XCTF 梅津美治郎

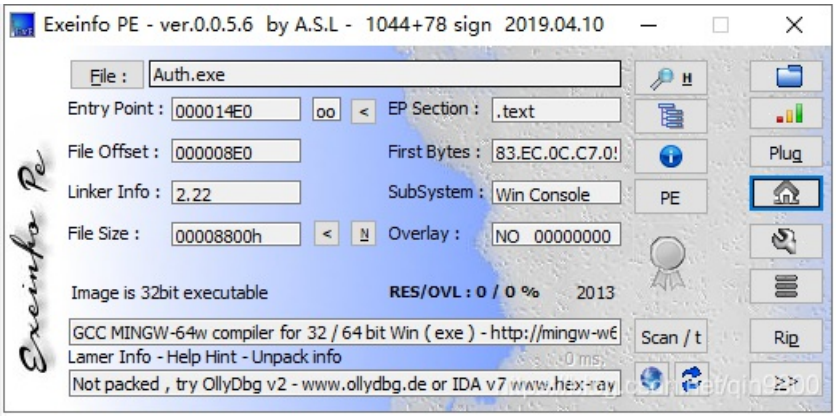
原创

夏了茶糜 于 2020-03-18 15:36:17 发布 994 收藏

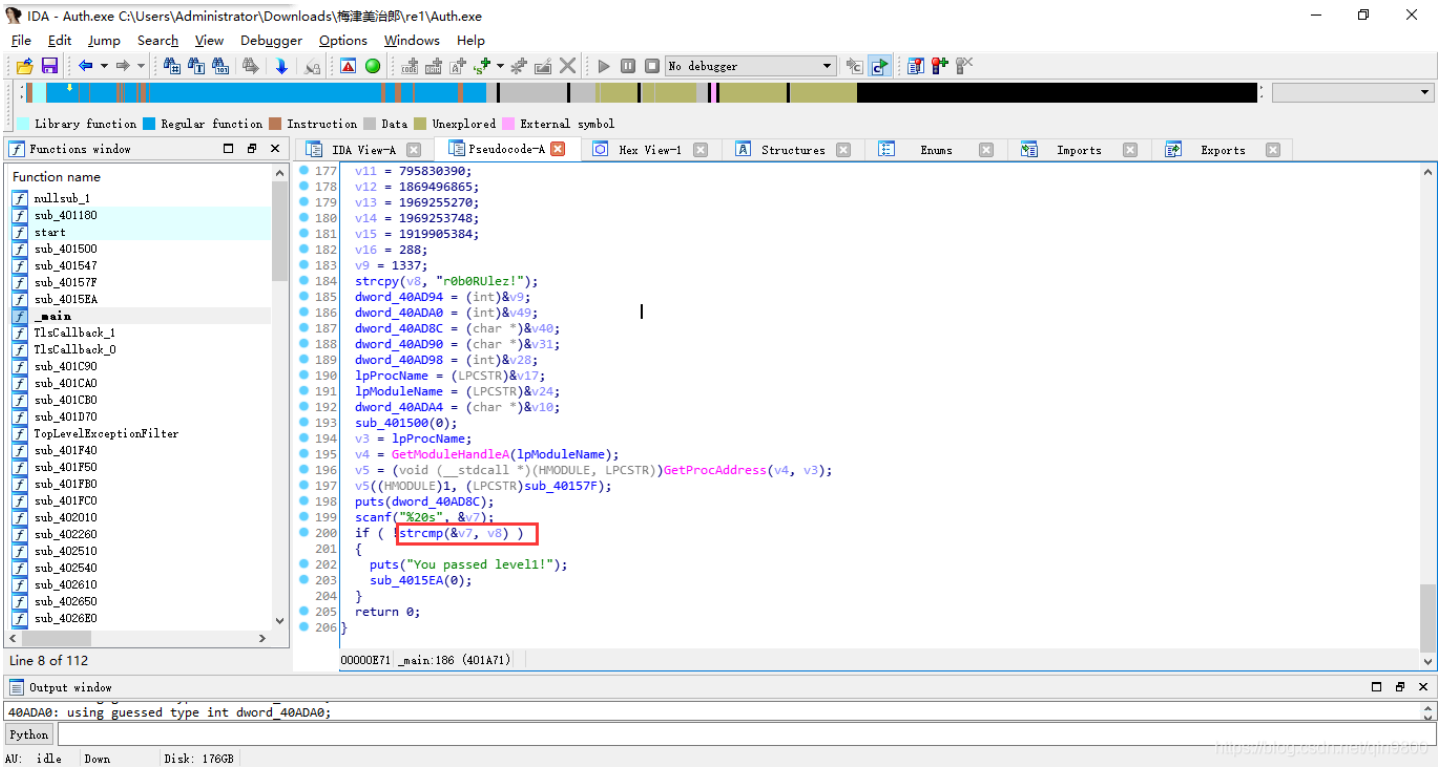
分类专栏： CTF-REVERSE 文章标签： 安全

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

查壳

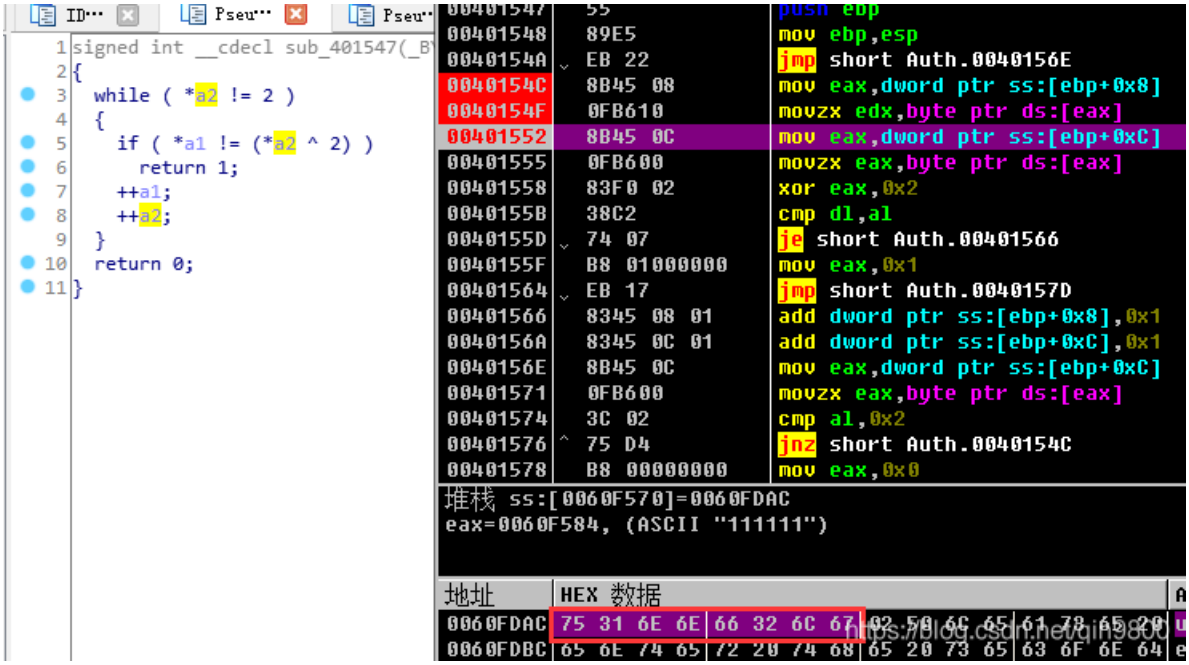


32位程序，IDA打开，分析main函数



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r0b0RUlez!
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)
```

```
w3lld0ne
```

这两个字符串通过下划线拼接起来就是flag
flag：

```
flag{r0b0RUlez!_w3lld0ne}
```