ctf攻防世界misc writeup

原创

OceanSec 于 2020-03-15 11:08:17 发布 8677 收藏 1

分类专栏： # CTF

本文链接：https://blog.csdn.net/q20010619/article/details/104875173

CTF 专栏收录该内容

66 篇文章 29 订阅

订阅专栏

misc：

this is flag：

直接get flag

pdf：

将pdf文档转换为word文档，移动图片显示下方隐藏的flag

如来十三章：

与佛论禅->rot13->base64

坚持60秒：

下载文件使用反编译工具xjad进行反编译，打开文件夹使用vscode打开PlaneGameFrame.java文件，找到flag，将内容base64进行解码得到真正的flag。

give your flag

使用stegslove打开文件使用flame模式发现残缺二维码使用ps补全

菜狗截获了一张菜鸡发给菜猫的动态图，却发现另有玄机

图片: https://uploader.shimo.im/f/wps4BdwghDUr9SxA.png图片: https://uploader.shimo.im/f/eGBFlRLoY5sHVKKe.png图片: https://uploader.shimo.im/f/kJ82hxku21Ml4T2X.png

掀桌子

图片: https://uploader.shimo.im/f/c3maiLvonUEWNceD.png

simpleRAR

1.使用winrar打开rar文件，发现内含一个png文件，而文件头有误图片: https://uploader.shimo.im/f/XHmG0j18g3Mv0227.png

2.在010将7A改为74，提取出png图片

图片: https://uploader.shimo.im/f/ZWcktW9R4G0s9k5R.png

3.将文件后缀改为gif使用stegsolve查看文件发现隐藏损坏二维码，题目提示为：双图层使用ps打开，发现两个相似图层，分别保存，分别使用stegsolve打开发现两个残缺二维码，使用ps将其拼合并加上定位符号

4.使用QR research扫描

图片: https://uploader.shimo.im/f/A6tKYQbEwrcHbY5z.png

使用010editor打开文件发现文件为伪加密，修改压缩源文件目录的标记为00打开文件
图片: https://uploader.shimo.im/f/qkWiLPbvLR82Klo8.png
txt文件为base64的加密文件进行解密得到flag
图片: https://uploader.shimo.im/f/bbt28gy1pgwOB0ZC.png
功夫再高也怕菜刀
附件是一个流量包，使用foremost分离出一个有密码的压缩包，压缩包里的文件名为“flag.txt”，所以剩下的就是找解压密码
图片: https://uploader.shimo.im/f/fbJ9EzHM1DwpTg5l.png
1