

# 【愚公系列】2022年01月 攻防世界-进阶题-MISC-79(双色块)

原创

愚公搬代码 于 2022-01-30 20:02:23 发布 6840 收藏

分类专栏: #CTF-攻防世界-MISC 文章标签: 网络安全

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/aa2528877987/article/details/122754982>

版权



[CTF-攻防世界-MISC 专栏收录该内容](#)

98 篇文章 0 订阅

订阅专栏

## 文章目录

[一、双色块](#)

[二、答题步骤](#)

[1.下载附件](#)

[2.脚本破解](#)

[3.foremost分离](#)

[4.DES解密](#)

[总结](#)

## 一、双色块

题目链接: [https://adworld.xctf.org.cn/task/task\\_list?type=misc&number=1&grade=1&page=5](https://adworld.xctf.org.cn/task/task_list?type=misc&number=1&grade=1&page=5)

百度一下，你就知道 学习教育 博客论坛 谷歌工具 开发文档 备考资料 网络安全 福建铁塔运营管理... 前端开发文档

其他收藏夹

返回 本题用时: 1分48秒

双色块 最佳Writeup由系统战队·admin提供

WP 建议

难度系数: ★★★★ 4.0

题目来源: 网鼎杯

题目描述: 分离

题目场景: 暂无

题目附件: 附件1

实时消息

用户逸瑾解出Pwn方向《CGfsb》,获得6.0积分,6金币,耗时29分20秒  
2022-01-30 19:01:07

用户plant44744解出Reverse方向《game》,获得3.0积分,3金币,耗时17分44秒  
2022-01-30 19:01:07

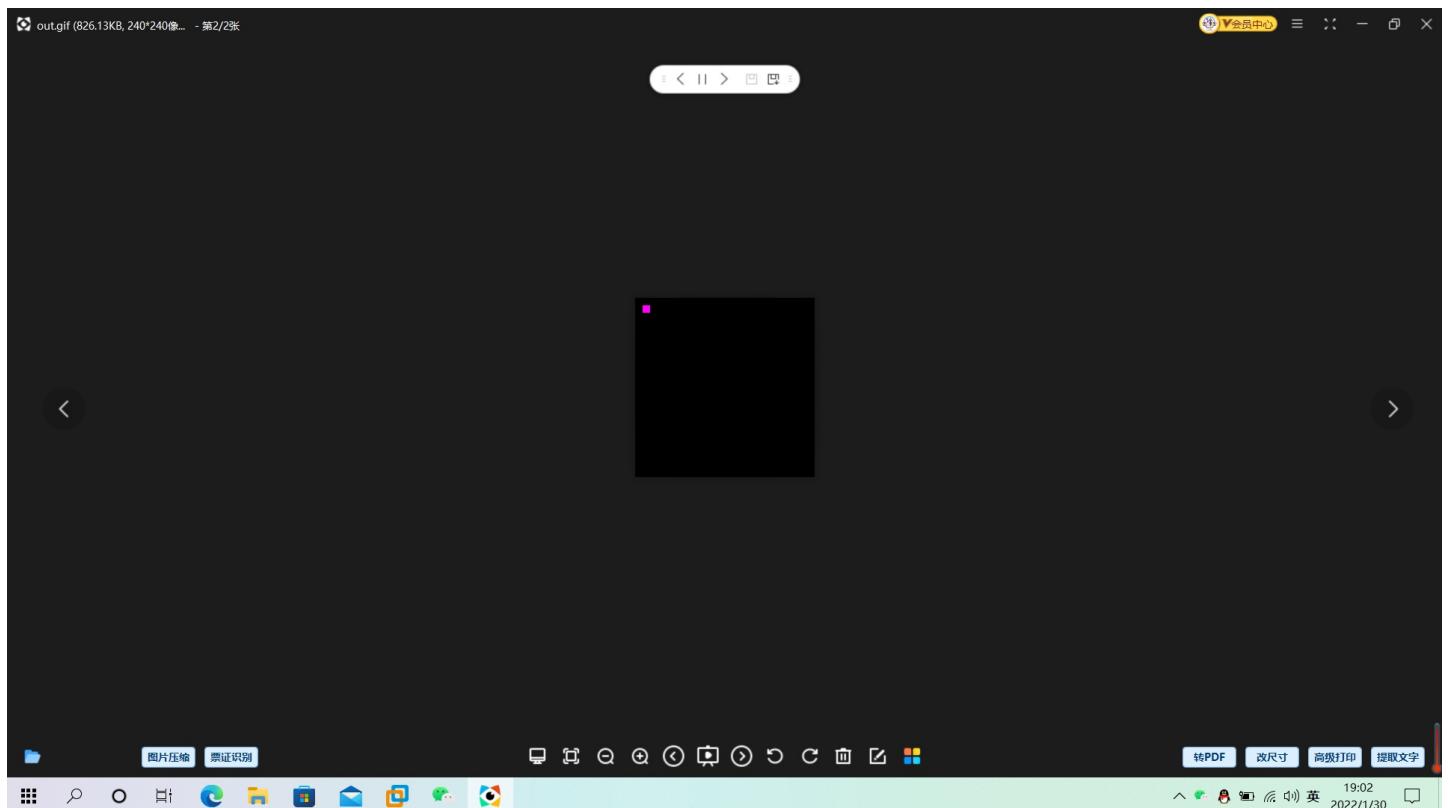
flag..

XCTF高校网络安全专题挑战赛 19:01 2022/1/30

## 二、答题步骤

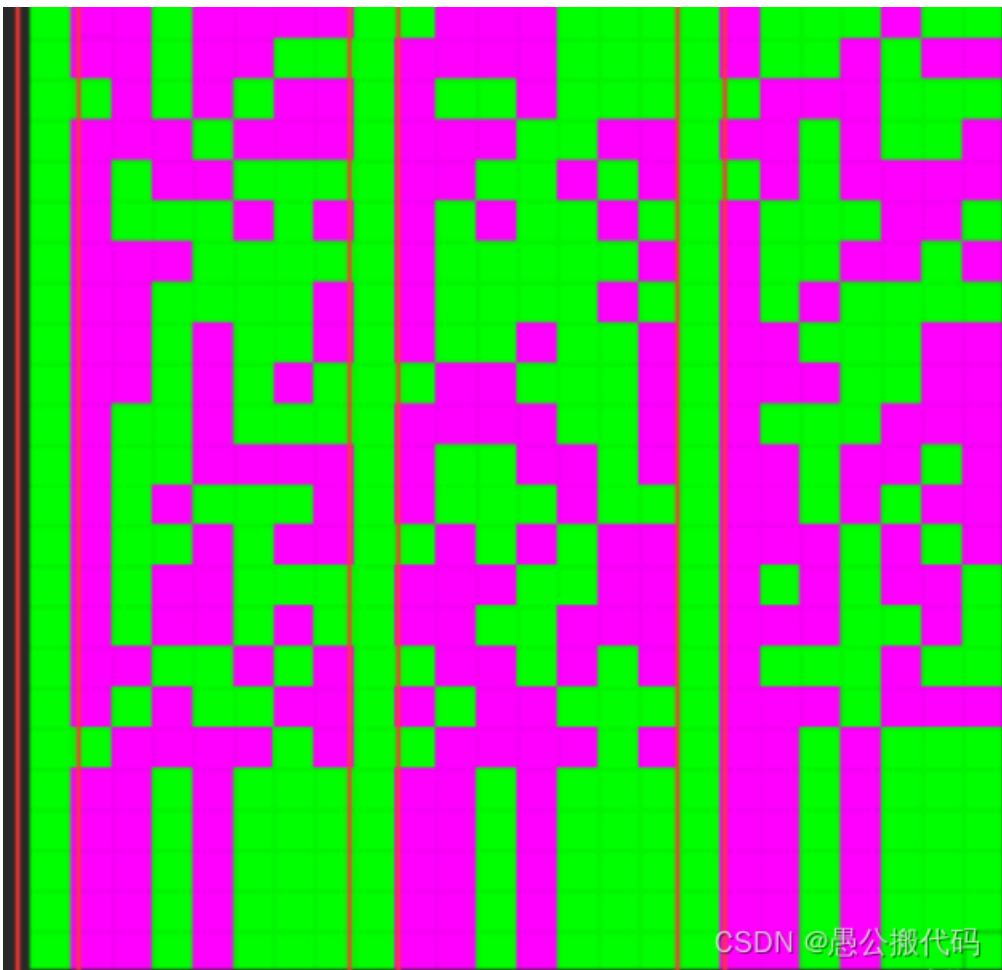
### 1. 下载附件

得到一个图片



用ps录制发现颜色规律





得到如图所示

- 一行是24个格,  $3 \times 8$ , 应该是8个一组
- 每组的第一个颜色都是一样的, 应该是ASCII码, 第一位是0,
- 所以绿色是0, 红色是1

## 2.脚本破解

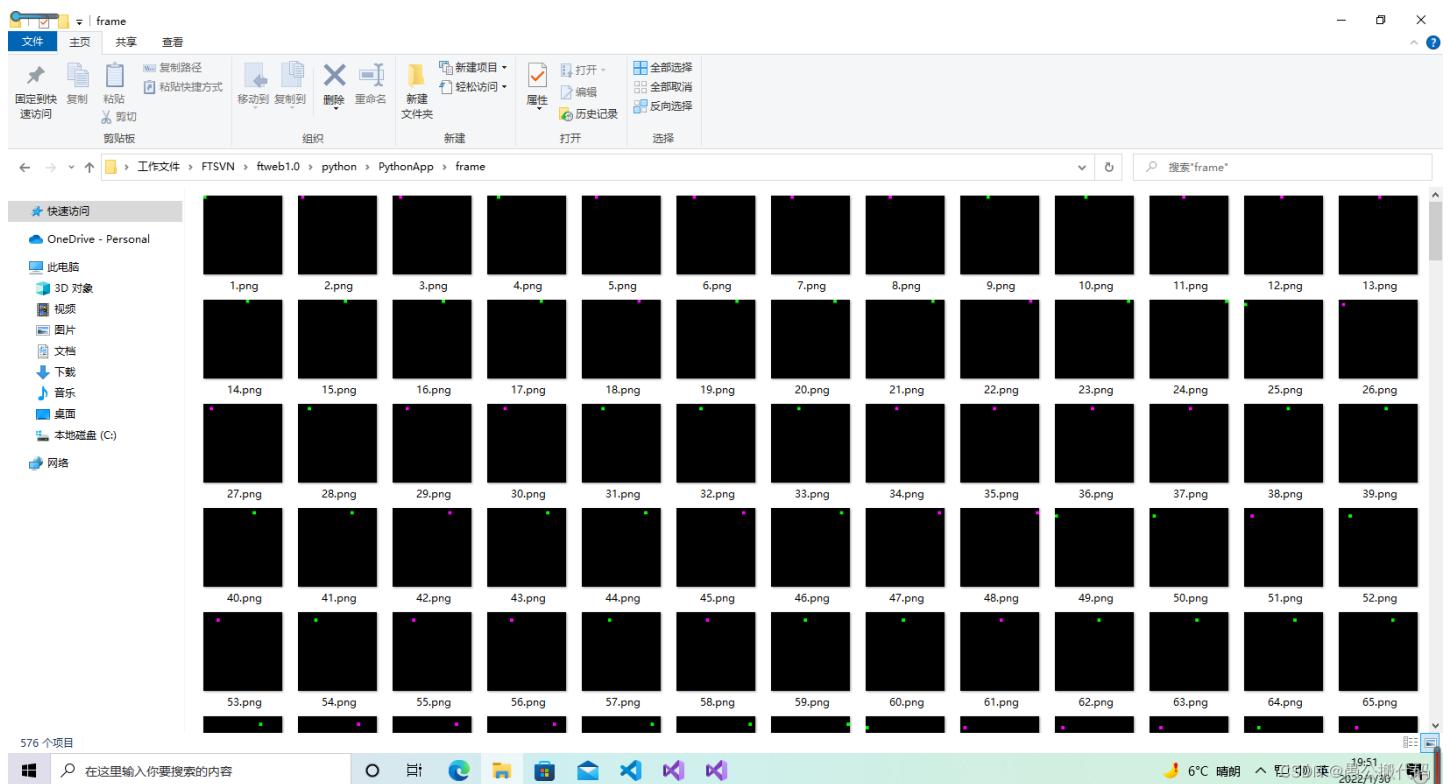
首先解析gif图片分离成单帧模式

```
#!/usr/bin/env python2
# -*- coding: utf-8 -*-

import os
from PIL import Image

def main(gif_file):
    png_dir = 'frame/'
    img = Image.open(gif_file)
    try:
        while True:
            current = img.tell()
            img.save(png_dir + str(current + 1) + '.png')
            img.seek(current + 1)
    except:
        pass
if __name__ == '__main__':
    gif_file = 'out.gif'
    main(gif_file)
```

## 得到frame文件夹



然后读取每个png中的对应点的信息，并按照8bit转换为ascii

```
#!/usr/bin/env python2
# -*- coding: utf-8 -*-

import os
from PIL import Image

def main():
    png_dir = 'frame/'
    ret = ""
    for i in range(0,24):
        line = ""
        for j in range(0,24):
            file_name = "frame/" + str(i * 24 + j + 1) + ".png"
            x = j * 10 + 5
            y = i * 10 + 5
            img = Image.open(file_name)
            img = img.convert("RGB")
            img_array = img.load()
            r, g, b = p = img_array[x, y]
            if g == 255:
                line += "0"
            if r == 255 and b == 255:
                line += "1"
            if len(line) == 8:
                ret += chr(int(line, 2))
                line = ""
    print(ret)

if __name__ == '__main__':
    main()
```

运行脚本得到

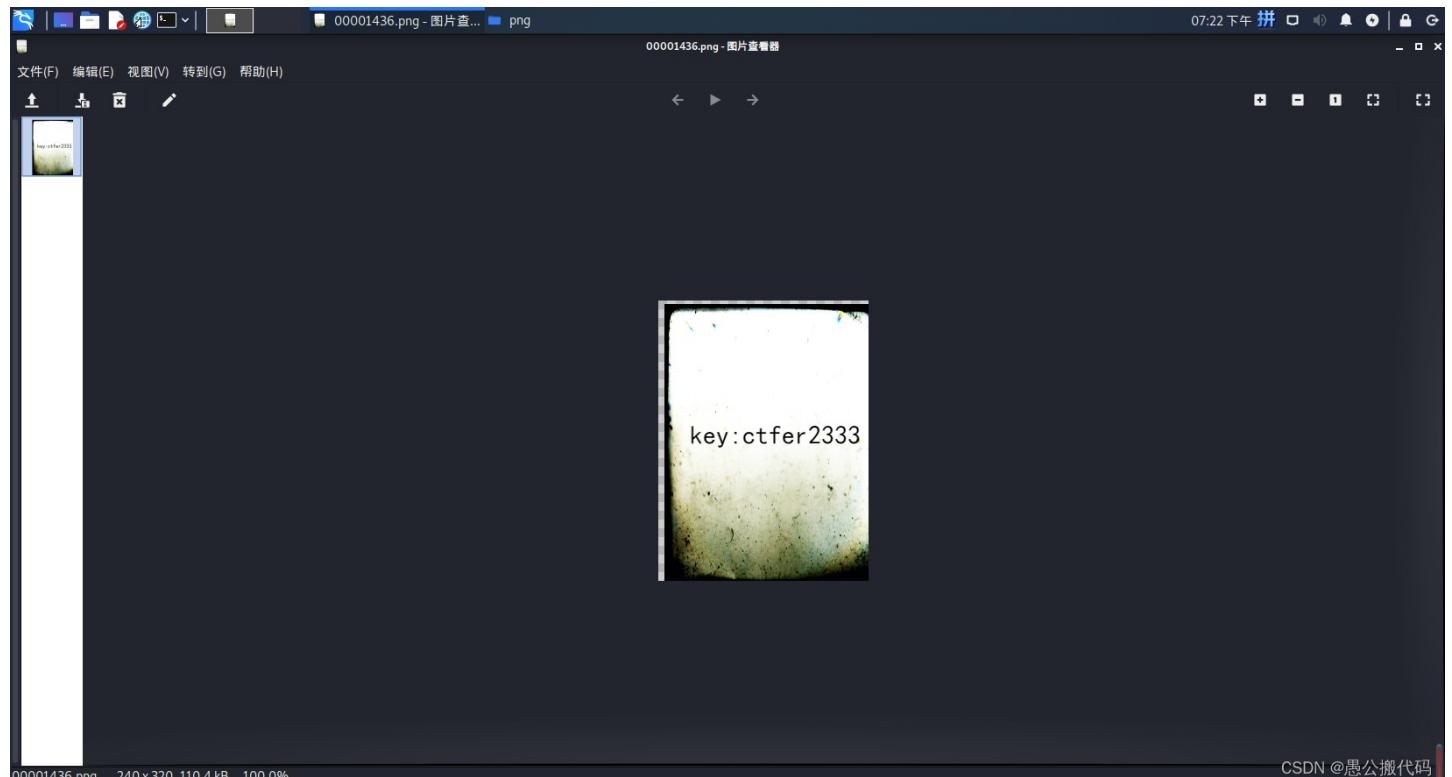
```
for j in range(0, 24):
    file = C:\Users\25288\Anaconda3\python.exe
    x = Press any key to continue . . .
    y =
    img
    img_
    img_
    r, g
    if g:
        if r:
            if l:
                print(ret)

if __name__ == '__main__':
    main()
```

得到: o8DlxK+H8wsiXe/ERFpAMaBPiIcj1sHyGOMmQDkK+uXsVZgre5DSXw==

### 3.foremost分离

foremost out.gif



得到密钥: ctfer2333

## 4.DES解密

在线解密网址: <http://tool.chacuo.net/cryptdes>

The screenshot shows the cryptdes online tool interface. At the top, there's a sidebar with a list of encryption/decryption methods: Rijndael加密解密, Cast加密解密, Xtea加密解密, 非对称性加密解密, rsa公钥加密解密, rsa私钥加密解密, RSA密钥清除, RSA私钥密码修改, PKCS#1转PKCS#8, 校验RSA密钥对, 私钥中提取公钥, Rsa公钥解析, DSA密钥对, 模数生成Rsa公钥. Below this is a blue banner for PayPal with text: '一个账户，收款全球。0费用开户，享卖家保障，赢逾2亿用户。' and a '打开' (Open) button.

The main area contains a form for DES encryption/decryption:

- DES加密模式: ECB (selected)
- 填充: zeropadding
- 密码: ctfer2333
- 偏移量: iv偏移量, ecc模式
- 输出: base64
- 字符集: gb2312编码

待加密、解密的文本框内输入了待解密的文本: oSDlxK+H8wxiXe/ERFpAMaBPiIcjishyGOMmQDkK+uXsVZgre5DSXw==. A note below says: '↑ 将你电脑文件直接拖入试试^~^'. Below the text box are two buttons: DES加密 (Encrypt) and DES解密 (Decrypt).

下方显示了解密结果: flag{2ce3b416457d4380dc9a6149858f71db}.

On the right side of the interface, there's a vertical pink bar with the word '分享' (Share) and a CSDN watermark at the bottom: CSDN @愚公搬代码.

得到flag: flag{2ce3b416457d4380dc9a6149858f71db}

## 总结

- 二进制转ascii
- foremost
- esb