

刷题之旅第40站,CTFshow 文本隐写

原创

圆圈勾勒成指纹 于 2020-02-20 14:19:12 发布 2035 收藏 7

分类专栏: [刷题之旅100站](#)

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/weixin_45940434/article/details/104409437

版权



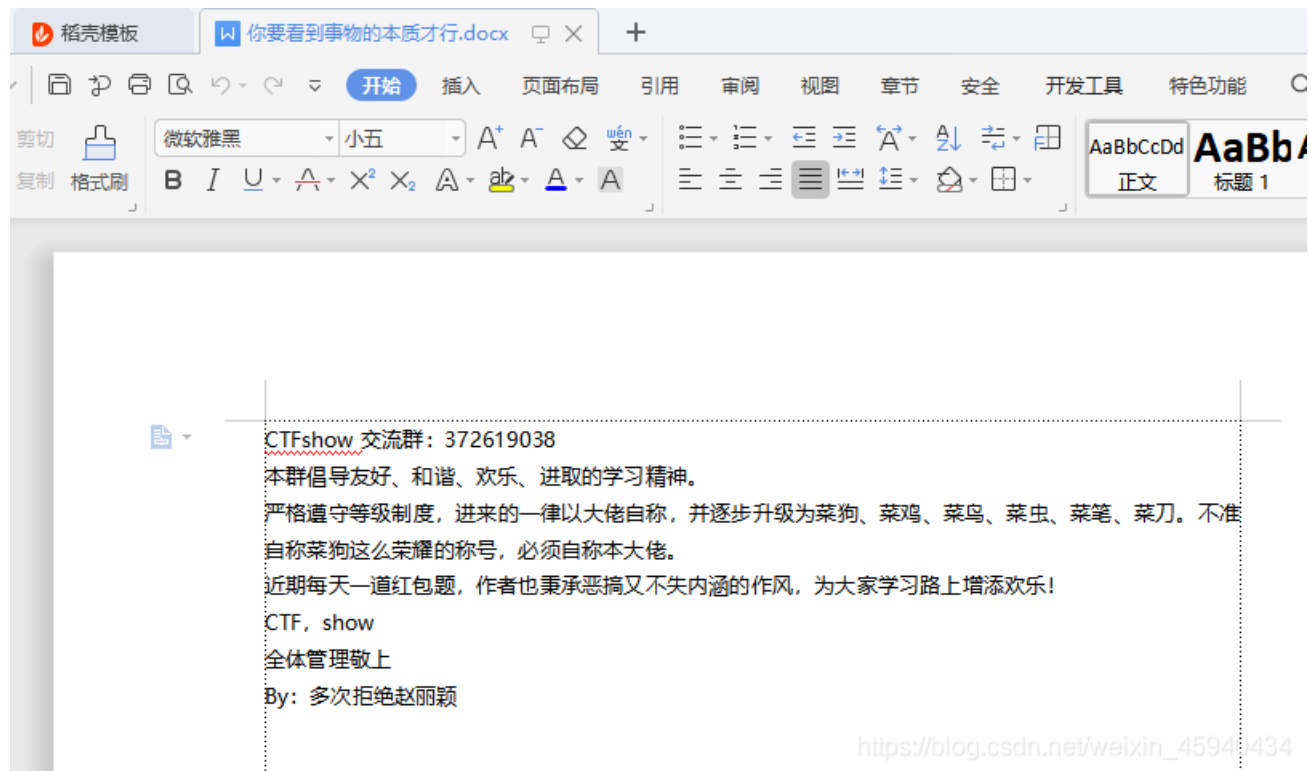
[刷题之旅100站 专栏收录该内容](#)

49 篇文章 11 订阅

订阅专栏

感谢 ctf show 平台提供题目

打开题目文件, 首先我们看到的是很正常的文本。



这时我们打开我们的显示隐藏文字, 才能看到隐藏信息。



选项

视图

- 编辑
- 常规与保存
- 文件位置
- 修订
- 中文版式
- 输出PDF
- 用户信息
- 打印
- 拼写检查
- 安全性
- 信任中心
- 自定义功能区
- 快速访问工具栏

页面显示选项

<input type="checkbox"/> 启动时展开任务窗格(R)	<input checked="" type="checkbox"/> 选择时显示浮动工具栏(D)	导航窗格(P):
<input type="checkbox"/> 隐藏空白(B)	<input checked="" type="checkbox"/> 右键时显示浮动工具栏(G)	<input type="button" value="隐藏"/>
<input checked="" type="checkbox"/> 垂直标尺(C)	<input checked="" type="checkbox"/> 屏幕提示(N)	
<input checked="" type="checkbox"/> 状态栏(U)	<input checked="" type="checkbox"/> 启用实时预览(V)	
<input checked="" type="checkbox"/> 进入页眉页脚提示(Q)		

显示文档内容


<input checked="" type="checkbox"/> 突出显示(H)	<input type="checkbox"/> 域代码(F)	域底纹(E):
<input checked="" type="checkbox"/> 正文边框(X)	<input checked="" type="checkbox"/> 书签(K)	<input type="button" value="选取时显示"/>
<input checked="" type="checkbox"/> 裁剪标记(R)		<input type="button" value="字体替换(O)"/>

格式标记

<input checked="" type="checkbox"/> 空格(S)	<input checked="" type="checkbox"/> 制表符(T)
<input checked="" type="checkbox"/> 段落标记(M)	<input checked="" type="checkbox"/> 隐藏文字(I)
<input checked="" type="checkbox"/> 对象位置(J)	<input checked="" type="checkbox"/> 全部(L)

功能区选项

- 双击选项卡时隐藏功能区(A)
- 单击方框时打勾(O)
- 打开文件, 展示智能识别目录(W)



我们在尾部发现一堆中文 和英文的逗号交替出现。

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,

https://blog.csdn.net/weixin_45940434

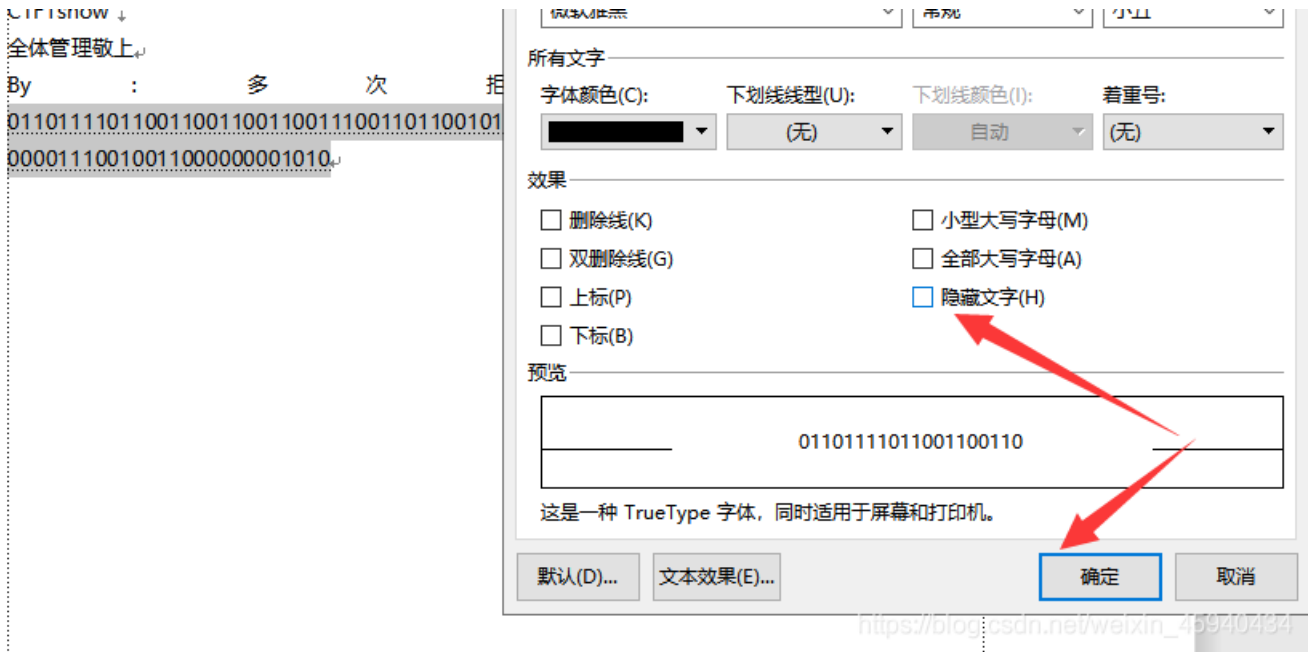
我们把英文逗号替换成0, 中文逗号替换成1.

全体管理敬上↓
By : 多 次 拒 绝 赵 丽 颖
011011110110011001100110011100110110010100111010001100000111100000110011001101
00001110010011000000001010↓



我们直接复制这串二进制是复制不出来的，需要把隐藏文字关了才能复制出来。

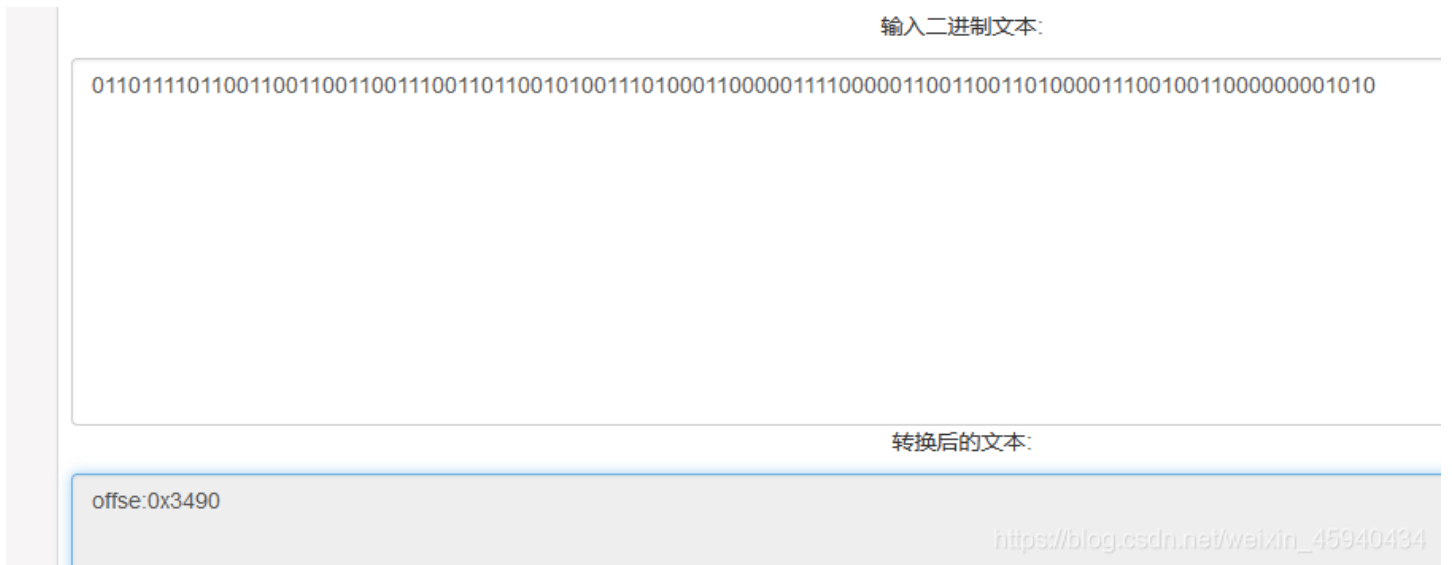
(选中→字体→取消勾选隐藏文字)



转成字符串得到了这个提示：

(这里我疏忽了，原本想打的是offset: 0x3490，少打了一个，但不影响做题。)

offset:0x3490



我们根据提示，使用010editor打开文件，找到偏移量 0x3490的地方。

在上面发现了一串密文，一看全是大写字母+数字，那么base32解密一下。

```

33D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
33E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
33F0h: 4E 4E 53 58 53 4F 52 52 47 54 53 4C 33 44 50 48 NNSXSORRGTSLS3DPH
3400h: 54 4B 43 4F 50 4F 56 50 34 32 4B 33 42 5A 4E 4E TKCOPOVP42K3BZNN
3410h: 53 34 3D 3D 3D 3D 3D 3D 00 00 00 00 00 00 00 00 S4=====
3420h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
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: b0 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...B-i
34F0h: 3F 10 DE A1 05 C1 A9 29 18 87 F3 69 D9 4C C4 F9 ?.Ë;.Ã@).#óïÛLÀù
3500h: 68 9A 72 95 66 D0 36 6D 35 FA EF 57 64 51 F6 BA hšr*fĐ6m5úíWdQó°
3510h: B7 7B CE 6D 4F BE F6 90 F9 A5 6D BC 33 68 C3 A5 -(ÏmO*ó.úÿm+3hÃ¥
3520h: C8 FC 28 C4 BE 07 82 C9 8A 8B 63 E6 6F CB 55 30 Èü(Ã%.ÉŠ<cæoÈU0
3530h: F1 3D 63 A9 A8 68 23 05 64 FE 15 8C 3F CF 9F 9F ñ=c@'h#.dp.Œ?IÝÝ
3540h: C8 5A 4B 05 DA 72 30 9E 8B 10 26 F3 6B 6B D5 0C ÈZK.Ûr0ž<.šókkõ.
3550h: 21 C3 6A 68 A9 09 DD 5A B8 CD 41 EA 96 5A 27 F5 !Ãjhø.ÝZ,ÍÁê-Z'õ
3560h: 11 C9 C3 81 33 58 4A 76 6A 41 58 14 63 3C 46 70 .ÉÃ.3XÛvjAX.c<Fp
3570h: B1 20 2A A8 02 75 0F F4 FB C4 D9 D9 FE 37 B4 92 ± *".u.óúÀÛÛp7'
3580h: AC E3 33 5F E5 55 39 E0 9C 94 D0 AA 86 5A C8 3F -ã3_âU9àœ"Đ*+2È?
3590h: 3A 9C 26 AC A4 6D 09 BA BB 64 4D 8F 60 F2 88 A0 :œ&-µm.º»dM.`ò"
35A0h: 7E 20 3B A9 2B 93 63 82 FA 81 14 35 D5 94 59 F7 ~ ;@+"c,ú,.5Õ"Y+
35B0h: 4F 9D 39 50 E4 9D 0B 77 D3 99 FD E0 92 34 3D 6A O.9Pâ..wÓ"vâ'4=i

```

NNSXSORRGTSLS3DPHTKCOPOVP42K3BZNNs4=====

编码 解码 清空

key:14位的纯数字

https://blog.csdn.net/weixin_45940434

这里的得到了提示:

key:14位的纯数字

再接着往下看0x3490 的地方。

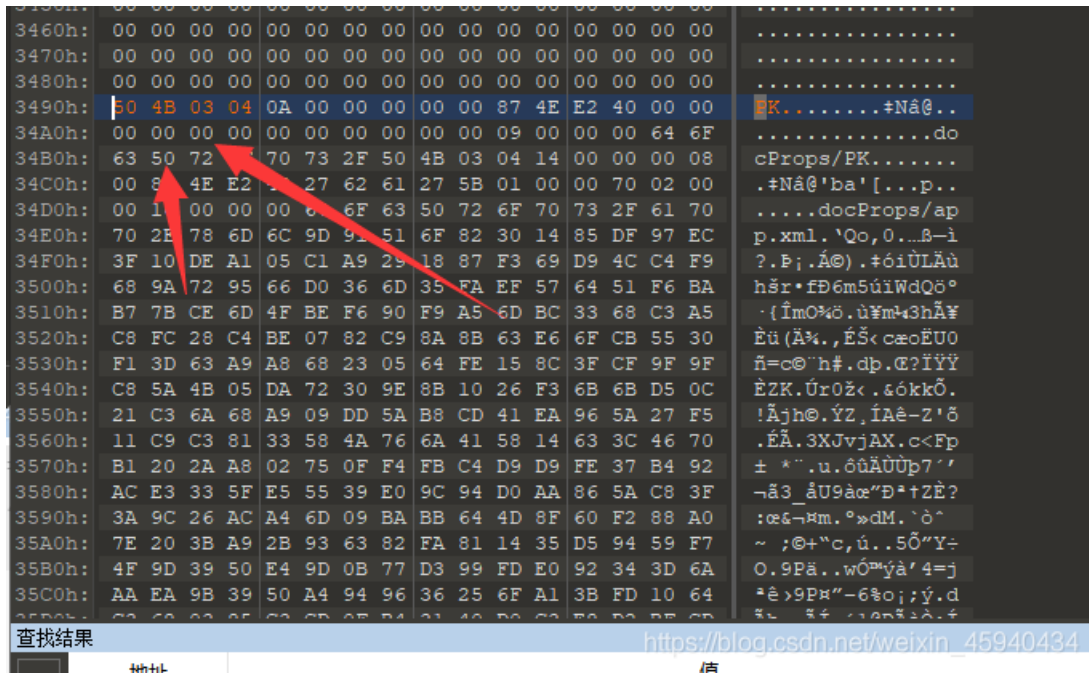
```

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: b0 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...B-i
34F0h: 3F 10 DE A1 05 C1 A9 29 18 87 F3 69 D9 4C C4 F9 ?.Ë;.Ã@).#óïÛLÀù
3500h: 68 9A 72 95 66 D0 36 6D 35 FA EF 57 64 51 F6 BA hšr*fĐ6m5úíWdQó°
3510h: B7 7B CE 6D 4F BE F6 90 F9 A5 6D BC 33 68 C3 A5 -(ÏmO*ó.úÿm+3hÃ¥
3520h: C8 FC 28 C4 BE 07 82 C9 8A 8B 63 E6 6F CB 55 30 Èü(Ã%.ÉŠ<cæoÈU0
3530h: F1 3D 63 A9 A8 68 23 05 64 FE 15 8C 3F CF 9F 9F ñ=c@'h#.dp.Œ?IÝÝ
3540h: C8 5A 4B 05 DA 72 30 9E 8B 10 26 F3 6B 6B D5 0C ÈZK.Ûr0ž<.šókkõ.
3550h: 21 C3 6A 68 A9 09 DD 5A B8 CD 41 EA 96 5A 27 F5 !Ãjhø.ÝZ,ÍÁê-Z'õ
3560h: 11 C9 C3 81 33 58 4A 76 6A 41 58 14 63 3C 46 70 .ÉÃ.3XÛvjAX.c<Fp
3570h: B1 20 2A A8 02 75 0F F4 FB C4 D9 D9 FE 37 B4 92 ± *".u.óúÀÛÛp7'
3580h: AC E3 33 5F E5 55 39 E0 9C 94 D0 AA 86 5A C8 3F -ã3_âU9àœ"Đ*+2È?
3590h: 3A 9C 26 AC A4 6D 09 BA BB 64 4D 8F 60 F2 88 A0 :œ&-µm.º»dM.`ò"
35A0h: 7E 20 3B A9 2B 93 63 82 FA 81 14 35 D5 94 59 F7 ~ ;@+"c,ú,.5Õ"Y+
35B0h: 4F 9D 39 50 E4 9D 0B 77 D3 99 FD E0 92 34 3D 6A O.9Pâ..wÓ"vâ'4=i

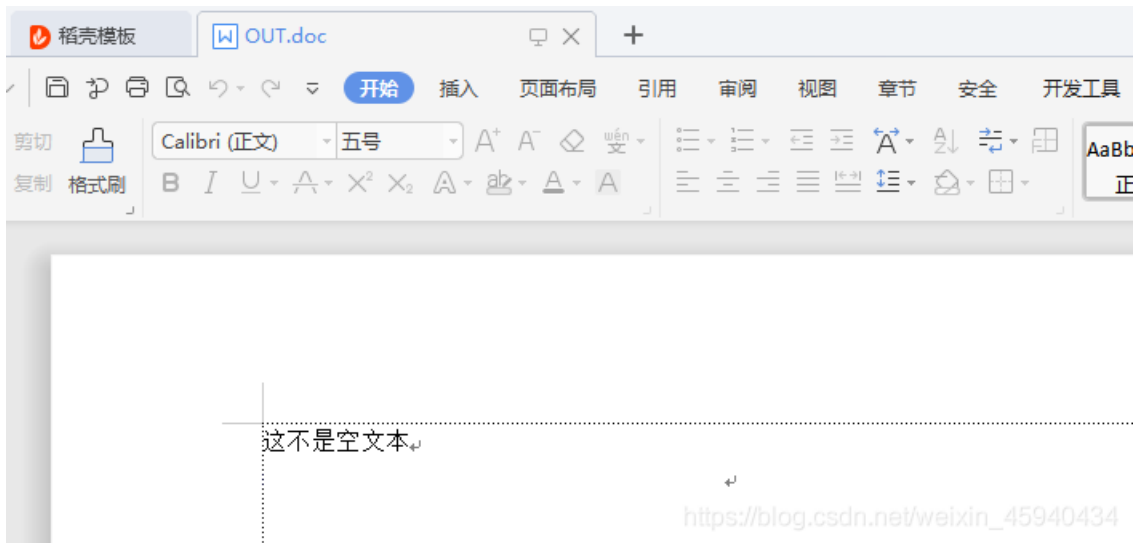
```

转到 字节: 0x3490 十六进制 选项 查找结果 https://blog.csdn.net/weixin_45940434

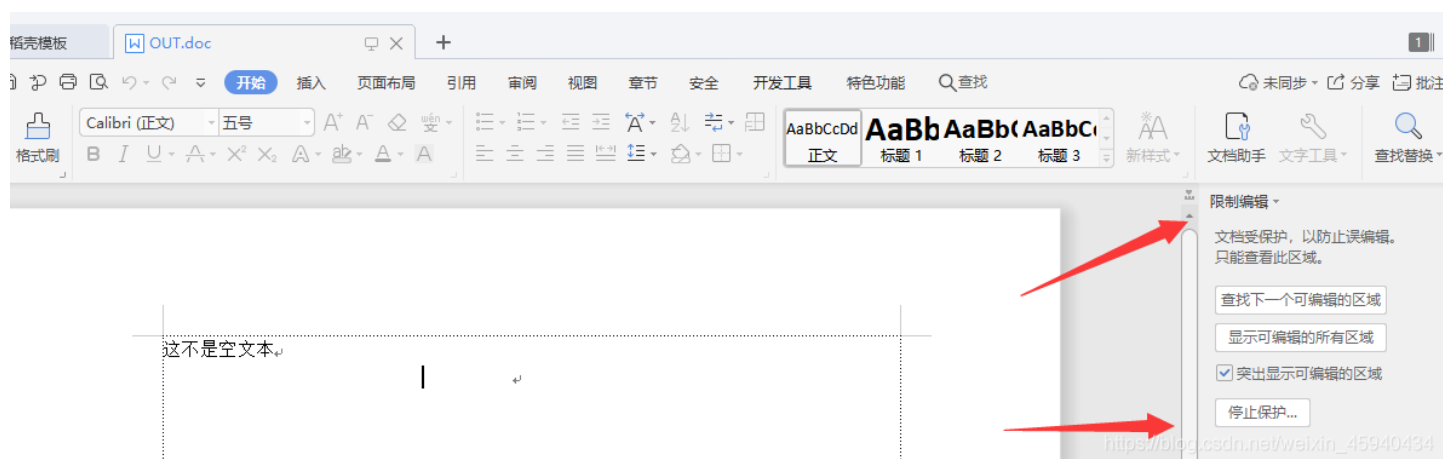
通过与上面的文件头对比，我们发现这个也是一个doc文件，但文件头却被损坏了，那么我们手动修复文件头。加入50 4B 03 04



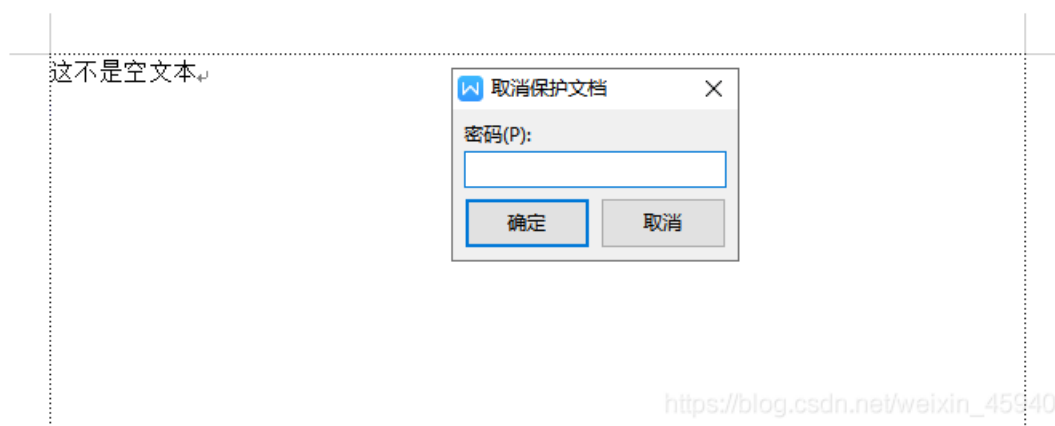
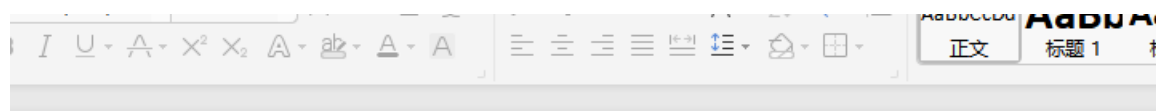
另存为doc文件，并打开。



通过换行符，我们能看到下面是有隐藏文字的，当我们尝试修改字体颜色的时候，发现无法进行操作。随便打入几个字符，右边出现保护提示。



点击停止保护，会让我们输入密码，根据之前的提示，我们要输入14位的纯数字密码，才能继续编辑。



接下来有两种方法，进行破解。

一、爆破

修改密码长度为14，字符为 数字

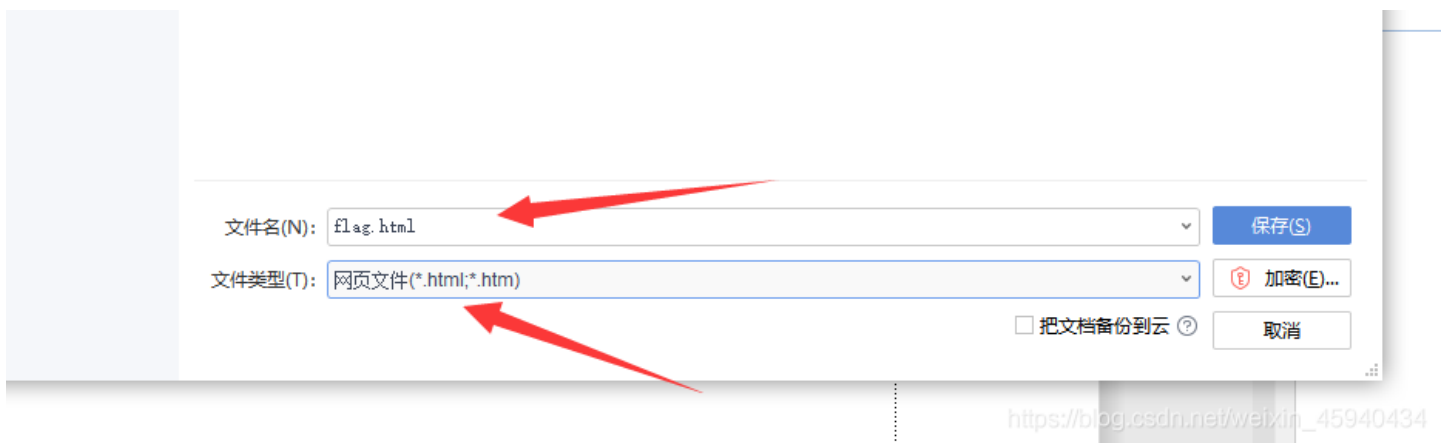


这个就不演示了，因为爆破时间太长，况且我们有简单方法。

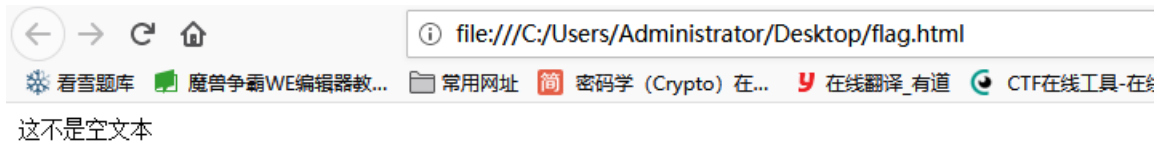


二、绕过

通过另存为html页面，查看文档内容。



正常浏览器打开：



F12翻到尾部，解密base64，即可得到flag

```
28 margin-top:72.0000pt;
29 margin-bottom:72.0000pt;
30 margin-left:90.0000pt;
31 margin-right:90.0000pt;
32 size:595.3000pt 841.9000pt;
33 layout-grid:15.6000pt;
34 }
35 div.Section0 {page:Section0;}</style></head><body style="tab-interval:21pt;text-justify-trim:punctuation;" ><!--StartFragment--><div class="Section0" style="1a
36 mso-hansi-font-family:Calibri;mso-bidi-font-family:'Times New Roman';font-size:10.5000pt;
37 mso-font-kerning: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;
38 mso-hansi-font-family:Calibri;mso-bidi-font-family:'Times New Roman';font-size:10.5000pt;
39 mso-font-kerning:1.0000pt;" ><o:p></o:p></span></p><p class=MsoNormal ><span style="mso-spacerun:'yes';font-family:Calibri;mso-areast-font-family:宋体;
40 mso-bidi-font-family:'Times New Roman';color:rgb(255,255,255);display:none;
41 mso-hide:all;font-size:10.5000pt;mso-font-kerning:1.0000pt;" >RmxhZyU3QnNob3dfY3RmX3Rzd19jYyU3RA==</span><span style="mso-spacerun:'yes';font-family:Calibri;mso-
42 mso-bidi-font-family:'Times New Roman';color:rgb(255,255,255);display:none;
43 mso-hide:all;font-size:10.5000pt;mso-font-kerning:1.0000pt;" ><o:p></o:p></span></p></div><!--EndFragment--></body></html> https://blog.csdn.net/weixin_45940434
```

结语：

菜鸡的cc师傅，将会持续写出100篇高质量的CTF题目，供大家进行CTF的入门以及进阶，如果觉得文章对您有所帮助，欢迎关注一下cc师傅。

原创文章不易，点个赞再走吧。

