

# 2021NepCTF REVERSE-Hardcsharp Writeup

原创

Nu1bzzi 于 2021-03-22 22:21:08 发布 191 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/Nu1bzzi/article/details/115099650>

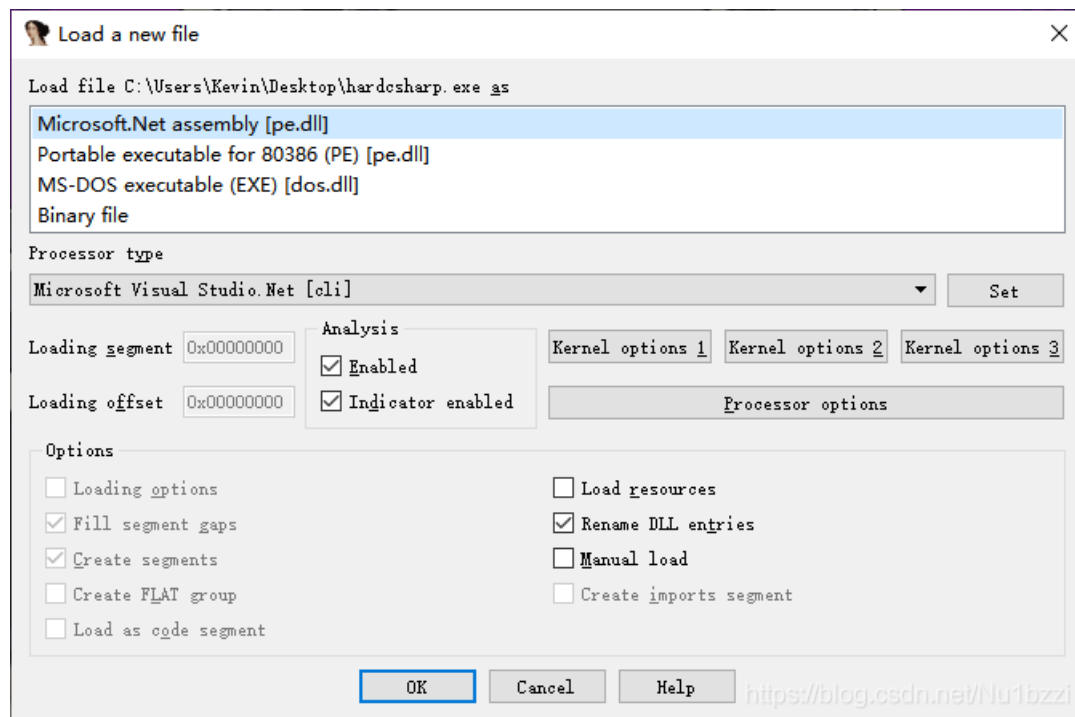
版权

## 2021NepCTF REVERSE-Hardcsharp

首先拿到文件第一步用PEiD查壳（养成好习惯）

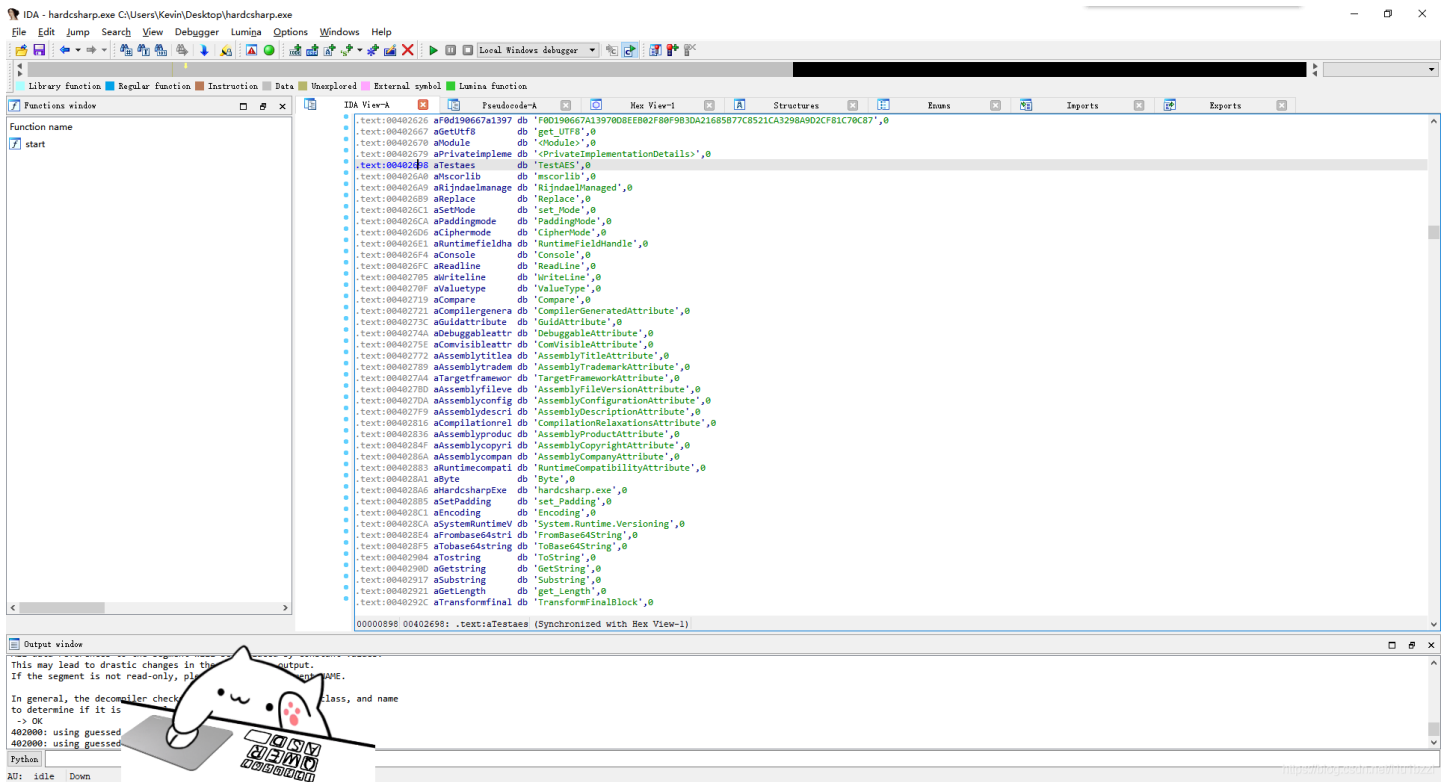


什么都没找到QAQ，萌新只知道是32位的程序于是顺手放进IDA进行分析

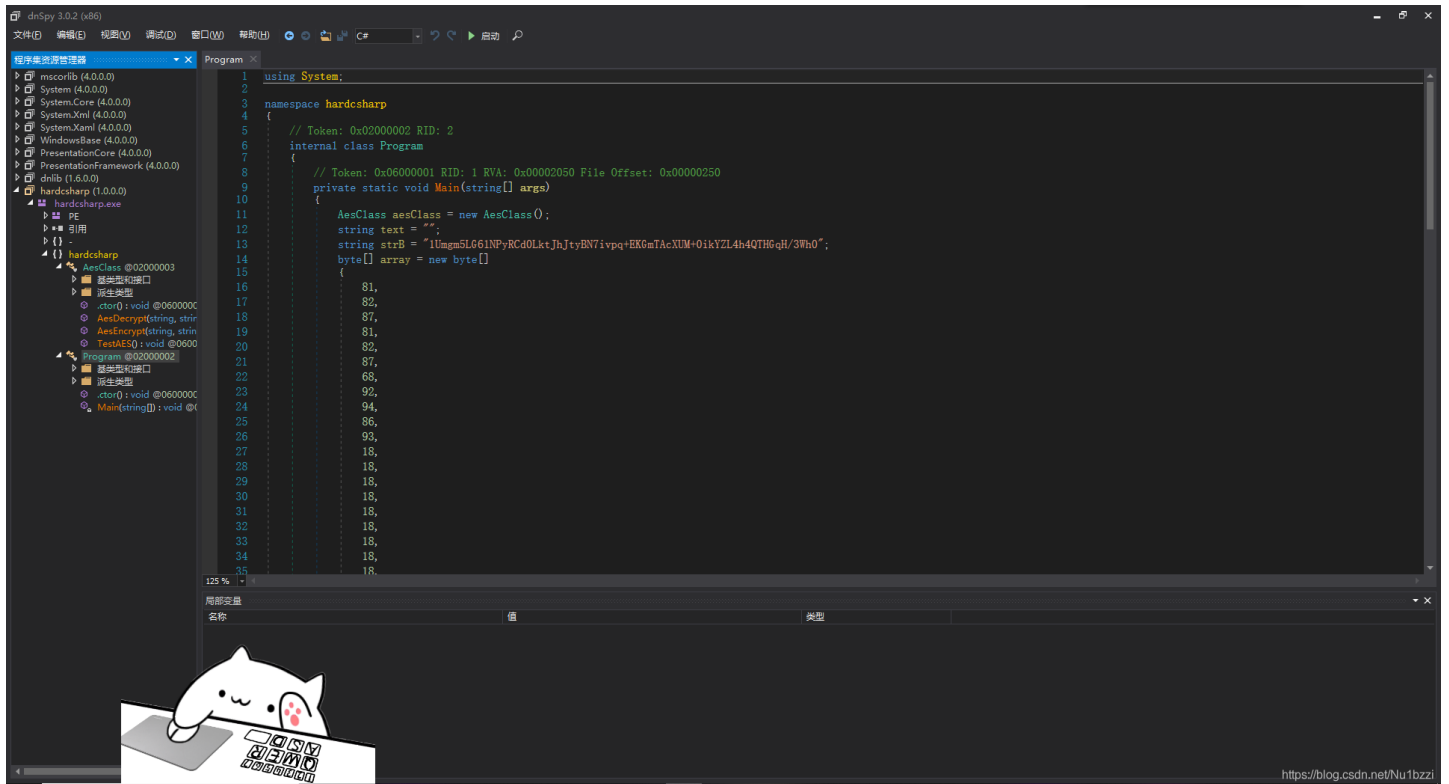


在放入时发现该程序是由.NET做的

进入后点进jmp后的函数果然发现了熟悉的东西

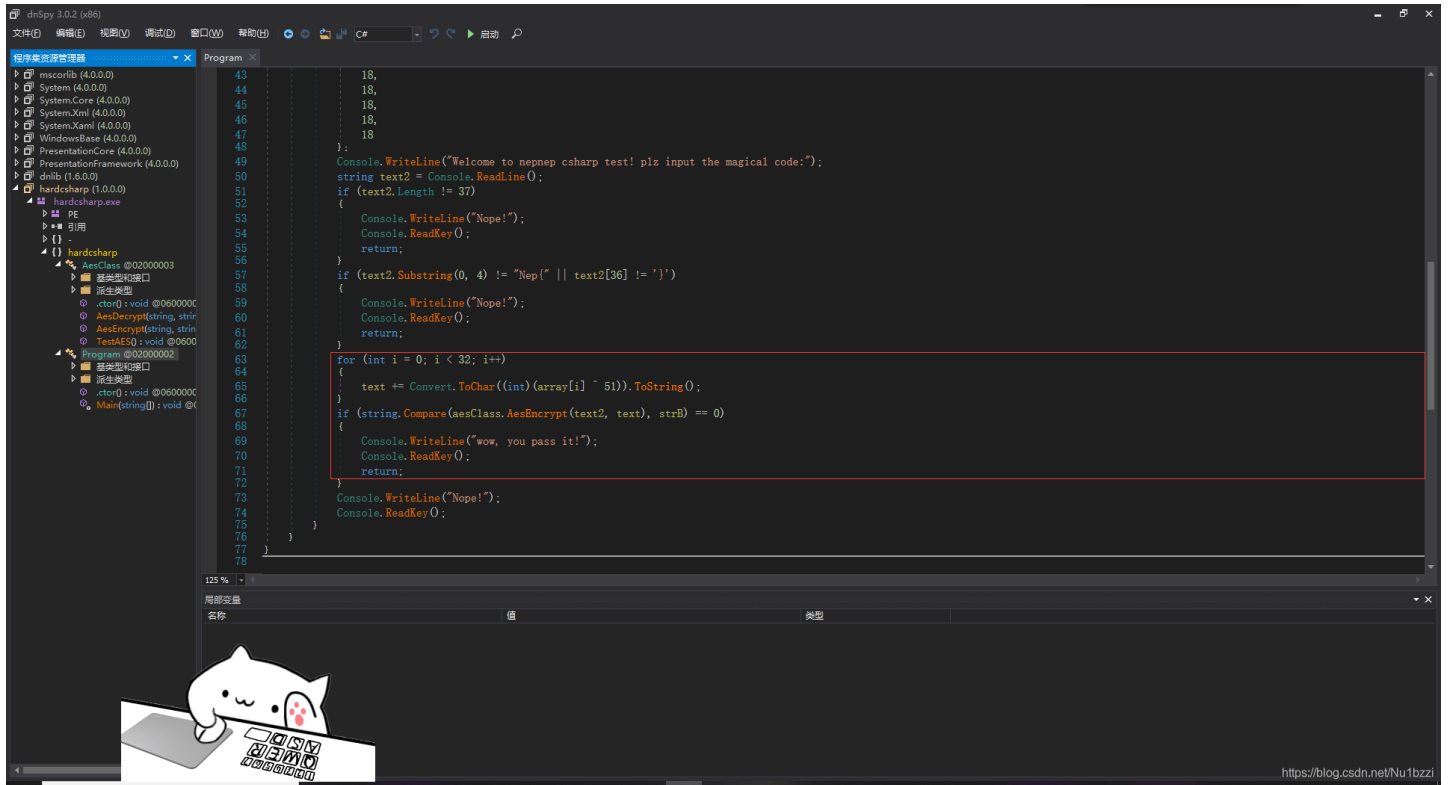


直接放入Dnspy中进行分析（Dnspy的详细使用方法和下载地址在这里☐QAQ）




一个个点开之后发现我们要分析的主要函数在@02000002中

而我们需要注意的是这部分的运算



```
43     18,  
44     18,  
45     18,  
46     18,  
47     18,  
48     18  
49     };  
50     Console.WriteLine("Welcome to nepnep csharp test! plz input the magical code:");  
51     string text2 = Console.ReadLine();  
52     if (text2.Length != 37)  
53     {  
54         Console.WriteLine("Nope!");  
55         Console.ReadKey();  
56         return;  
57     }  
58     if (text2.Substring(0, 4) != "Nep(" || text2[36] != ')')  
59     {  
60         Console.WriteLine("Nope!");  
61         Console.ReadKey();  
62         return;  
63     }  
64     for (int i = 0; i < 32; i++)  
65     {  
66         text += Convert.ToChar(((int)(array[i] ^ 51)).ToString());  
67     }  
68     if (string.Compare(aesClass.AesEncrypt(text2, text), strB) == 0)  
69     {  
70         Console.WriteLine("wow, you pass it!");  
71         Console.ReadKey();  
72         return;  
73     }  
74     Console.WriteLine("Nope!");  
75     Console.ReadKey();  
76 }  
77 }  
78 }
```

名称	值	类型



https://blog.csdn.net/Nu1bzzi

由for循环函数可知array[]数组中每一项都与51做了异或运算

而在后面有一串这样的代码

```
if (string.Compare(aesClass.AesEncrypt(text2, text), strB) == 0)
```

即需要满足这个条件才算正确，在不知道的情况下百度了之后发现AesEncrypt是一种加密运算：

AES\_ENCRYPT(加密前字符串,key)通过key加密后得到密文

AES\_DECRYPT(已加密字符串,key)通过key解密后得到明文

其中key是需要指定的



现在我们已经知道了密码text与密文strB，剩下的就是找在线解密网站了  
□wyyyyyyy!!! (找了半天这个有用，其他的不是失败就是半天加载不出)

在线AES加密解密、AES在线加密解密、AES encryption and decryption

AES高级加密标准 (英语: Advanced Encryption Standard, 缩写: AES), 在密码学中又称Rijndael加密法, 是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的DES, 已经被多方分析且广为全世界所使用。严格地说, AES和Rijndael加密法并不完全一样 (虽然在应用中二者可以互换), 因为Rijndael加密法可以支持更大范围的区块和密钥长度: AES的区块长度固定为128比特, 密钥长度可以是128, 192或256比特; 而Rijndael使用的密钥和区块长度可以是32位的整数倍, 以128位为下限, 256比特为上限。包括AES-ECB,AES-CBC,AES-CTR,AES-OFB,AES-CFB

密钥如何恢复 商家接单平台 加密解密工具 csgo网页开箱 国外vps网站 接单平台 游戏源码 和黄crm在线  
可以挖矿的app 短信接口平台 crm在线系统 u盘恢复数据 美国服务器网址 接单平台 加密解密软件 网上接单平台  
丑丸外皮发痒 解密软件 中文版MT4 平台短信接口 md5加密解密 美国服务器网站 2344网页游戏 菱阳如何恢复

AES加密模式: ECB 填充: zeropadding 数据块: 128位 密钥: badbadwomen!!!!!!!!!!!! 偏移量: iv偏移量, ecb模式不用 输出: base64 字符集: gb2312编码 (简体)

待加密、解密的文本

```
11hgA5L091NfyRC4LkrtJhJty8W7ivpqrER6wTAcXRM+0kkYZL4h4QTH9qH/3W6A
```

↑ 将你的电脑文件直接拖入试试 ^-^

AES加密 AES解密

AES加密、解密转换结果(base64了)

```
Nep {up_up_down_down_B_a_b_A_Nep_nep~}
```

© 2021 蜜糖IT网. Update Ctrl+D 收藏 粤ICP备13083991号 站点地图 最新信息 To: 8292669@qq.com

于是乎：最终flag就是Nep{up\_up\_down\_down\_B\_a\_b\_A\_Nep\_nep~}

由于卑微的实力以及周末有事没什么时间（当然菜是本质，菜才是重点）所以只做了这一题（别骂了别骂了在学了