第一次参加ctf



yzj977 于 2

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/yzj977/article/details/80151788

版权

第一次写技术博客,可能写的很不好,请大家体谅!(之后还会有我上学期参加的acm题目,看我有没有时间写,一些oj的题目我也会发上来)

第一届XX大学网络安全技术对抗赛

Writeup模板

0x00 (题目名字)

操作内容:

XXXX

FLAG值:

第一题: misc(签到)



1.按照flag格式,把它复制黏贴就行,图:

第二题: misc (Steganography)

打开并下载:



://blog.csdn.net/yzj977

, 点击另存为桌面,

这个是属于隐写题,我用

Stegsolve,使用说明:下载好了是个安装包, stegsolveljar t/yz j977 , (不要解压!!这个我卡了一个晚上才清楚)

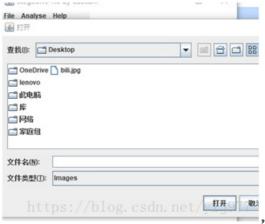
然后需要下载 Stegsolve.jar ,看到打开方式没?选择刚刚下载的



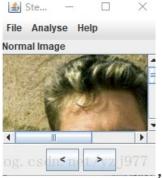
💃 JavaSetup8u171.exe

打开它,

,看到左上角的File了吗?点开,然后看到

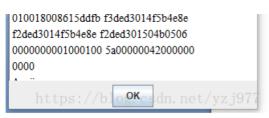


open了,把刚刚的bili.jpg图片加进去,

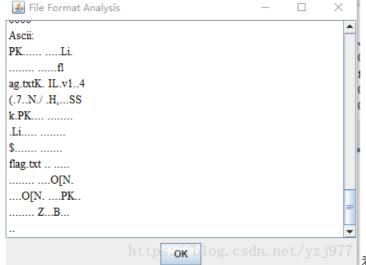


Analyes,点开选择第一个(File Format),看到这个





, 往下看一直看到它最后,



看到它显示的flag.txt没?证明图片包含了flag.txt。

y zbiji jipi gr

接下来, 关掉这些东西, 回到桌面, 看到

,更改后缀名,得到这个

,点开看到



看到flag.txt,打开它就是我们要的flag了,,把它输进答案吧。



第三题.crypto(Pig raising)

和上题一样打开后下载图片保存在桌面上。看了看图片,应该是猪圈密码(卡了我半天,各种工具试了一遍),话不多说,上图



对着写,得到PIGSTY,它题目后来改了!是的改了!不然我不知道这个要加上flag{...},害我交几次都不行,{}里面的东西就是这个密码,最后flag是flag{PIGSTY},提交ok



第四题: crypto (base64?)



人!),用base64在线解密或者包含base64的工具就行

看到这东西并不是



flag!!!还要用栅栏解密,

得到这个flag, g2uc ctf{Nice d0ct0r}, 提交



第五题: Reverse(ez.net)



同上面操作一样下载到桌面,得到这个

C:\Users\lenovo\AppData\Local\Temp\Rar\$EXa0.660\veryea

ts a kighPin:puzzleOso voicGüstNeedytőjinput:

什么玩意???随便输些内容,

a sign in puzzle so you just need to input: tepsykébbogutedn. net/yzj977

什么鬼???好的这道题我问了下q群的大佬们,被骂了一顿。。。(要注

意提问方式啊!),然后一位和蔼的大佬偷偷告诉了我用c#的反编译工具就行了(只学过c, c++, python的我

Reflector.exe

2015/3/3 12:15

应用程序

5,535 KB

```
Reflector.exe.config
                                                         2015/3/3 12:11
                                                                           XML Configurati...
                                                                                                   2 KB
                  ReflectorCmd.exe
                                                         2015/3/3 12:19
                                                                           应用程序
                                                                                                  16 KB
                                                                           应用程序 CSdn. net 9,533 KB 977
                   ReflectorInstaller.exe
                                                         2015/4/7 14:09
瑟瑟发抖)。
                                                                                                                下载之后,运行这个
 (这些都是我自己琢磨了这个工具一个小时耶,知道了使用方法,还有c#的一些语法和c/c++差不多。。。),
NET Reflector 8.5.0.179 - 14 days remaining
 File Edit View Tools Help
 G 5 | P ... 2 | A ... 2 / C#

∨ .NET 4.! ∨ 
✓
Search Object Browser (Ctrl-F)
⊕ -□ System (2.0.0.0)

⊕ -□ System.Xml (2.0.0.0)

    ⊕ - System.Web (2.0.0.0)

                                                                点开File.选择open (第一个),
                                                                                    NET Reflector 8.5.0.179 - 14 days rer
                                                                                     File Edit View Tools Help
                                                                                     NET Reflector 8.5.0.179 - 14 days re
                                                                                    - mscorlib (2.0.0.0)

■ CommonLanguageRuntimeLibrary

  銀行 * 新建文件完

 Resources
  ■ 点面 メヘ

■ - System (2.0.0.0)

■ - System.Xml (2.0.0.0)

   ♣ 下數
                                                                                    ■ - System.Data (2.0.0.0)

■ - System.Web (2.0.0.0)

   图 文档

■ - System.Drawing (2.0.0.0)

   FileRecy

■ - System, Windows, Forms (2,0,0,0)

    ⊕ - System.Core (3.5.0.0)

    20市場市田和

■ - System, ServiceModel (3.0.0.0)

    System.Workflow.ComponentM

    ⊕ - System.Workflow.Runtime (3.0.0.0)

  OneDrive
                                                                                    E MEDS
                              met/yzj977
                                                                                    ■ WindowsBase (3.0.0.0)
                                                     打开后看看这边的项目
                                                                                                                  往下翻,看到这个了
         ⊕ - System.Drawing (2.0.0.0)

    ₩ • WindowsBase (3.0.0.0)

         ☐ - ConsoleApplication1 (1.0.0.0)
        OS 🖪 📉 ConsoleApplication1.exe
没??
                                                      看到main函数里面吧
P .NET Reflector 8.5.0.179 - 14 days ren
 File Edit View Tools Help
 Search Object Browser (0

⊕ -□ WindowsBase (3.0.0.0)

                                               private static void Main(string[] args)
⊞ - PresentationCore (3.0.0.0)
⊕ - PresentationFramework (3.0.0.0)
                                                byte[] bytes = new byte[] {
0x66, 0x6c, 0x61, 0x67, 0x7b, 0x4e, 0x30, 0x77, 0x59, 0x76, 0x65, 0x6c, 90, 0x65, 0x72, 0x30, 0x21, 0x7d 0x30
⊟ -□ ConsoleApplication1 (1.0.0.0)
  ☐ In ConsoleApplication1.exe
   References
                                                   sole.WriteLine(*======="):
       - mscorlib
                                                Console.WriteLine(" = Veryeasy.net = ");

Console.WriteLine(" = Veryeasy.net = ");

Console.WriteLine(" ==============");

Console.WriteLine(" is a sign in puzzle so you just need to input:");

if (Base64Encode(Console.ReadLine()) == "UmVZZXJzZYNpZZ5pbiE=")
    B O -

    □ () ConsoleApplication1

       ⊕ 👣 Base Types
                                                      ole.WriteLine(Encoding.ASCII.GetString(bytes));
         octor()
                                                  Console.WriteLine("We dont have to try");
private static void Main(string[] args);
Declaring Type: ConsoleApplication1.Progra
          ConsoleApplication1, Version=1,0.0.0
Assembly:
                                               tps://blog.csdn.net/yzj977
 if (Base64Encode(Console.ReadLine()) == "UmV2ZXJzZVNpZ25pbiE=")
 {
   Console.WriteLine("");
   Console.WriteLine(Encoding.ASCII.GetString(bytes));
 else
```

Console.WriteLine("We don't have to try"); csdn. net/yz j977
和c/c++差不多的语法,只有输入这个才能正确执行



看到前面还写了Base64Encode了吗?提示我们要用base64解密,步骤也

和上面的base64解密一样。以下我再说一遍:,看到了解密后的内容了吗?打开 ,输入破解后的密



码ReverseSignin!,按回车,运行后得到flag:



以上为作者自己编写,未经允许,禁止转载(如需转载,请注明转载来源和作者名字)!!!(否则将依靠法律途径解决)