攻防世界 Reverse高手进阶区 2分题 debug

原创

思源湖的鱼 于 2020-12-25 15:13:07 发布 128 收藏 1

分类专栏： ctf 文章标签： ctf 攻防世界 reverse .net

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111681784

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

本篇是debug的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

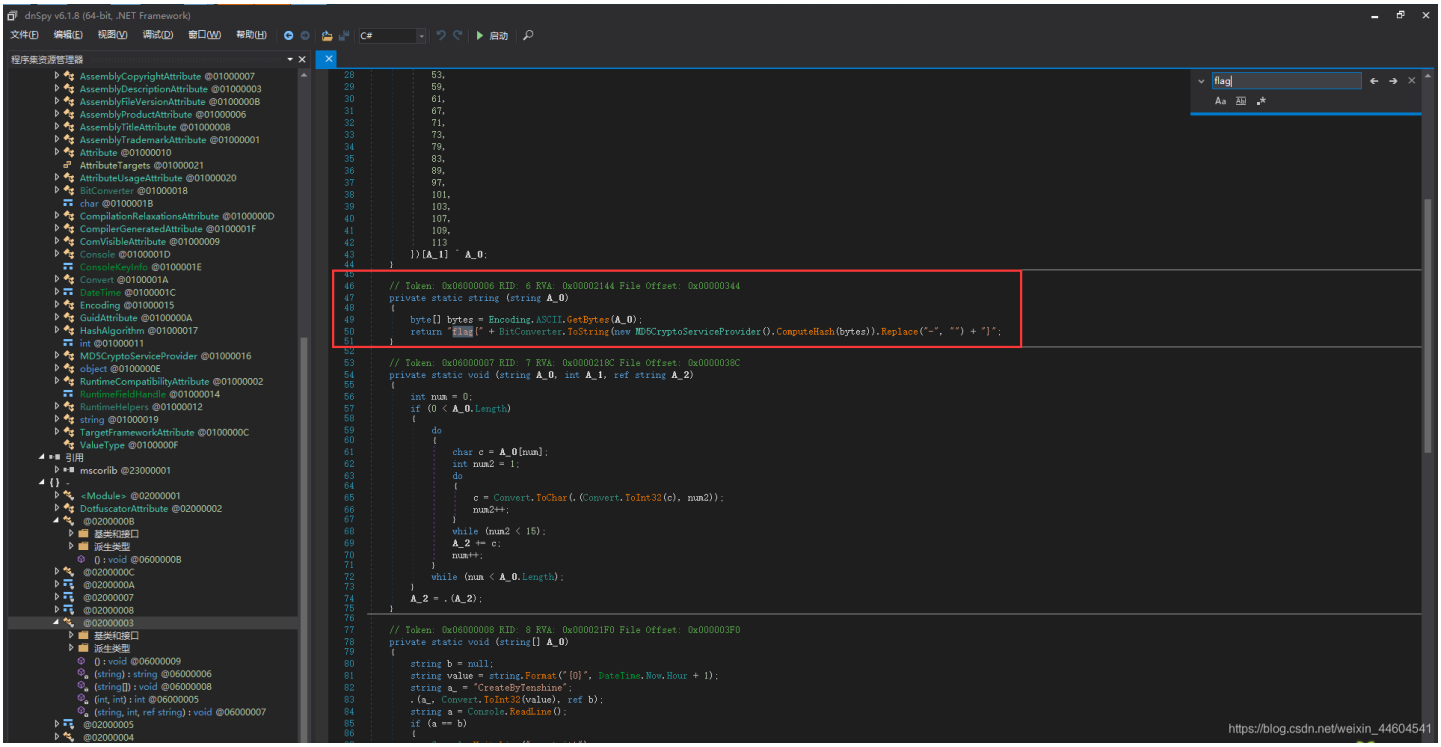
解题过程

PE查壳

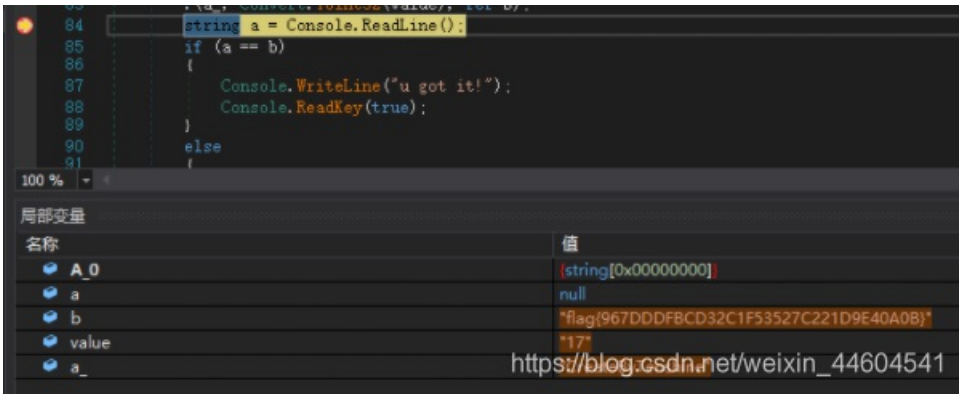
扔进IDA

没法分析

查了查
net文件
用dnspy



发现这个flag直接给出了
那就在他算完的时候给中断



得到flag

BTW
根据逻辑给出的脚本

```
import hashlib
a=[2,3,5,7,0xb,0xd,0x11,0x13,0x17,0x1d,0x1f,0x25,0x29,0x2b,0x2f,0x35,0x3b,0x3d,0x43,0x47,0x49,0x4f,0x53,0x59,0x6
1,0x65,0x67,0x6b,0x6d,0x71]
b="CreateByTenshine"
c=""
for i in range(len(b)):
    d=ord(b[i])
    for j in range(1,15):
        d=a[j]^d
    c+=chr(d)
print(c)
m=hashlib.md5(c.encode("utf-8")).hexdigest()
print("flag{",m,"}")
```

结语

NET文件的反编译