2021NepCTF REVERSE-Hardcsharp Writeup

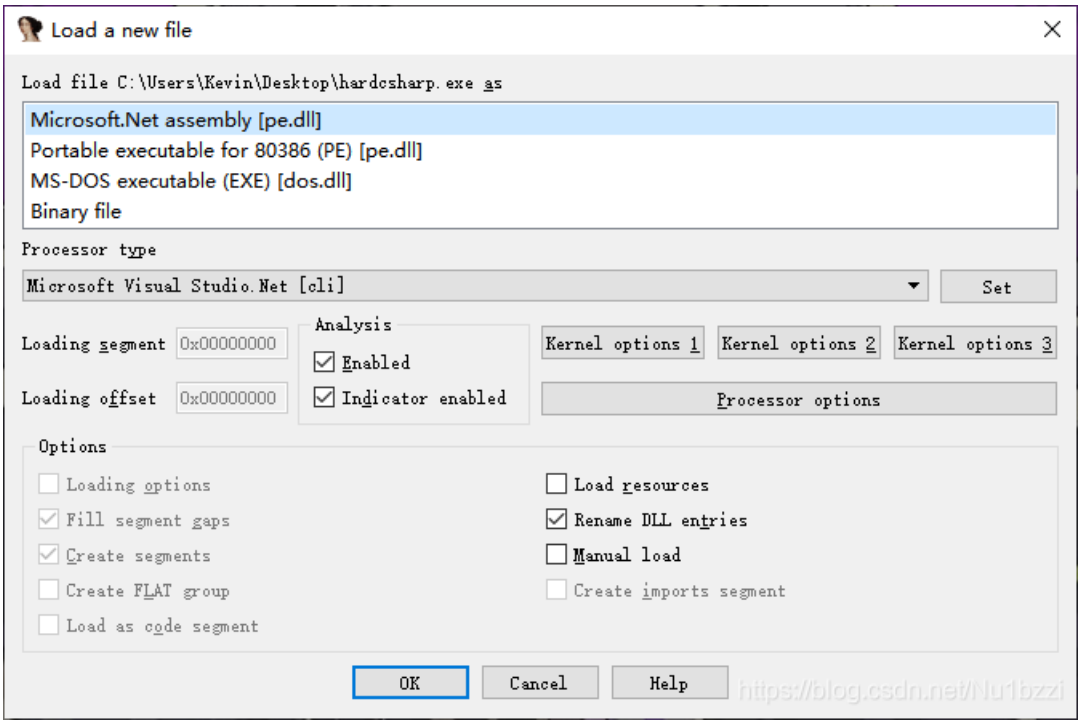
原创

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

2021NepCTF REVERSE-Hardcsharp

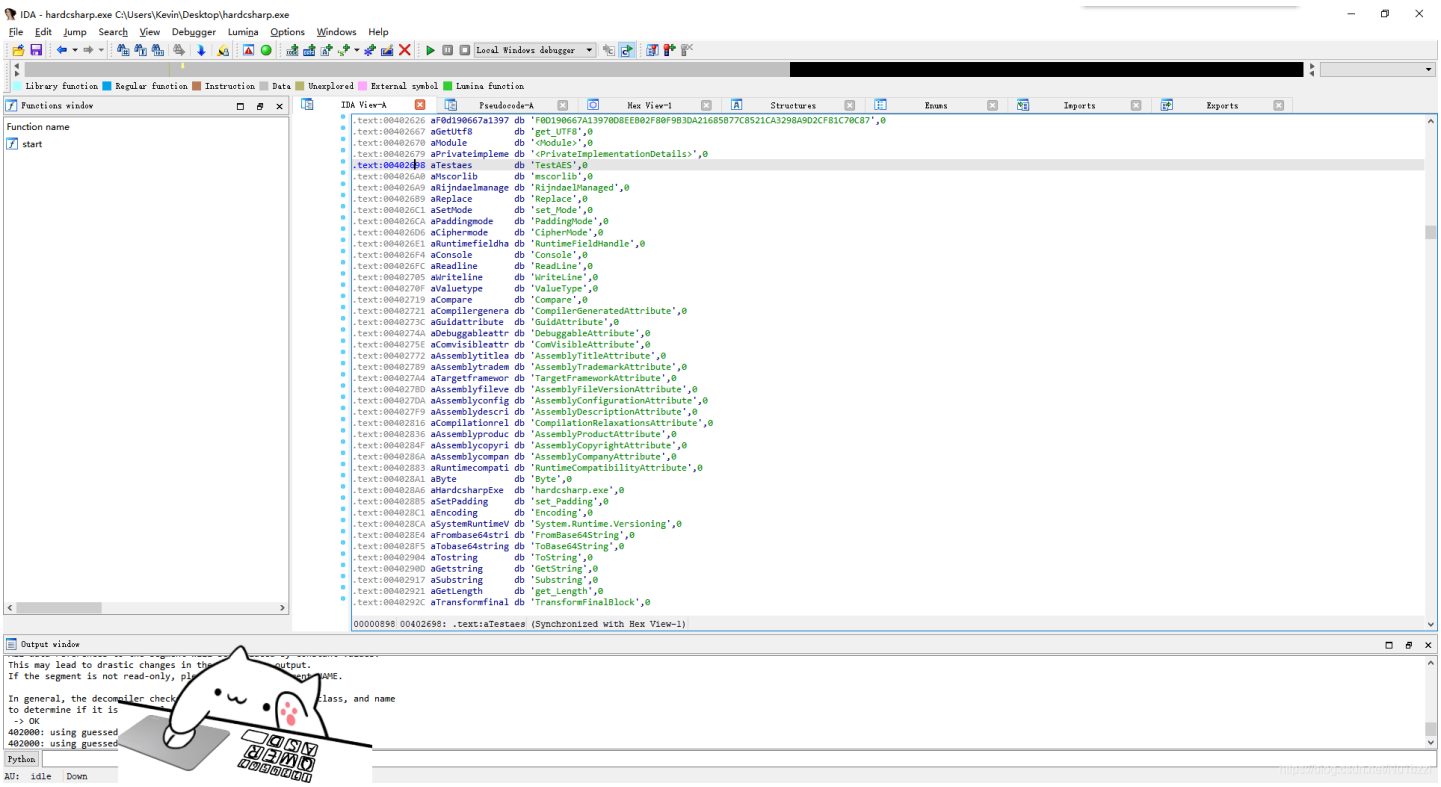
首先拿到文件第一步用PEiD查壳（养成好习惯）

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

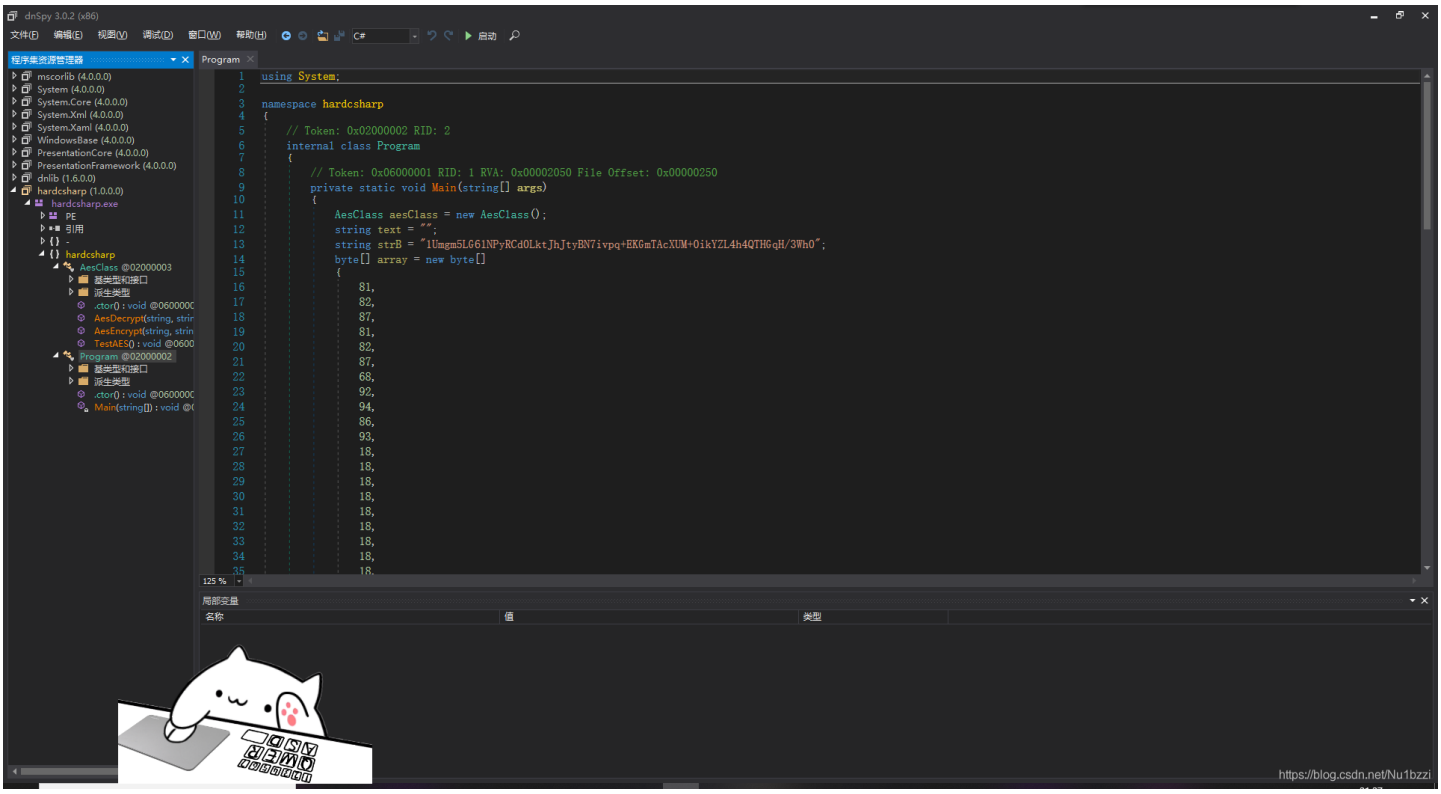


在放入时发现该程序是由.NET做的

进入后点进jmp后的函数果然发现了熟悉的东西

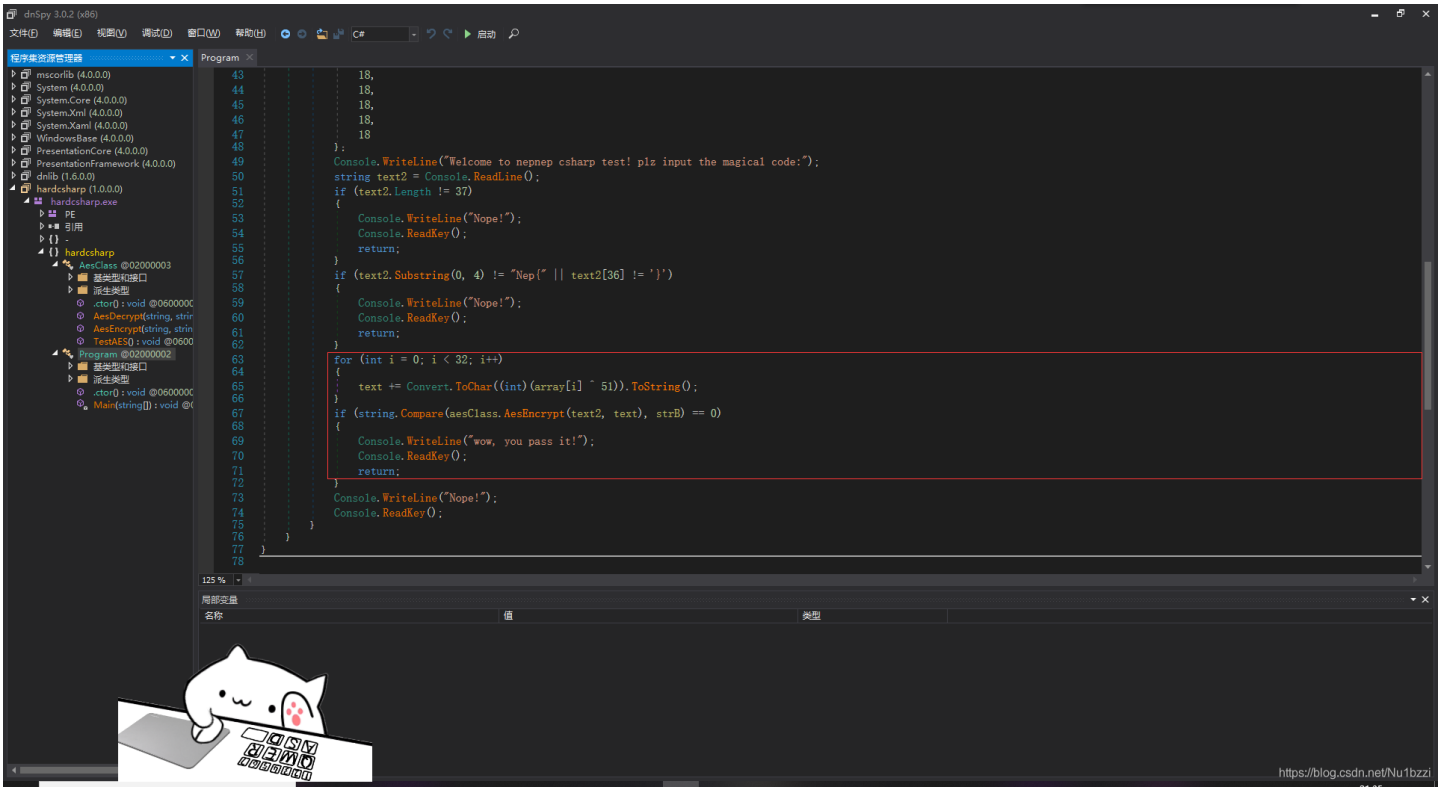


直接放入Dnspy中进行分析（Dnspy的详细使用方法和下载地址在这里□QAQ）



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



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)

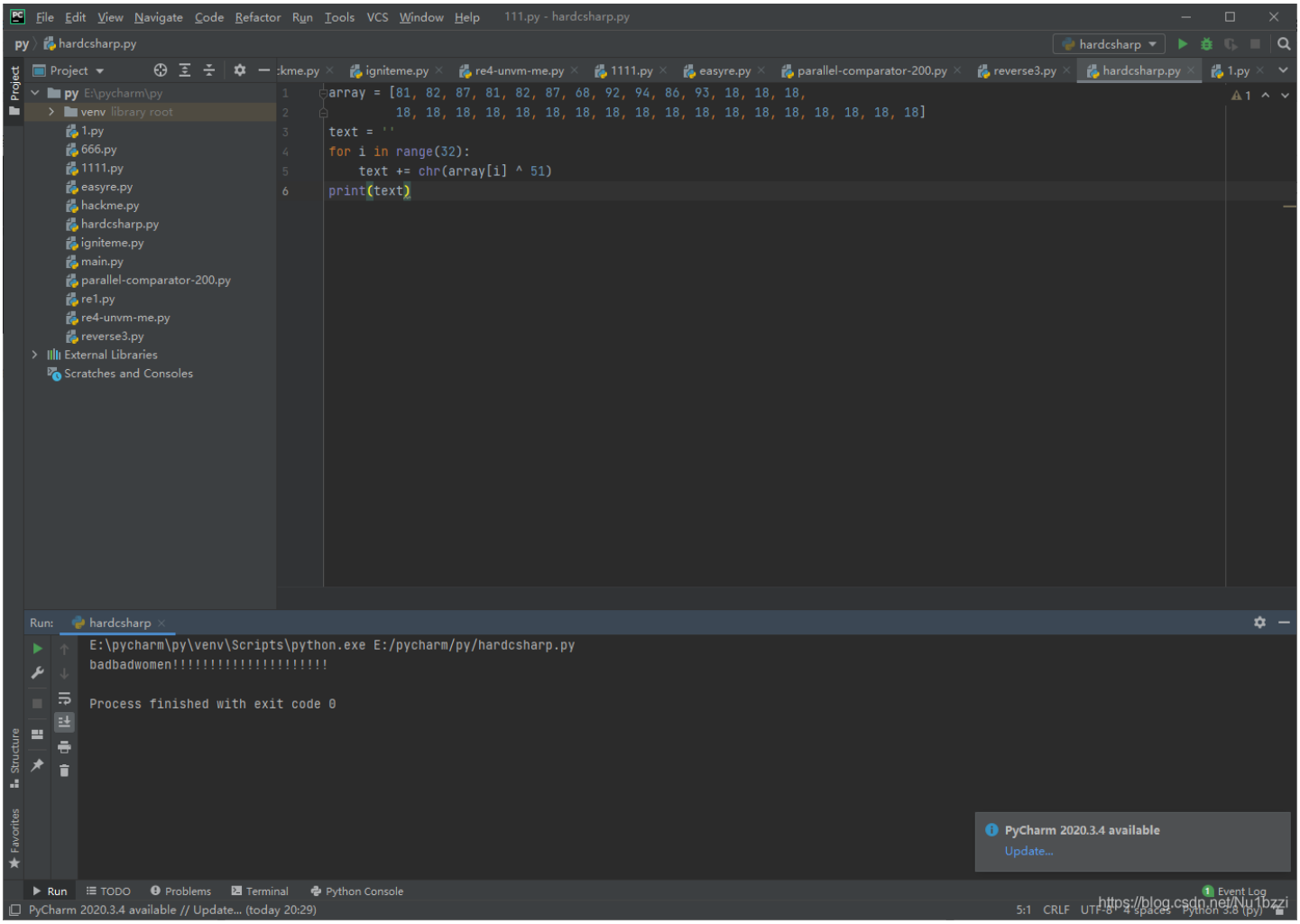
即需要满足这个条件才算正确，在不知道的情况下百度了之后发现AesEncrypt是一种加密运算：

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

简简单单写个小脚本`array = [81, 82, 87, 81, 82, 87, 68, 92, 94, 86, 93, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18] text = '' for i in range(32): text += chr(array[i] ^ 51) print(text)`



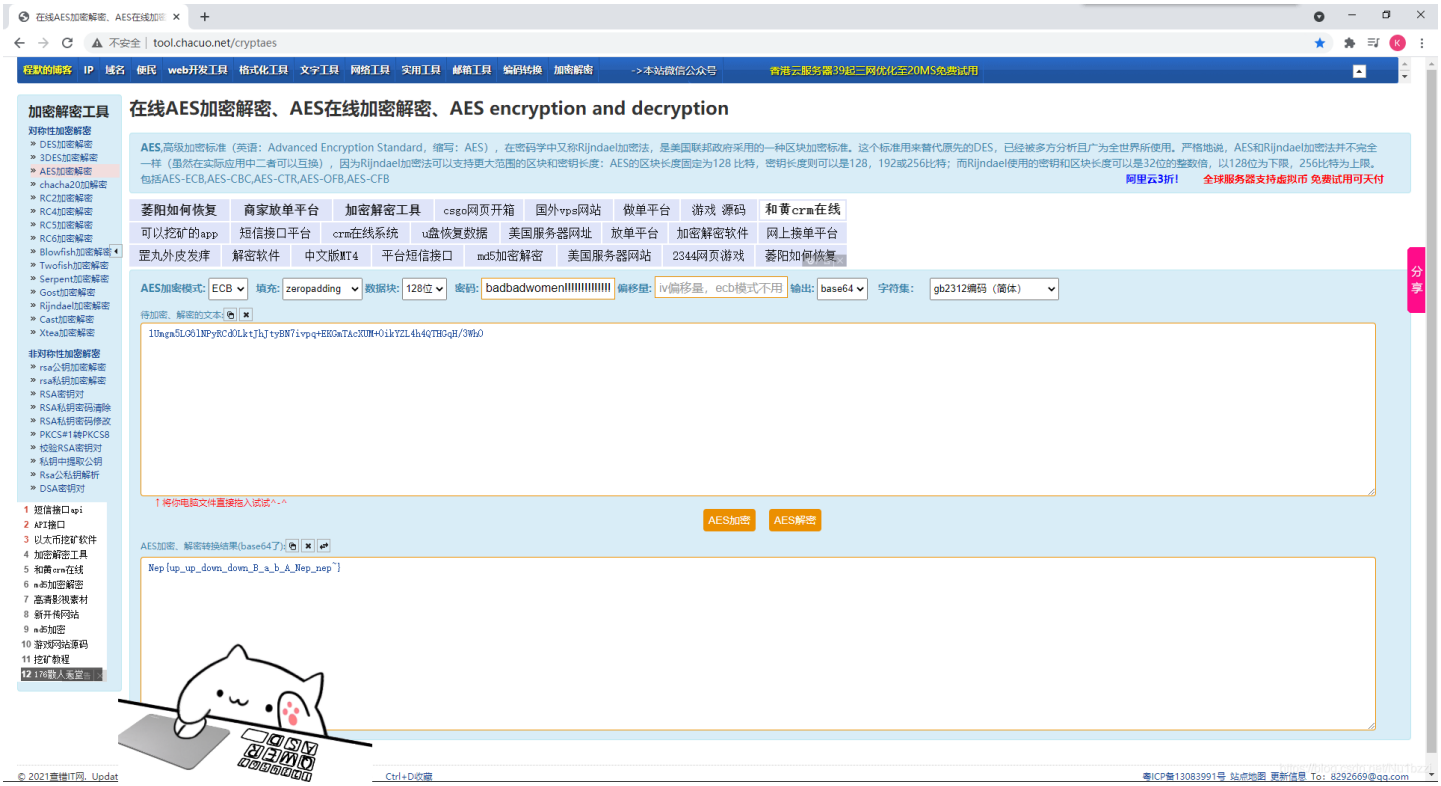
这个代码是得到的是text，即该程序中的AesEncrypt的密码key

我们需要的是明文text2

而if (string.Compare(aesClass.AesEncrypt(text2, text), strB) == 0)这串代码的意思就是：text2以text为密码进行Aes加密后要与strB一致才能pass it

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）



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