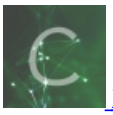
XCTF reverse 高手进阶区 Mysterious

原创

YQK易乾坤 于 2020-11-18 14:56:41 发布 122 收藏

分类专栏： XCTF REVERSE 高手进阶区 文章标签： 安全

本文链接：https://blog.csdn.net/qq_30076719/article/details/109745451



XCTF REVERSE 高手进阶区 专栏收录该内容

1 篇文章 0 订阅

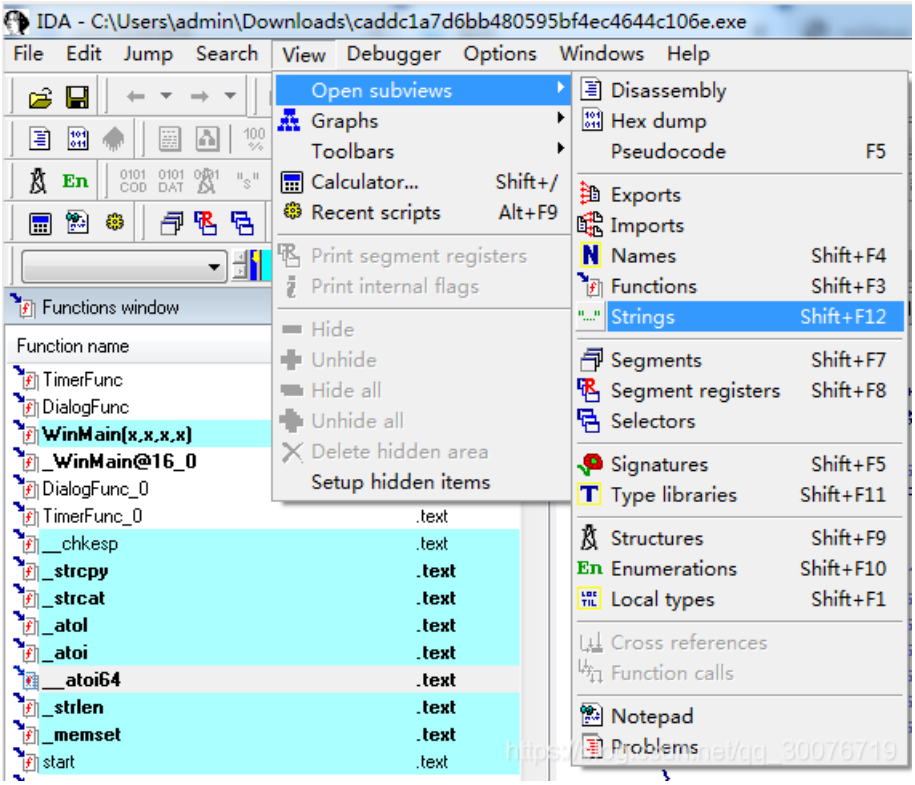
订阅专栏

这是一道基本的逆向题。。。

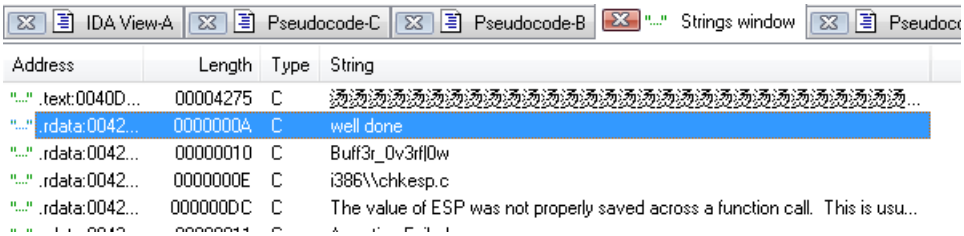
打开软件，然我们输入口令，猜测是输对了就能得到flag吧：

那就话不多说，直接放进ida啦

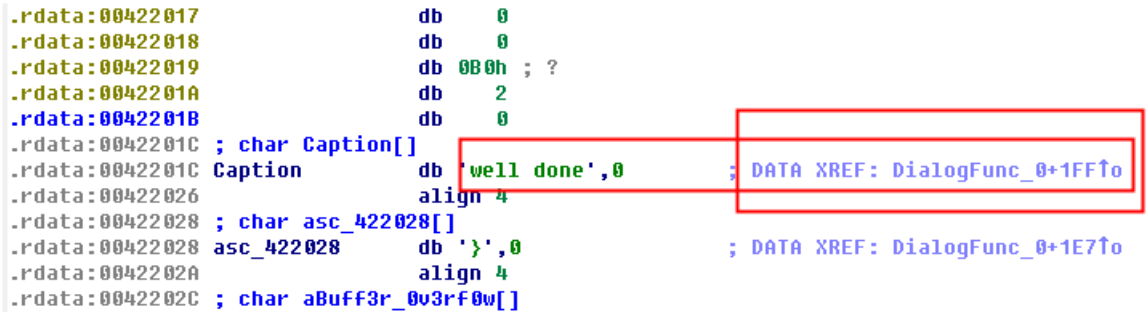
直接查看字符串，查看方法如下：



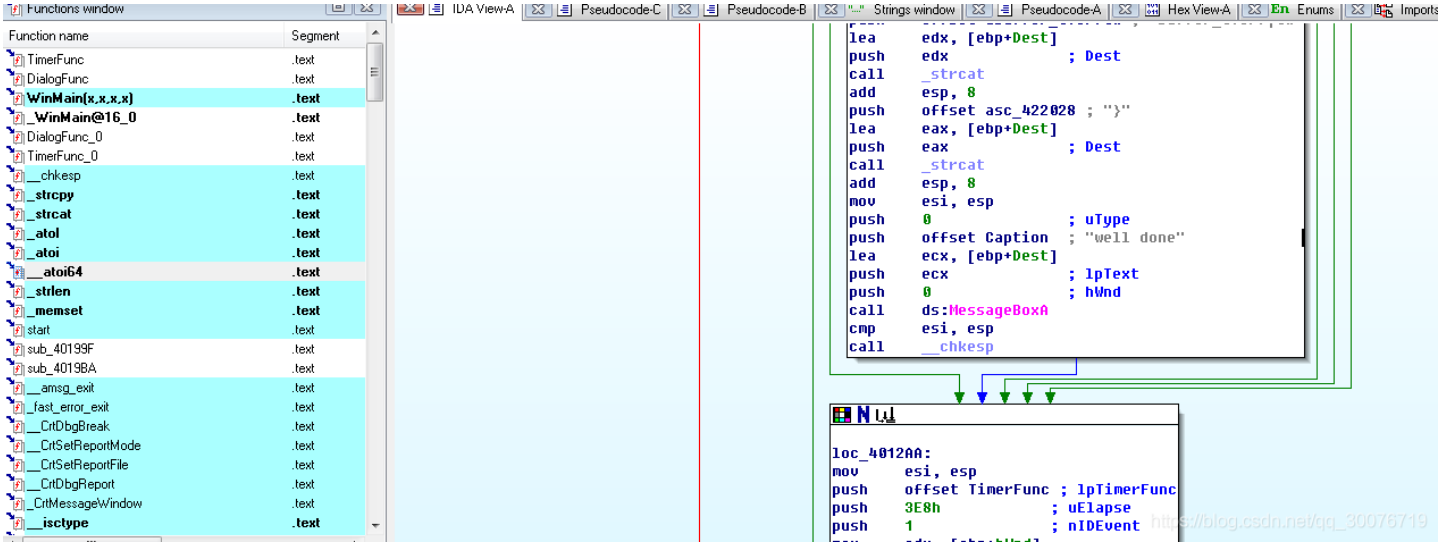
然后就能在字符串的窗口看到well done



双击打开



然后双击上图那里，打开对应的函数



然后按下F5，查看伪代码（敲重点！！！64位的按F5是没用的，必须要用32位的打开才有反应，我也被坑了，所以如果你看到这里，你也恰巧打开的是64位的，那么请重新来一遍）

打开如下：

```
{
  if ( a3 == 1000 )
  {
    GetDlgItemTextA(hWnd, 1002, &Dst, 260);
    _chkesp();
    strlen(&Dst);
    if ( strlen(&Dst) > 6 )
      ExitProcess(0);
    Value = atoi(&Dst) + 1;
    if ( Value == 123 && v14 == 120 && v16 == 122 && v15 == 121 )
    {
      strcpy((char *)Dest, "flag");
      memset(&v9, 0, 0xFCu);
      v10 = 0;
      v11 = 0;
      _itoa(Value, &Source, 10);
      strcat((char *)Dest, "{");
      strcat((char *)Dest, &Source);
      strcat((char *)Dest, "_");
      strcat((char *)Dest, "Buff3r_0v3rf|0w");
      strcat((char *)Dest, "}");
      MessageBoxA(0, Dest, "well done", 0);
      _chkesp();
    }
    SetTimer(hWnd, 1u, 0x3E8u, (TIMERPROC)TimerFunc);
    _chkesp();
  }
  if ( a3 == 1001 )
  {
```


好了，看了代码之后，已经很明显了，框柱的连起来不就是我们平时看的flag格式嘛，那么只要得出绿色框中的的那个参数就可以了，于是打开_itoa函数，发现值为123，那么flag既可以拼接出来了，为：

flag{123_Buff3r_0v3rf|0w}