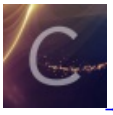
【reversing.kr逆向之旅】Easy Crack的writeup

原创

iqiqiya 于 2018-10-31 19:31:26 发布 398 收藏
分类专栏： 我的逆向之路 ------reversing.kr 我的CTF之路 文章标签： 【reversing.kr逆向之旅】 Easy Crack记录 reversing.kr逆向之旅 Easy Crack的writeup


我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


------reversing.kr
11 篇文章 0 订阅
订阅专栏

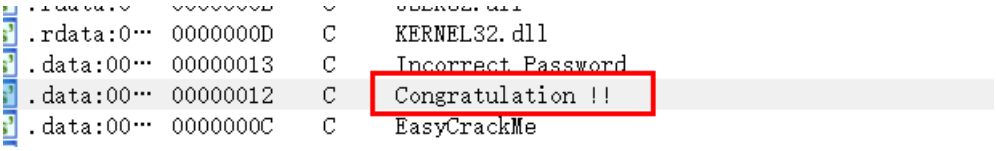

我的CTF之路
92 篇文章 5 订阅
订阅专栏

本来是想看看师傅视频的 结果今天换了个屋子 网络贼差 开了手机热点 想起来这个平台没玩过 就记录一下吧

这道题直接静态分析最简单了

查壳无壳 vc++

IDA载入 shift+f12找到关键字符串



双击进去 再双击引用 接着F5

```
int __cdecl sub_401080(HWND hDlg)
{
  CHAR String; // [esp+4h] [ebp-64h]
  char v3; // [esp+5h] [ebp-63h]
  char v4; // [esp+6h] [ebp-62h]
  char v5; // [esp+8h] [ebp-60h]
  __int16 v6; // [esp+65h] [ebp-3h]
  char v7; // [esp+67h] [ebp-1h]

  String = 0;
  memset(&v3, 0, 0x60u);
  v6 = 0;
  v7 = 0;
  GetDlgItemTextA(hDlg, 1000, &String, 100);
  if ( v3 != 'a' || strncmp(&v4, a5y, 2u) || strcmp(&v5, aR3versing) || String != 'E' )// Ea5yR3versing
    return MessageBoxA(hDlg, aIncorrectPassw, Caption, 0x10u);
  MessageBoxA(hDlg, Text, Caption, 0x40u);
  return EndDialog(hDlg, 0);
}
```

分段比较与目标串进行比较'a'　'5y'　'R3versing'　'E'　只有分别等于他们才可以输出Text 也就是

```
.data:00406044 ; CHAR Text[]
.data:00406044 Text            db 'Congratulation !!',0
```

再看栈中存放顺序

```
-00000065                      db ? ; undefined
-00000064 String               db ?
-00000063 v3                   db ?
-00000062 v4                   db ?
-00000061                      db ? ; undefined
-00000060 v5                   db ?
-0000005F                      db ? ; undefined
```

那我们的输入就应该是

Ea5yR3versing

验证 成功！