

XCTF 梅津美治郎

原创

夏了茶糜 于 2020-03-18 15:36:17 发布 994 收藏

分类专栏: [CTF-REVERSE](#) 文章标签: [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/qin9800/article/details/104942620>

版权

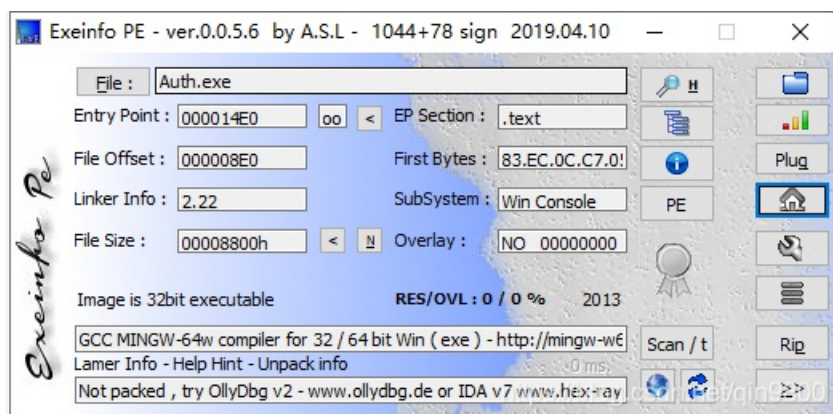


[CTF-REVERSE](#) 专栏收录该内容

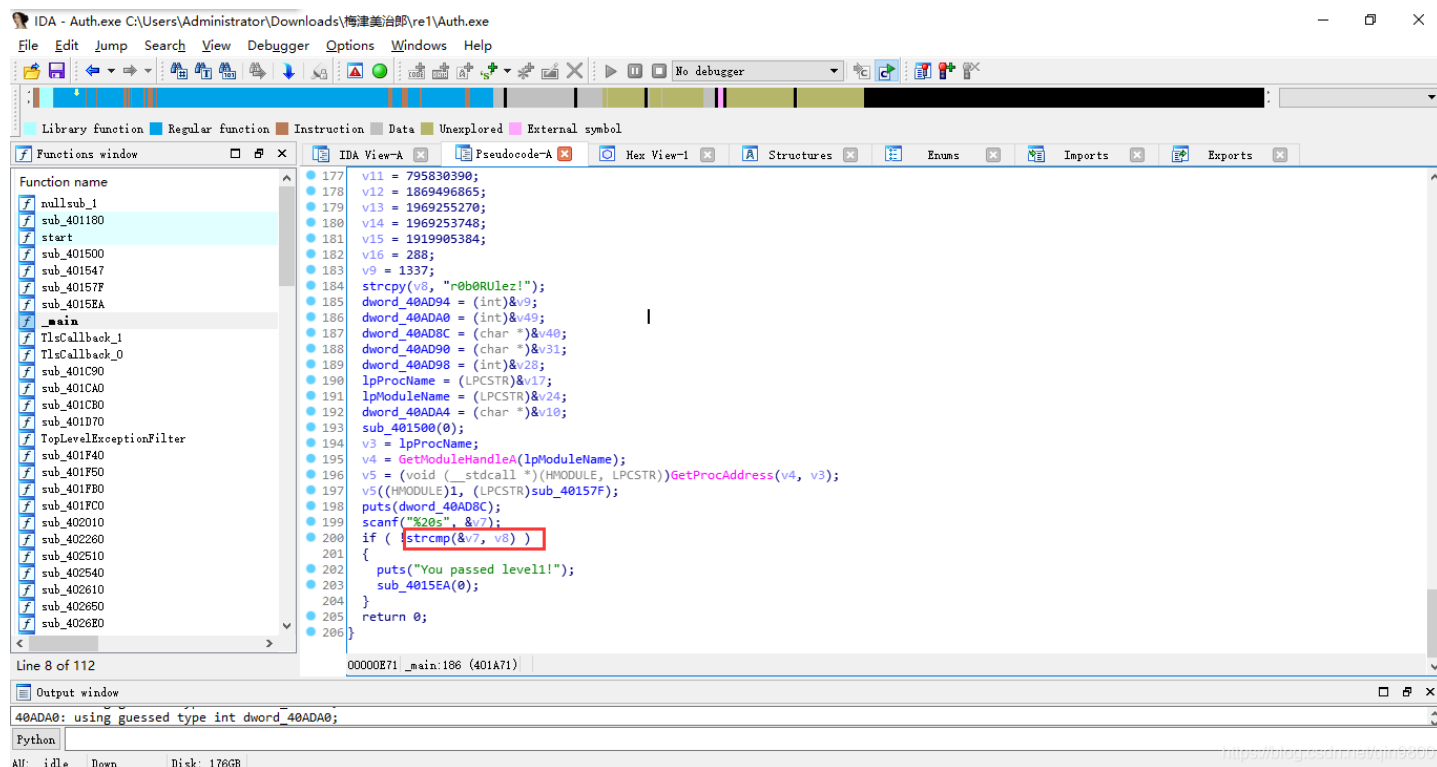
18 篇文章 0 订阅

订阅专栏

查壳



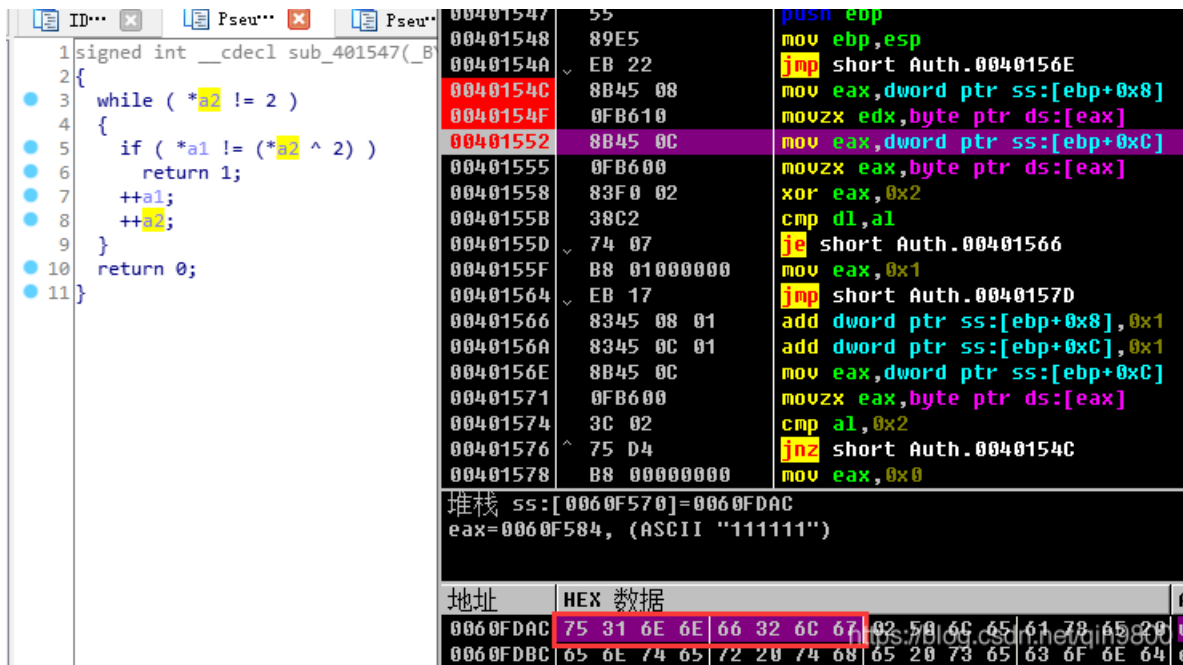
32位程序, IDA打开, 分析main函数



发现第一重校验，就是对比v7和v8，v7就是用户输入，v8就是固定的r0b0RU1ez!
运行程序，输入这个字符串看下效果



成功通过第一个校验，接着往下分析



通过调试获取到了第二个校验处的数据，对这段数据解密

```
tmp = "75 31 6E 6E 66 32 6C 67"
tmp = tmp.split(" ")
print(tmp)
key = ""
for i in tmp:
    key += chr(int(i,16)^2)
print(key)
```

w31ld0ne

这两个字符串通过下划线拼接起来就是flag

flag:

```
flag{r0b0RU1ez!_w31ld0ne}
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)