刷题之旅第40站,CTFshow 文本隐写





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。

🕑 稻壳模板	₩ 你要看到	事物的本质才	行.docx (₽ ×	+								
6760	9 . (2 ⊽	开始	插入页	面布局	引用	审阅	视图	章节	安全	开发工具	特	色功能	С
剪切 微软 复制格式刷 _ B		y 小五 → X ² X ₂ ℓ	- A⁺ A A - ab₂ -	_				*A` -	£) ≑,- ¢,-⊡-	AaE	BbCcDd 正文	AaBk 标题 1) /

₽ -	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—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

这时我们打开我们的显示隐藏文字,才能看到隐藏信息。

🕑 稻壳模板	₩ 你要看到事	物的本质才行.docx	⊋ × +		
6760	9 . 6 ≥	开始插入了	瓦面布局 引用 审阅 视图 章节	5 安全 开发工具 特色功能 (Q.查找
朝 山 微软 副格式刷 B	雅黑 - I U - Ą -	小五 · A* A × ² × ₂ A · 超·	A · A J E E E E E E E E E E E E E E E E E E	AaBbCcDd AaBb ☆ ☆ 冊 - 」 正文 标题 1	AaBb(Aal _{标题 2} 标
		🛚 选项			
		视图	页面显示选项		
		编辑	 □ 启动时展开任务窗格(R) □ 隐藏空白(B) 	☑ 选择时显示浮动工具栏(D) ☑ 右键时显示浮动工具栏(G)	导航窗格(P): 隐藏
	CTFsh	常规与保存	☑ 垂直标尺(C)	☑ 屏幕提示(N)	
	本群倡 严格遵	文件位置	 ✓ 状态栏(U) ✓ 进入页眉页脚提示(Q) 	☑ 启用实时预览(V)	
	自称菜	修订			
	近期每	中文版式	☑ 突出显示(H)	□ 域代码(F)	域底纹(E):
	CTF, s	输出PDF	☑ 正文边框(X)	☑ 书签(K)	选取时显示
	奎体官 By:多	用户信息	☑ 裁剪标记(R)		字体替换(O)
		打印	格式标记	✓ 制表符(T)	
		拼写检查	✓ 段落标记(M)	✓ 隐藏文字(I)	
		安全性	☑ 对象位置(J)	☑ 全部(L)	
		信任中心	功能区选项		
		白定义功能区	双击选项卡时隐藏功能区(A)		
			✓ 单击方框时打勾(O)		
		伏速访问工具任	□ 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——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! д	
	CTF, show [°] +	
	全体管理敬上。	
Ŧ	By:多次拒绝赵丽颖,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	ų.
	https://blog.csdn.net/weixin_459404	134
		:

我们把英文逗号替换成0,中文逗号替换成1.

b

全体官坦	ÉQV_E.√								
Ву	:	多	次	拒	绝	赵	00	颖	
0110111	1101100110	0011001100	1110011011	00101001	11010001100	000111100	0001100110	01101	
0000111	100100110	0000001010) ⊷						
		Γ		~					
			🛛 查找机替热	ė.					
			查找(<u>D</u>)	替换(<u>P</u>)	定位(G)				
			查找内容(N):					
			选项:	区分全/=	¥角				
			替换为(l):	1	htt	ne://blocur	edn nat/wa	ivin 45040	1/12/1
					-70	pomorogie	ournnorre	Min_100-16	-10-1

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)

	叔秋准赤	· шт. жат.
全体管理敬上↓	所有文字	
By : 多次 指	字体颜色(C): 下划线线型(U):	下划线颜色(I): 着重号:
0110111101100110011001100111001101101010	▼ (无)	▼ 自动 ▼ (无) ▼
00001110010011000000001010	效果	
	□ 删除线(K)	□ 小型大写字母(M)
	□ 双删除线(G)	□ 全部大写字母(A)
	□ 上标(P)	□ 隐藏文字(H)
	□ 下标(B)	
	预览	
	011011	
	」 这是一种 TrueType 字体,同时话用于	屏幕和打印机。
	默认(D) 文本效果(E)	确定取消
L		ittps://blog.csdn.net/weixin_2092/02/32

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。)

offse:0x3490

01101111011001100110011001	4004404400404004440	100011000001111	000001100110011	1000011100100110000000	04040
01101111011001100110011001	10011011001010001110	100011000001111	0000011001100110	10000111001001100000000	01010
			转换后的文本		
			转换后的文本		
0x3490					
01100.070400					

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。

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:	þo	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,0ß-ì
34F0h:	ЗF	10	DE	A1	05	C1	Α9	29	18	87	F3	69	D9	4C	C4	F9	?.₽¡.Á©).‡óiÙLÄù
3500h:	68	9A	72	95	66	D0	36	6D	35	FA	EF	57	64	51	F6	BA	hšr•fÐ6m5úïWdQö°
3510h:	B7	7B	CE	6D	4F	BE	F6	90	F9	A 5	6D	BC	33	68	C3	A5	{ÎmO¾ö.ù¥m¼3hÃ¥
3520h:	C8	FC	28	C4	BE	07	82	C9	8A	8B	63	E6	6F	CB	55	30	Èü(ľ.,ÉŠ< cæoËU0
3530h:	Fl	ЗD	63	A9	A8	68	23	05	64	FE	15	8C	ЗF	CF	9F	9F	ñ=c©"h#.dþ.Œ?ÏŸŸ
3540h:	C8	5A	4B	05	DA	72	30	9E	8B	10	26	F3	6B	6B	D5	0C	ÈZK.Úr0ž<.&ókkÕ.
3550h:	21	C3	6A	68	A9	09	DD	5A	B8	CD	41	EA	96	5A	27	F5	!Ãjh©.ÝZ,ÍAê-Z'õ
3560h:	11	C9	C3	81	33	58	4A	76	6A	41	58	14	63	3C	46	70	.ÉÃ.3XJvjAX.c <fp< td=""></fp<>
3570h:	B1	20	2A	A 8	02	75	OF	F4	FB	C4	D9	D9	FE	37	B4	92	± *".u.ôûÄÙÙþ7′′
3580h:	AC	EЗ	33	5F	E5	55	39	E0	9C	94	DO	AA	86	5A	C8	ЗF	−ã3_åU9àœ″Đª†ZÈ?
3590h:	3A	9C	26	AC	A 4	6D	09	BA	BB	64	4D	8F	60	F2	88	AO	:œ&¬¤m.°»dM.`ò^
35A0h:	7E	20	ЗB	A9	2B	93	63	82	FA	81	14	35	D5	94	59	F7	~ ;©+"c,ú5Õ″Y÷
35B0h:	4F	9D	39	50	E4	9D	0B	77	D3	99	FD	EO	92	34	ЗD	6A	0.9PäwÓ™ýà′4=i
×转到	字	节: /		x3490			,	~ -	> -	+六ì	曲制		选项	ą 🔿			
本地社由																httos	s://blog.csdn.net/weixi
旦採結禾																	

再接着往下看0x3490的地方。

key:14位的纯数字

key:14位的纯数字

这里的得到了提示:

	33DUN:	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	ЗD	ЗD	ЗD	ЗD	00	00	00	00	00	00	00	00	S4=====
X	3420h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	—
ă,t	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	55	
	3450h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	25	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,0ß-ì
	34F0h:	ЗF	10	DE	A 1	05	Cl	Α9	29	18	87	F3	69	D9	4C	C4	F9	?.₽;.Á©).‡óiÙLÄù
	3500h:	68	9A	72	95	66	DO	36	6D	35	FA	EF	57	64	51	F6	BA	hšr•fÐ6m5úïWdQö°
	3510h:	B7	7B	CE	6D	4F	BE	F6	90	F9	A 5	6D	BC	33	4#tt	ps:	/Astoc	1.cscfm.pret/wieixiph245940434
	3520h:	C8	FC	28	C4	BE	07	82	C9	84	88	63	E6	6F	CB	55	30 Ĭ	Èü (ľ, ÉŠ(cæoËU0

FC 28 C4 BE 07 82 C9 8A 8B 63 E6 6F CB 55 30

NNSXSORRGTSL3DPHTKCOPOVP42K3BZNNS4=====

Èü (ľ.

编码

解码

清空

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:	50				0A	00	00	00	00	00	87	4E	E2	40	00	00	■ K‡Nâ@
34A0h:	00	00	00	00	00	00	00	00	00	00	09	00	00	00	64	6F	do
34B0h:	63	50	72	1	70	73	2F	50	4B	03	04	14	00	00	00	08	cProps/PK
34C0h:	00	8	4E	E2	-	27	62	61	27	5B	01	00	00	70	02	00	.‡Nâ@'ba'[p
34D0h:	00	1	00	00	00	0.	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,0B-ì
34F0h:	ЗF	10	DE	A1	05	C1	Α9	29	18	87	F3	69	D9	4C	C4	F9	?.₽;.Á©).‡óiÙLÄù
3500h:	68	9A	72	95	66	DO	36	6D	35	FA	EF	57	64	51	F6	BA	hšr•fÐ6m5úïWdQö°
3510h:	B7	7B	CE	6D	4F	BE	F6	90	F9	A5	6D	BC	33	68	C3	A 5	·{ÎmO¾ö.ù¥m₄3hÃ¥
3520h:	C8	FC	28	C4	BE	07	82	C9	8A	8B	63	E6	6F	СВ	55	30	Èü(ľ.,ÉŠ< cæoËU0
3530h:	Fl	ЗD	63	Α9	A 8	68	23	05	64	FE	15	8C	ЗF	CF	9F	9F	ñ=c©"h#.dþ.Œ?ÏŸŸ
3540h:	C8	5A	4B	05	DA	72	30	9E	8B	10	26	F3	6B	6B	D5	0C	ÈZK.Úr0ž∢.&ókkÕ.
3550h:	21	C3	6A	68	A 9	09	DD	5A	B8	CD	41	EA	96	5A	27	F5	!Ãjh©.ÝZ,ÍAê-Z'Ő
3560h:	11	C9	C3	81	33	58	4A	76	6A	41	58	14	63	3C	46	70	.ÉÃ.3XJvjAX.c <fp< td=""></fp<>
3570h:	B1	20	2A	A 8	02	75	0F	F4	FB	C4	D9	D9	FE	37	В4	92	± *".u.ôûÄÙÙþ7′′
3580h:	AC	E3	33	5F	E.5	55	39	EO	9C	94	DO	AA	86	5A	C8	ЗF	−ã3_åU9àœ″Đª†ZÈ?
3590h:	ЗA	9C	26	AC	Α4	6D	09	BA	BB	64	4D	8F	60	F2	88	A 0	:œ&¬¤m.°»dM.`ò^
35A0h:	7E	20	ЗB	Α9	2B	93	63	82	FA	81	14	35	D5	94	59	F7	~ ;©+"c,ú5Õ″Y÷
35B0h:	4F	9D	39	50	E4	9D	0B	77	D3	99	FD	EO	92	34	ЗD	6A	0.9PäwÓ™ýà′4=j
35C0h:	AA	EA	9B	39	50	Α4	94	96	36	25	6F	A1	ЗB	FD	10	64	°ê>9P¤″-6%o;;ý.d
AFRAL.	00	00	00	0.5	00	CID	077	T 14	21	40	DO	00	70	nn.	10177	0D	%≥ % + /105%≥À. +
宣 执结果															http)s://b	olog.csdn.net/weixin_459404
	44	n+ı-														店	

另存为doc文件,并打开。

ة 🕑	韬売模板		M OU	T.doc			ΨX	+							
6	178	Q	9-6	~	开始	插入	页面布局	5 31	用	审阅	视图	章节	安全	开发	江具
剪切 复制	格式刷	Calib B	ori(正文) I ⊔ -		五号 × ² × ₂	► A+ A ► at	A ⁻ ⊘ ≩• <u>A</u> •	^{wén} ≁ A	0 0 0 0			*A* <u>‡≡</u> -	A) ‡;+ ⊉-⊞	₽ ₽ ₽	AaBb IE
1															
			ij	这不是3	之文本→					ہ ne•//hl					

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。

								_	~	-	-			<i>·</i> · ·		-	ABDUCCDU	Hadu) MC
}	Ι	<u>U</u> -	$\frac{1}{\sqrt{1}}$	\times^2	\times_2	A-	ab -	<u>A</u> -	A	_	_		(\leftrightarrow)	<u>*</u>	Q-		正文	标题 1	枝

这不是空文本↩	▶ 取消保护文档 ×	
	密码(P): 備定 取消	
		net/weixin_4594043

接下来有俩种方法,进行破解。

一、爆破

修改密码长度为14,字符为数字

Advanced Office Pass 文件 恢复 Internet VBA	rord Recovery Professional Edition - 未命名 后门 语言 帮助	? _ 🗆 🗙
打开文件] 🔗 🚴 🧖	帰 停止
恢复 暴力 字典 法	选项 系统信息 密码缓存	
密码长度 : 最小 最大 14 ★ 14 ★	字符集: 起始密码: □ a - z □ 0 - 9 □ A - Z □ 10 □ 空格 「 □ 前有可打印字符 「 □ 自定义字符集 □	?
日志窗口		
日期・时间 ② 2020/2/20 14:12:04 ③ 2020/2/20 14:12:04 ③ 2020/2/20 14:12:04	事件 AOPR 5.10 Professional Edition 已加载 操作系统版本: Windows Server 2008 R2 [6.1.7601] Service Pack CPU: 1, NVidia CUDA: 0, ATI CAL: 0	1
	」CH │ │ 🕑 □	-
进程指示器	htt <mark>%</mark> ://blog.osdn.net/weix	in_45940 <mark>43</mark> 4

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。

▼ 保存(<u>S</u>)	flag. html	文件名(N):
~	网页文件(*.html;*.htm)	文件类型(T):
把文档备份到云 ⑦ 取消		



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{bage:Section0;} <body style="tab-interval:21pt;text-justify-trim:punctuation;"><!--StartFragmentXdiv class="Section0" style="la"</td--></body>
36 mso-hansi-font-family:Calibri;mso-bidi-font-family:'Times New Roman';font-size:10.5000pt;
37 mso-font-kerning:1.0000pt;" > 这不是空文本 tyle="mso-spacerun:'yes';font-family:宋体;mso-ascii-font-family:定alibri;
38 mso-hansi-font-family:Calibri;mso-bidi-font-family:'Times New Roman';font-size:10.5000pt;
39 mso-font-kerning:1.0000pt;" Xo:pX/o:pX/spanX/pXp class=WsoNormal Xspan style="mso-spacerun:'yes';font-family:Calibri;mso-fareast-font-family:宋体;
40 mso-bidi-font-family:'Times New Roman';color:rgb(255,255,25,25,25);display:none;
41 mso-hide:all;font-size:10.5000pt;mso-font-kerning:1.0000pt >RmxhZyU3QnNob3dfY3RmX3Rzd19jYyU3RA==
42 mso-bidi-font-family:'Times New Roman';color:rgb(255,255,25 <mark>5);dicplay:pone:</mark>
43 mso-hide:all;font-size:10.5000pt;mso-font-kerning:1.0000pt; "> <o:p>//o:p>//span>//p>//div>/:-EndFragment->/body>//html>hllps://blog.csdn.net/weixin_45940434</o:p>

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。

