攻防世界 Misc高手进阶区 3分题 双色块

原创

思源湖的鱼 于 2020-11-04 14:54:15 发布 521 收藏 1

分类专栏： ctf 文章标签： 攻防世界 ctf misc DES

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109489680

前言

继续ctf的旅程

攻防世界Misc高手进阶区的3分题

本篇是双色块的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

下下来一个gif

是不断闪烁的紫色绿色小块

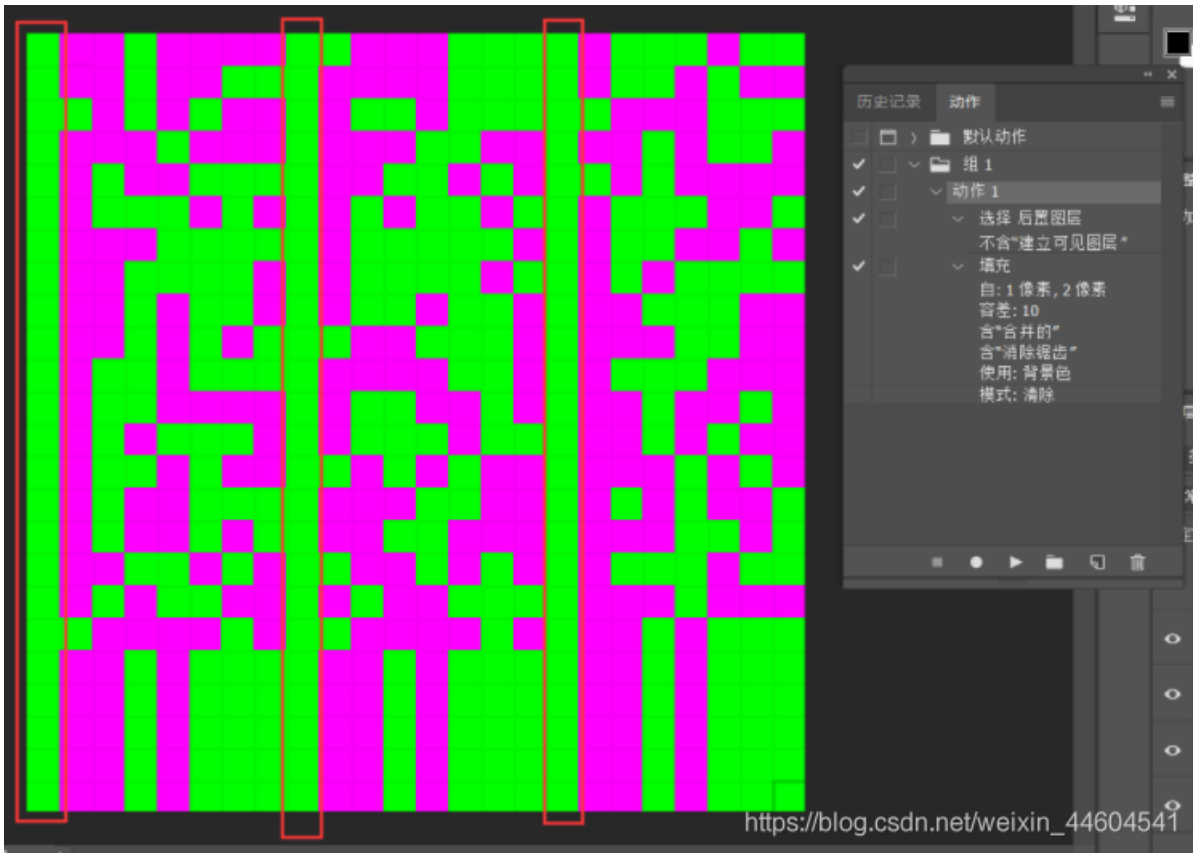
猜测跟二进制有关

先扔进stegsolve看看

无果

扔进winhex
无果

那就回过头来处理gif里的小块
扔进ps
录制动作



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

那就处理下

```python
#! /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)
    while True:
        current = img.tell()
        img.save(png_dir + str(current + 1) + '.png')
        img.seek(current + 1)
    res = ""
    for i in range(0,24):
        line = ""
        for j in range(0,24):
            file_name = png_dir + 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:
                res+= chr(int(line, 2))
                line = ""
    print res
if __name__ == '__main__':
    gif_file = 'out.gif'
 main(gif_file)
```

得到一个base64或DES

尝试base64
失败

那应该是DES
还要找key

foremost分离

得到key

解密

得到flag

结语

知识点

- ascii码
- DES加密
- foremost分离