Defcon 2019 Qualify: redacted puzzle Writeup

原创

LiRiu 于 2021-04-26 18:23:21 发布 66 收藏

分类专栏： 非专业知识积累 文章标签： 信息安全 python haproxy web development

文章目录

Defcon 2019 Qualify: redacted-puzzle

1.Attachments

2.source code

3.author: bboe

4.writeups

5.知识点

5.1 图像模式

5.2 pallete

5.3 Python PIL包使用

5.4 Base系列编码原理

6 [Defcon 2020q uploooadit](https://github.com/o-o-overflow/dc2020q-uploooadit)

总结

Defcon 2019 Qualify: redacted-puzzle

ctftime link: https://ctftime.org/task/8526

1.Attachments

redacted-puzzle.gif
Everything you need is in this file.

2.source code

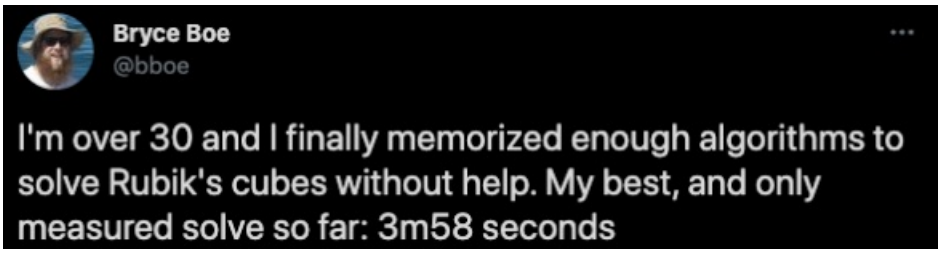
dc2019q-puzzle

3.author: bboe

Bryce Boe是defcon的组织者，AppFolio公司的软件工程师\Tech Leader，加州大学圣巴巴拉分校 助教。

- Social Media
  - twitter
  - Blog
  - Github
  - Google Scholar

这位老师最后一篇论文发表于2014年，其博客也停更于2014年。
其主要贡献在于可视化的编程工具与教育事业的结合。
在论文Organizing large scale hacking competitions中提出了大规模黑客技术比赛的设想。
身为人父的他已经在享受生活了，羡慕。



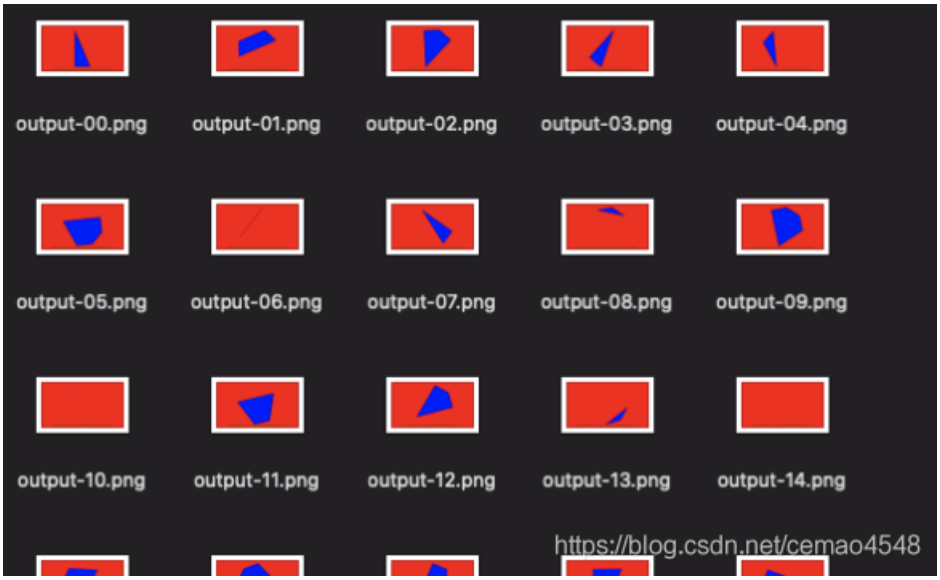
另外，可以找到他在defcon2020q中出的另一道题目Defcon 2020q uploooadit

4.writeups

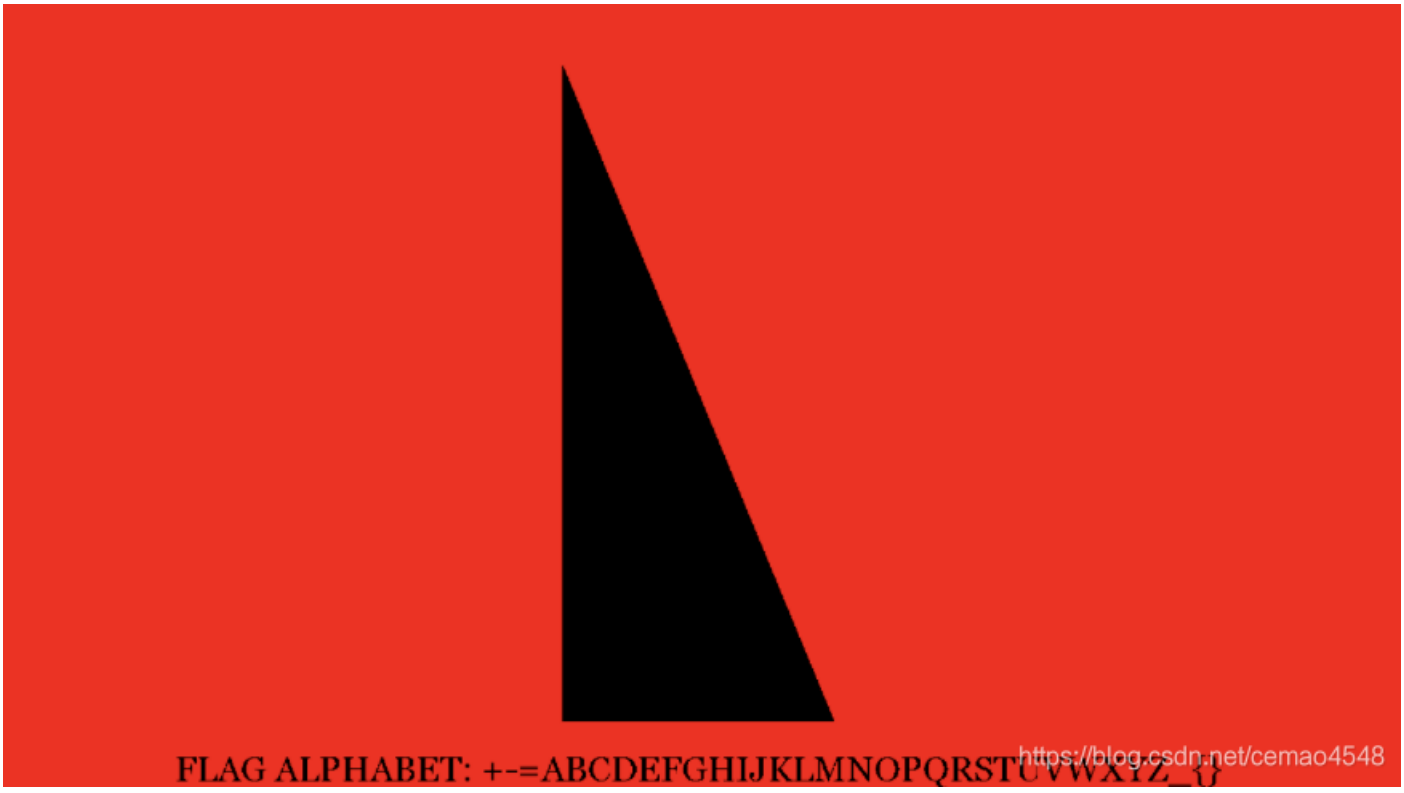
- ThreatLevelMidnight
- OSUSEC
- IDontHaveATeam
- ThreatLevelMidnight
- 2019 defcon 学习

题目给出一个全黑的gif。分析发现图片的调色板为纯黑。
我们逐帧修改其调色板，让画面变得多彩一些。

```
from PIL import Image
imageObject = Image.open("./redacted-puzzle.gif")
for frame in range(0,imageObject.n_frames):
    imageObject.seek(frame)
    imageObject.putpalette([255,0,0,0,255,0,0,0,255])
    imageObject.save("./tmp/output-%02u.png" % frame)
```



可以得到一组 类似八边形的图片。
其中给出了一个长32的字母表 `flag_alphabet = "+-=ABCDEFGHIJKLMNOPQRSTUVWXYZ_{}"`



每一张图都是一个8bit的2进制数字。

```
verticies = ['10001100', '01100011', '11100100', '01000110', '10000101', '00111101', '01000010', '10011000', '11
100000',
             '11110100', '10000000', '00101101', '01110010', '00011100', '00001000', '10100101', '11010111',
 '01101110',
             '10100110', '10010001', '10111100', '10000100', '10000001', '10111001', '11010100', '00111011',
 '11001110',
             '11110010', '00011110', '10011101', '11001001', '11000111', '01100101', '00011110', '10011111']
```

由于`flag_alphabet`中有32个可见字符，想到Base32编码方式。
用符号表中的字母编码gif，得到flag。

```
result:  OOO{FORCES-GOVERN+TUBE+FRUIT_GROUP=FALLREMEMBER_WEATHER}

Process finished with exit code 0
```

```
verticies = ['10001100', '01100011', '11100100', '01000110', '10000101', '00111101', '01000010', '10011000', '11
100000',
                '11110100', '10000000', '00101101', '01110010', '00011100', '00001000', '10100101', '11010111',
 '01101110',
                '10100110', '10010001', '10111100', '10000100', '10000001', '10111001', '11010100', '00111011',
 '11001110',
                '11110010', '00011110', '10011101', '11001001', '11000111', '01100101', '00011110', '10011111']

alphabet = '+-=ABCDEFGHIJKLMNOPQRSTUVWXYZ_{}'

def solve(verticies):
    combined = ''
    for v in verticies:
        combined += v

    indicies = []
    for x in range (0, len(combined)//5):
        indicies.append(combined[x * 5:x * 5 + 5])

    answer = ''
    for x in indicies:
        answer += alphabet[int(x, 2)]

    print (answer)

def twist(verticies):
    newverticies = []

    for v in verticies:
        # v = abcdefgh -> habcdefg
        newv = ''
        newv+=v[7]
        newv+=v[0:7]
        newverticies.append(newv)

    return newverticies

for x in range (0,8):
    solve(verticies)
    verticies = twist(verticies)

print("Finished Program")
```

5.知识点

5.1 图像模式

https://www.osgeo.cn/pillow/handbook/concepts.html#modes

这个 mode 是一个字符串，它定义图像中像素的类型和深度。每个像素使用位深度的全部范围。所以1位像素的范围是0-1，8位像素的范围是0-255，依此类推。
当前版本支持以下标准模式：

- 1 （1位黑白像素，每字节存储一个像素）
- L （8位像素，黑白）
- P （8位像素，使用调色板映射到任何其他模式）
- RGB （3x8位像素，真彩色）
- RGBA （4x8位像素，带透明蒙版的真彩色）
- CMYK （4x8位像素，分色）
- YCbCr （3x8位像素，彩色视频格式）
- LAB （3x8位像素，L A B颜色空间）
- HSV （3x8位像素、色调、饱和度、值颜色空间）
- I（32位有符号整数像素）
- F （32位浮点像素）

Image库还支持一些特殊模式:

- LA （L和阿尔法）
- PA （P与阿尔法）
- RGBX （带填充的真彩色）
- RGBa （带预乘alpha的真彩色）
- La （L带预乘α）
- I;16 （16位无符号整数像素）
- I;16L （16位小端无符号整数像素）
- I;16B （16位大端无符号整数像素）
- I;16N （16位本机端无符号整数像素）
- BGR;15 （15位反转真彩色）
- BGR;16 （16位反转真彩色）
- BGR;24 （24位反转真彩色）
- BGR;32 （32位反转真彩色）

> 我怀疑MISC题目的常用工具 stegsolve 就是在各种Mode之间做切换。

5.2 pallete

使用PIL库 改变图片的调色板
当图片模式选择`P`时，ImageObject有pallete参数。
pallete默认为`RGB`格式，是一个长度为768的list对象。
在`RGB`格式下，pallete的list对象被3个一组，表示RGB颜色。
最多记录256个`RGB`颜色。

```
palette = []
for i in range(256):
    palette.extend((i, i, i)) # grayscale wedge

assert len(palette) == 768

im.putpalette(palette)
```

5.3 Python PIL包使用

PIL包文档

5.4 Base系列编码原理

Base64, Base32 和 Base16，用通俗的语言深入到内部

6 Defcon 2020q uploooadit

`uploooadit`是一道`WEB`题，主要考点是`haproxy 1.9.10`中存在的`HTTP smuggling`漏洞。
Writeup可以看这篇文章

总结

Bryce Boe 老师总共出过两道Defcon的题目。
我没有找到他在题目上线之前对考点的研究痕迹。
其社交媒体或发布的论文中也没有对应的体现。
因此无法预测在2021 defcon中，bboe老师将带来什么样的题目。