[CTF]Dino安全小组第三次内部赛“remix_欧皇的游戏2.0”Writeup

原创

∑on. 于 2021-04-05 22:35:26 发布 99 收藏 1

文章标签： 信息安全 反编译 加密解密

本文链接：https://blog.csdn.net/bvygcty/article/details/115450021

[CTF]Dino安全小组第三次内部赛“remix_欧皇的游戏2.0”Writeup

前言

你好！ 这是一个大一网安专业学生的第一篇博客，同样也是我自己第一次出题的wp。如有错误请各位大佬批评指正（respect!）

题目描述

几个月之前，出题人的小游戏被人轻而易举的解开了，出题人很生气，所以推出了这款游戏的2.0版本，但是出题人觉得题出的有点难了，所以出题人决定告诉你们密码是**MD5**。这是欧皇的游戏，只有欧皇才能获得最后的胜利！（出题人的QQ签名是7wrd）

题目附件戳：这里 密码:b66b

Reverse部分

这个题得到一个压缩包，解压后得到一个.exe程序，根据程序的图标判断，应该是python脚本打包成.exe文件。

方法一：

拼运气：这个题最开始就是从1到300中随机抽取一个数字，总共有三次机会，每次猜错会告诉你数字与正确答案的大小关系，可以靠运气当欧皇猜对得到线索。

方法二

考点一：反编译python打包的.exe文件

参考链接：https://www.cnblogs.com/QKSword/p/10540431.html

反编译后得到py文件（即程序源码）

```
print('--------------Dino出品--------------')
import random
answer = random.randint(1, 300)
times = 3
while times > 0:
    temp = input('猜猜Eon.心里在想哪个数字吧！：')
    guess = int(temp)
    if guess == answer:
        print('哇哇哇，你是宇阳心里的蛔虫吗？')
        print('好了好了，给你奖励')
print('U2FsdGVkX1/k5Mm7uWjmDgqM6U7eizZkAnCQ/R7KWCry+ofsnt+kPvDvgHtju/TqLh8qL0koIKkEdZWJwjHiKA==')
        print('还少个东西？？在我的QQ签名里找吧！')
        break
    else:
        if guess < answer:
            print('小了小了')
        else:
            print('大了大了')
        times = times - 1
print('Game over!')
```

得到神秘字符串：
U2FsdGVkX1/k5Mm7uWjmDgqM6U7eizZkAnCQ/R7KWCry+ofsnt+kPvDvgHtju/TqLh8qL0koIKkEdZWJwjHiKA==

Crypto部分

考点二：DES解密
根据题意，‘密码’是MD5，但如果MD5加密后的字符串不会出现‘=’号，所以这里的密码的种类不可能是MD5，进而猜测是DES加密，密文是‘MD5‘。
解密后得到新的字符串：
aHR0cHM6Ly93d3MubGFuem91cy5jb20vaU5PTVdramhrdWI
考点三：base64解码
字符串经过base64解码后得到网址：https://wws.lanzous.com/iNOMWkjhkub
进入蓝奏云的文件分享，根据反编译得到的另一个提示：
还少个东西？？在我的QQ签名里找吧！
社工出题人的QQ，发现密码(本来是内部赛嘛，大家都认识，找签名很容易，但是这里直接就在题目里把QQ签名嘻嘻)

下载文件压缩包。至此题目进入misc阶段

Misc阶段

考点四：图片隐写
得到一张624kb的图片，但是这张图片的清晰度低，所以一定藏着什么东西，用winhex打开，搜索文件头

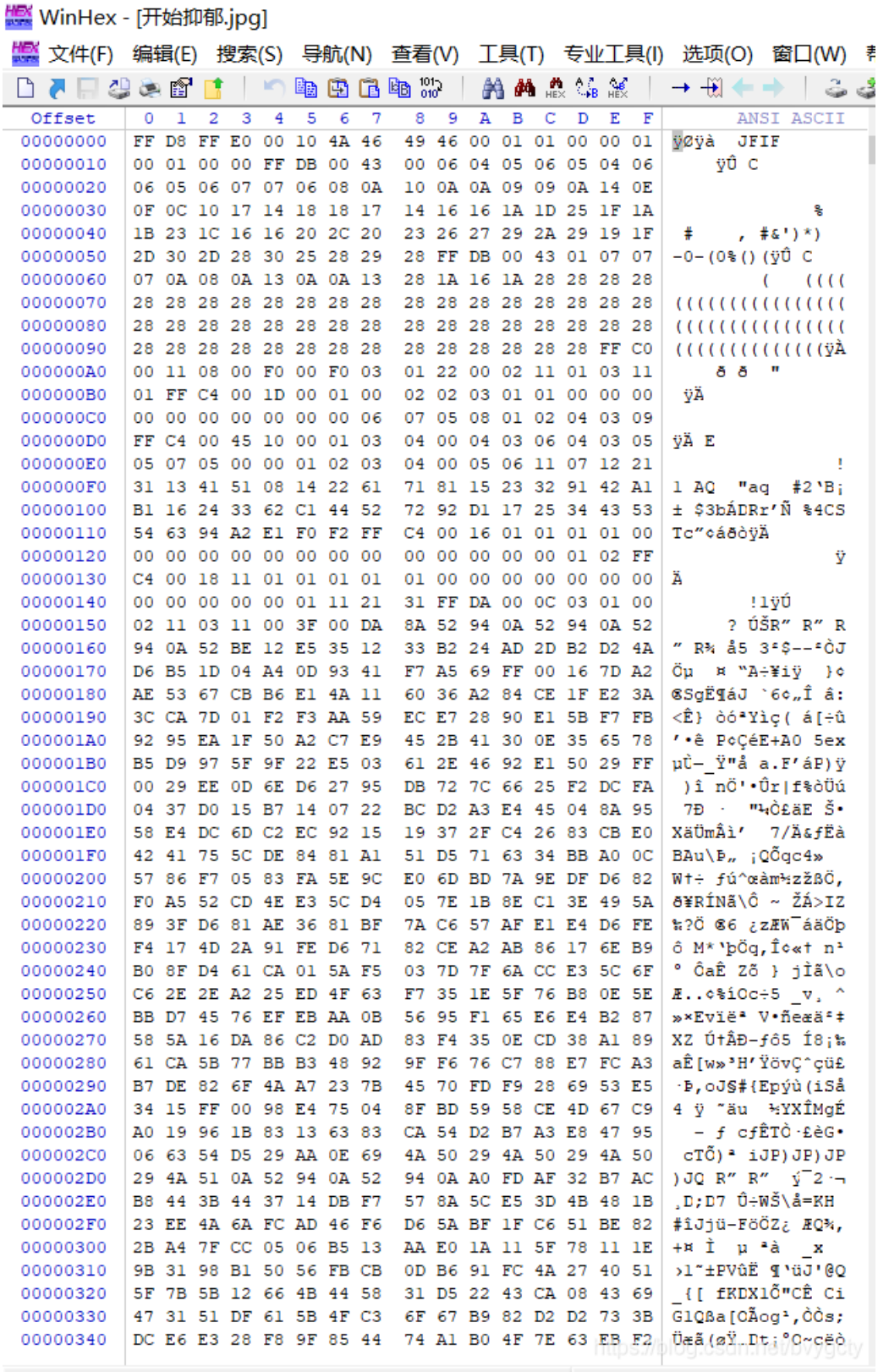
常见文件头图片:

各文件的文件头和尾标识符

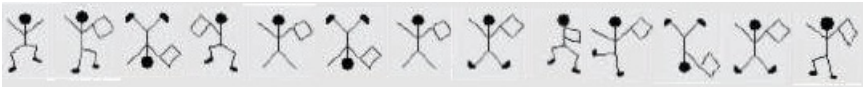
GIF文件头：47 49 46 38 39 61
JPG文件头：FF D8 FF E0 00 10 4A 46 49 46
FF D8 FF E1 00 10 4A 46 49 46
JPG文件尾：FF D9

PNG文件头：89 50 4E 47 0D 0A 1A 0A
PNG文件尾：00 00 00 00 49 45 4E 44 AE 42 60 82
PSD文件头：38 42 50 53
TIFF文件头：49 49 2A 00
BMP文件头：42 4D

Rar文件头：52 61 72 21
zip文件头：50 4B 03 04



发现小小的一张图片其中竟又藏着两张图片和一个压缩包。



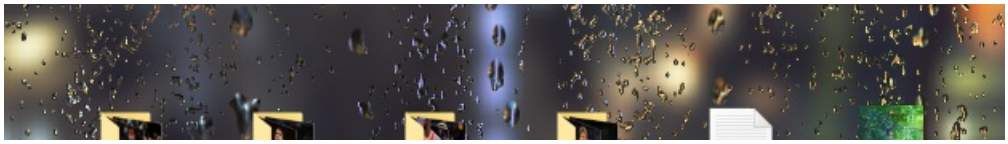
考点五：图片处理工具的熟练运用
得到一张缺失的二维码，利用图片处理工具补全，

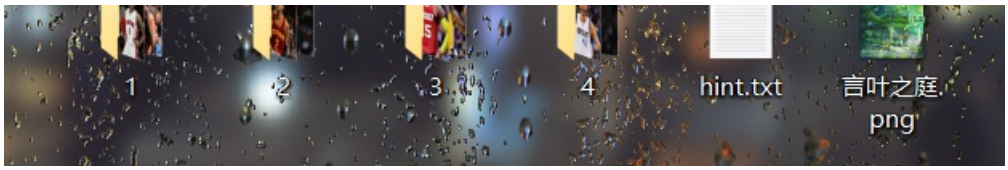
扫描得到以下字符串：
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook. Ook! Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook! Ook. Ook! Ook. Ook! Ook. Ook! Ook. Ook! Ook. Ook? Ook.

考点六：Ook编码
利用在线解密网站：https://www.splitbrain.org/services/ook
解码得到神秘数字：20020613111111（出题人的生日）

考点七：unix时间戳
得到数字，想要解开压缩包，结果密码错误，根据图片名称“开始抑郁“猜测经过unix时间戳转换

得到压缩包密码“1023937871”，解开压缩包，得到如下东西





考点八：福尔摩斯密码

打开分离的另一张图片，发现是福尔摩斯密码，对比对照表解出小人密文：

WATCH THE VIDEO

考点九：哔哩哔哩的熟练掌握

根据给出言叶之庭电影的海报和观看地址，以及解出的提示“WATCH THE VIDEO“和hint的笔记本

以及每个部分文件夹对应的球员球衣号

得到解出答案的方法：寻找电影中各个时间出现的单词组成最后的flag

时间点

1：40————LUMINE

2：00————EXIT

15：27————IANA

41：14————LADY

所以最后的flag：

dino{LUMINE-EXIT-IANA-LADY}

证毕。