

CTF答题夺旗赛（第四季）i春秋wp

原创

JoJo48 于 2019-12-27 15:29:39 发布 1253 收藏 1

分类专栏: [CTFwp](#) 文章标签: [信息安全 wp](#)

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/JoJo48/article/details/103732025>

版权



[CTFwp](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

i春秋CTF答题夺旗赛(4th)

地址:<https://ictf.ichunqiu.com/>

1、Misc题

下载地址: <http://120.55.43.255:34536/115FA9AF83B2997E/Xlmg.zip>

解题思路: 下载后是一张图片, 因此觉得是图片隐写的可能性很大。先看图片本身的样子是不全的, 所以有想法是不是要改变图片长、宽。还是老规矩先看看图片里有没有东西拖到虚拟机。

(1) [binwalk代码](#)

```
binwalk -e Xlmg.png //图片名
```

执行得到

```
root@you:~# binwalk -e XImg.png
```

| DECIMAL | HEXADECIMAL | DESCRIPTION |
|---------|-------------|-----------------------------------------------------|
| 0 | 0x0 | PNG image, 1024 x 633, 8-bit/color RGB, non-interla |
| 41 | 0x29 | Zlib compressed data, default compression |



(2) 打开文件

```
cd _XImg.png.extracted
```

在.extracted目录下

```
ls -al
```

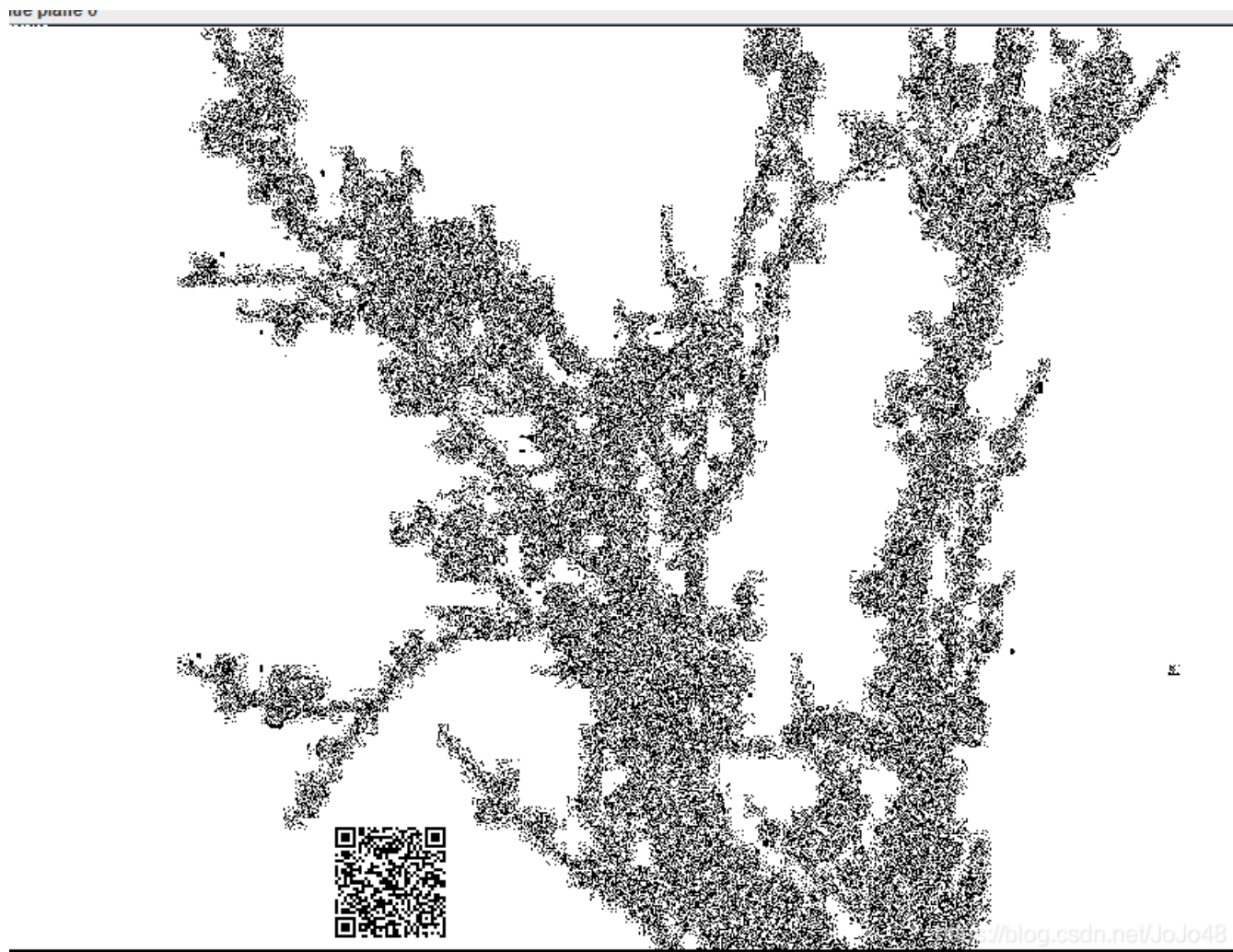
```
root@you:~# cd _XImg.png.extracted
root@you:~/_XImg.png.extracted# ls -al
total 412
drwxr-xr-x  2 root root   4096 Dec 27 14:18 .
drwxr-xr-x 25 root root   4096 Dec 27 15:00 ..
-rw-r--r--  1 root root      0 Dec 27 14:18 29
-rw-r--r--  1 root root 413135 Dec 27 14:18 29.zlib
```

```
chmod a+x 1 //改变文件1位可执行并执行
```

但是执行结果无任何信息

(3) 使用StegSolve

答案就出来了



然后找一个在线扫码工具得到flag

qrcode: <http://tool.chinaz.com/qrcode/>

后记：因为作者在编写这篇blog时还未结束比赛，且本篇文章为作者第一次编写，速度较慢，不熟练。之前还有很多笔记，笔者在没想过写blog的情况下都先编成了word版，如图（仅部分）：

| | | |
|-----------------------------|------------------|--------------------|
| CTF电子书 | 2019/12/10 12:52 | 文件夹 |
| WEB | 2019/11/27 22:07 | 文件夹 |
| 脚本 | 2019/12/12 11:09 | 文件夹 |
| 密码学 | 2019/12/12 20:00 | 文件夹 |
| 隐写 | 2019/12/27 14:19 | 文件夹 |
| BIOS | 2019/11/27 21:13 | Microsoft Word ... |
| burpsuite-Intruder模块 (暴力破解) | 2019/12/12 13:37 | Microsoft Word ... |
| ident-user-enum | 2019/10/12 10:18 | Microsoft Word ... |
| irpas-ass | 2019/10/12 11:20 | Microsoft Word ... |
| nmap | 2019/10/10 20:40 | Microsoft Word ... |
| nmap | 2019/10/10 20:45 | 文本文档 |
| pwn-writeup | 2019/11/14 10:44 | Adobe Acrobat ... |
| pwn教程环境配置 | 2019/11/14 11:24 | Microsoft Word ... |
| SQL注入 | 2019/11/14 12:22 | Microsoft Word ... |
| WEB-session | 2019/12/12 19:50 | Microsoft Word ... |
| win10安全模式 | 2019/11/22 21:21 | Microsoft Word ... |
| 磁盘映射 | 2019/12/12 20:31 | Microsoft Word ... |
| 电子书大全 | 2012/6/12 9:22 | Internet 快捷方式 |
| 解决网络连接失败问题 | 2019/11/22 20:07 | Microsoft Word ... |
| 网络实验室 | 2019/12/12 20:31 | 文本文档 |

现在非常后悔，在此提醒跟笔者一样的CTF小白，可以在一开始就整理自己的blog！！

ps：后续文档内容都会转为blog的形式供大家参考学习和交流。共同进步。

们对Markdown编辑器进行了一些功能拓展与语法支持，除了标准的Markdown编辑器功能，我们增加了如下几点新功能，帮助你用它写博客：

1. 全新的界面设计，将会带来全新的写作体验；
2. 在创作中心设置你喜爱的代码高亮样式，Markdown将代码片显示选择的高亮样式进行展示；
3. 增加了图片拖拽功能，你可以将本地的图片直接拖拽到编辑区域直接展示；
4. 全新的KaTeX数学公式语法；
5. 增加了支持甘特图的mermaid语法1功能；
6. 增加了多屏幕编辑Markdown文章功能；
7. 增加了焦点写作模式、预览模式、简洁写作模式、左右区域同步滚轮设置等功能，功能按钮位于编辑区域与预览区域中间；
8. 增加了检查列表功能。

功能快捷键

| | | | |
|-------|--------------|---|-----------|
| 撤销: | Ctrl/Command | + | Z |
| 重做: | Ctrl/Command | + | Y |
| 加粗: | Ctrl/Command | + | B |
| 斜体: | Ctrl/Command | + | I |
| 标题: | Ctrl/Command | + | Shift + H |
| 无序列表: | Ctrl/Command | + | Shift + U |
| 有序列表: | Ctrl/Command | + | Shift + O |
| 检查列表: | Ctrl/Command | + | Shift + C |
| 插入代码: | Ctrl/Command | + | Shift + K |
| 插入链接: | Ctrl/Command | + | Shift + L |
| 插入图片: | Ctrl/Command | + | Shift + G |
| 查找: | Ctrl/Command | + | F |
| 替换: | Ctrl/Command | + | G |

合理的创建标题，有助于目录的生成

直接输入1次 `#`，并按下 `space` 后，将生成1级标题。

输入2次 `#`，并按下 `space` 后，将生成2级标题。

以此类推，我们支持6级标题。有助于使用 `TOC` 语法后生成一个完美的目录。

如何改变文本的样式

强调文本 强调文本

加粗文本 加粗文本

标记文本

删除文本

引用文本

H₂O is是液体。

2¹⁰ 运算结果是 1024.

插入链接与图片

链接: [link](#).



图片:



带尺寸的图片:

居中的图片:



居中并且带尺寸的图片:



当然,我们为了让用户更加便捷,我们增加了图片拖拽功能。

如何插入一段漂亮的代码片

去博客设置页面,选择一款你喜欢的代码片高亮样式,下面展示同样高亮的 `代码片` .

```
// An highlighted block  
var foo = 'bar';
```

生成一个适合你的列表

- 项目
 - 项目
 - 项目

1. 项目1
2. 项目2
3. 项目3

- 计划任务
- 完成任务

创建一个表格

一个简单的表格是这么创建的:

| 项目 | Value |
|----|--------|
| 电脑 | \$1600 |
| 手机 | \$12 |
| 导管 | \$1 |

设定内容居中、居左、居右

使用 `:-----`: 居中

使用 `:-----` 居左

使用 `-----`: 居右

| | | |
|-----|-----|-----|
| 第一列 | 第二列 | 第三列 |
|-----|-----|-----|

| 第一列 | 第二列 | 第三列 |
|---------|---------|---------|
| 第一列文本居中 | 第二列文本居右 | 第三列文本居左 |

SmartyPants

SmartyPants将ASCII标点字符转换为“智能”印刷标点HTML实体。例如：

| TYPE | ASCII | HTML |
|------------------|-------------------------------|----------------------------|
| Single backticks | 'Isn't this fun?' | 'Isn't this fun?' |
| Quotes | "Isn't this fun?" | "Isn't this fun?" |
| Dashes | -- is en-dash, --- is em-dash | – is en-dash, — is em-dash |

创建一个自定义列表

Markdown

Text-to- [HTML](#) conversion tool

Authors

John

Luke

如何创建一个注脚

一个具有注脚的文本。2

注释也是必不可少的

Markdown将文本转换为 [HTML](#)。

KaTeX数学公式

您可以使用渲染LaTeX数学表达式 KaTeX:

Gamma公式展示 $\Gamma(n) = (n-1)! \forall n \in \mathbb{N}$ 是通过对欧拉积分

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt$$

你可以找到更多关于的信息 [LaTeX](#) 数学表达式 [here](#).

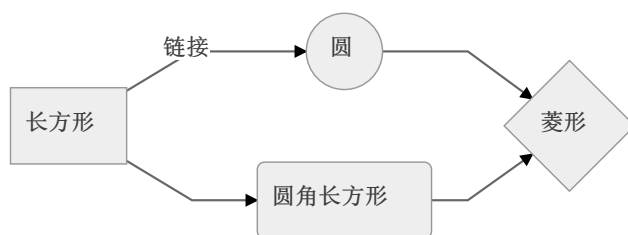
新的甘特图功能，丰富你的文章

- 关于 [甘特图](#) 语法，参考 [这儿](#),

UML 图表

可以使用UML图表进行渲染。 [Mermaid](#). 例如下面产生的一个序列图：

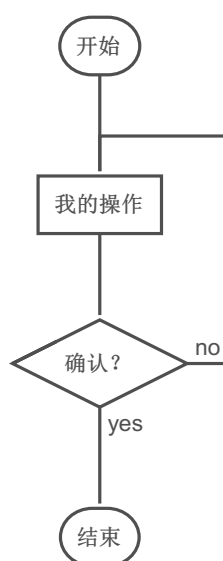
这将产生一个流程图。：



- 关于 **Mermaid** 语法，参考 [这儿](#)，

Flowchart流程图

我们依旧会支持flowchart的流程图：



- 关于 **Flowchart**流程图 语法，参考 [这儿](#)。

导出与导入

导出

如果你想尝试使用此编辑器，你可以在此篇文章任意编辑。当你完成了一篇文章的写作，在上方工具栏找到 **文章导出**，生成一个.md文件或者.html文件进行本地保存。

导入

如果你想加载一篇你写过的.md文件，在上方工具栏可以选择导入功能进行对应扩展名的文件导入，继续你的创作。

[mermaid语法说明](#) □□

[注脚的解释](#) □□