REVERSE

ezPYC

pyinstxtractor 解包

讲它的pyc文件进行反汇编

```
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:')
```

```
for i in range(0, 36, 1):
    if ord(input[i]) ^ c[i % 4] != flag[i]:
        print('Sry, try again...')
        exit()
        continue
        print('Wow!You know a little of python reverse')
        return None
```

```
#解题

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(0, 36, 1):
    print(chr(c[i % 4]^ flag[i]),end="")
```

得到flag　VIDAR{Python_R3vers3_1s_1nter3st1ng!}

ezASM

```
flag=[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(flag)):
    print(chr(0x22^ flag[i]),end="")
    #hgame{ASM_Is_Imp0rt4nt_4_Rev3rs3}
```

ezIDA

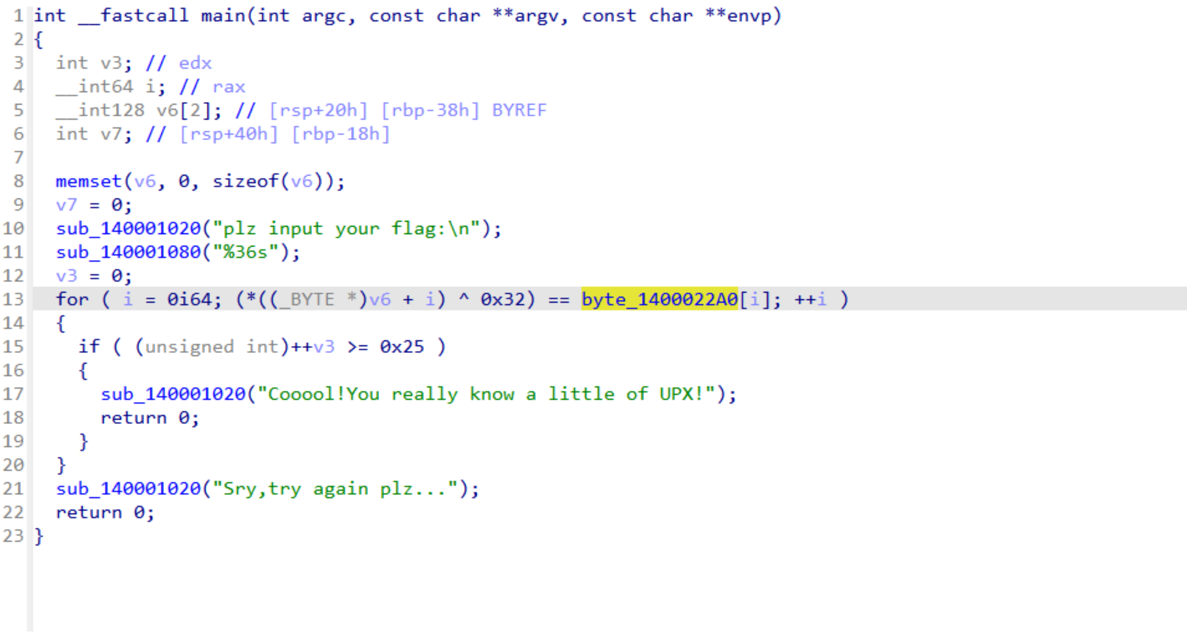
先查壳，64位

进去就有

hgame{W3lc0me_T0_Th3_World_of_Rev3rse!}

ezUPX

upx -d 脱壳



```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  int v3; // edx
  __int64 i; // rax
  __int128 v6[2]; // [rsp+20h] [rbp-38h] BYREF
  int v7; // [rsp+40h] [rbp-18h]

  memset(v6, 0, sizeof(v6));
  v7 = 0;
  sub_140001020("plz input your flag:\n");
  sub_140001080("%36s");
  v3 = 0;
  for ( i = 0i64; (*((_BYTE *)v6 + i) ^ 0x32) == byte_1400022A0[i]; ++i )
  {
    if ( (unsigned int)++v3 >= 0x25 )
    {
      sub_140001020("Cooool!You really know a little of UPX!");
      return 0;
    }
  }
  sub_140001020("Sry,try again plz...");
  return 0;
}
```

```
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, 0x00]
for i in range(len(flag)):
    print(chr(flag[i]^0x32),end="")
#VIDAR{Wow!Y0u_kn0w_4_l1ttl3_0f_UPX!}
```

MISC

signIn

图片倒过来看

签到

手机公众号