最详细攻防世界MISC新手区（已完结）小白解法

原创

开着拖拉机卖茄子 于 2020-04-05 22:47:25 发布 7404 收藏 47

分类专栏： 攻防世界解题集合 文章标签： 信息安全 经验分享 安全

本文链接：https://blog.csdn.net/qq_42906381/article/details/105335021

攻防世界MISC！安排

新手区已完结

001 this_is_flag

002 pdf

003 如来十三掌

004 give_you_flag

005 坚持60s

006 gif

007 掀桌子

008 ext3

009 stegano

010 SimpleRAR

011 base64stego

012 功夫再高也怕菜刀

新手区已完结

001 this_is_flag

flag就在眼前我却迟迟没有发现

002 pdf

根据题意，只需要把图片**移开**，就能发现flag

003 如来十三掌

原本以为这是一个隐藏文件，结果什么都没解出来
于是看着这段话，尝试读取佛文，果不其然，参悟了其中奥秘
猜这是一段密码，百度发现，需要进入一个名叫与佛论禅的网址解密

加上 佛曰 之后，解了一段base64编码，解密发现乱码

然后又发现这是一种**rot-13**加密方式

转化之后，再次解码

即得到flag

004 give_you_flag

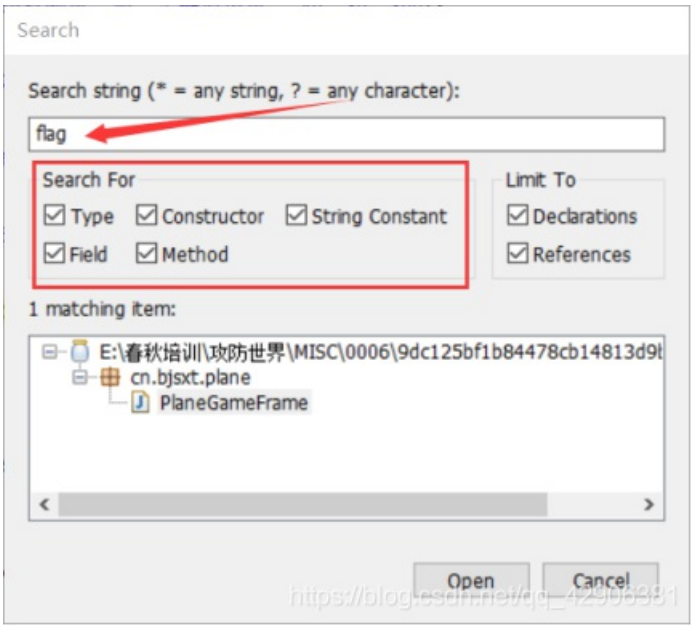
下载下来之后，发现真的是个表情包，里面还闪现了一个二维码！
利用**Stegsolve.jar** 打开之后，**Analyse-Frame Browser**一帧一帧的看
在50个发现了残缺的二维码

少了三个块块，想办法补上。PS可以补，但是涉及到我的知识盲区了,只好找朋友帮忙。
机缘就这么来了！
准备给同学截图的时候，忽然想起来qq截图还有**画笔**的功能！

试了试，成功了哈哈哈
微信扫描就出结果了！
一点都看不出来哈哈哈哈

005 坚持60s

下载之后发现可以进行反编译
下载个**java反编译器**，打开文件之后
英文应该不难懂，查找输入flag，全选上



得到位置，双击进入

看到flag，复制过去
提交不对，看见等号，想是不是base64，解码还真是！

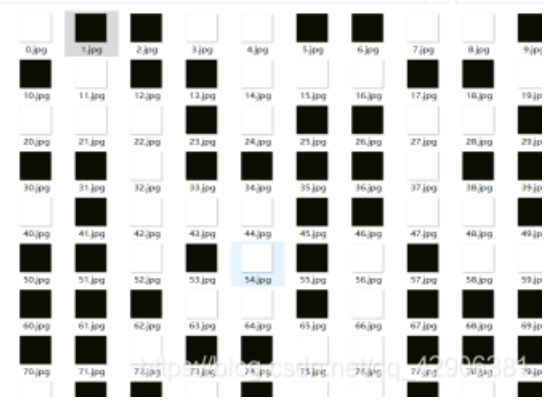
DajiDali_JinwanChiji

RGFqaURhbGlfSmlud2FuQ2hpamk=

得到flag

006 gif

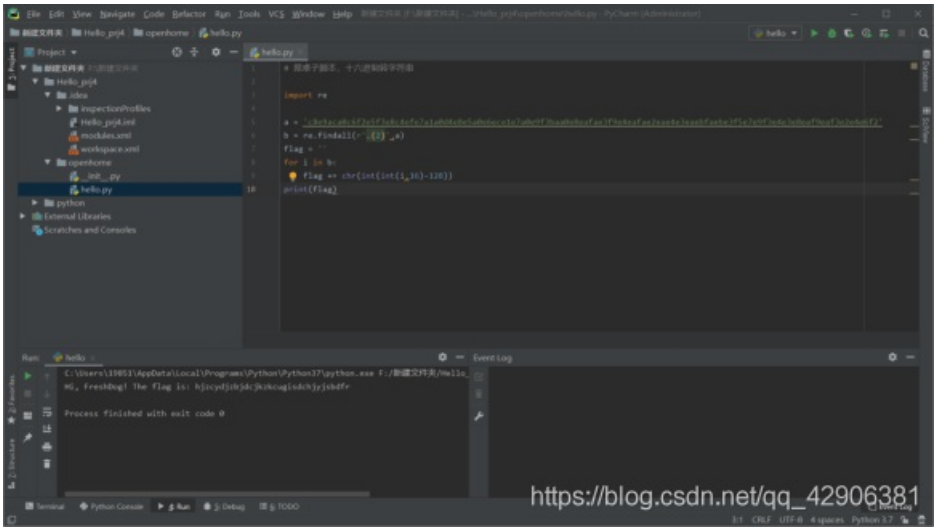
下载前以为是一个gif动态图
下载后发现事情没那么简单
居然是一个一个的黑白图片，看似有规律



难带代表什么东西？看了一眼手机上**电信公司10001**发来的短信
想到二进制！表示完之后，二进制转字符串得结果

007 掀桌子

这个题让我聪明的大脑无处安放
还是百度方法多
通过观察，试着将16进制字符转为字符串，发现不能直接转化，试着将ascii码值减去128再转化，得到flag.
两个一位，16进制转10进制，然后减去128再转成字符即可

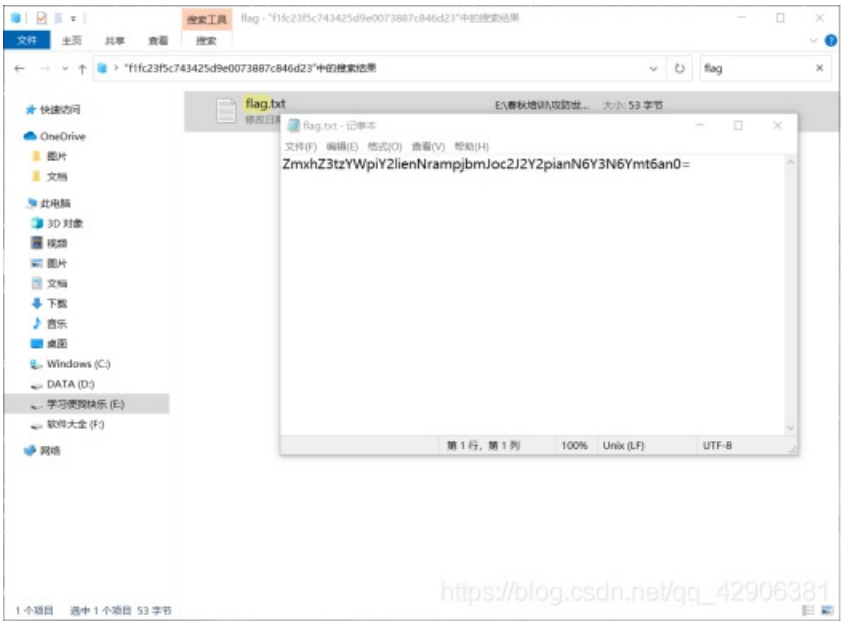


这样一整就出来结果了The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr
改格式就行了

008 ext3

这么明显的提示一定有问题！
倒不如直接用上次说到的**foremost**
一下子就整出了哈哈哈

打开图片之后把flag输进去就发现事情没这么简单
居然是**错的**！
又想起来这种东西都能够解压，于是改后缀，解压，然后搜索flag



发现了一个.txt打开，=结尾用base64解码

得到flag

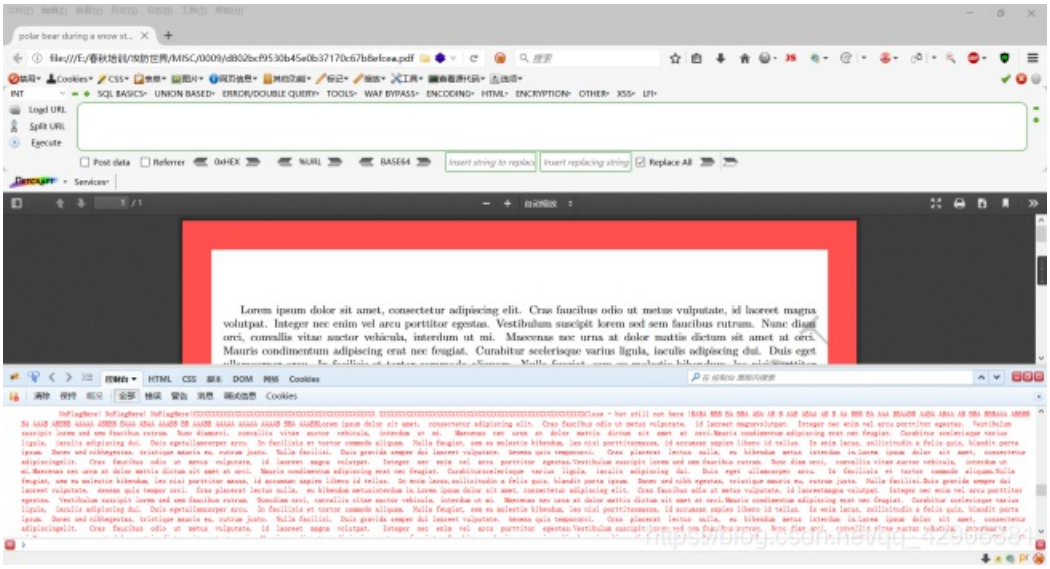
009 stegano

用火狐浏览器打开刚才下载的pdf文件

按下**F12**进入控制台，输入**document.documentElement.textContent**

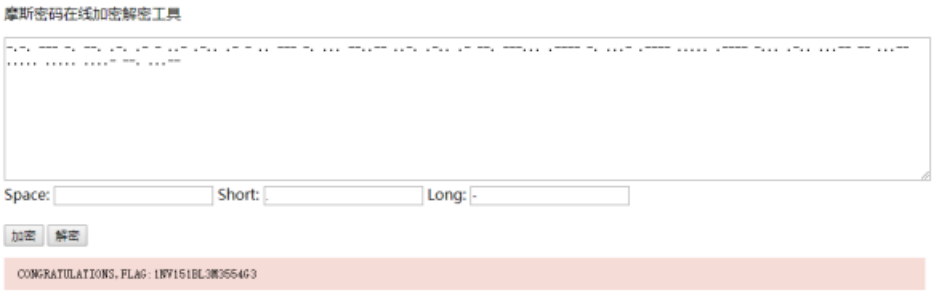
回车查看

BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB



发现一大段AABABA样式的东西，猜测是01但是这些有分割，能想到的只有摩斯密码有分割的，于是尝试改成摩斯密码（卑微的我只能一个一个改）

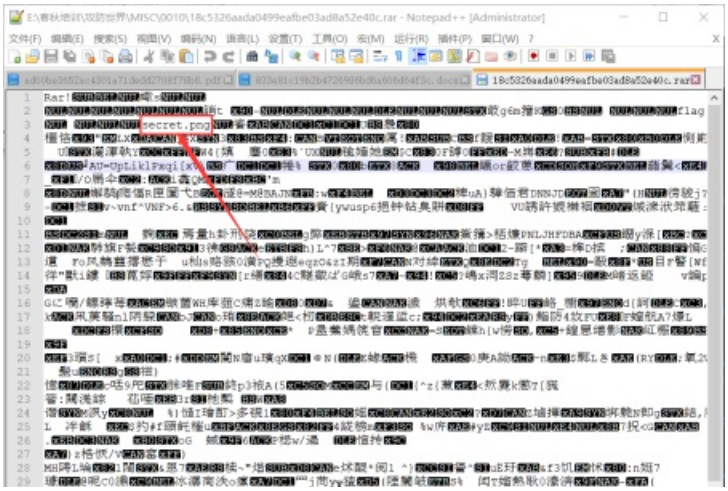
-.-. — -. --. .-. .- - ...- .-... .- - ... — -. ... –...– ...-. .-... .- --. —... .---- -. ...- .---- ... .---- -... .-... ...– – ...– ... ...- -. ...–



发现flag

010 SimpleRAR

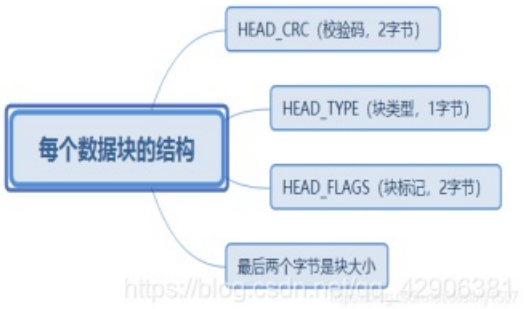
下载文件之后，解压只有一个.Txt文件，但是用**Notepad++打开，发现了不一样的.png**



猜测应该是丢失了。寻找方法。

顺便整了一波大佬的学习笔记

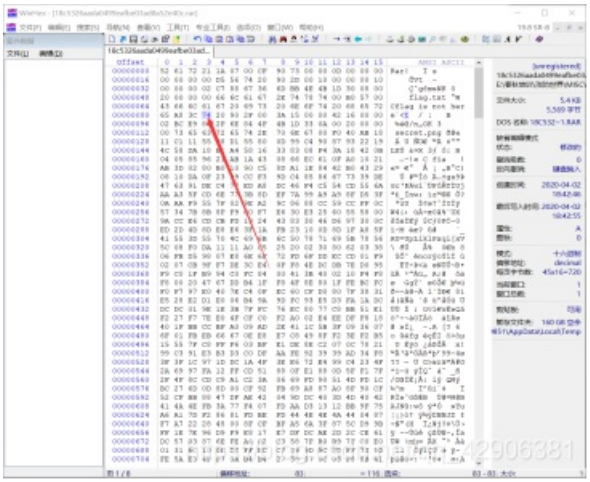
大佬笔记



尽管还是不太懂

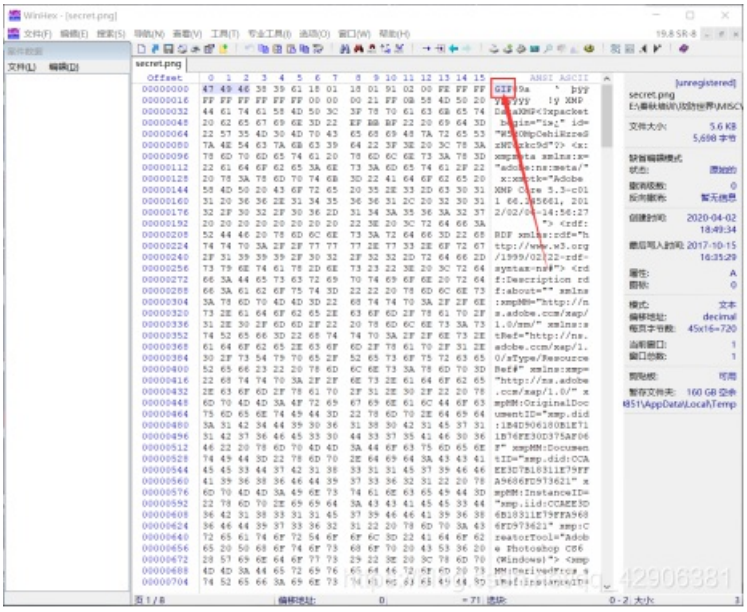
但依旧掌握了精髓！

把箭头处的7A改为74再次保存解压



发现出现了一个名为**secret.png**的文件

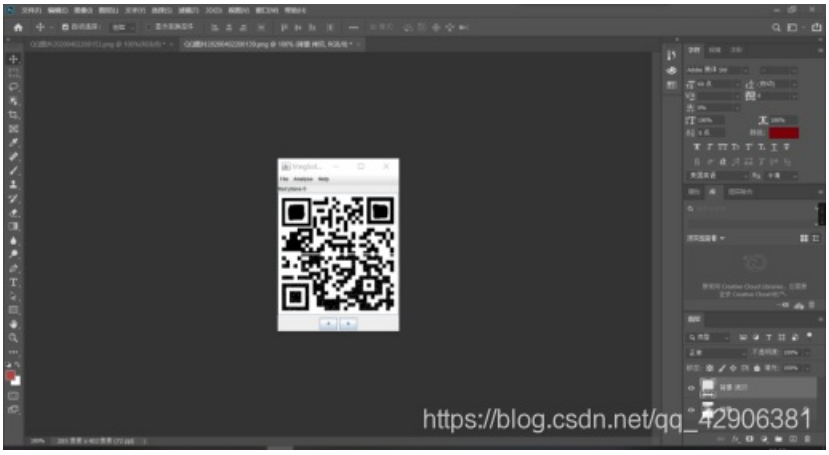
拉进**Winhex**打开，看见了开头的**gif**



改后缀之后打开是一张单纯的白纸
然后用上我毕生所学的PS技能
打开之后发现里面有两个白底图层，分离出来
再用**StegSolve.Jar**打开直接点下面的左右符号，进行调色曝光
得到下面两张图片

这一张是下半部分

右边那张是经过我细心处理又加上角块后的图片
然后再次打开PS继续使出毕生所学，把两张图片合成在了一起



再次打开曾经用过的**QR-Research**,直接得出了flag

011 base64stego

这个题再一次证明了Python的重要性！吹爆Python

不多说，下载完文件直接解压就能发现一个.txt文件

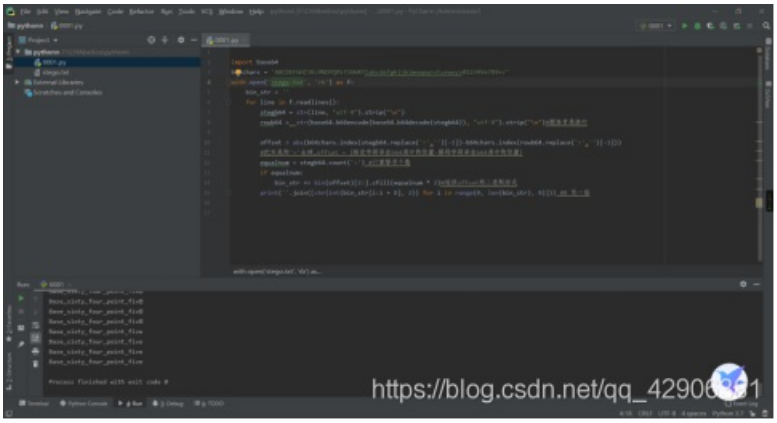
然后百度知道这个题是一种base64位的加密版

然后顺便研究了研究：

原文链接

还是好迷糊啊

找到python代码之后运行



得到flag

我要是会python能卑微的去看别人的代码？？？？？

012 功夫再高也怕菜刀

下载之后利用**foremost**获得一个压缩包，解压发现需要密码

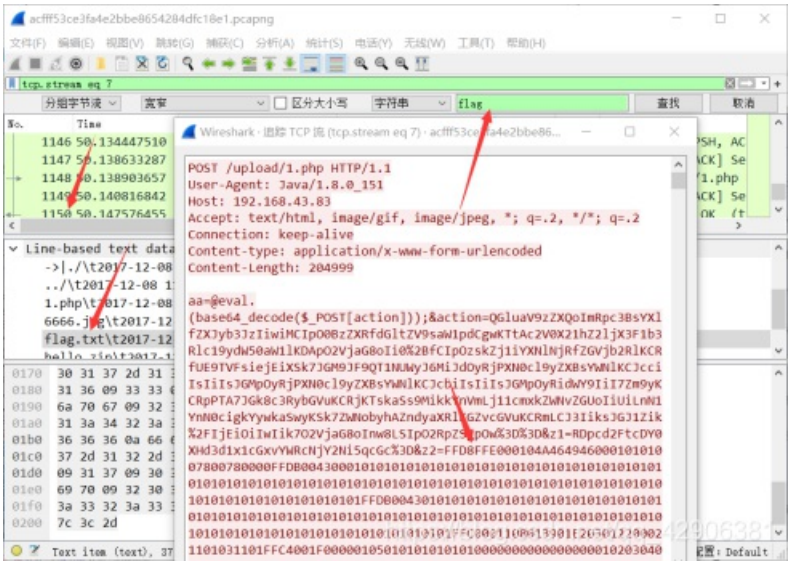
于是追踪数据流

CTRL+F搜索flag，发现了一个文本文档

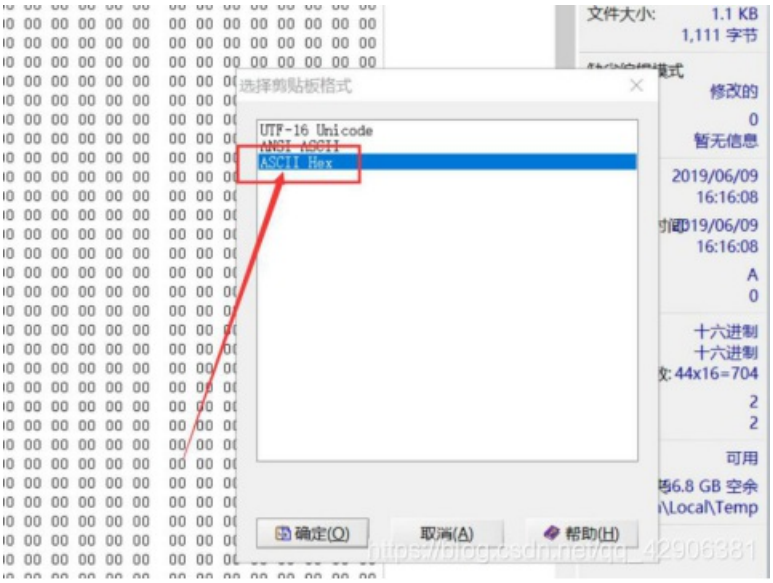
对他进行追踪**TCP流**

点击下面的**Save as**...保存到本地

然后从 FFD8FF 开始到 FFD9 复制出来



再利用Winhex
把那些粘贴进去，并选择到**ASCII HEX**
进行写入



按照.jpg保存下之后，就可以得到一张图片
这个图片中的字符就是解压密码
输入即可得到flag