

昵称： cat47
园龄： 2年2个月
粉丝： 19
关注： 2
+加关注

< 2021年10月 >						
日	一	二	三	四	五	六
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

搜索

找找看

谷歌搜索

常用链接

我的随笔

我的评论

我的参与

最新评论

我的标签

我的标签

不要空手套博客哦(1)

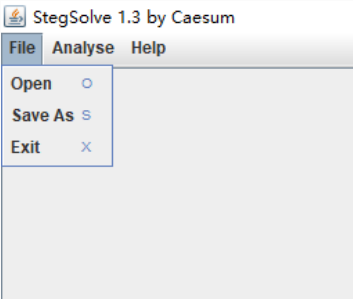
要是转载请附上我的链接(1)

随笔分类

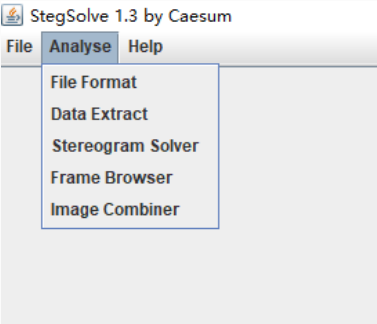
CTF解题思路(15)

stegsolve使用方法

Stegsolve使用方法（是因为ctf题总是遇到并且目前百度没有十分详细的探究说明）



这个没什么好说的，打开文件，保存，退出



在分析里面从上到下的依次意思是

File Format:文件格式

Data Extract:数据提取

Stereogram Solve:立体试图 可以左右控制偏移

Frame Browser:帧浏览器

Image Combiner:拼图，图片拼接

用法（使用场景）

1.File Format:这里你会看见图片的具体信息有时候有些图片隐写的flag会藏在这里

2.Data Extract:(好多涉及到数据提取的时候，很多博主在wp中都是一带而过，小白们还以为要一个个试。。)

CTF线下赛(1)

PWN入门前基础(16)

python爬虫(2)

python自制小代码小工具(1)

sql注入全通关(5)

工具使用(2)

黑客攻击实战（仅供学习！！！！）(3)

精选博客转载(29)

墨者学院(9)

提权心法(7)

挖洞(15)

随笔档案

2020年7月(1)

2020年5月(1)

2020年4月(14)

2020年3月(15)

2020年2月(17)

2020年1月(10)

2019年12月(3)

2019年11月(5)

2019年10月(1)

2019年9月(7)

2019年8月(13)

相册

走马观花(9)

阅读排行榜

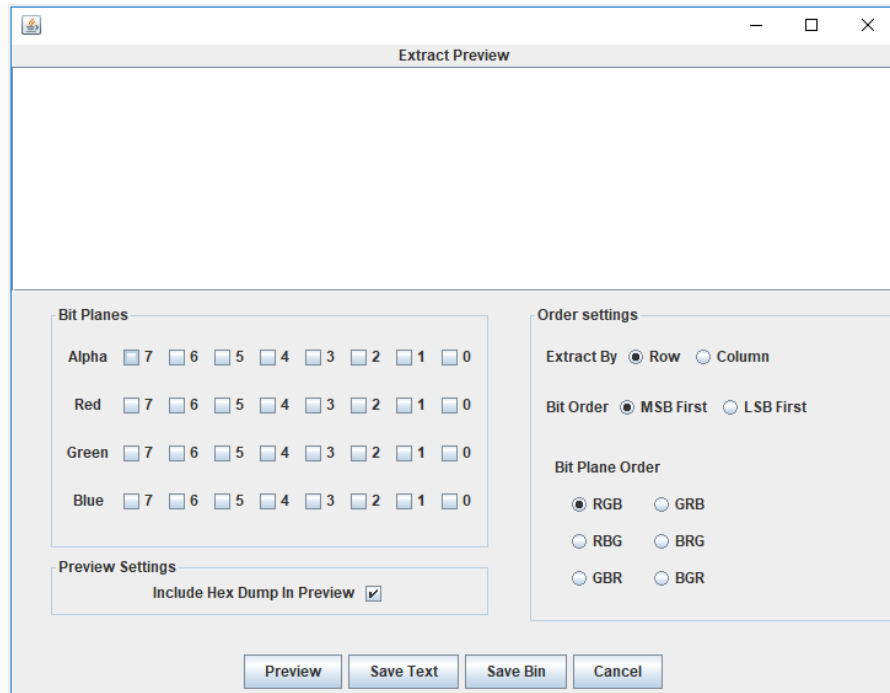
1. stegsolve使用方法(26998)

2. CTF -bugku-misc（持续更新直到全部刷完）(5348)

3. CTF -攻防世界-web高手区-ics-06(4694)

4. CTF -攻防世界-misc新手区(4037)

5. python 正则 提取HTML标签文本内容的(3127)



左边一大部分主要是讲了RGBA（Alpha是透明度）的颜色通道

为了方便理解我们分开说

RGB是红绿蓝 但他们的值代表的实际上是亮度

R的数字越大，则代表红色亮度越高；R的数字越小，则代表红色亮度越低。G，B同理

R的亮度各有256个级别，GB同理。即从0到255，合计为256个。从数字0到255的逐渐增高，我们人眼观察到的就是亮度越来越大，红色、绿色或蓝色越来越亮。然而256是2的8次方 所以你会看见上图的7~0 一共8个通道

而Alpha就是透明度 该通道用256级灰度来记录图像中的透明度信息，定义透明、不透明和半透明区域 alpha的值为0就是全透明，alpha 的值为 255 则表示不透明

因此左半部分就理解了

右半部分就是Extra By(额外的)和Bit Order（位顺序）和Bit Plane Order（位平面的顺序）

1) .Extra By(额外的): 分为row（行）和column（纵）

每个像素用R，G，B三个分量表示，那么一张图片就像一个矩阵，矩阵的每个单位就是（0~255，0~255，0~255）

也就会有纵排列和行排列了，一般事先访问行再访问列（如果相反会引起ve使用方法）

2) .Bit Order（位顺序）:MSB是一串数据的最高位，LSB是一串数据的最低位。

3) .Bit Plane Order（位平面的顺序）

整个图像分解为8个位平面，从LSB(最低有效位0)到MSB（最高有效位7）随着从位平面0 到位平面7，位平面图像的特征逐渐变得复杂，细节不断增加。（一般我们的图片如果是RGB那么就是24位 3乘8嘛）

4) Bit Plane Order（位平面的顺序）:一般图片是24位 也就是3个8 大家可以想像成三明治 比如BGR就是B为三明治第一层 G为第二层 R为第三层。

3.Stereogram Solve:立体试图 可以左右控制偏移 可以放张图片试一下就知道这个是什么意思了

4.Frame Browser:帧浏览器 主要是对GIF之类的动图进行分解，把动图一帧帧的放，有时候会是二维码

5.Image Combiner:拼图，图片拼接（意思显而易见）

接下来会带大家实战去深入理解一下Data Extract里面ctf经常用到的LSB隐写

评论排行榜

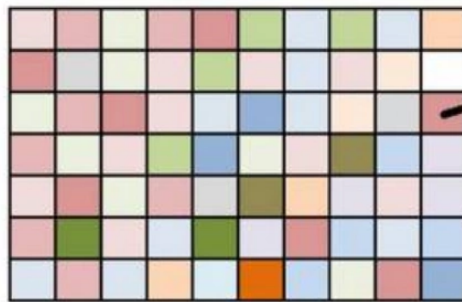
1. stegsolve使用方法(3)
2. CTF -攻防世界-crypto新手区(1~4)(2)
3. Apache Struts2远程代码执行漏洞(S2-015)(1)
4. CTF-bugku-PWN(1)

推荐排行榜

1. stegsolve使用方法(3)
2. CTF -攻防世界-crypto新手区 (5~11)(1)
3. CTF -攻防世界-web高手区-ics-06(1)

最新评论

1. Re:stegsolve使用方法
666
--Ca1m
2. Re:stegsolve使用方法
love love
--紫羽踮跹
3. Re:Apache Struts2远程代码执行漏洞(S2-015)
求工具
--可乐-kele
4. Re:CTF-bugku-PWN
问下，找rdi的地址为什么要找pop|ret呢？直接找rdi为什么找不了？
--Gygert
5. Re:stegsolve使用方法
师傅，膜拜一下！
--AlexANSO






RGB (218, 150, 149)

R = 11011010
G = 10010110
B = 10010101

这个我们之前介绍的很详细

而LSB隐写就是修改RGB颜色分量的最低二进制位也就是最低有效位 (LSB)，而人类的眼睛不会注意到这前后的变化，（人类的眼睛只能识别一部分颜色的变化）

Color (Green)	Base 10	Binary	Change
	238	11101110	+3
	235	11101011 (base)	
	232	11101000	-3

如果我们修改lsb那么颜色依然和没修改的一样，并且修改的话每个像数可以携带3比特的信息。

Red

☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 ☒ 0

Green

☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 ☒ 0

Blue

☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 ☒ 0

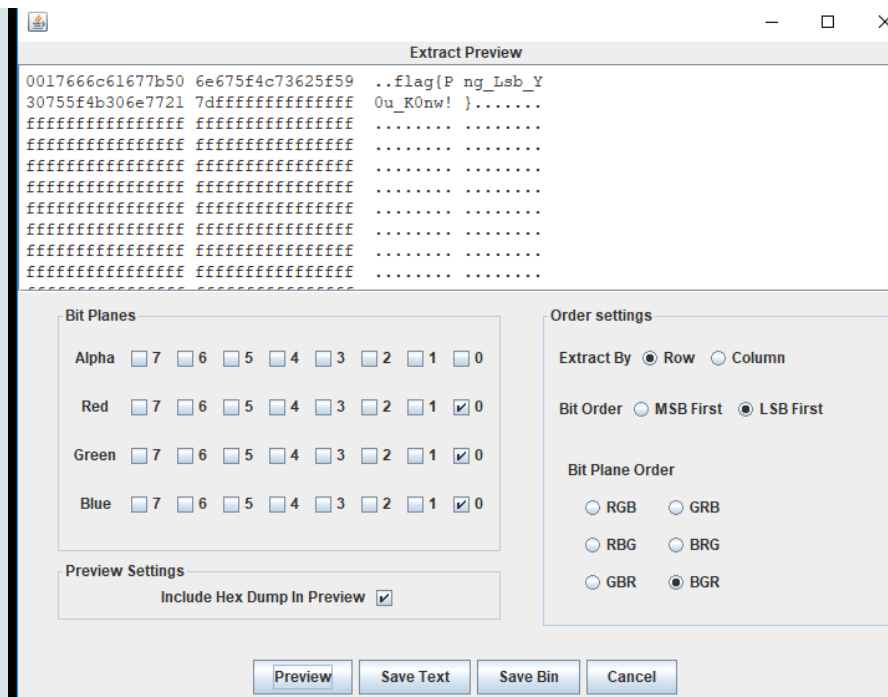
review Settings

这个作用是在于把最低位的二进制全部提取出来

Bit Order ☐ MSB First ☒ LSB First

Bit Plane Order

这个作用在于对提取出来的最低位使用lsb解码算法



分类: [工具使用](#)



cat47
关注 - 2
粉丝 - 19

[+加关注](#)

3
[推荐](#)
0
[反对](#)

« 上一篇: [CTF-bugku-misc \(持续更新直到全部刷完\)](#)
» 下一篇: [wireshark教程](#)

posted @ 2019-09-07 22:25 cat47 阅读(27003) 评论(3) 编辑 收藏 举报

[刷新评论](#) [刷新页面](#) [返回顶部](#)

登录后才能查看或发表评论, 立即 [登录](#) 或者 [逛逛](#) 博客园首页

【推荐】并行超算云面向博客园粉丝推出“免费算力限时申领”特别活动

【推荐】百度智能云超值优惠: 新用户首购云服务器1核1G低至69元/年

【推荐】跨平台组态\工控\仿真\CAD 50万行C++源码全开放免费下载!

【推荐】和开发者在一起: 华为开发者社区, 入驻博客园科技品牌专区

【注册】App开发者必备: 打造增长变现闭环, 高效成长, 收入提升28%



编辑推荐:

- [跳槽一年后的回顾](#)
- [在 Unity 中渲染一个黑洞](#)
- [理解 ASP.NET Core - 配置\(Configuration\)](#)
- [CSS 奇技淫巧 | 妙用 drop-shadow 实现线条光影效果](#)
- [详细分析 JDK 中 Stream 的实现原理](#)

最新新闻:

- [太空旅行火爆前, 必须先看这份《太空漫游指南》 \(2021-10-12 11:04\)](#)