

misc—txt零宽度字符隐写+例题理解

原创

[LJW_wenjingli7](#) 于 2021-12-23 12:17:02 发布 317 收藏 1

文章标签: [css3](#) [css](#) [html](#)

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/LJW_wenjingli7/article/details/122096840

版权

**放在最前面, 收获新知识! 感谢大佬:

[零宽度字符: 和谐? 屏蔽? 不存在的 - 掘金 \(juejin.cn\)misc学习笔记1-txt零宽度字符隐写_Amherstieae的博客-CSDN博客_零宽隐写](#)

零宽度字符概念

零宽度字符是一种字节宽度为0的不可打印的Unicode字符, 在浏览器等环境不可见, 但是真实存在, 获取字符串长度时也会占位置, 表示某一种控制功能的字符。

**常见的零宽度字符及它们的unicode码和原本用途

(1) 零宽空格 (zero-width space, ZWSP) 用于可能需要换行处。

Unicode: U+200B HTML: `​`

(2) 零宽不连字 (zero-width non-joiner, ZWNJ)放在电子文本的两个字符之间, 抑制本来会发生的连字, 而是以这两个字符原本的字形来绘制。

Unicode: U+200C HTML: `‌`

(3) 零宽连字 (zero-width joiner, ZWJ) 是一个控制字符, 放在某些需要复杂排版语言 (如阿拉伯语、印地语) 的两个字符之间, 使得这两个本不会发生连字的字符产生了连字效果。

Unicode: U+200D HTML: `‍`

(4) 左至右符号 (Left-to-right mark, LRM) 是一种控制字符, 用于计算机的双向文稿排版中。

Unicode: U+200E HTML: `‎` 或 `‎`

(5) 右至左符号 (Right-to-left mark, RLM) 是一种控制字符, 用于计算机的双向文稿排版中。

Unicode: U+200F HTML: `‏` 或 `‏`

(6) 字节顺序标记 (byte-order mark, BOM) 常被用来当做标示文件是以UTF-8、UTF-16或UTF-32编码的标记。

Unicode: U+FEFF

零宽度字符的作用

1.数据防爬

将零宽度字符插入关键词文本中, 使得匹配关键字时不能正确匹配, 但是不影响用户的正常阅读

2.信息隐藏 (类似水印)

类似上面例子我们可以将信息隐藏在正常文字中而不影响阅读, 也可做加密信息分享

0x03零宽度字符怎么进行隐写呢

隐写方法是可逆的，但是需要是相同的方法或者是网站呀~

具体可以参考盖乐希师傅的博客2333（日常膜盖乐希

[浅谈基于零宽度字符的隐写方式 - Ga1@xy's Wor1d](#)

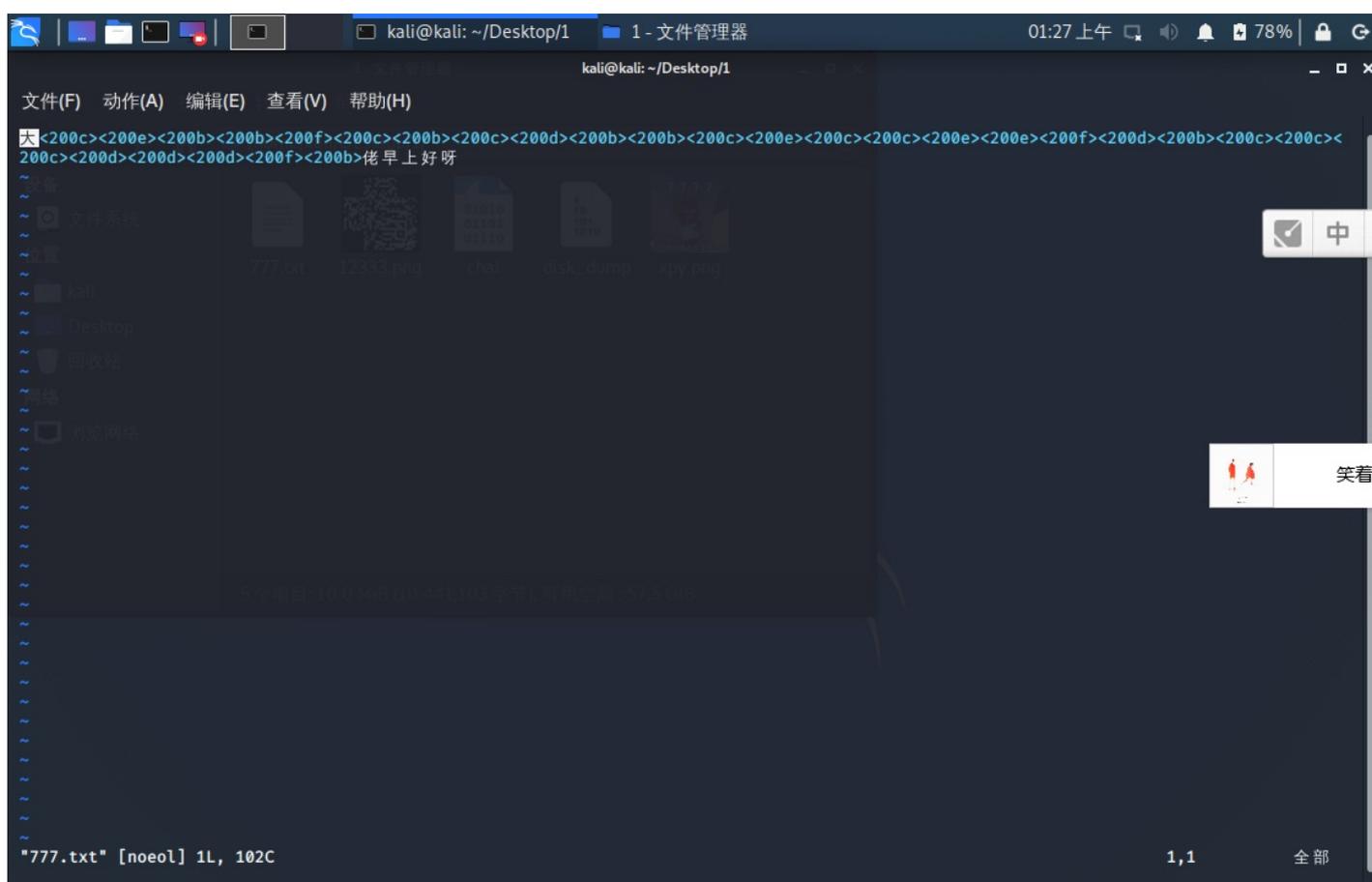
这个水平有限，没来得及学脚本语言，没有很好理解怎么隐写，就附上大佬的分享了 Orz

判断零宽度字符

1.Kali中

vim file.txt

(测试一下比较好)



蓝色部分就是零宽度字符

2.在010或者winhex打开



3.在光标移动中有明显的停顿感

*我自己在复制题目文本的时候明显感觉到光标闪烁，以为是正常现象，看到这个总结就去试了别的正常文本，反而是比较顺滑的。嘿，下次遇到题目再试试！

看文本区，可以找到原本那句话。那么中间有规律的字符串就是零宽度字符，确定是零宽度字符，那就可以解密了。

Unicode Steganography with Zero-Width Characters

http://330k.github.io/misc_tools/unicode_steganography.js

Text in Text Steganography Sample

Original Text: (length: 39)

can you find out the flag in this word?

Hidden Text: (length: 24)

flag{you_are_so_clever!}

Steganography Text: (length: 231)

can you find out the flag in this word?

CSDN @LJW_wenjingli7

按照提示将原始文本放入，encode可查看真实长度，decode即得。