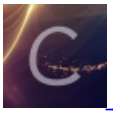
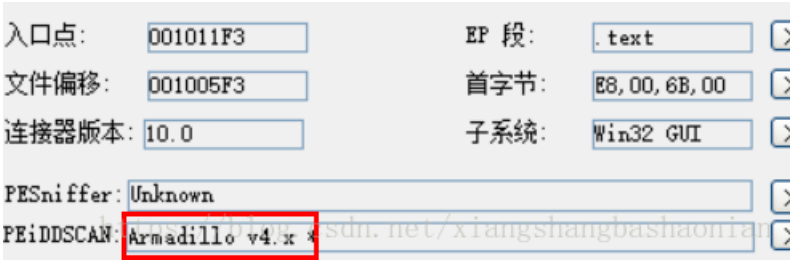
【jarvisoj刷题之旅】逆向题目软件密码破解-1的writeup

原创

iqiqiya 于 2018-09-10 20:26:24 发布
分类专栏： 我的逆向之路 我的CTF之路 我的CTF进阶之路 文章标签： REVERSE 【jarvisoj刷题之旅】逆向题目软件密码破解-1的wri 软件密码破解-1 writeup



刚开始PEiD查到



百度了一下说是一个壳

把我吓坏了 没见过这玩意

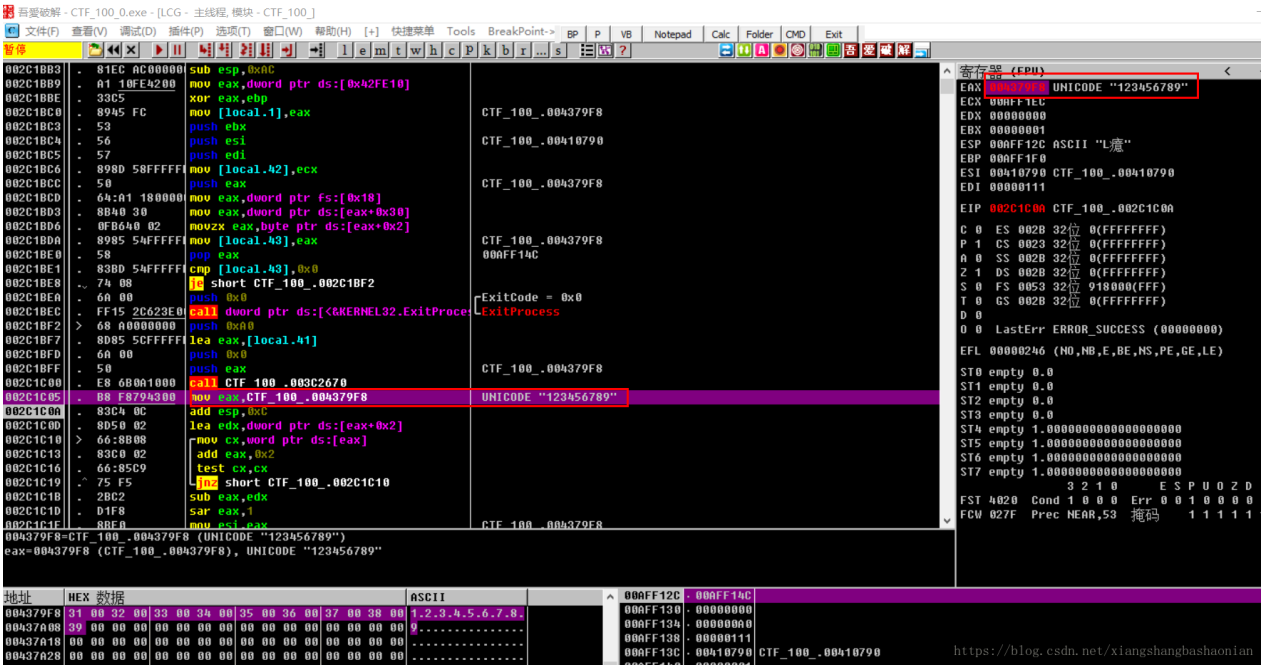
找了几个脱壳机发现都没用

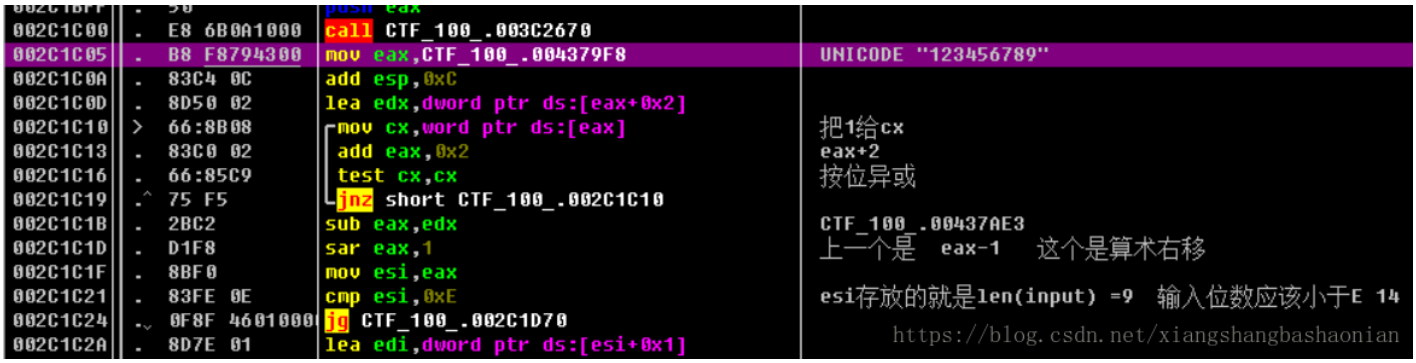
于是直接载入IDA 但好多函数 看不懂 又载入OD

中文搜索引擎发现“你赢了”

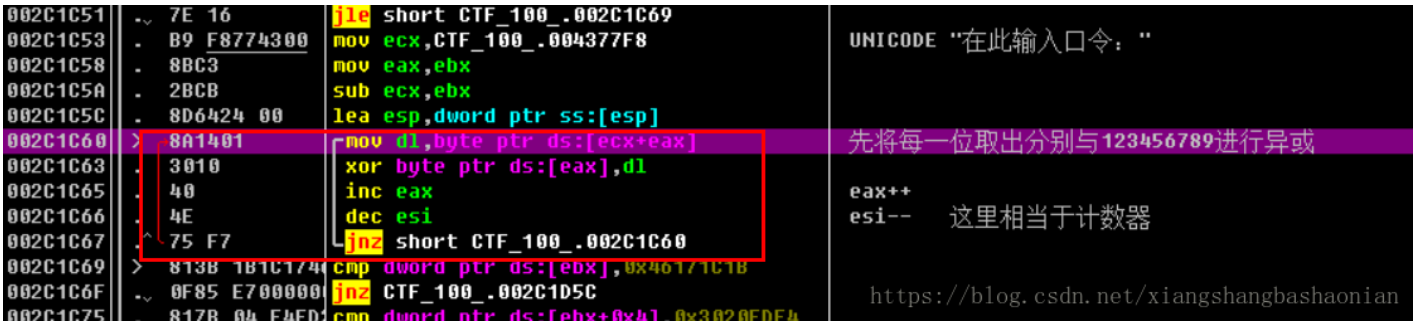
于是在段首下断

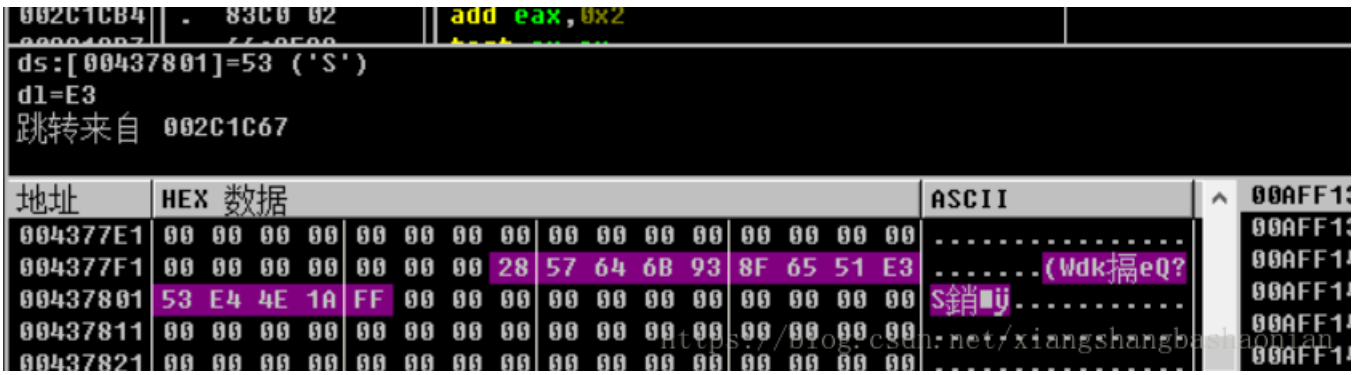
下图是正读取输入123456789





下面是重要的一个地方





将与我们的input对比的数据抠出来

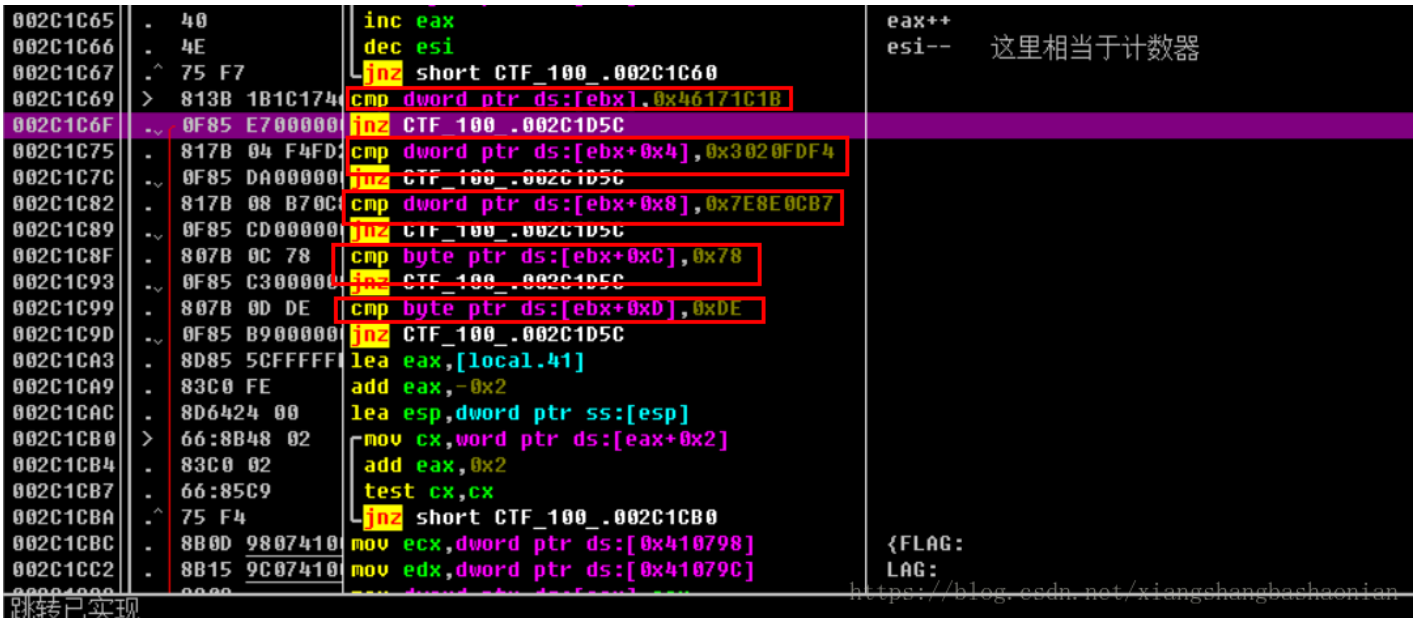
004377F1　　28 57 64 6B 93 8F 65 51 E3　　(Wdk搞eQ?

00437801 53 E4 4E 1A FF　　S銷□.

整理一下得到**28,57,64,6B,93,8F,65,51,E3,53,E4,4E,1A,FF**

正好14个数据

下面是接下来将异或后的结果分开 分别与这些作比较



将这些数据也抠出来

002C1C69 |> \813B 1B1C1746 cmp dword ptr ds:[ebx],0x46171C1B

002C1C75 |. 817B 04 F4FD2>cmp dword ptr ds:[ebx+0x4],0x3020FDF4

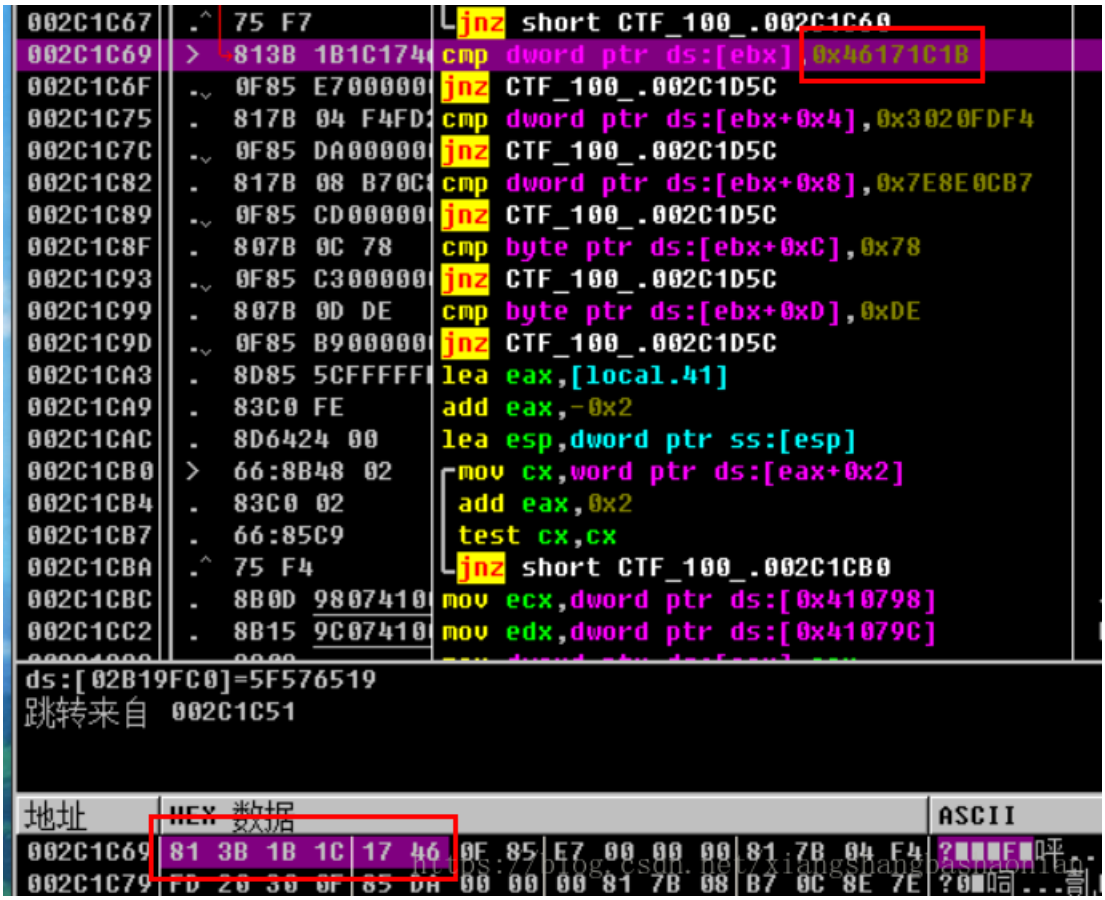
002C1C82 |. 817B 08 B70C8>cmp dword ptr ds:[ebx+0x8],0x7E8E0CB7

002C1C8F |. 807B 0C 78   cmp byte ptr ds:[ebx+0xC],0x78

002C1C99 |. 807B 0D DE   cmp byte ptr ds:[ebx+0xD],0xDE

46,17,1C,1B 30,20,FD,F4 7E,8E,0C,B7 78,DE

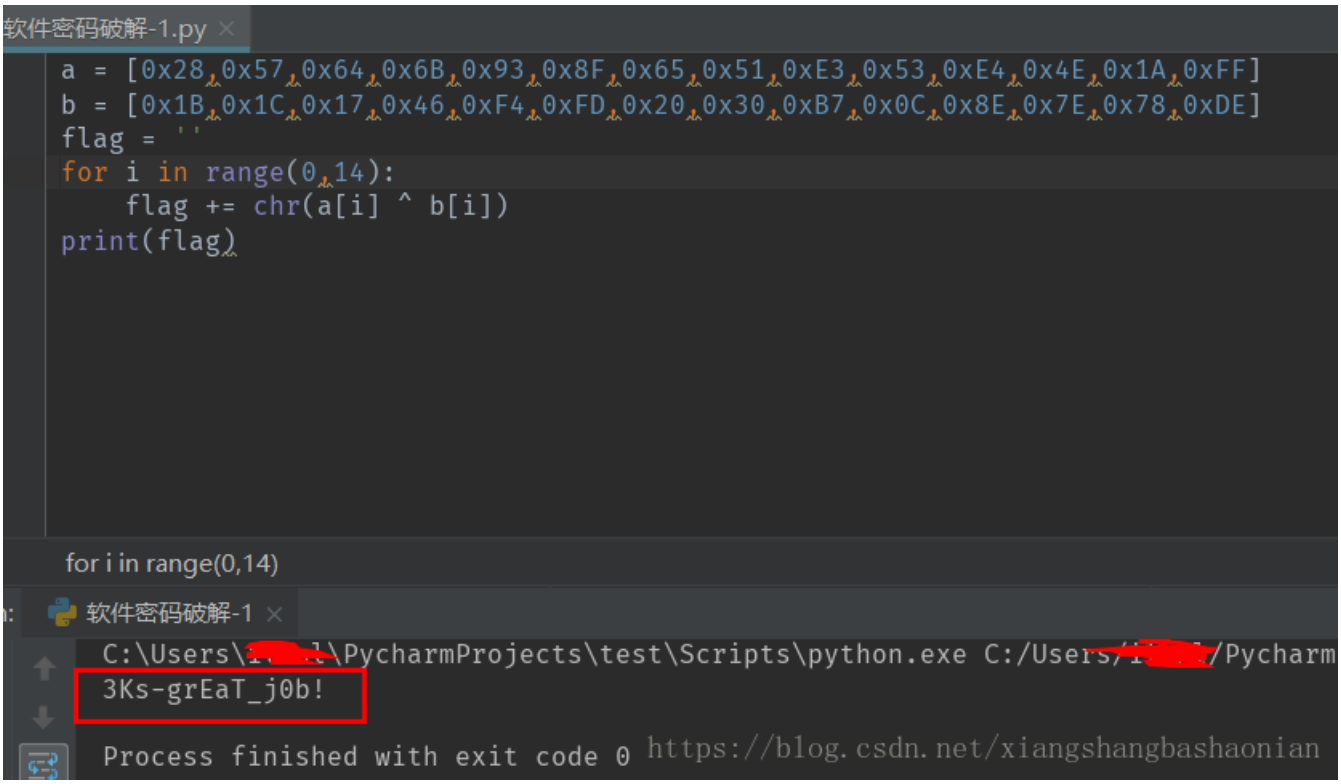
但是这里顺序是相反的 我们可以选中那一行 右键数据窗口跟随—》选择就可以明白



所以最后应该是

1B,1C,17,46,F4,FD,20,30,B7,0C,8E,7E,78,DE

也是14位



提交显示正确