攻防世界 逆向 hackme

原创

与日平肩以头抢地 于 2020-02-20 09:40:27 发布 536 收藏

分类专栏： 逆向 文章标签： 安全

本文链接：https://blog.csdn.net/fool_best/article/details/104405333

逆向 专栏收录该内容

12 篇文章 0 订阅

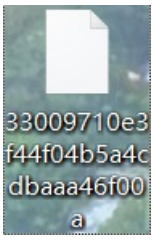
订阅专栏

攻防世界 逆向 hackme

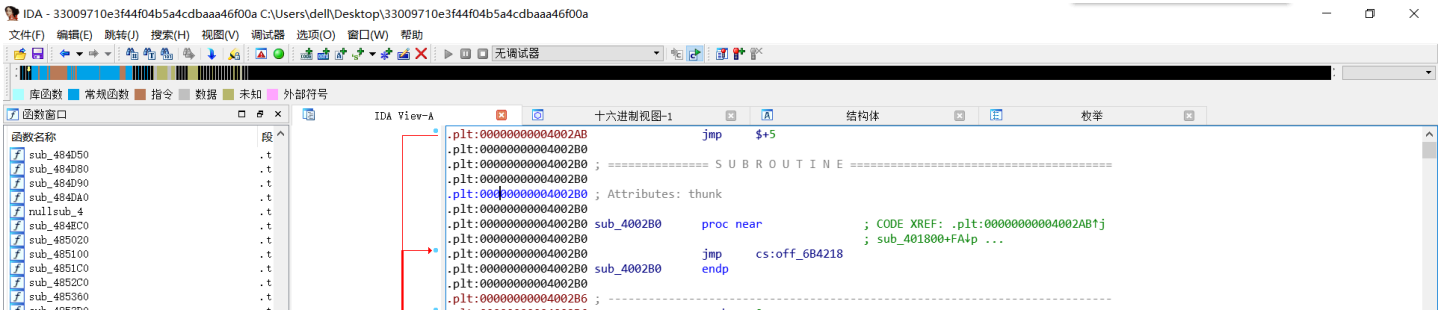
（原创）

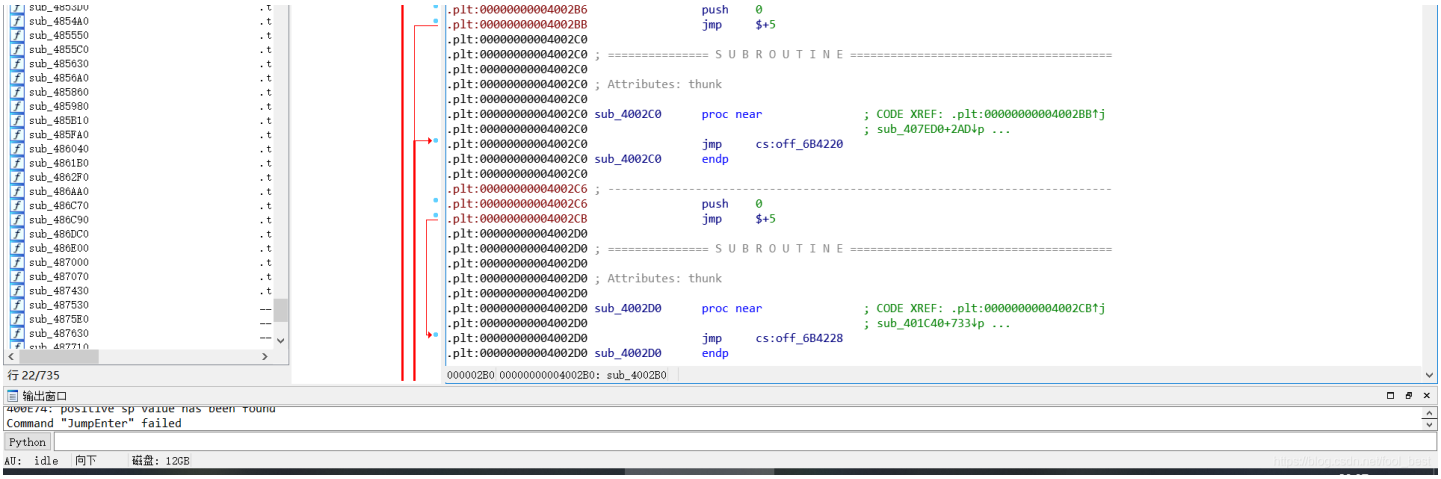
原题如下：

下载文件

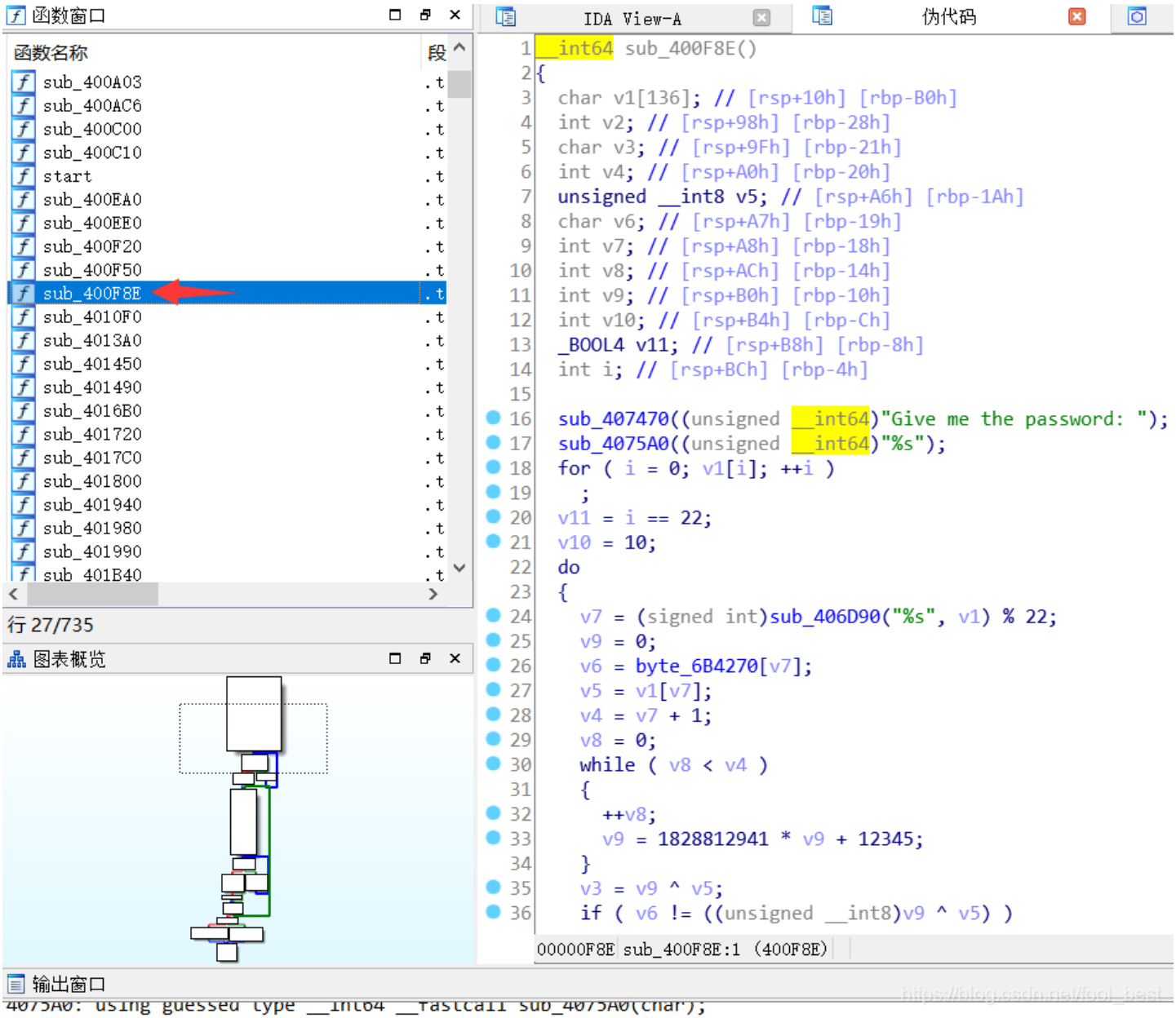


IDA打开





确定sub_400F8E()函数找flag。



伪代码如下：

```
__int64 sub_400F8E()
{
  char v1[136]; // [rsp+10h] [rbp-B0h]
  int v2; // [rsp+98h] [rbp-28h]
  char v3; // [rsp+9Fh] [rbp-21h]
  int v4; // [rsp+A0h] [rbp-20h]
  unsigned __int8 v5; // [rsp+A6h] [rbp-1Ah]
  char v6; // [rsp+A7h] [rbp-19h]
  int v7; // [rsp+A8h] [rbp-18h]
  int v8; // [rsp+ACh] [rbp-14h]
  int v9; // [rsp+B0h] [rbp-10h]
  int v10; // [rsp+B4h] [rbp-Ch]
  _BOOL4 v11; // [rsp+B8h] [rbp-8h]
  int i; // [rsp+BCh] [rbp-4h]

  sub_407470((unsigned __int64)"Give me the password: ");
  sub_4075A0((unsigned __int64)"%s");
  for ( i = 0; v1[i]; ++i )
    ;
  v11 = i == 22;
  v10 = 10;
  do
  {
    v7 = (signed int)sub_406D90("%s", v1) % 22;
    v9 = 0;
    v6 = byte_6B4270[v7];
    v5 = v1[v7];
    v4 = v7 + 1;
    v8 = 0;
    while ( v8 < v4 )
    {
      ++v8;
      v9 = 1828812941 * v9 + 12345;
    }
    v3 = v9 ^ v5;
    if ( v6 != ((unsigned __int8)v9 ^ v5) )
      v11 = 0;
    --v10;
  }
  while ( v10 );
  if ( v11 )
    v2 = sub_407470((unsigned __int64)"Congras\n");
  else
    v2 = sub_407470((unsigned __int64)"Oh no!\n");
  return 0LL;
}
```

程序：验证输入22位–>生成随机数验证10位数
用脚本运行

```
bs=[0x5F, 0xF2, 0x5E, 0x8B, 0x4E, 0x0E, 0xA3, 0xAA, 0xC7, 0x93,
  0x81, 0x3D, 0x5F, 0x74, 0xA3, 0x09, 0x91, 0x2B, 0x49, 0x28,
  0x93, 0x67]
flag=[0 for i in range(22)]
for index in range(22):
    b=bs[index]
    temp=0
    for i in range(index+1):
        temp=(0x6D01788D * temp + 0x3039)
    flag[index]=(temp^b)&0xff
print(''.join(map(chr,flag)))
```

得到flag{d826e6926098ef46}