**空白隐写**

1. **零宽字符隐写**

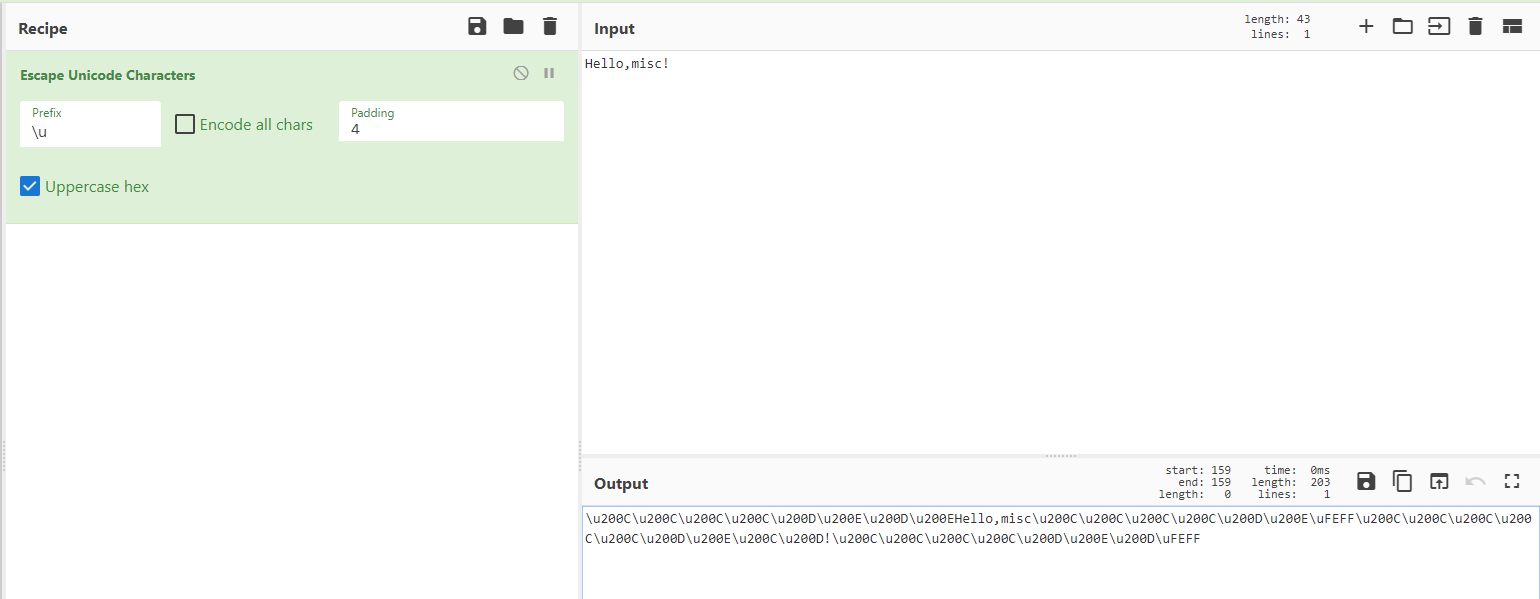
## 什么是零宽度字符

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：

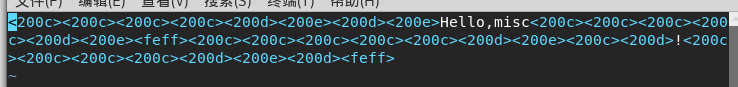
* 零宽度空格符 (zero-width space) U+200B : 用于较长单词的换行分隔
* 零宽度非断空格符 (zero width no-break space) U+FEFF : 用于阻止特定位置的换行分隔
* 零宽度连字符 (zero-width joiner) U+200D : 用于阿拉伯文与印度语系等文字中，使不会发生连字的字符间产生连字效果
* 零宽度断字符 (zero-width non-joiner) U+200C : 用于阿拉伯文，德文，印度语系等文字中，阻止会发生连字的字符间的连字效果
* 左至右符 (left-to-right mark) U+200E : 用于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

## 为什么可以用于隐写

零宽度字符在通常情况下，在一般的文本编辑器中是不可见的，比如：‌‌‌‌‍‎‍‎Hello,misc‌‌‌‌‍‎﻿‌‌‌‌‌‍‎‌‍!‌‌‌‌‍‎‍﻿  
在这句话中我就用零宽度字符隐藏了信息，用CyberChef查看一下即可发现其中的奥秘

[](https://s1.ax1x.com/2020/04/04/GwBA41.png)

当然，将文本储存为txt格式，用vim查看也可以直接看到其中隐藏的零宽度字符

[](https://s1.ax1x.com/2020/04/04/GwBZ36.png)

## 如何达到隐写的目的

关于这一点，我查找了很多的资料，其实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……

在此我先贴上几篇文章，供大家参考：

* 转化为二进制的加密：[https://zhuanlan.zhihu.com/p/87919817](https://zhuanlan.zhihu.com/p/87919817" \t "http://www.ga1axy.top/index.php/archives/20/_blank)
* 转化为Morse编码的加密：[https://zhuanlan.zhihu.com/p/75992161](https://zhuanlan.zhihu.com/p/75992161" \t "http://www.ga1axy.top/index.php/archives/20/_blank)

加密方式虽多种多样，但万变不离其宗。使用零宽度字符隐写，关键是将想要隐藏的内容用零宽度字符来表示，通过使用不同的零宽度字符，以及不同字符间的排列组合方式来达到隐写的目的

****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****

## 相关工具

在线解密[1]：[http://330k.github.io/misc\_tools/unicode\_steganography.html](http://330k.github.io/misc_tools/unicode_steganography.html" \t "http://www.ga1axy.top/index.php/archives/20/_blank)  
在线解密[2]：[https://offdev.net/demos/zwsp-steg-js](https://offdev.net/demos/zwsp-steg-js" \t "http://www.ga1axy.top/index.php/archives/20/_blank)

GitHub上相关的项目（这两个项目在上面的文章中都有提到）：

* [https://github.com/yuanfux/zero-width-lib](https://github.com/yuanfux/zero-width-lib" \t "http://www.ga1axy.top/index.php/archives/20/_blank)
* [https://github.com/rover95/morse-encrypt](https://github.com/rover95/morse-encrypt" \t "http://www.ga1axy.top/index.php/archives/20/_blank)

## 零宽度字符的其他用法

* 隐形水印
* 逃脱敏感词匹配
* 传递隐秘信息

相关文章：

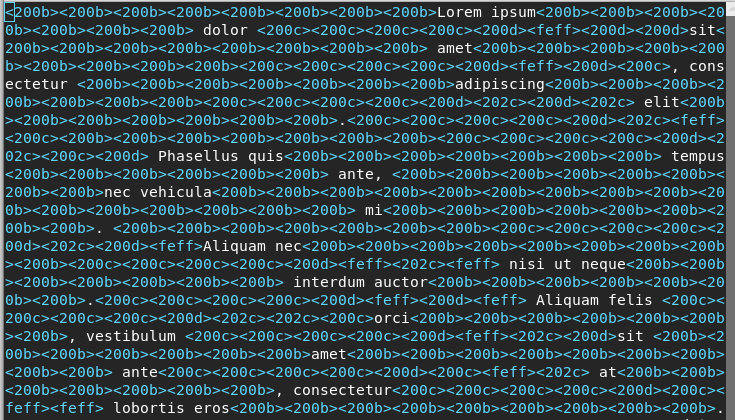
* [用零宽度字符水印揭露泄密者身份](https://www.freebuf.com/articles/web/167903.html" \t "http://www.ga1axy.top/index.php/archives/20/_blank)
* [零宽度字符：和谐？屏蔽？不存在的](https://juejin.im/post/5b87a6e26fb9a019b953ee8b" \t "http://www.ga1axy.top/index.php/archives/20/_blank)

## 例题：[UTCTF2020] zero

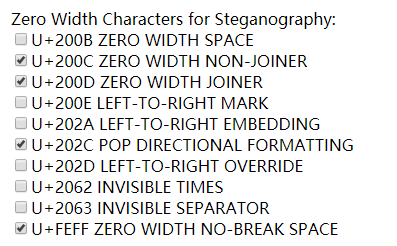
附件链接：[https://pan.baidu.com/s/1Ivadp2r9cbKjIZM2vSFDQw](https://pan.baidu.com/s/1Ivadp2r9cbKjIZM2vSFDQw" \t "http://www.ga1axy.top/index.php/archives/20/_blank)

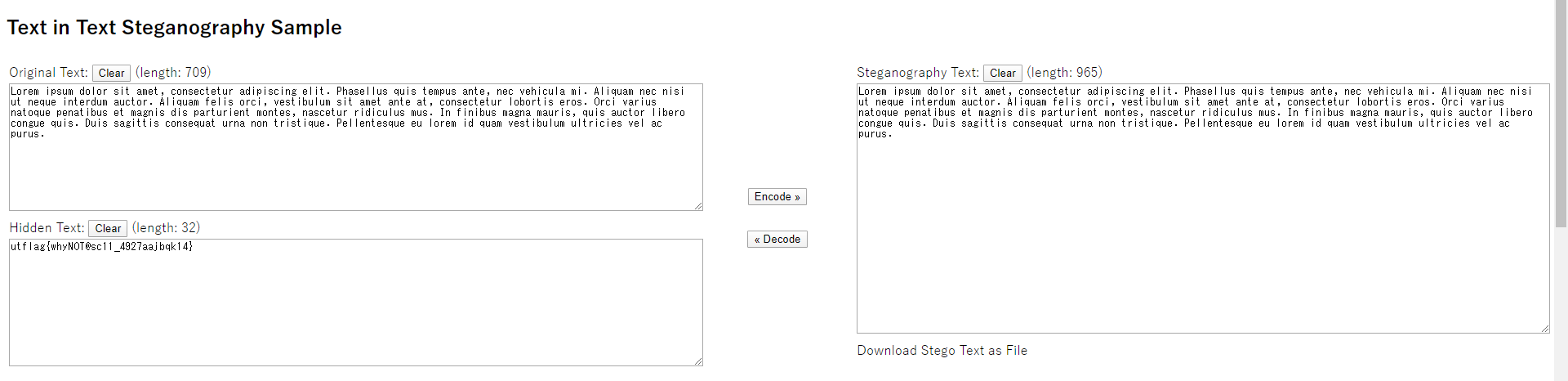
提取码：7vmf

下载附件得到一个txt文件，里面是一长段英文，乍一看没有什么特别的地方，但是将这个文件用vim查看，就会发现其中隐藏了大量的信息

[](https://s1.ax1x.com/2020/04/04/GwBuuD.png)

很显然是零宽度字符隐写，[在线网站](http://330k.github.io/misc_tools/unicode_steganography.html" \t "http://www.ga1axy.top/index.php/archives/20/_blank)弄一下，在上图中可以看到共有五种零宽度字符，尝试一下将U+200B这一项去掉，选择其他四种字符进行解密，就可以得到flag（但是我还不是很清楚为什么要将U+200B去掉）

[](https://s1.ax1x.com/2020/04/04/GwBUKS.png)

[](https://s1.ax1x.com/2020/04/04/GwBvad.png)

得到flag：flag{whyNOT@sc11\_4927aajbqk14}

**来源：**[浅谈基于零宽度字符的隐写方式](http://www.ga1axy.top/index.php/archives/20/)

**其他题目：**

[BUUCTF Misc 色彩&彩虹题](https://www.cnblogs.com/LEOGG321/p/14095849.html)（autokey+零宽字符隐写+RGB值+encrypto）

1. **Snow隐写**

**Snow HTML 隐写**

snow 是一款在html嵌入隐写信息的软件，

它的原理是通过在文本文件的末尾嵌入空格和制表位的方式嵌入隐藏信息，

不同空格与制表位的组合代表不同的嵌入信息。

解密网址：<http://fog.misty.com/perry/ccs/snow/snow/snow.html>

**Snow加密**

这里介绍几个参数

-C 在隐藏或解压数据时压缩数据

-q 安静模式，如果没有设置，程序报告统计数据，例如压缩百分比和可用存储空间的数量

-S 显示可用空间的概数

-p 如果设置了这个参数，那么数据会被加密，则解密需要设定的密码

-l 设定一个数值，则加密产生的空格总会小于它，默认为80

-f 指定文件名，把该文件中的内容存储到制定输出文件中

-m 指定消息字符串，将其隐藏在文件中

来源：[Snow加密了解一下？](https://www.cnblogs.com/Paranoid-4/p/9284090.html)

**利用snow**

     实现步骤：在又snow和文件的界面打开命令窗口输入snow.exe   -C   -m  "被隐藏的信息“ -p "文件名“   用winhex可查看被插入数据

-C为压缩或解压选项      
-M后跟需要隐藏的数据   
-p为加密密码

**题目：**

**[5.snow隐写](https://blog.csdn.net/zippo1234/article/details/109447787)**

**[Here are three packages！](https://blog.csdn.net/solitudi/article/details/114115801)**