ctfshow-文本隐写

原创		
<u>admin_9111</u> 与 _已	于 2022-04-20 20:31:12 修改 🔍	135 论 收藏
分类专栏: <u>ctfshow-</u> 于 2022_04_20 20:29	<u>Misc</u> 文章标签: <u>系统安全</u> 05 首次发布	
版权声明:本文为博	.05 百八 <i>风</i> 师 尊主原创文章,遵循 <u>CC 4.0 BY</u>	SA 版权协议,转载请附上原文出处链接和本声明。
本文链接: <u>https://blc</u>	og.csdn.net/m0_67507776/article/de	etails/124305063
成权 <u>ctfshow-Mi</u> 5 篇文章 0 订阅	isc 专栏收录该内容	
订阅专栏		
Challenge	146 Solves	×
	文木陷写	
	20	
无限接近死亡,	方能领悟生存的真谛。	
感谢@TSW_cc排	是供的题目	
📩 stega20.zip		

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 3 本群倡导友 严格遵守等 自称菜狗这 近期每天一	交流群:372619038 好、和谐、欢乐、进取的学 级制度,进来的一律以大佬 么荣耀的称号,必须自称本 道红包题,作者也秉承恶搞	习精神。 自称,并逐步升级为菜狗、菜鸡、菜鸟 大佬。 又不失内涵的作风,为大家学习路上增	3、菜虫、菜笔、菜刀。不准 舔欢乐!										
CTF, show													
全体管理敬	۲ <u>۲</u>												
—…———————————————————————————————————													
			×										
10.00	西南日二进西												
视图	贝里亚示远坝												
编辑	✓ 社労園伯(K)		→加固怕(P): 陶森										
常规与保存	○ 總載土山(B) ✓ 垂直标尺(C)	☑ 石融的亚尔中的工具(=(0) ☑ 屏幕提示(N)	PetriB6										
جہ (<u>11) ج</u>	 ■ 並直はv ((c)) ☑ 状态栏(U) 	✓ 启用实时预览(V)											
又14111111	☑ 进入页眉页脚提示(Q)												
修订													
中文版式	☑ 突出显示(H)	□ 域代码(F)	域底纹(E):										
龄HDDF	□ 正文边框(X)	□ 书签(K)	选取时显示 ▼										
	✓ 裁剪标记(R)		字体替换(O)										
用户信息													
打印	1月3V10410 つ 広格(C)												
拼写检查		□ 利求付(1)											
安全性		□ 王司(L)											
信任中心	功能区选项												
自定义功能区	双击选项卡时隐藏功能区(A)	1											
	✓ 单击方框时打勾(O)												
快速访问上具栏	□ 打开文件, 展示智能识别目;	录(W)											

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:

字符转二进制

二进制转字符

输出结果

offse: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

				_	_					_						••		
起始页	ſ.	腰看	到手	物的	的本同	678	j .do	cx@	x									
	Ŏ	1	2	3	4	5	6	7	8					D			0123456789ABCDEF	
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	NNSXSORRGTSL3DPH	
3400h:	54	4B	43	4F	50	4F	56	50	34	32	4B	33	42	5A	4E	4E	TKCOPOVP42K3BZNN	
3410h:	53	34	ЗD	ЗD	3D	ЗD	ЗD	ЗD	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:	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	

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	修	要看	到手	物的	的本月	17	ī.do	cx 🖰	×	无标题1*							
	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	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	80	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.ʻQo,0ß—ì
34F0h:	3F	10	DE	A1	05	C1	A9	29	18	87	F3	69	D9	4C	C4	F9	?.Þ¡.Á©).‡óiÙLÄù

^{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	K	家要看	到马	制物的	的本质	577	. do	cx		无标	题1	*x					
	ð	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F	0123456789ABCDEF
0000h:	50	4B	03	04	0A	00	00	00	00	00	87	4E	E2	40	00	00	<mark>РК</mark> ‡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,0ß-ì
0060h:	3F	10	DE	A1	05	C1	Α9	29	18	87	F3	69	D9	4C	C4	F9	?.Þ¡.Á©).‡óiÙLÄù
0070h:	68	9A	72	95	66	D0	36	6D	35	FA	EF	57	64	51	F6	BA	hšr•fÐ6m5úïWdQö°
0080h:	B7	7B	CE	6D	4F	BE	F6	90	F9	A5	6D	BC	33	68	C3	A5	·{ÎmO¾ö.ù¥m¼3hÃ¥
0090h:	C8	FC	28	C4	BE	07	82	C9	8A	8B	63	E6	6F	CB	55	30	Èü(ľ.,ÉŠ‹cæoËUO

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

开始 播入 页面布局 引用 (11月) 視園 章节 开发工具 会员专家 桶先资源 🔍 查找命令、滚紧微板	○ 未同步 2 协作
A () 通知時期 (新人社主 1989年 1月一本 (新) - 10 三万元(14年)(1454 - 175 (147) - 1454 日 (147) - 1454 - 1	
	- 限制编辑 -
	文档受保护,以防止误编辑。 只能查看此区域。
	查找下一个可编辑的区域
	显示可编辑的所有区域
	✓ 突出显示可编辑的区域
	停止保护
这不是空文本	
(1940); (1940);	

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[bage:Section0;}</style></head>Chody style="tab-interval:21pt;text-justify-trim:punctuation;" ><!--StartFragment--><div class="Section0" style="layout-grid:15.6000pt;" >mso-fansi-font-family:Calibri:mso-bidi-font-family; 'lines New Roman':font-size:10.5000pt; mso-font-kerning:1.0000pt;" >这不是空文本这不是空文本<op></op>

RmxhZyU3QnNob3dfY3RmX3Rzd19jYyU3RA==

11.base64解码得到flag

