

# ctfshow-文本隐写

原创

[admin\\_9111](#) 已于 2022-04-20 20:31:12 修改 135 收藏

分类专栏: [ctfshow-Misc](#) 文章标签: [系统安全](#)

于 2022-04-20 20:29:05 首次发布

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/m0\\_67507776/article/details/124305063](https://blog.csdn.net/m0_67507776/article/details/124305063)

版权



[ctfshow-Misc](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

Challenge

146 Solves

×

## 文本隐写

20

无限接近死亡, 方能领悟生存的真谛。

感谢@TSW\_cc提供的题目

[stega20.zip](#)

Flag

Submit

1.打开文档, 结尾处回车发现无反应, 可能有东西点击文件-选项-视图-隐藏文字, 发现两种不同的符号

CTFshow 交流群: 372619038

本群倡导友好、和谐、欢乐、进取的学习精神。

严格遵守等级制度, 进来的一律以大佬自称, 并逐步升级为菜狗、菜鸡、菜鸟、菜虫、菜笔、菜刀。不准自称菜狗这么荣耀的称号, 必须自称本大佬。

近期每天一道红包题, 作者也秉承恶搞又不失内涵的作风, 为大家学习路上增添欢乐!

CTF, show

全体管理敬上

By: 多次拒绝赵丽颖



2.将两种字符, 短的替换为0, 长的替换为1, 然后二进制转ascii字符

输入文本内容:

```
0110111101100110011001100110011011001010011101000110000011110000011001100110100001110010011000000001010
```

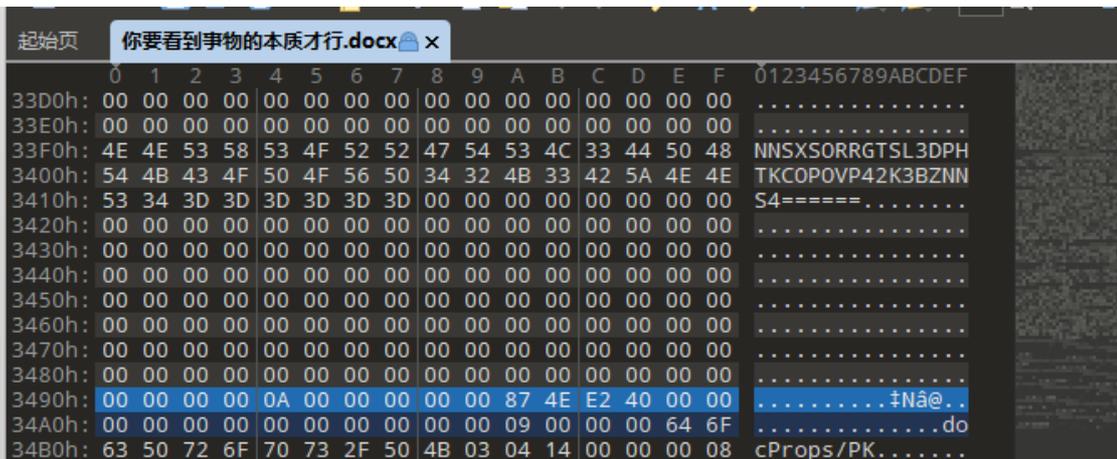
字符转二进制

二进制转字符

输出结果

```
offset:0x3490
```

3.根据提示使用二进制工具 (010 Editor) 找到位置, 发现上面有字符串编码



NNSXSORRGTSL3DPHTKCOPOVP42K3BZNNS4=====

#### 4.使用base32解码

NNSXSORRGTSL3DPHTKCOPOVP42K3BZNNS4=====

编码 解码 清空

key:14位的纯数字

key:14位的纯数字

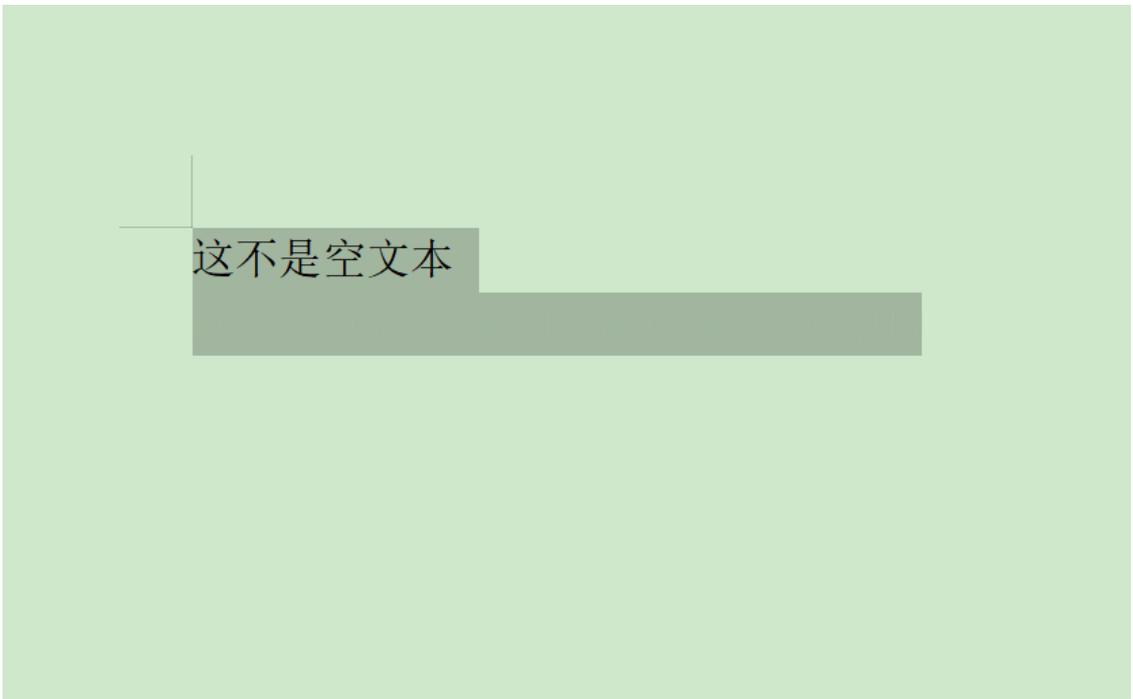
#### 5.自33940行起，复制编码，新建粘贴

起始页	你要看到事物的本质才行.docx	无标题1*
	0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF	
3430h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
3440h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
3450h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
3460h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
3470h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
3480h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
3490h:	00 00 00 00 0A 00 00 00 00 00 87 4E E2 40 00 00	..... †Nâ@..
34A0h:	00 00 00 00 00 00 00 00 00 00 09 00 00 00 64 6F	..... do
34B0h:	63 50 72 6F 70 73 2F 50 4B 03 04 14 00 00 00 08	cProps/PK.....
34C0h:	00 87 4E E2 40 27 62 61 27 5B 01 00 00 70 02 00	.†Nâ@'ba' [...p..
34D0h:	00 10 00 00 00 64 6F 63 50 72 6F 70 73 2F 61 70	....docProps/ap
34E0h:	70 2E 78 6D 6C 9D 91 51 6F 82 30 14 85 DF 97 EC	p.xml.'Qo,0...ß-i
34F0h:	3F 10 DE A1 05 C1 A9 29 18 87 F3 69 D9 4C C4 F9	?..þj.Á@).†óíÛLÄù

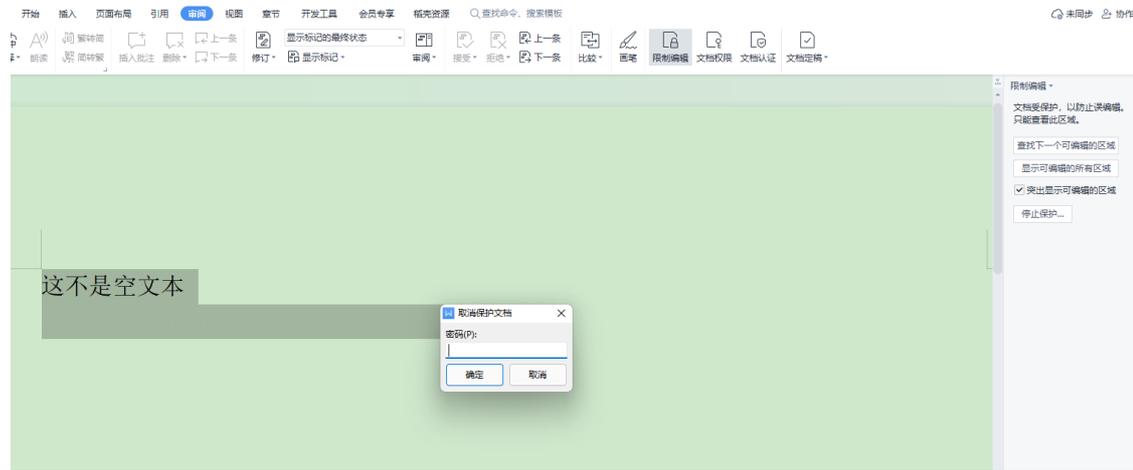
#### 6.新建文件中头部更改为文档格式，另存为doc格式（zip与doc头部标识一样）

起始页	你要看到事物的本质才行.docx	无标题1* x
	0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF	
0000h:	50 4B 03 04 0A 00 00 00 00 00 87 4E E2 40 00 00	PK..... †Nâ@..
0010h:	00 00 00 00 00 00 00 00 00 00 09 00 00 00 64 6F	..... do
0020h:	63 50 72 6F 70 73 2F 50 4B 03 04 14 00 00 00 08	cProps/PK.....
0030h:	00 87 4E E2 40 27 62 61 27 5B 01 00 00 70 02 00	.†Nâ@'ba' [...p..
0040h:	00 10 00 00 00 64 6F 63 50 72 6F 70 73 2F 61 70	....docProps/ap
0050h:	70 2E 78 6D 6C 9D 91 51 6F 82 30 14 85 DF 97 EC	p.xml.'Qo,0...ß-i
0060h:	3F 10 DE A1 05 C1 A9 29 18 87 F3 69 D9 4C C4 F9	?..þj.Á@).†óíÛLÄù
0070h:	68 9A 72 95 66 D0 36 6D 35 FA EF 57 64 51 F6 BA	hšr•fÐ6m5úîWdQø°
0080h:	B7 7B CE 6D 4F BE F6 90 F9 A5 6D BC 33 68 C3 A5	·{Îm0%ö.ù¥m¼3hÃ¥
0090h:	C8 FC 28 C4 BE 07 82 C9 8A 8B 63 E6 6F CB 55 30	ÈÛ(Á¾.,ÉŠ<cæøÉUO

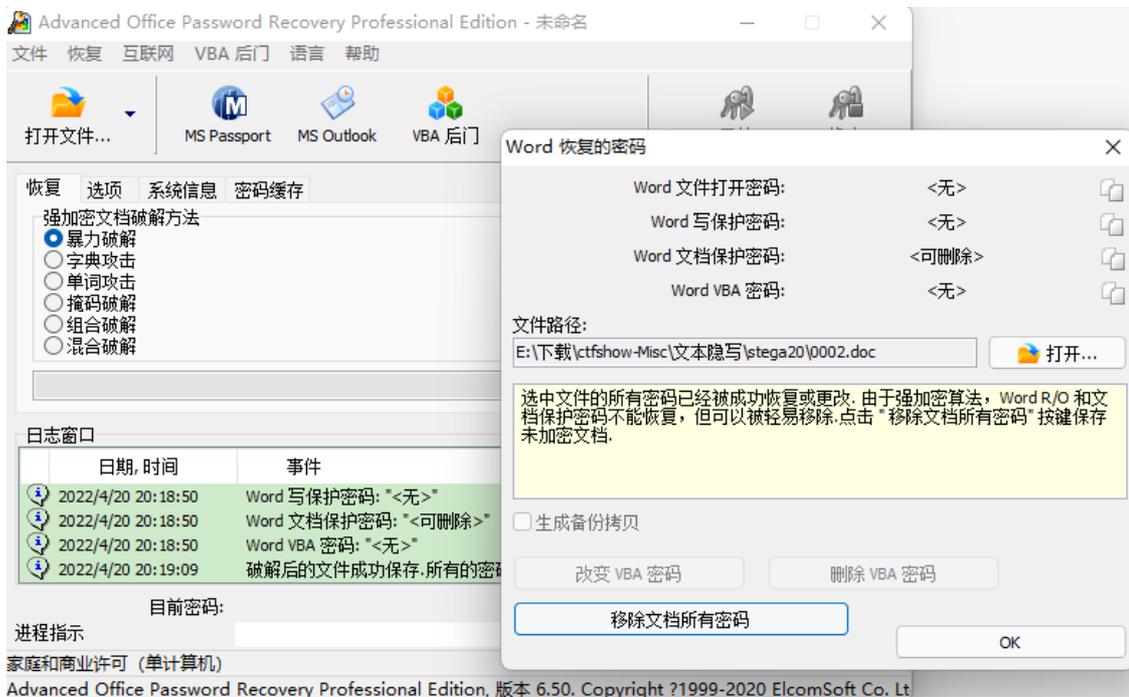
#### 7.打开doc文档，发现有隐藏内容



8.一番操作没有什么用，点击审阅-限制编辑-右侧停止保护，发现需要输入密码



9.此处可用word文档密码爆破工具爆破，根据提示为14位进行暴力破解



10.也可以直接将文档另存为html格式，直接浏览器打开，右键查看网页源码找到隐藏部分

```
div.Section0[page:Section0:]</style></head><body style="tab-interval:21pt;text-justify-trim:punctuation;" ><!--StartFragment--><div class="Section0" style="layout-grid:15.6000pt;" ><p class=Msc
mso-hansi-font-family:Calibri;mso-bidi-font-family:'Times New Roman';font-size:10.5000pt;
mso-font-kering:1.0000pt;" ><font face="宋体" >这不是空文本</font></span><span style="mso-spacerun:'yes';font-family:宋体;mso-ascii-font-family:Calibri;
mso-hansi-font-family:Calibri;mso-bidi-font-family:'Times New Roman';font-size:10.5000pt;
mso-font-kering:1.0000pt;" ><o:p></o:p></span></p><p class=MsoNormal ><span style="mso-spacerun:'yes';font-family:Calibri;mso-fareast-font-family:宋体;
mso-bidi-font-family:'Times New Roman';color:rgb(206,234,202);display:none;
mso-hide:all;font-size:10.5000pt;mso-font-kering:1.0000pt;" >RmxhZyU3QnNob3dfY3RmX3Rzd19jYyU3RA==</span><span style="mso-spacerun:'yes';font-family:Calibri;mso-fareast-font-family:宋体;
mso-bidi-font-family:'Times New Roman';color:rgb(206,234,202);display:none;
mso-hide:all;font-size:10.5000pt;mso-font-kering:1.0000pt;" ><o:p></o:p></span></p></div><!--EndFragment--></body></html>
```

RmxhZyU3QnNob3dfY3RmX3Rzd19jYyU3RA==

11.base64解码得到flag



flag{show\_ctf\_tsw\_cc}