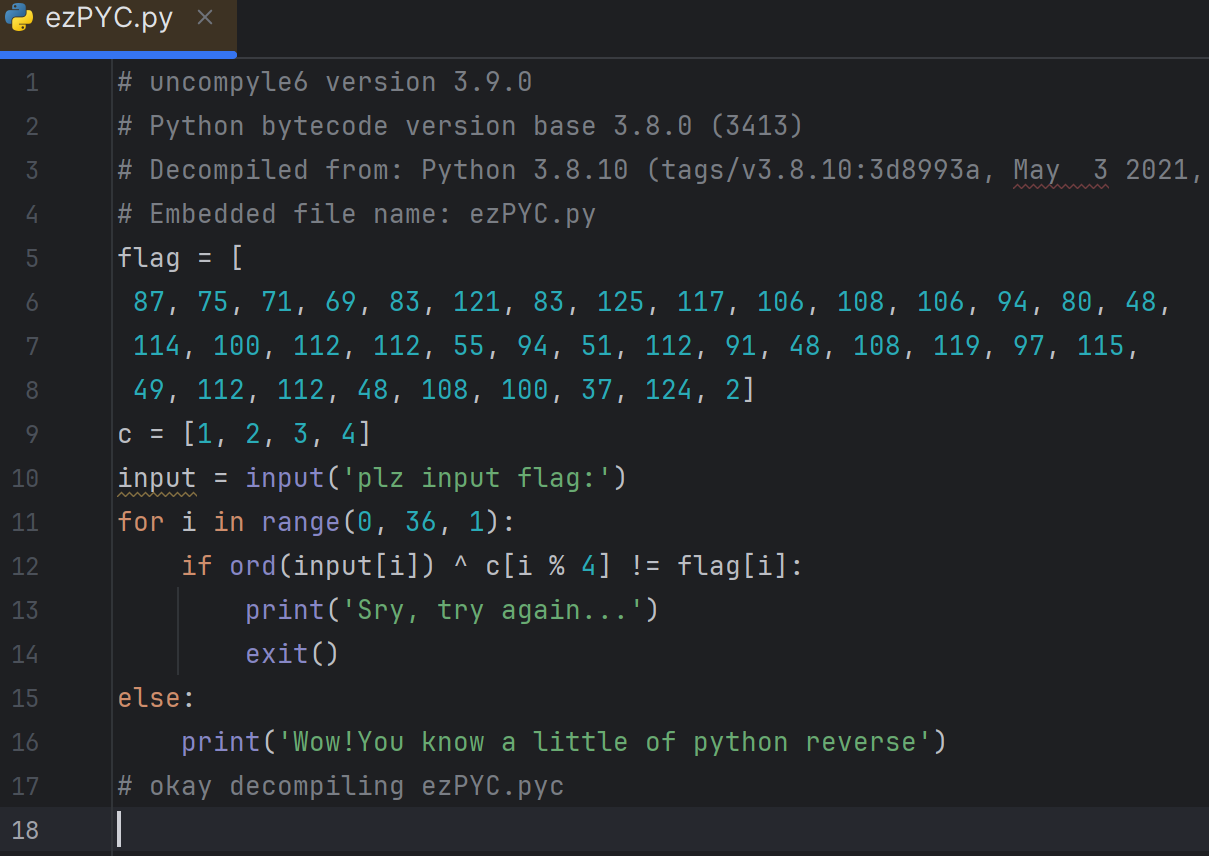
**解题过程：先查壳，使用upx4.2.1,将文件放置同一目录下，使用命令行upx -d ezUPX.exe,脱壳后ida分析，定位关键代码，将数据提取出来与0x32异或**

****

****

**题目四：ezPYC**

**解题过程：先将exe文件反编译为py文件得到源码，再进行分析写出脚本**

****

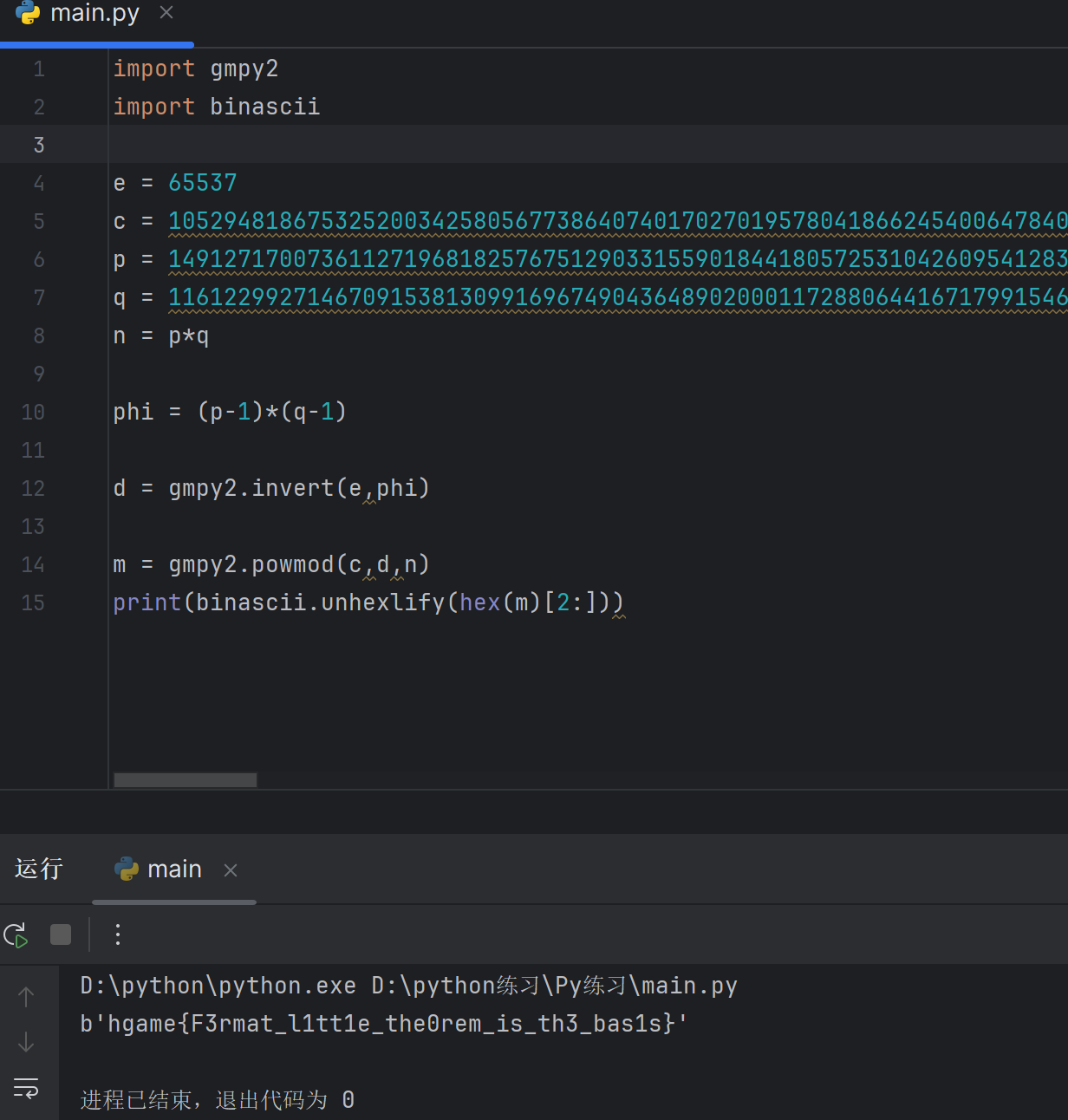
**脚本如下：**a = [87, 75, 71, 69, 83, 121, 83, 125, 117, 106, 108, 106, 94, 80, 48,  
 114, 100, 112, 112, 55, 94, 51, 112, 91, 48, 108, 119, 97, 115,  
 49, 112, 112, 48, 108, 100, 37, 124, 2]  
c = [1, 2, 3, 4]  
flag=""  
for i in range(0, 36, 1):  
 flag+=chr(a[i]^ c[i % 4])  
print(flag)

**Flag：VIDAR{Python\_R3vers3\_1s\_1nter3st1ng!}**

**Crypto**

**题目五：ezRSA**

**解题过程：题目看着复杂，关键在于leak1和leak2，由费马小定理得leak1=p，leak2=q，接下来随便找个脚本就好了**

****

**Flag：hgame{F3rmat\_l1tt1e\_the0rem\_is\_th3\_bas1s}**

**Misc**

**题目：Signin**

**解题过程：打开是一张图片，按照提示从下面看，可以直接看到flag**

**Flag：hgame{WOW\_GREAT\_YOU\_SEE\_IT\_WONDERFUL}**

**题目：签到**

**解题过程：关注公众号即可**