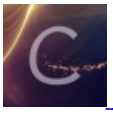
【WhaleCTF逆向题】第二期入门语言【初级】writeup

原创

iqiqiya 于 2018-09-26 22:22:01 发布 1201 收藏
分类专栏： 我的CTF之路 我的逆向之路 ------WhaleCTF 我的CTF进阶之路 文章标签： 【WhaleCTF逆向题】第二期入门语言【初级】writeu 第二期入门语言【初级】writeup 入门语言【初级】writeup writeup

本文链接：https://blog.csdn.net/xiangshangbashaonian/article/details/82860388


我的CTF之路 同时被 3 个专栏收录
92 篇文章 5 订阅
订阅专栏


我的逆向之路
108 篇文章 10 订阅
订阅专栏


------WhaleCTF
8 篇文章 0 订阅
订阅专栏

题目信息：

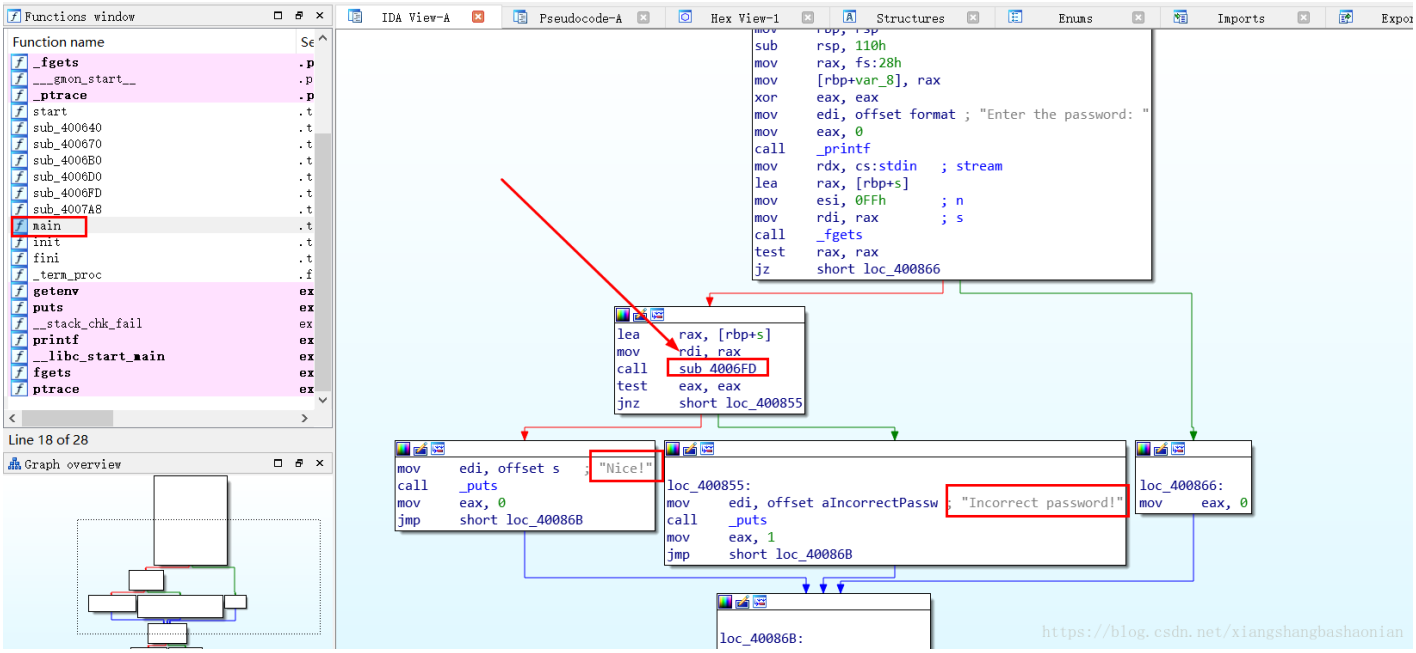
这道题目有两种做法

0x01:常规逆向

0x02:是利用 使用Angr符号执行来求解CTF逆向题

简单记录一下0x01的做法

载入x64IDA 直接就可以看到主函数



直接就可以发现sub_4006FD这个函数就是关键

双击进入

F5

得到伪代码如下

```
signed __int64 __fastcall sub_4006FD(__int64 a1)
{
  signed int i; // [rsp+14h] [rbp-24h]
  const char *v3; // [rsp+18h] [rbp-20h]
  char *v4; // [rsp+20h] [rbp-18h]
  char *v5; // [rsp+28h] [rbp-10h]

  v3 = "Dufhbmf";
  v4 = "pG`imos";
  v5 = "ewUglpt";
  for ( i = 0; i <= 11; ++i )
  {
    if ( (&v3)[i % 3][2 * (i / 3)] - *(i + a1) != 1 )
      return 1LL;
  }
  return 0LL;
}
```

一个for循环 对三个串(以二维数组的形式)进行操作 就可以得到密码

在解之前 先把三个串转成ascii

```
b = [[68, 117, 102, 104, 98, 109, 102],
     [112, 71, 96, 105, 109, 111, 115],
     [101, 119, 85, 103, 108, 112, 116]]
flag = ''
for i in range(12):
    flag += chr(b[i % 3][2* (i / 3)] -1)
    print(flag)
```

运行就可以得到flag