

CTF Geek Challenge——第十一届极客大挑战Misc Write Up

原创

Starzkg 于 2020-11-18 10:38:36 发布 516 收藏 2

分类专栏: [安全 # Misc](#) 文章标签: [CTF Misc](#)

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/weixin_43272781/article/details/109145159

版权



[安全](#) 同时被 2 个专栏收录

45 篇文章 2 订阅

订阅专栏



[Misc](#)

1 篇文章 0 订阅

订阅专栏

比赛时间: 2020年10月17日早上9点

比赛时限: 一个月

0x1 一“页”障目

一“页”障目

作者: lingze

简介: 宣传单里藏了啥?

分数: 50

答案: **已提交**

https://blog.csdn.net/weixin_43272781

宣传单里藏有flag, 不过分成了三份

极客大挑战

三叶草安全技术小组招新

Syclover & Geek

SYC{sic_20_ver}

SYC{sic_20_ver}

SYC{sic_20_ver}

主题：三叶草安全技术小组招新

第十一届极客大挑战宣讲

宣讲会：2020-10-16 19:00 4213教室

特别赞助：奇安信技术研究院



北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022



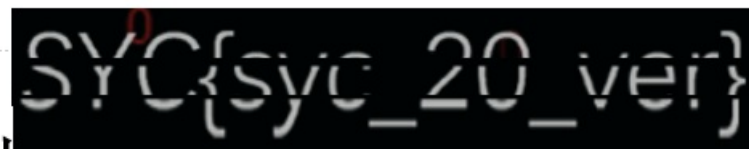
比赛QQ群
1121885420



招新QQ群
736564955

https://blog.csdn.net/weixin_43272781

拼好如图：



0x2 壮言壮语

壮言壮语

×

作者：liuZhuang

简介：佛曰：豆梵能佛冥謹沙怯隸道等孕喝伽訶恐奢耶尼殿怯怖奢三鉢南怛鉢娑幡寫數幡究呐者醯幡勝孕幡顛幡耶夜哆悉侄羯涅悉怯老若俱勝菩知菩所蘇奢以梵世心亦呐耨夷哆至哆醯即波怯明除怯闍怯集怯尼明幡實怯一心鉢呼侄羯夢室諳耨呐提迦梵都都呐孕礙諳那呐彌豆鉢智遮諳槃提伽俱穆離冥伊冥那藐罰摩迦諳有諳盡即怯多逝侄婆冥涅神

提示：什么是佛曰

分数：100

答案：已提交

https://blog.csdn.net/weixin_43272781

工具：

与佛论禅：<http://www.keyfc.net/bbs/tools/tudoucode.aspx>

与佛论禅

我刘壮就是np，给你flag吧，SYC {i_love_Japanese_wife}

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

坐亦禅，行亦禅

佛曰：豆梵能佛冥謹沙怯隸道等孕喝伽訶恐奢耶尼殿怯怖奢三鉢南怛鉢娑幡寫數幡究呐者醯幡勝孕幡顛幡耶夜哆悉侄羯涅悉怯老若俱勝菩知菩所蘇奢以梵世心亦呐耨夷哆至哆醯即波怯明除怯闍怯集怯尼明幡實怯一心鉢呼侄羯夢室諳耨呐提迦梵都都呐孕礙諳那呐彌豆鉢智遮諳槃提伽俱穆離冥伊冥那藐罰摩迦諳有諳盡即怯多逝侄婆冥涅神

https://blog.csdn.net/weixin_45696568

0x3 秘技·反复横跳

秘技·反复横跳



作者: AFKL

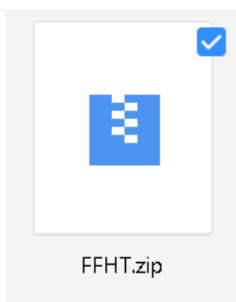
简介: 题目附件: 链接: <https://share.weiyun.com/6oCZShYV>
密码: 114514 对图片...使用binwalk拳吧!

分数: 100

答案:

https://blog.csdn.net/weixin_43272781

下载文件



得到一种图片



将图片后缀名改成rar，用WinRAR打开（或者用binwalk分析，显然图片里藏有其他东西，或者foremost得到一个压缩包（foremost的使用方法）），里面是一张错位的二维码



位置调整



https://blog.csdn.net/weixin_43272781

扫描得到flag

0x4 来拼图



给了一张图片source.jpg和一个压缩包，压缩包里有1600个小图片，这1600个小图片是将source.jpg 编辑加上flag以后的图片切割得来的。

利用python的CV2库的图像匹配算法，由于修改原图，将flag写入到图片上会造成小图片与原图上相应位置的图片匹配度降低，当匹配度低于某个阈值时，可认为是将flag写到了这张小图片上，阈值取的是 $5e-10$ 。

同时将小图片拼接成原图片并且保存。

因为开启多线程，比较时间较短，但运行时比较占CPU

```
# python3
import cv2
from PIL import Image
import numpy as np
import os
import shutil
import threading

# 读取目标图片
source = cv2.imread("C:/Users/12345/Desktop/12345/source.jpg")
```

```

source = cv2.imread(r"C:/Users/Lenovo/Desktop/pt/source.jpg")
# 拼接结果
target = Image.fromarray(np.zeros(source.shape, np.uint8))
# 图库目录
dirs_path = r"C:/Users/Lenovo/Desktop/pt/pingTu"
# 差异图片存放目录
dst_path = r"C:/Users/Lenovo/Desktop/pt/new1"

def match(temp_file):
    # 读取模板图片
    template = cv2.imread(temp_file)
    # 获得模板图片的高宽尺寸
    theight, twidth = template.shape[:2]
    # 执行模板匹配, 采用的匹配方式cv2.TM_SQDIFF_NORMED
    result = cv2.matchTemplate(source, template, cv2.TM_SQDIFF_NORMED)
    # 归一化处理
    cv2.normalize(result, result, 0, 1, cv2.NORM_MINMAX, -1)
    # 寻找矩阵(一维数组当做向量, 用Mat定义)中的最大值和最小值的匹配结果及其位置
    min_val, max_val, min_loc, max_loc = cv2.minMaxLoc(result)
    target.paste(Image.fromarray(template), min_loc)
    return abs(min_val)

class MThread (threading.Thread):
    def __init__(self, file_name):
        threading.Thread.__init__(self)
        self.file_name = file_name

    def run(self):
        real_path = os.path.join(dirs_path, k)
        rect = match(real_path)
        if rect > 5e-10:
            print(rect)
            shutil.copy(real_path, dst_path)

count = 0
dirs = os.listdir(dirs_path)
threads = []
for k in dirs:
    if k.endswith('.jpg'):
        count += 1
        print("processing on pic"+str(count))
        mt = MThread(k)
        mt.start()
        threads.append(mt)
    else:
        continue
# 等待所有线程完成
for t in threads:
    t.join()
target.show()
target.save(r"C:/Users/Lenovo/Desktop/pt/target.jpg")

```




https://blog.csdn.net/welxin_43272781

拼接结果（不知道为什么存在色差）需要手动拼合部分内容



参考文章

第十一届极客大挑战部分WP（无re和pwn）

从DDCTF2020-拼图题,学习如何做拼图题