零宽字符隐写——2021网刃杯CTF 签到

原创

iO快到碗里来 于 2021-09-22 22:35:38 发布 604 收藏 3

分类专栏： Web安全 CTF 文章标签： 加密解密

本文链接：https://blog.csdn.net/qq_45927266/article/details/120423818

Web安全 同时被 2 个专栏收录

15 篇文章 0 订阅

订阅专栏

CTF

4 篇文章 0 订阅

订阅专栏

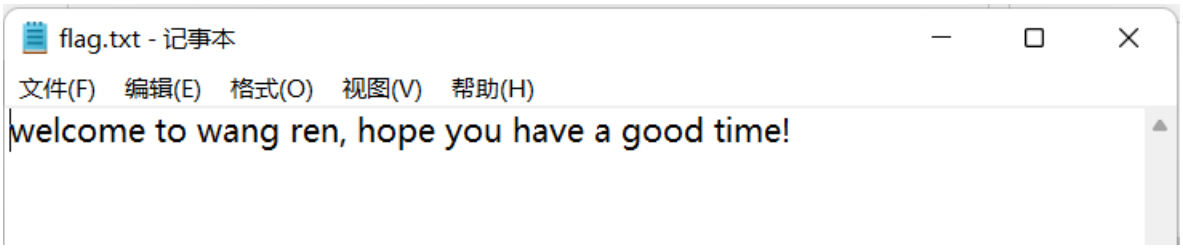
0x01 零宽字符

零宽度字符是一些不可见的，不可打印的字符。它们存在于页面中主要用于调整字符的显示格式，下面就是一些常见的零宽度字符及它们的unicode码和原本用途：

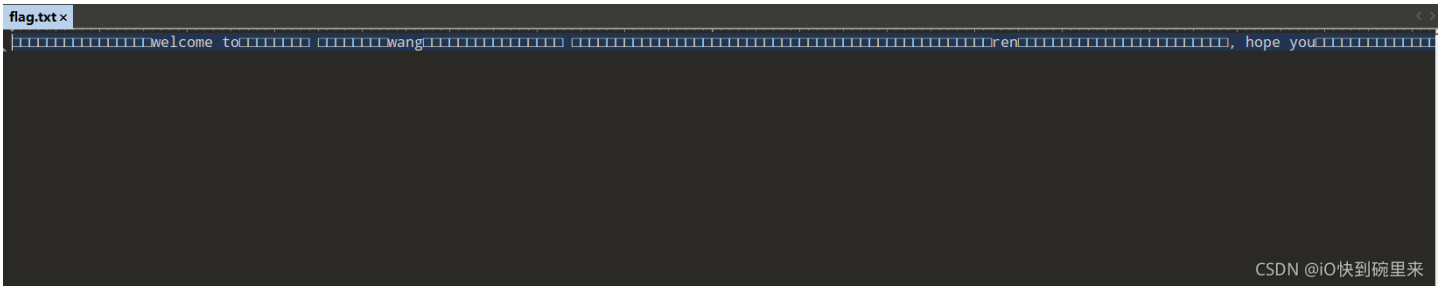
- 零宽度空格符 (zero-width space) U+200B : 用于较长单词的换行分隔
- 零宽度非断空格符 (zero width no-break space) U+FEFF : 用于阻止特定位置的换行分隔
- 零宽度连字符 (zero-width joiner) U+200D : 用于阿拉伯文与印度语系等文字中，使不会发生连字的字符间产生连字效果
- 零宽度断字符 (zero-width non-joiner) U+200C : 用于阿拉伯文，德文，印度语系等文字中，阻止会发生连字的字符间的连字效果
- 左至右符 (left-to-right mark) U+200E : 用于在混合文字方向的多种语言文本中（例：混合左至右书写的英语与右至左书写的希伯来语），规定排版文字书写方向为左至右
- 右至左符 (right-to-left mark) U+200F : 用于在混合文字方向的多种语言文本中，规定排版文字书写方向为右至左

0x02 字符特征

一般的文本编辑器：



010Editor/WinHex：



vim：

通常情况下，零宽度字符在一般的文本编辑器中是不可见的，这也是其被作为隐写的根本原因。

0x03 如何隐写

> 每一种基于零宽度字符的隐写都可以有自己的隐写方式及加密方式，所以可能用这一个工具（或脚本）加密过的字符串在另一个解密网站就无法成功解密……

- 转化为二进制的加密：https://zhuanlan.zhihu.com/p/87919817
- 转化为Morse编码的加密：https://zhuanlan.zhihu.com/p/75992161

加密方式虽多种多样，但万变不离其宗。零宽度字符隐写就是将想要隐藏的内容，用各种零宽字符的排列组合来代替，从而达到隐写的目的。本质上其实就是一种编码，类似于Unicode或ASCII。

注：加密和解密是一个可逆的过程，但是一定要用相同的方式（相同的工具/网址）进行加解密。

0x04 相关工具

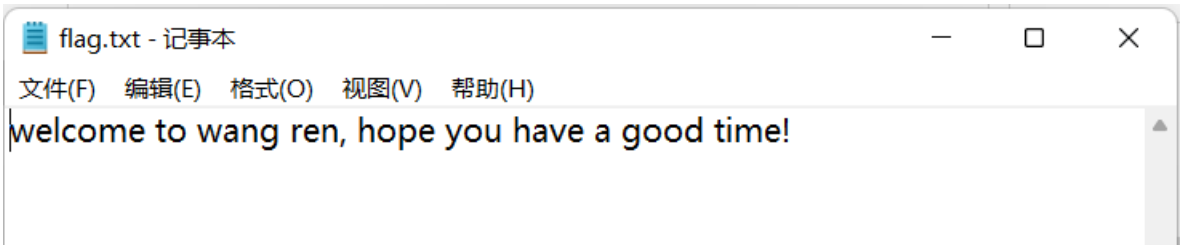
- http://330k.github.io/misc_tools/unicode_steganography.html
- https://offdev.net/demos/zwsp-steg-js

0x05 相关使用

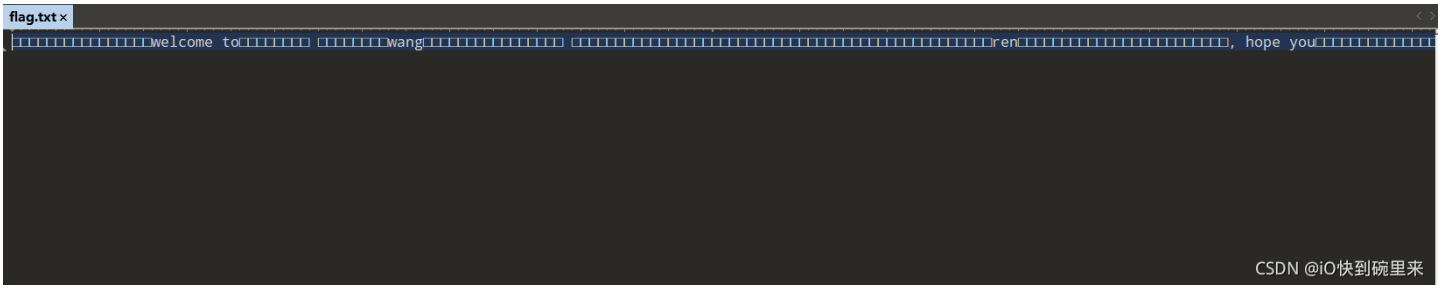
- 隐形水印
- 逃脱敏感词匹配
- 传递隐秘信息

0x06 网刃杯CTF

进入题目拿到一个压缩包，解压后得到 flag.txt 和 cipher.txt， 打开 flag.txt：



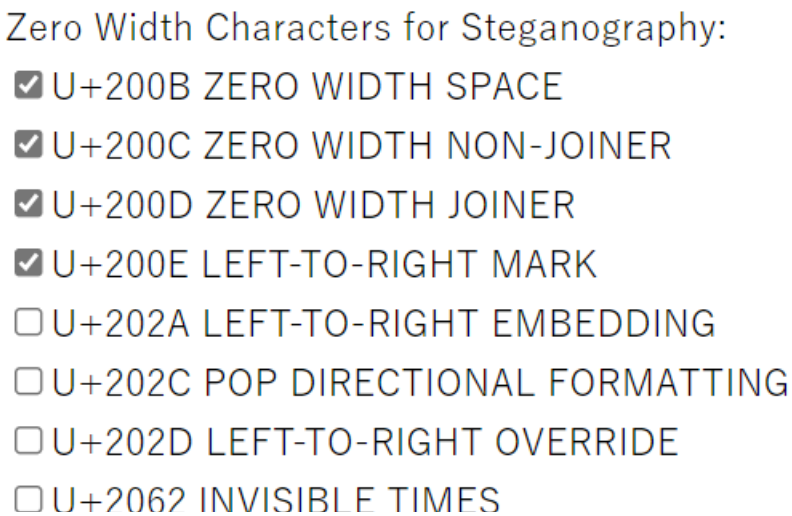
010editor 打开：

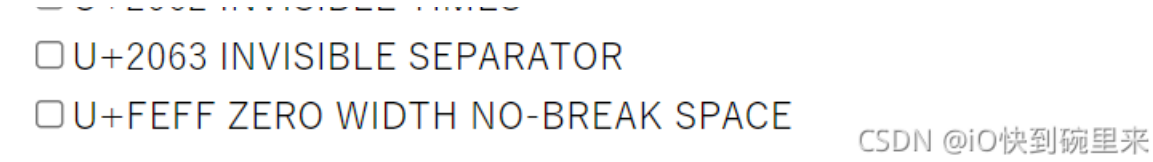


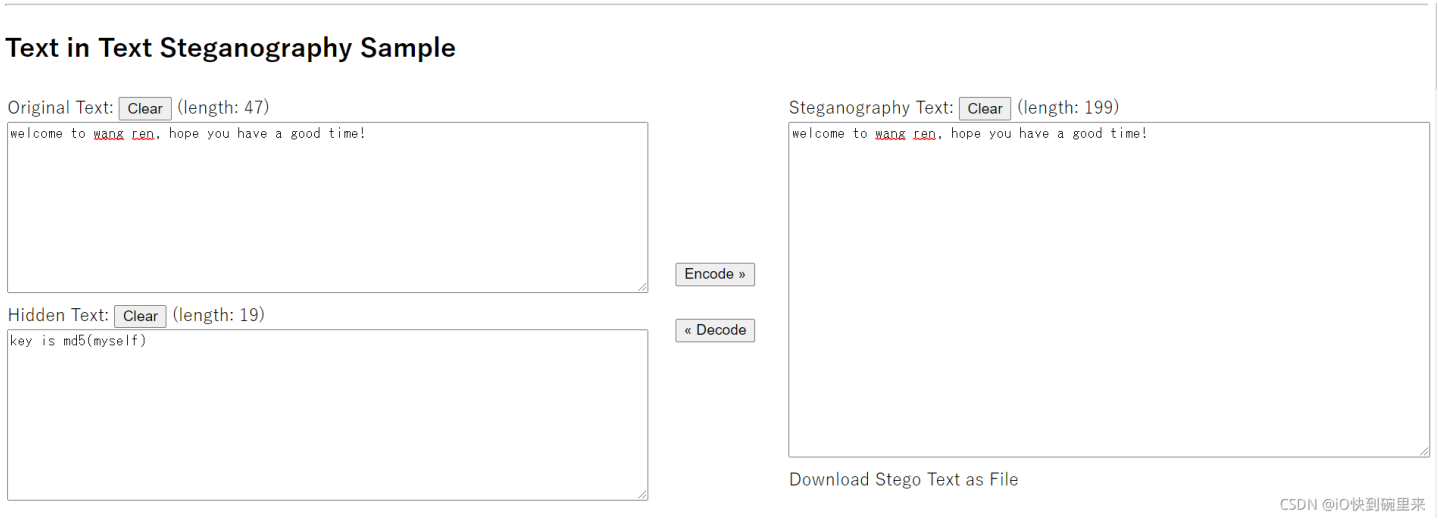
存在隐藏字符，初步判定是零宽隐写。

vim 打开：

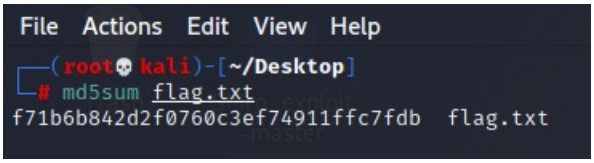
发现 200b、200c、200d、200e，用 http://330k.github.io/misc_tools/unicode_steganography.html 勾选这四个选项：







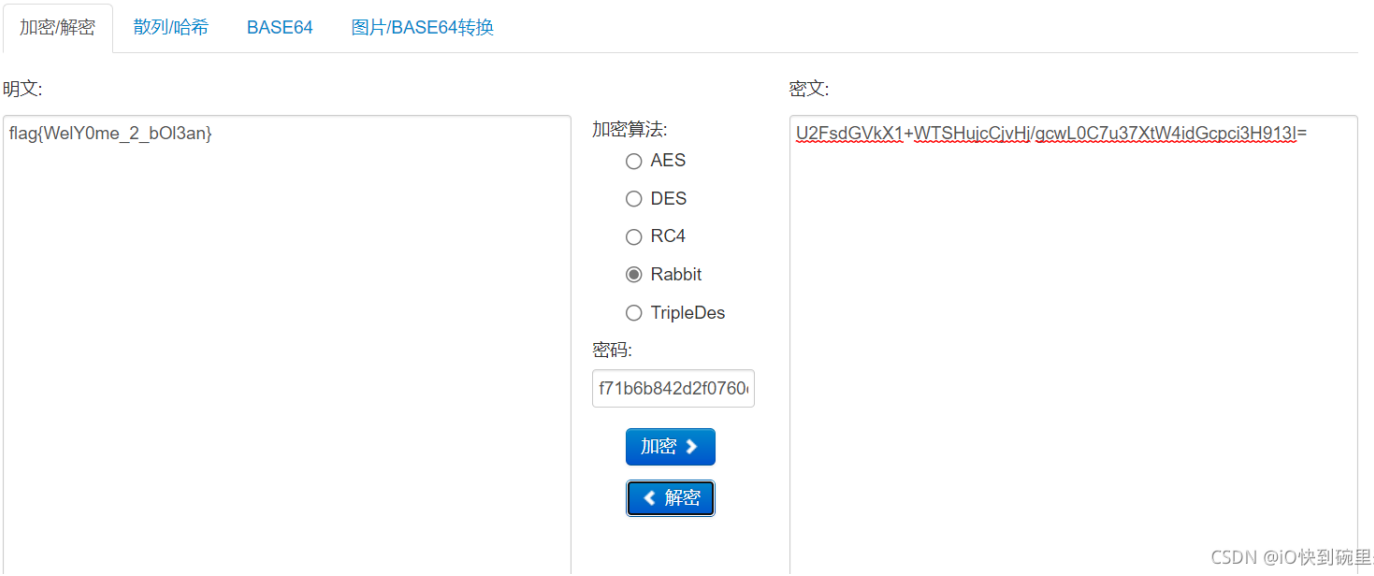
根据提示，生成 flag.txt md5 校验和：



key = f71b6b842d2f0760c3ef74911ffc7fdb

注：这里不能直接拿 flag.txt 的文本内容进行 md5 加密

用 https://tool.oschina.net/encrypt 尝试对 cipher.txt 中的内容进行解密：



最终使用 Rabbit 算法解得 flag{WelY0me_2_bOl3an}

0x07 Reference

http://www.ga1axy.top/index.php/archives/20/