

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/xiangshangbashaonian/article/details/88830542>

版权



[我的逆向之路](#) 同时被 3 个专栏收录

108 篇文章 10 订阅

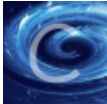
订阅专栏



[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: 0x0000209B
    private static void a(string[] A_0)
    {
        Console.WriteLine("Please Input Serial:");
        if (global::a.a(Console.ReadLine(), "Kanxue2019") == "4RT1F9Ca2+oqExJwx68FiA==")
        {
            Console.WriteLine("Congratulations! : )");
            Console.ReadLine();
        }
    }

    // Token: 0x06000005 RID: 5 RVA: 0x000020D4 File Offset: 0x000020D4
    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“4RTIF9Ca2+oqExJwx68FiA==”相比较 若一致 则输入正确

```

19
20 // Token: 0x06000005 RID: 5 RVA: 0x00020D4 File Offset: 0x00002D4
21 public static string a(string A_0, string A_1)
22 {
23     byte[] bytes = Encoding.UTF8.GetBytes("Kaxue2019CTF-Q1");
24     byte[] bytes2 = Encoding.UTF8.GetBytes(A_0);
25     byte[] bytes3 = new PasswordDeriveBytes(A_1, null).GetBytes(32);
26     ICryptoTransform transform = new RijndaelManaged
27     {
28         Mode = CipherMode.CBC
29     }.CreateEncryptor(bytes3, bytes);
30     MemoryStream memoryStream = new MemoryStream();
31     CryptoStream expr_4F = new CryptoStream(memoryStream, transform, CryptoStreamMode.Write);
32     expr_4F.Write(bytes2, 0, bytes2.Length);
33     expr_4F.FlushFinalBlock();
34     byte[] inArray = memoryStream.ToArray();

```

Memory 1

```

000000003513015 7F 00 00 20 17 44 03 00 00 00 14 01 00 00 06 00 00 02 00 00 00 F0 23 00 00 ... .D.....#..
000000003513016 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A3 DE 7C FB 7F 00 00 20 00 00 ... .....
000000003513017 03 00 00 00 00 00 6D DE F7 A4 3C 00 4F 7D 69 83 04 4B 1E 36 A9 34 59 F1 8B C8 37 C4 ... .m...<0}i..K.6.4Y...7.
000000003513018 6E AF 32 11 32 73 41 63 A0 84 00 00 00 00 00 00 01 40 78 EF F9 7C FB 7F 00 00 D0 ... .2sAc.....@x..|....
000000003513019 48 F8 00 00 00 00 02 00 00 00 01 01 00 00 00 00 00 00 00 00 00 00 00 00 50 ... ..

```

解密代码如下

```

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

miwen = base64.b64decode("4RT1F9Ca2+oqExJwx68FiA==")
iv = "Kaxue2019CTF-Q1"
key = ''.join([chr(i) for i in [0x6D, 0xDE, 0xF7, 0xA4, 0x3C, 0x00, 0x4F, 0x7D, 0x69, 0x83, 0x04, 0x4B, 0x1E, 0x36, 0xA9, 0x34, 0x59, 0xF1, 0x8B, 0xC8, 0x37, 0xC4]])
cryptor = AES.new(key,AES.MODE_CBC,iv)
print cryptor.decrypt(miwen)
#Kaxue2019Q1CTF

```