【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

本文链接：https://blog.csdn.net/aa2528877987/article/details/122754982

文章目录

一、双色块

二、答题步骤

1.下载附件

2.脚本破解

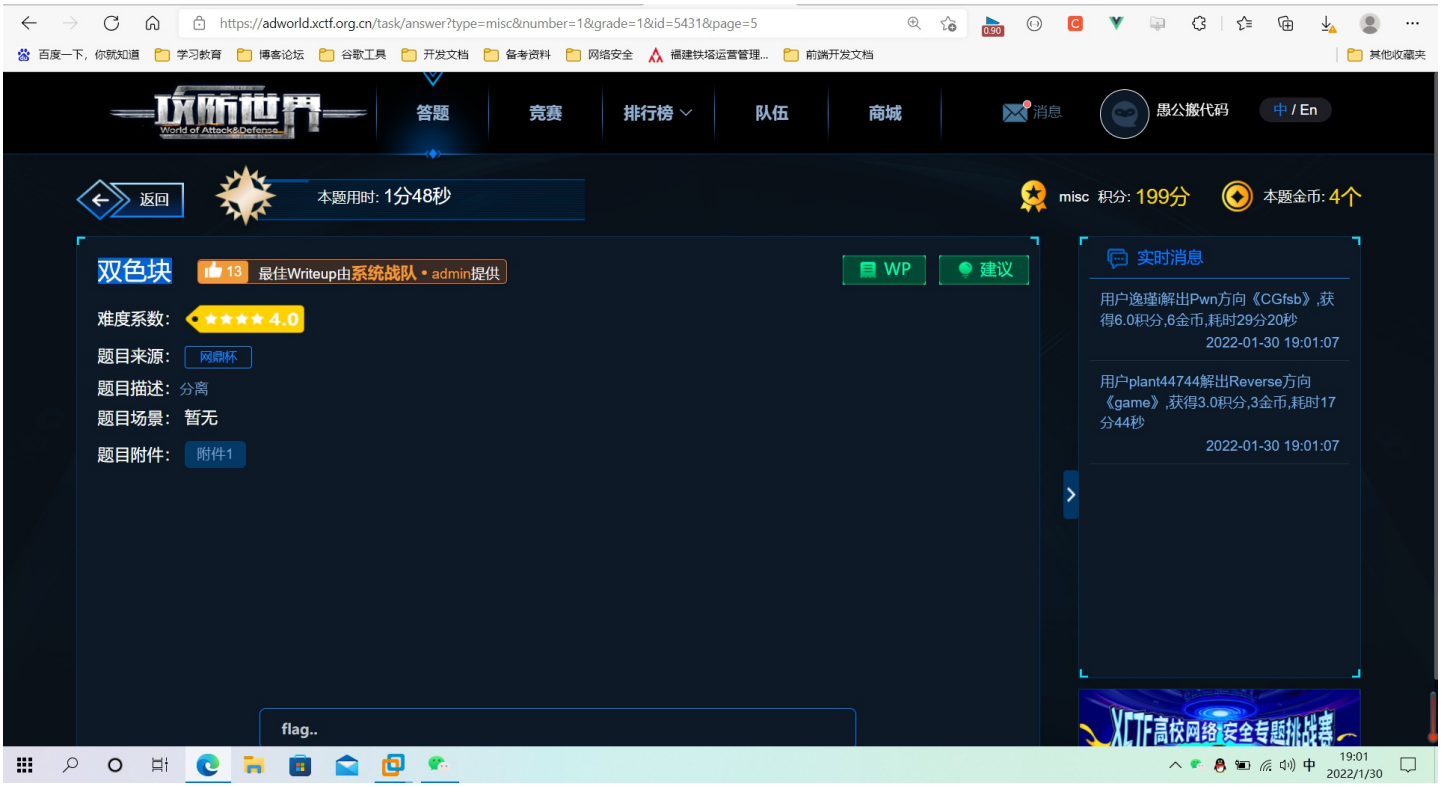
3.foremost分离

4.DES解密

总结

一、双色块

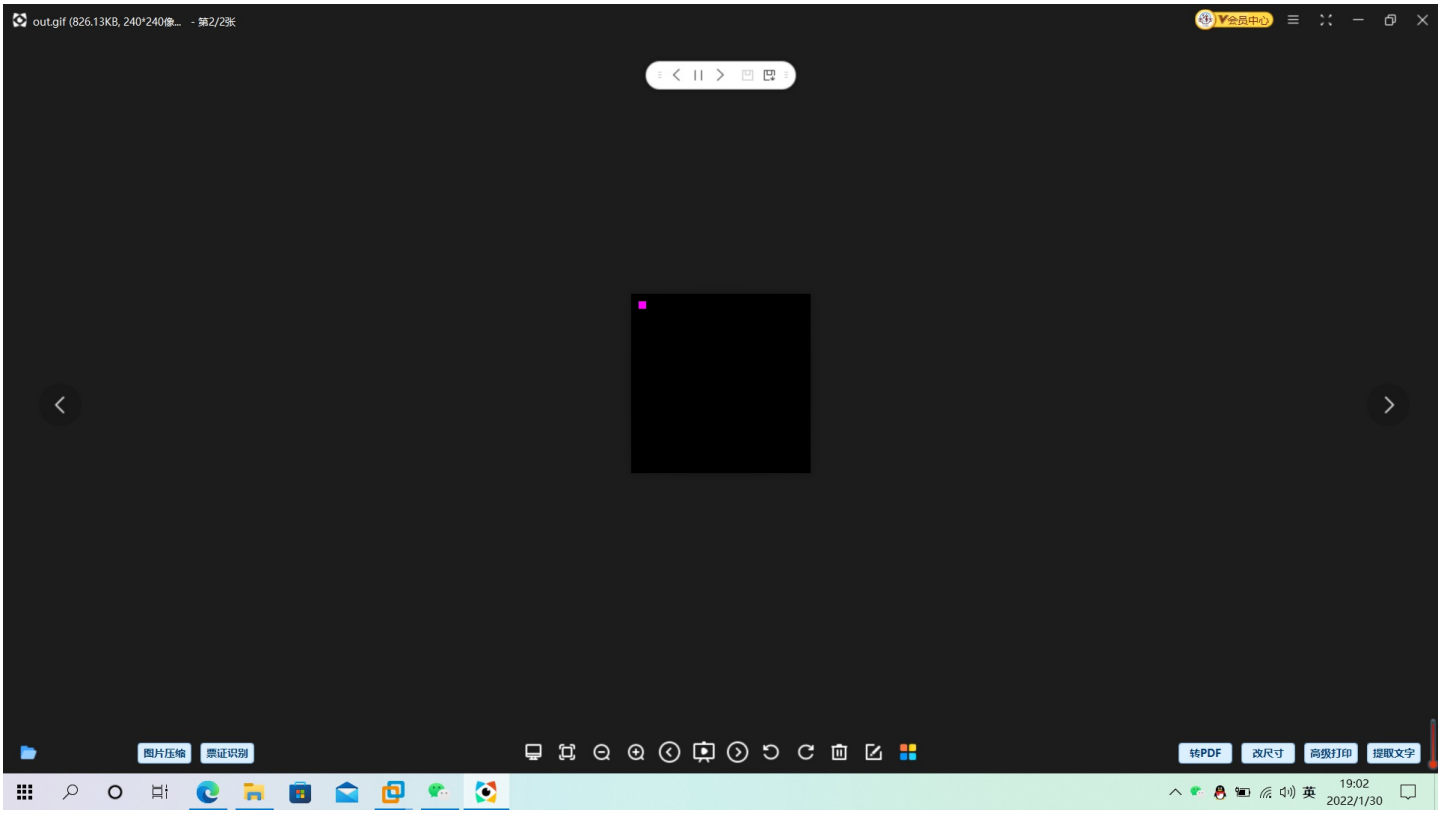
题目链接：https://adworld.xctf.org.cn/task/task_list?type=misc&number=1&grade=1&page=5



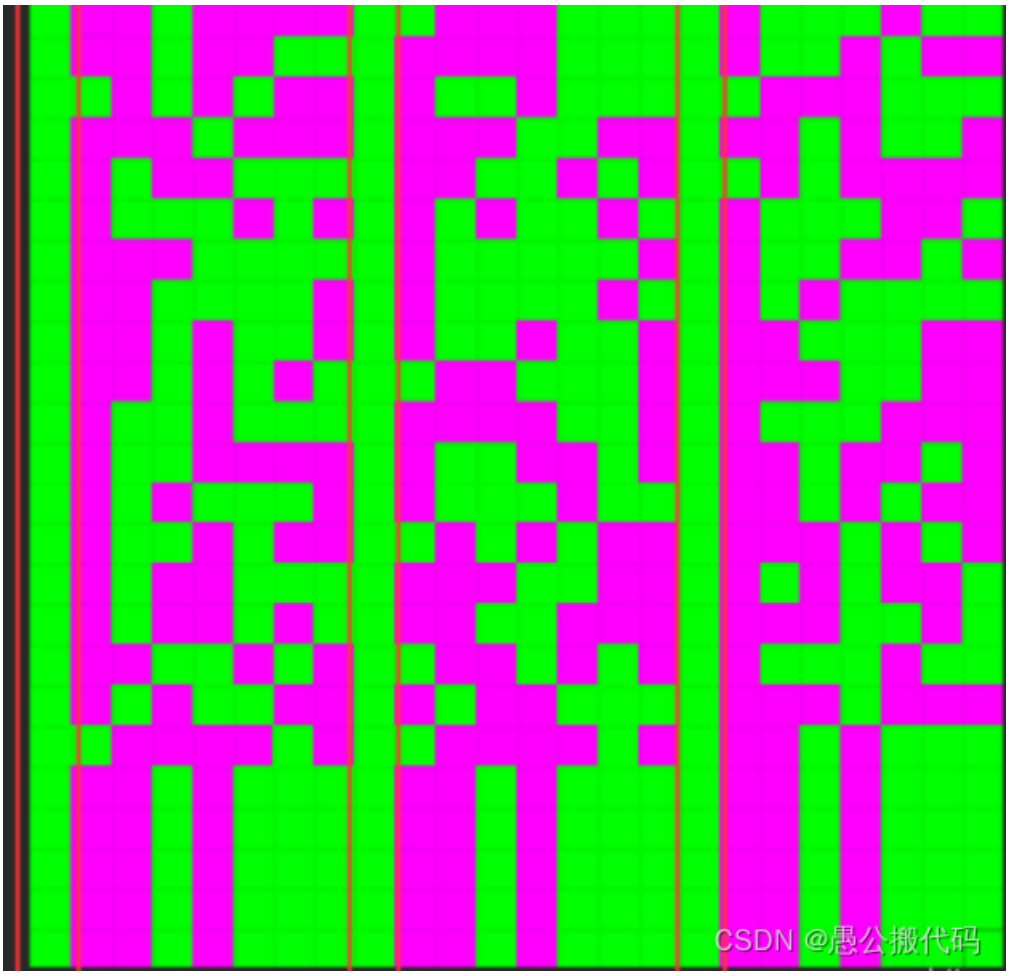
二、答题步骤

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*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

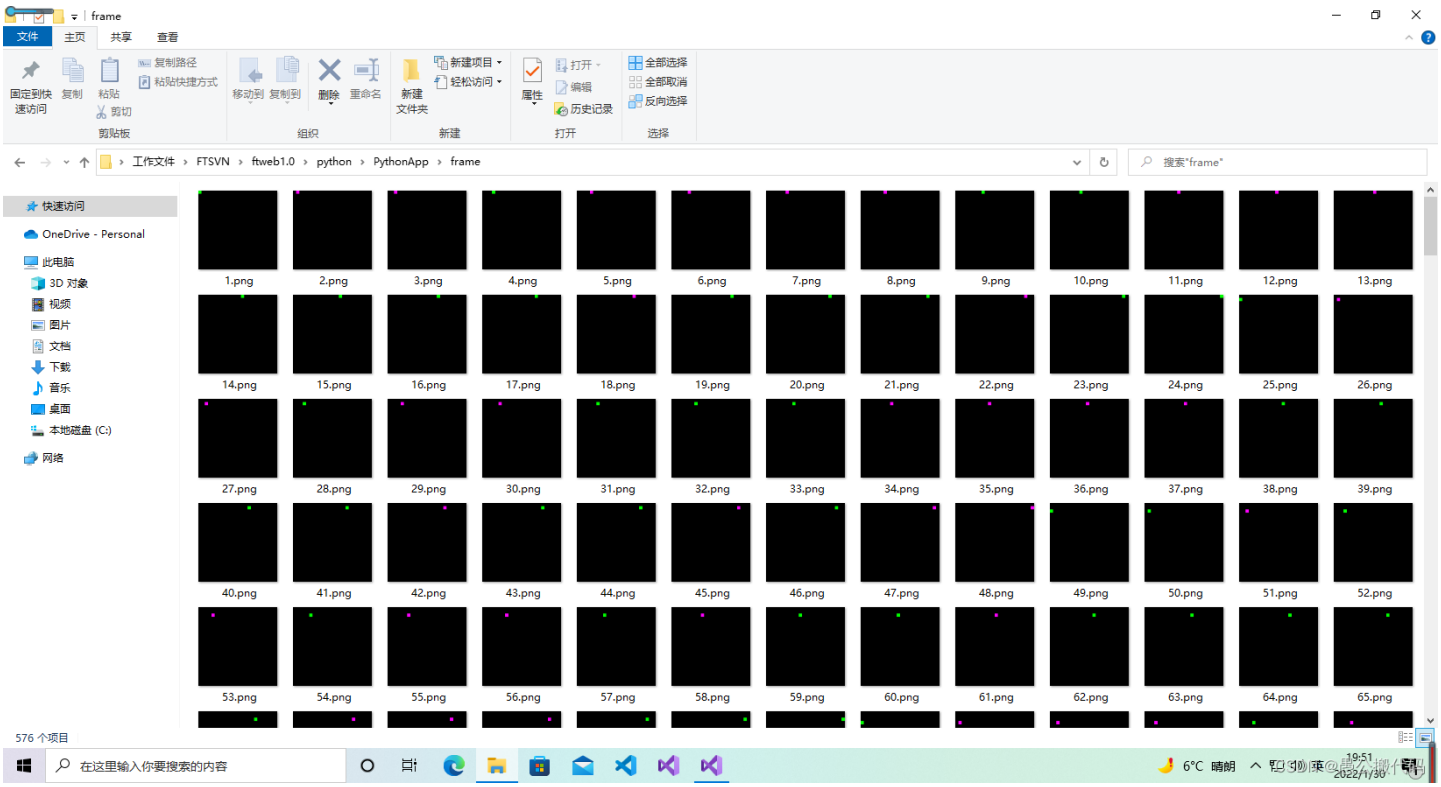
首先解析gif图片分离成单帧模式

```
#! /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

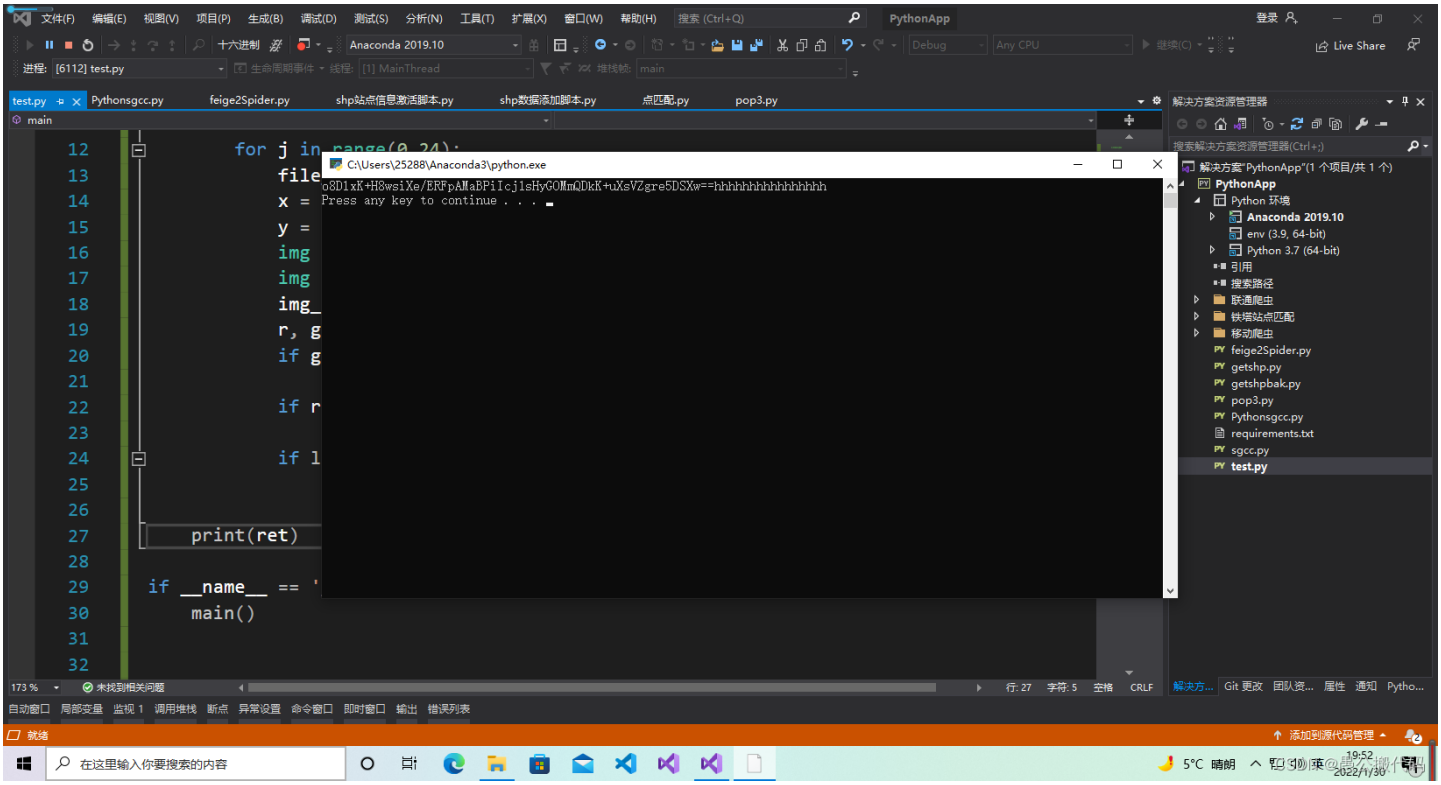
```
#! /usr/bin/env python2
# -*- coding: utf-8 -*-

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()
```

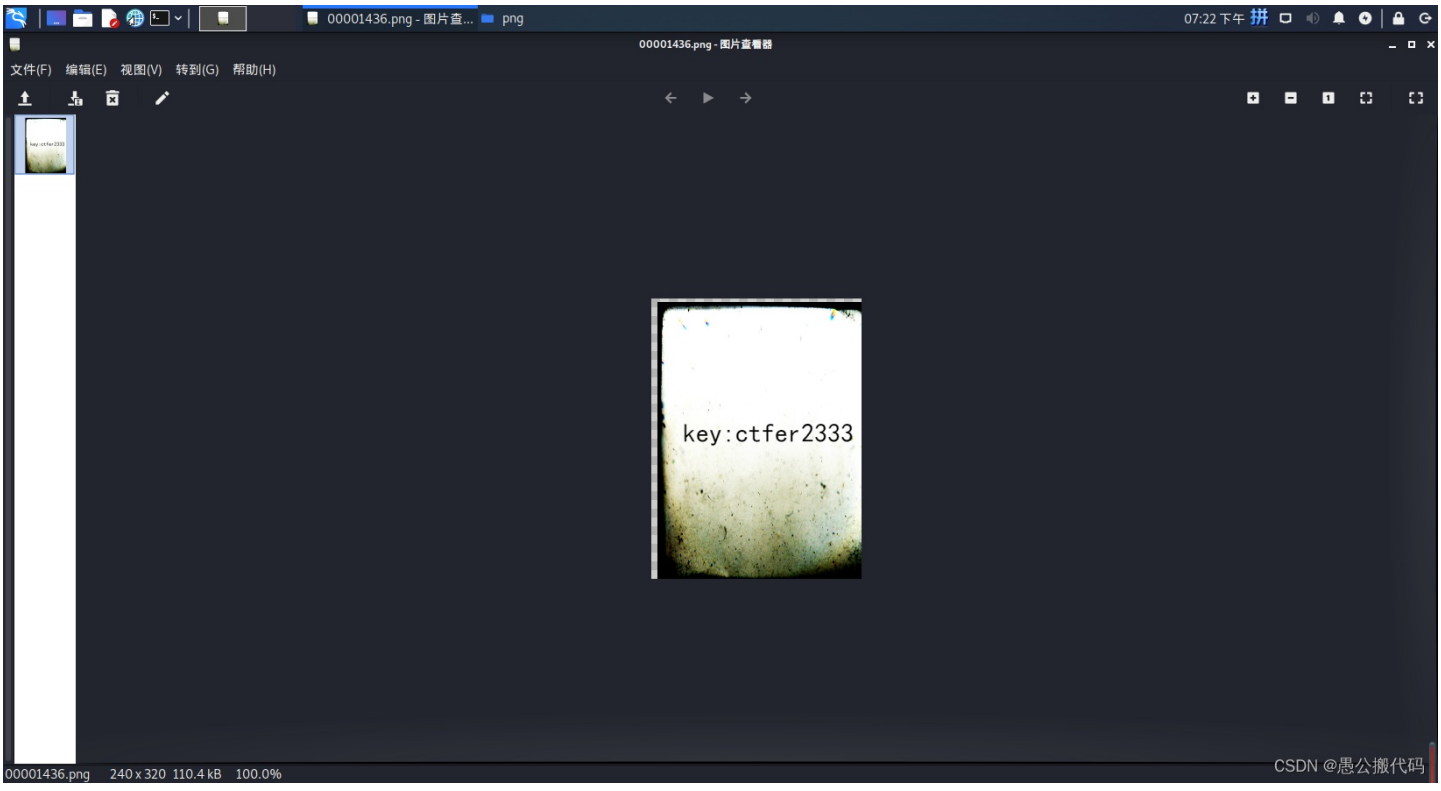
运行脚本得到



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

得到flag: `flag{2ce3b416457d4380dc9a6149858f71db}`

总结

- 二进制转ascii
- foremost
- esb