攻防世界Misc入门题之stegano

原创

沐一 · 林 于 2021-08-11 11:59:01 发布 342 收藏

分类专栏： CTF 杂项 文章标签： unctf

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/xiao__1bai/article/details/119601257

版权

CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏

杂项

19 篇文章 0 订阅

订阅专栏

攻防世界Misc入门题之stegano

继续开启全栈梦想之逆向之旅~

这题是攻防世界Misc入门题之stegano

又是做逆向累了来写一些其它题放松一下~

下载附件，是个PDF，照例winhex64位打开，ASCII码和UNICODE码都试一遍，啥都没有。

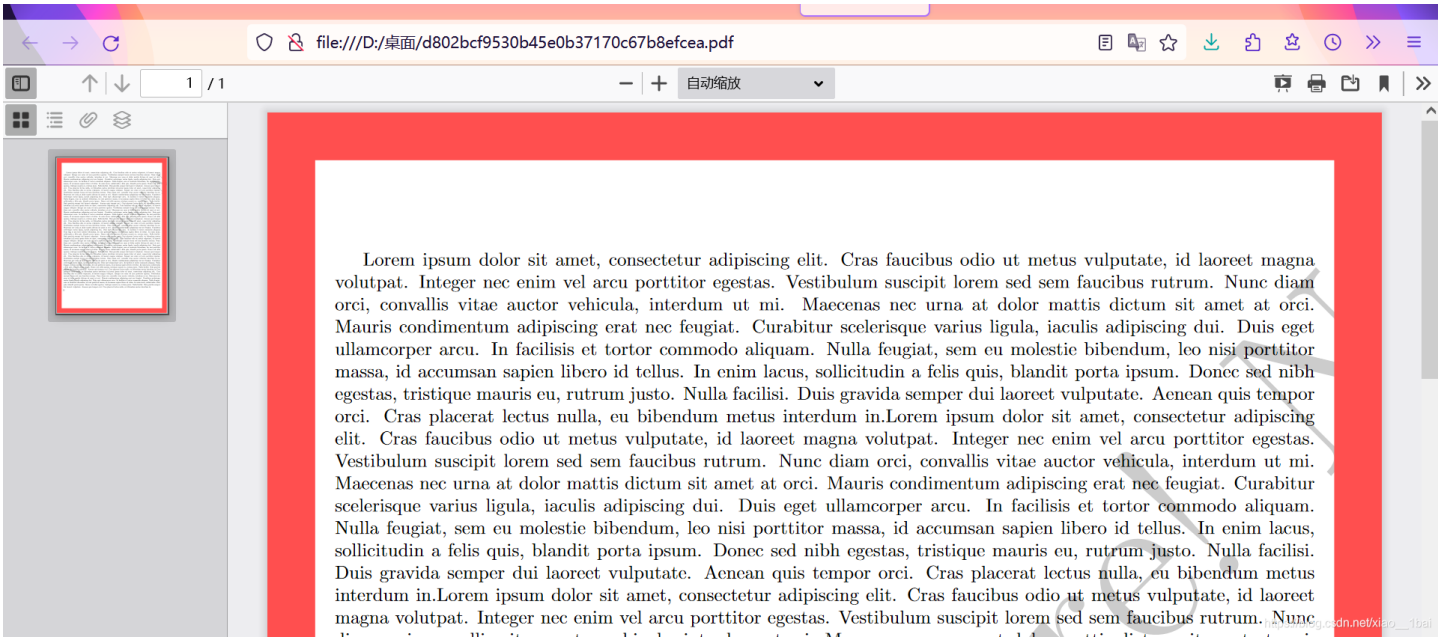
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	ANSI ASCII
00000000	25	50	44	46	2D	31	2E	35	0A	25	D0	D4	C5	D8	0A	38	20	%PDF-1.5 %ÐÔÅØ 8
00000011	30	20	6F	62	6A	20	3C	3C	0A	2F	4C	65	6E	67	74	68	20	0 obj << /Length
00000022	33	32	34	39	20	20	20	20	20	20	0A	2F	46	69	6C	74	65	3249 /Filte
00000033	72	20	2F	46	6C	61	74	65	44	65	63	6F	64	65	0A	3E	3E	r /FlateDecode >>
00000044	0A	73	74	72	65	61	6D	0A	78	DA	ED	9B	DD	8F	DB	C6	11	stream xÚí›Ý ÛÆ
00000055	C0	DF	EF	AF	60	DE	78	40	C4	90	5C	EE	92	7C	EB	9D	DD	ÀßÏ¯`Þx@Ä \î'|ë Ý

```
00000066  A4 2E 1A 03 6E 8D A2 45  9A 07 9E C4 93 59 50 D2  59  ¤.  n ¢Eš žA"YPOY
00000077  22 9D 7F BF F3 B9 5C 52  B4 83 22 4F 71 64 FB EE  76  "  ¿ó¹\R´ƒ"Oqdûîv
00000088  67 67 F6 73 76 7E 1C 1D  9D 45 29 FC CD A2 4D 91  66  ggösv~   E)üÍ¢M'f
00000099  49 6A AA 68 63 F2 2C B1  45 1E 6D 0F 77 1F EF 92  32  Ijªhcò,±E m w ï'2
000000AA  2D D3 3A 92 1F 9B 79 15  2D 49 CB 52 D1 AA 20 4D  AA  -Ó:' ›y -IËRÑª Mª
000000BB  68 1F E1 F7 1F EE 32 E9  5F BB 0F 7A 7F 7C 7F F7  DD  h á÷ î2é_» z | ÷Ý
000000CC  F7 59 19 E5 45 52 56 65  16 BD 7F 86 C1 EB 32 29  41  ÷Y åERVe ½ †Áë2)A
000000DD  E6 67 F1 7E 17 FD 14 BF  3D 7D DF 37 FB BF B4 E7  F6  ægñ~ ý ¿=}ß7û¿´çö
000000EE  9B 7B 98 A8 8B DF DE 6F  B2 F8 4A 18 08 7E 7E FF  D7  ›{˜¨‹ßÞo²øJ  ~~ÿ×
000000FF  BB 14 27 01 53 F8 F3 7B  3F 8B D5 55 BE 83 BF AA  BB  » ' Søó{?‹ÕU¾ƒ¿ª»
00000110  FC E9 A7 6F B3 A4 AE F2  28 CB B2 32 29 5C 4D EB  8E  üé§o³¤®ò(Ë²2)\MëŽ
00000121  40 ED 87 88 74 61 CD A6  AE 6C F4 4B 84 62 F8 F7  DD  @í‡ˆtaÍ¦®lôK„bø÷Ý
00000132  CB FE F9 4F AF 1E A0 ED  22 95 6D C3 95 2F 36 BE  A3  ËþùO¯  í"•mÃ•/6¾£
00000143  76 3F 6A 52 15 26 DA 94  2E 4D D2 8C 77 16 C4 49  11  v?jR &Ú".MÒŒw ÄI
00000154  6D F0 1B 56 F4 6B 7B 88  E6 F3 F1 2B B6 16 77 17  16  mð Vôk{ˆæóñ+¶ w
00000165  6C 93 1A 36 D6 EF BB 8B  EA A4 76 B9 C3 6D 17 1D  51  l" 6Öï»‹ê¤v¹Ãm  Q
00000176  A1 2D FF D7 F2 CF 7D 76  2D 5B 68 6C 8C 31 F1 FF  6D  ¡-ÿ×òÏ}v-[hlŒ1ñÿm
00000187  16 68 D1 B1 05 C7 35 9F  17 1E 55 B0 30 DE 9C 69  6F  hÑ± Ç5Ÿ  U°0Þœio
00000198  DE 45 F2 EF 18 85 7A 29  6C 16 9C 9D B5 BF 7A 64  B9  ÞEòï …z)l œ µ¿zd¹
000001A9  4D 6C 96 67 39 4A C0 2E  31 F2 ED BC 8F C2 EA DF  7F  Ml–g9JÀ.1òí¼ ÂêÞ
000001BA  B8 B3 06 9C A7 82 BD 2B  6C 92 B9 BC A8 23 D8 FE  2F  ¸³ œ§‚½+l'¹¼¨#Øþ/
000001CB  0B 37 65 99 25 39 14 FA  E8 6E 63 AA 24 AB 2A 98  D2  7e™%9 úènc ª$«*˜Ò
000001DC  BA D4 77 00 D2 0F AB EA  D0 F3 3F 22 EF A4 EF 66  4E  ºÔw Ò «êÐó?"ï¤ïfN
000001ED  95 E4 33 B7 92 2A 4E BE  A0 2F 59 0E 57 60 31 BF  C1  •ä3·'*N¾ /Y W`1¿Á
000001FE  F4 F3 2D 73 3F B6 79 95  58 B8 E1 1B 03 B7 27 E5  A3  ôó-s?¶y•X¸á  ·'å£
0000020F  40 AF 05 37 CE 22 FC 5A  71 E5 B0 BB C5 1C 02 E7  2E  @¯ 7Î"üZqå°»Å  ç.
00000220  6B 38 33 D8 98 C2 B9 2F  B8 B7 68 A9 12 39 F8 AB  FE  k83Ø˜Â¹/¸·h© 9ø«þ
00000231  74 69 D9 65 37 F8 A3 88  9F C6 81 EB 97 A1 EB 7B  2E  tiÙe7ø£ˆŸÆ ë—¡ë{.
00000242  1E 4F 03 37 7E 80 B0 C2  A2 6F AE BC 74 D1 FD C2  4F  O 7~€°Â¢o®¼tÑýÂO
00000253  75 F1 C1 DA DF CD CE EE  37 B8 AC 3F B8 7A 7E 70  F5  uñÁÚßÍÎî7¸¬?¸z~põ
00000264  32 D2 AC 2B 2C A2 4D 0D  D7 CD 45 39 CC D3 56 0E  C7  2Ò¬+,¢M ×ÍE9ÌÓV Ç
00000275  DE A4 89 F5 E7 32 AB 7C  21 DE 14 0E F0 00 21 AA  AE  Þ¤‰õç2«|!Þ  ð !ª®
00000286  EA C4 A5 E6 33 47 22 5A  AA 44 47 F2 F8 F0 F8 C0  7B  êÄ¥æ3G"ZªDGòøðøÀ{
```

https://blog.csdn.net/xiao__bai

转为docx后移开图片，还是空白一片：
图略~

懵了，查看资料(wp)，说是一道PDF隐写题。可以，又有新知识可以学习了，常规做法是用浏览器打开，然后全选复制粘贴到文本编辑器就可以显示出被隐藏的内容，我也不知道什么原理，先照着做吧。



未用浏览器打开前的文本是这样的：

```
e! NoFlagHere! N
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Close - but still not here !
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna
volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam
orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci.
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas.
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi.
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur
scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam.
Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus,
sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi.
Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus
interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet
magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc
diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci.
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas.
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi.
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur
scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam[
Your flag is not here !olestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus,
```

在浏览器复制粘贴后是这样的：

```
NoFlagHere! NoFlagHere! NoFlagHere!
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Close - but still not here !
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna
volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam
orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci.
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas.
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi.
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur
scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam.
Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus,
sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi.
Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus
interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet
magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc
diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci.
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing
elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor egestas.
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi.
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur
```

可以看到第四行多了ABAB，一开始以为是培根密码，解密后都是未定义，后来查了资料发现培根密码是5位一组的，那么就只剩下摩斯密码了，写脚本转换一下：

```
key1="BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AA
AAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABB"
key1=key1.replace('A','.')
key1=key1.replace('B','-')
key1=key1.replace(' ','/')
print(key1)
```

```
└─$ python 2.py
-.-./---/-./--./.-./.-/-/..-/.-../.-/-/../---/-./.../--..--/..-./.-../.-/--./---../.----/-./...-
/.----/...../.----/-.../.-../...--/--/...--/...../...../....-/--./...--
```

扔到摩斯密码在线解密处解密即可得到flag(记得小写)：

```
https://www.bejson.com/enc/morse/
```

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖