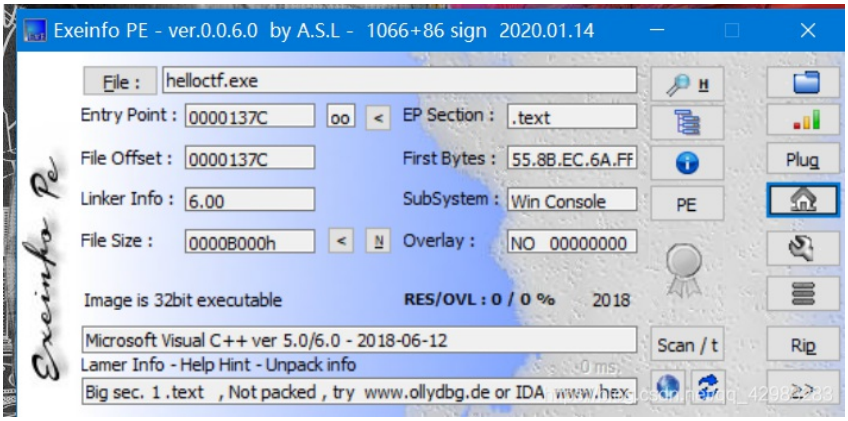
攻防世界Hello, CTF writeup

原创

qq_112419837 于 2020-11-05 11:08:26 发布 305 收藏

下载，查看：



ida打开分析，f5进入伪代码：

应该是一串字符串'437261636b4d654a757374466f7246756e'赋值给v13，然后输入赋值给v9，经过16进制字符串转换，v9的值就变成v10，然后和v13做对比。

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  signed int v3; // ebx@3
  char v4; // al@4
  int result; // eax@9
  int v6; // [sp+0h] [bp-70h]@0
  int v7; // [sp+0h] [bp-70h]@2
  char v8; // [sp+12h] [bp-5Eh]@5
  char v9[20]; // [sp+14h] [bp-5Ch]@2
  char v10; // [sp+28h] [bp-48h]@2
  __int16 v11; // [sp+48h] [bp-28h]@2
  char v12; // [sp+4Ah] [bp-26h]@2
  char v13; // [sp+4Ch] [bp-24h]@1

  qmemcpy(&v13, a437261636b4d65, 0x23u);
  while ( 1 )
  {
    memset(&v10, 0, 0x20u);
    v11 = 0;
    v12 = 0;
    sub_40134B(aPleaseInputYou, v6);
    scanf(aS, v9);
    if ( strlen(v9) > 0x11 )
      break;
    v3 = 0;
    do
    {
      v4 = v9[v3];
      if ( !v4 )
        break;
      sprintf(&v8, asc_408044, v4);
      strcat(&v10, &v8);
      ++v3;
    }
    while ( v3 < 17 );
    if ( !strcmp(&v10, &v13) )
      sub_40134B(aSuccess, v7);
    else
      sub_40134B(aWrong, v7);
  }
  sub_40134B(aWrong, v7);
  result = stru_408090._cnt-- - 1;
  if ( stru_408090._cnt < 0 )
    result = _filbuf(&stru_408090);
  else
    ++stru_408090._ptr;
  return result;
}
```

只要把v13的值转换成字符串就行了：

```
(py27) C:\Users\Administrator\Desktop>python
Python 2.7.18 |Anaconda, Inc.| (default, Apr 23 2020, 17:26:54) [MSC v.1500
Type "help", "copyright", "credits" or "license" for more information.
>>> import binascii
>>> binascii.a2b_hex("437261636b4d654a757374466f7246756e")
'CrackMeJustForFun'
>>>
```

py脚本：

```
list=[0x43,0x72,0x61,0x63,0x6b,0x4d,0x65,0x4a,0x75,0x73,0x74,0x46,0x6f,0x72,0x46,0x75,0x6e]
flag=''
for x in list:
   flag+=chr(x)
print flag
```