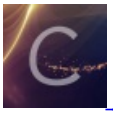
Kanxue看雪KCTF2019-Q1第十题【初入好望角】Writeup

原创

iqiqiya 于 2019-03-26 21:17:50 发布 361 收藏
分类专栏： 我的逆向之路 我的CTF之路 ------看雪KCTF2019-Q1 我的CTF进阶之路 文章标签： 初入好望角 KCTF2019-Q1第十题


我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏


------看雪KCTF2019-Q1
4 篇文章 0 订阅
订阅专栏

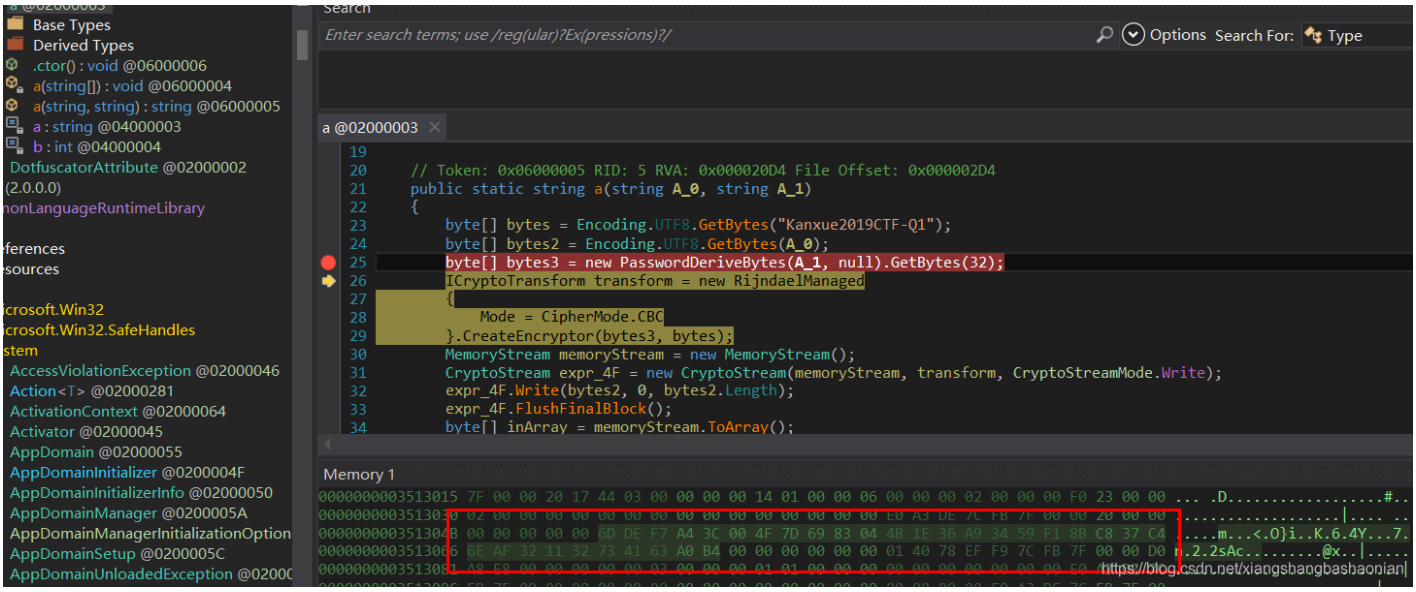
> 第十题：初入好望角

PEiD查到是C#编写的程序

直接用dnspy载入 得到源代码

```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;

// Token: 0x02000003 RID: 3
internal class a
{
 // Token: 0x06000004 RID: 4 RVA: 0x0000209B File Offset: 0x0000029B
 private static void a(string[] A_0)
 {
  Console.WriteLine("Please Input Serial:");
  if (global::a.a(Console.ReadLine(), "Kanxue2019") == "4RTlF9Ca2+oqExJwx68FiA==")
  {
   Console.WriteLine("Congratulations!  : )");
   Console.ReadLine();
  }
 }

 // Token: 0x06000005 RID: 5 RVA: 0x000020D4 File Offset: 0x000002D4
 public static string a(string A_0, string A_1)
 {
  byte[] bytes = Encoding.UTF8.GetBytes("Kanxue2019CTF-Q1");
  byte[] bytes2 = Encoding.UTF8.GetBytes(A_0);
  byte[] bytes3 = new PasswordDeriveBytes(A_1, null).GetBytes(32);
  ICryptoTransform transform = new RijndaelManaged
  {
   Mode = CipherMode.CBC
  }.CreateEncryptor(bytes3, bytes);
  MemoryStream memoryStream = new MemoryStream();
  CryptoStream expr_4F = new CryptoStream(memoryStream, transform, CryptoStreamMode.Write);
  expr_4F.Write(bytes2, 0, bytes2.Length);
  expr_4F.FlushFinalBlock();
  byte[] inArray = memoryStream.ToArray();
  memoryStream.Close();
  expr_4F.Close();
  return Convert.ToBase64String(inArray);
 }

 // Token: 0x04000003 RID: 3
 private const string a = "Kanxue2019CTF-Q1";

 // Token: 0x04000004 RID: 4
 private const int b = 256;
}
```

分析可以知道就是AES加密 用的是CBC模式 最后与“4RTlF9Ca2+oqExJwx68FiA==“相比较 若一致 则输入正确



解密代码如下

```
import base64
from Crypto.Cipher import AES
from binascii import b2a_hex,a2b_hex

miwen = base64.b64decode("4RTlF9Ca2+oqExJwx68FiA==")
iv = "Kanxue2019CTF-Q1"
key = ''.join([chr(i) for i in [0x6D, 0xDE, 0xF7, 0xA4, 0x3C, 0x00, 0x4F, 0x7D, 0x69, 0x83, 0x04, 0x4B, 0x1
cryptor = AES.new(key,AES.MODE_CBC,iv)
print cryptor.decrypt(miwen)
#Kanxue2019Q1CTF
```