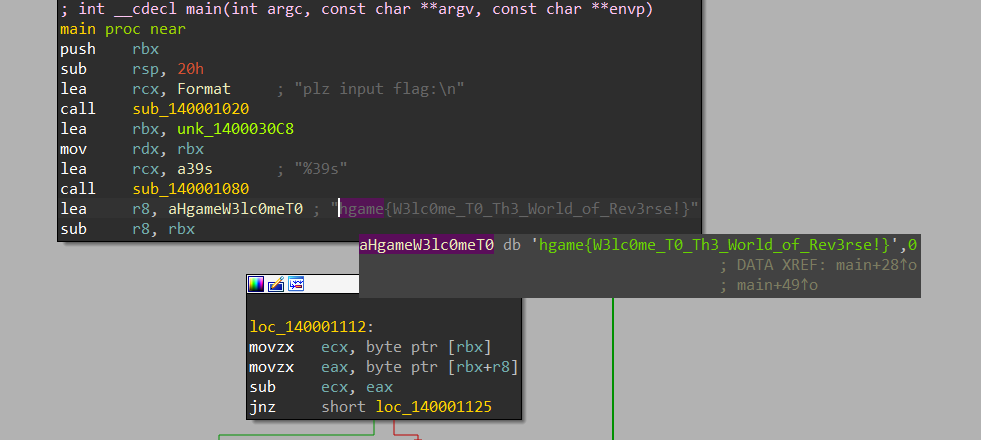
# HGAME 2024

# REVERSE

## [WEEK 1]ezIDA



## [WEEK 1]ezASM

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  
  
section .text  
 global \_start  
  
\_start:  
 ; Print prompt  
 mov eax, 4  
 mov ebx, 1  
 mov ecx, format  
 mov edx, 20  
 int 0x80  
  
 ; Read user input  
 mov eax, 3  
 mov ebx, 0  
 mov ecx, flag  
 mov edx, 33  
 int 0x80  
  
 ; Check flag  
 xor esi, esi  
check\_flag:  
 mov al, byte [flag + esi]  
 xor al, 0x22  
 cmp al, byte [c + esi]  
 jne failure\_check  
  
 inc esi  
 cmp esi, 33  
 jne check\_flag  
  
 ; Print success message  
 mov eax, 4  
 mov ebx, 1  
 mov ecx, success  
 mov edx, 14  
 int 0x80  
  
 ; Exit  
 mov eax, 1  
 xor ebx, ebx  
 int 0x80  
  
failure\_check:  
 ; Print failure message  
 mov eax, 4  
 mov ebx, 1  
 mov ecx, failure  
 mov edx, 18  
 int 0x80  
  
 ; Exit  
 mov eax, 1  
 xor ebx, ebx  
 int 0x80

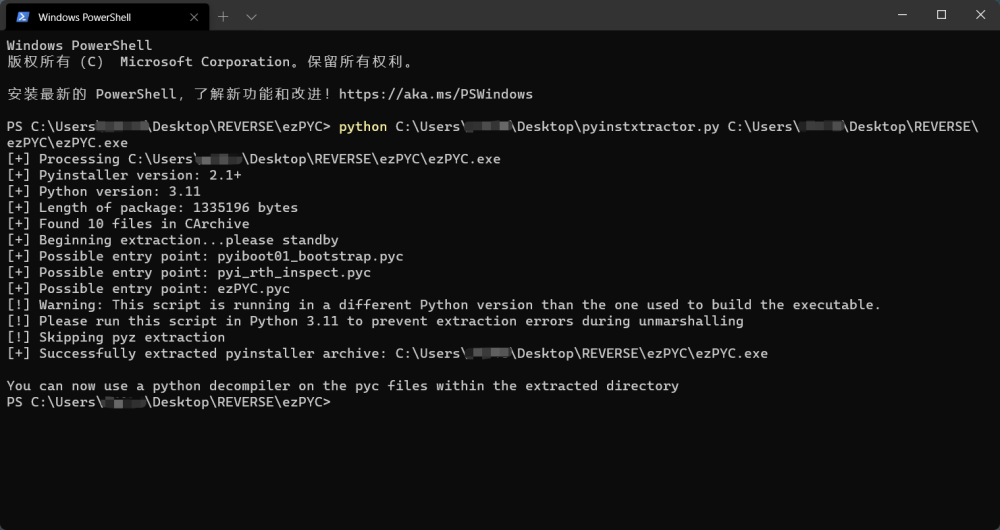
chatgpt一下

#include <stdio.h>  
#include <string.h>  
  
char c[] = { 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 };  
char flag[33] = { 0 };  
char format[] = "plz input your flag: ";  
char success[] = "Congratulations!";  
char failure[] = "Sry, plz try again";  
  
int main() {  
 // Print prompt  
 printf("%s", format);  
  
 // Read user input  
 fgets(flag, sizeof(flag), stdin);  
 flag[strcspn(flag, "\n")] = '\0'; // Remove trailing newline  
  
 // Check flag  
 int i = 0;  
 for (i = 0; i < 33; i++) {  
 char al = flag[i] ^ 0x22;  
 if (al != c[i]) {  
 printf("%s\n", failure);  
 return 0;  
 }  
 }  
  
 // Print success message  
 printf("%s\n", success);  
  
 return 0;  
}

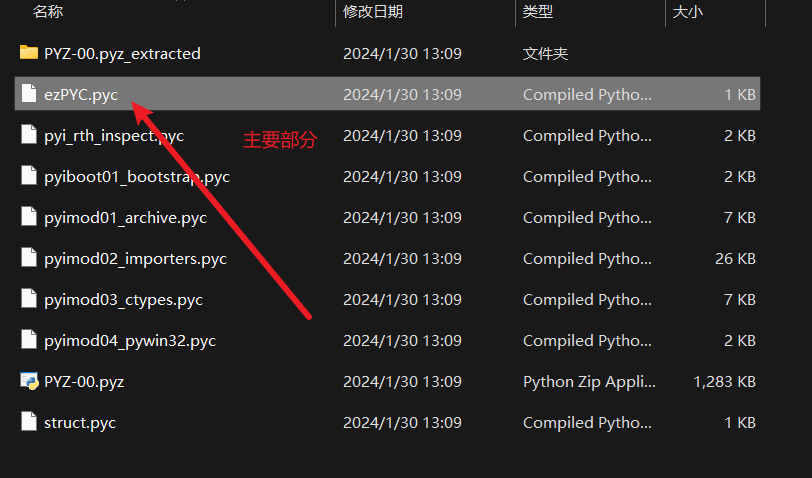
EXP

enc = [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]  
for i in range(len(enc)):  
 print(chr(enc[i] ^ 0x22), end='')  
#hgame{ASM\_Is\_Imp0rt4nt\_4\_Rev3rs3}

## [WEEK 1]ezPYC







利用[python反编译在线工具](https://tool.lu/pyc/)

#!/usr/bin/env python  
# visit https://tool.lu/pyc/ for more information  
# Version: Python 3.11  
  
flag = [  
 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]  
input = input('plz input flag:')  
# WARNING: Decompyle incomplete

还是有部分未反编译出来

但是还是可是猜测加密方式为异或（经验）

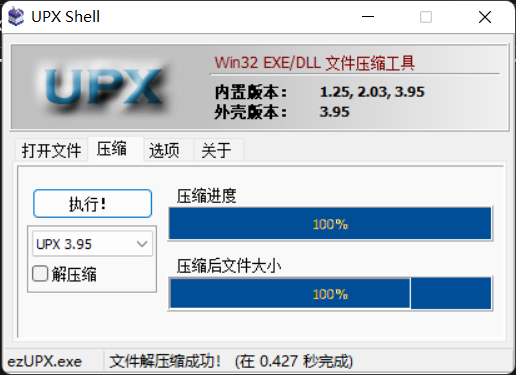
很幸运我猜对了

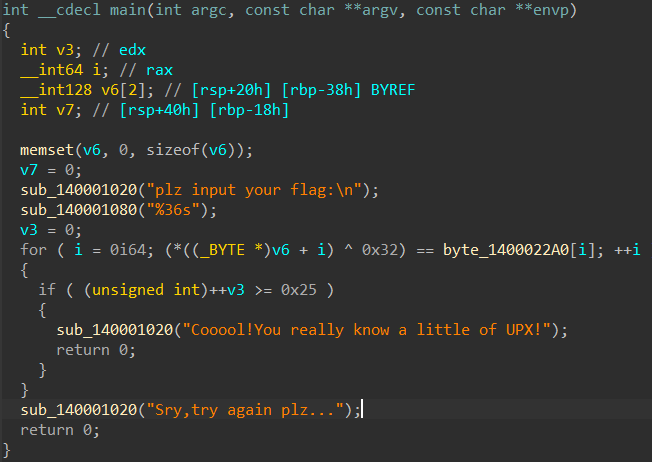
EXP

flag = [  
 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]  
for i in range(len(flag)):  
 print(chr(flag[i] ^ c[i % len(c)]), end='')  
#VIDAR{Python\_R3vers3\_1s\_1nter3st1ng!}

## [WEEK 1]ezUPX

脱壳





EXP

flag = [0x64, 0x7B, 0x76, 0x73, 0x60, 0x49, 0x65, 0x5D, 0x45, 0x13,  
 0x6B, 0x02, 0x47, 0x6D, 0x59, 0x5C, 0x02, 0x45, 0x6D, 0x06,  
 0x6D, 0x5E, 0x03, 0x46, 0x46, 0x5E, 0x01, 0x6D, 0x02, 0x54,  
 0x6D, 0x67, 0x62, 0x6A, 0x13, 0x4F, 0x32]  
for i in range(len(flag)):  
 print(chr(flag[i] ^ 0x32), end='')  
#VIDAR{Wow!Y0u\_kn0w\_4\_l1ttl3\_0f\_UPX!}