2021鹤城杯writeup

原创

NNanfeng 于 2021-10-08 19:26:37 发布 646 收藏 2

分类专栏： 2021CTF首届鹤城杯 文章标签： qt 深度学习 python unctf

本文链接：https://blog.csdn.net/qq_51724251/article/details/120658086

2021CTF首届鹤城杯 专栏收录该内容

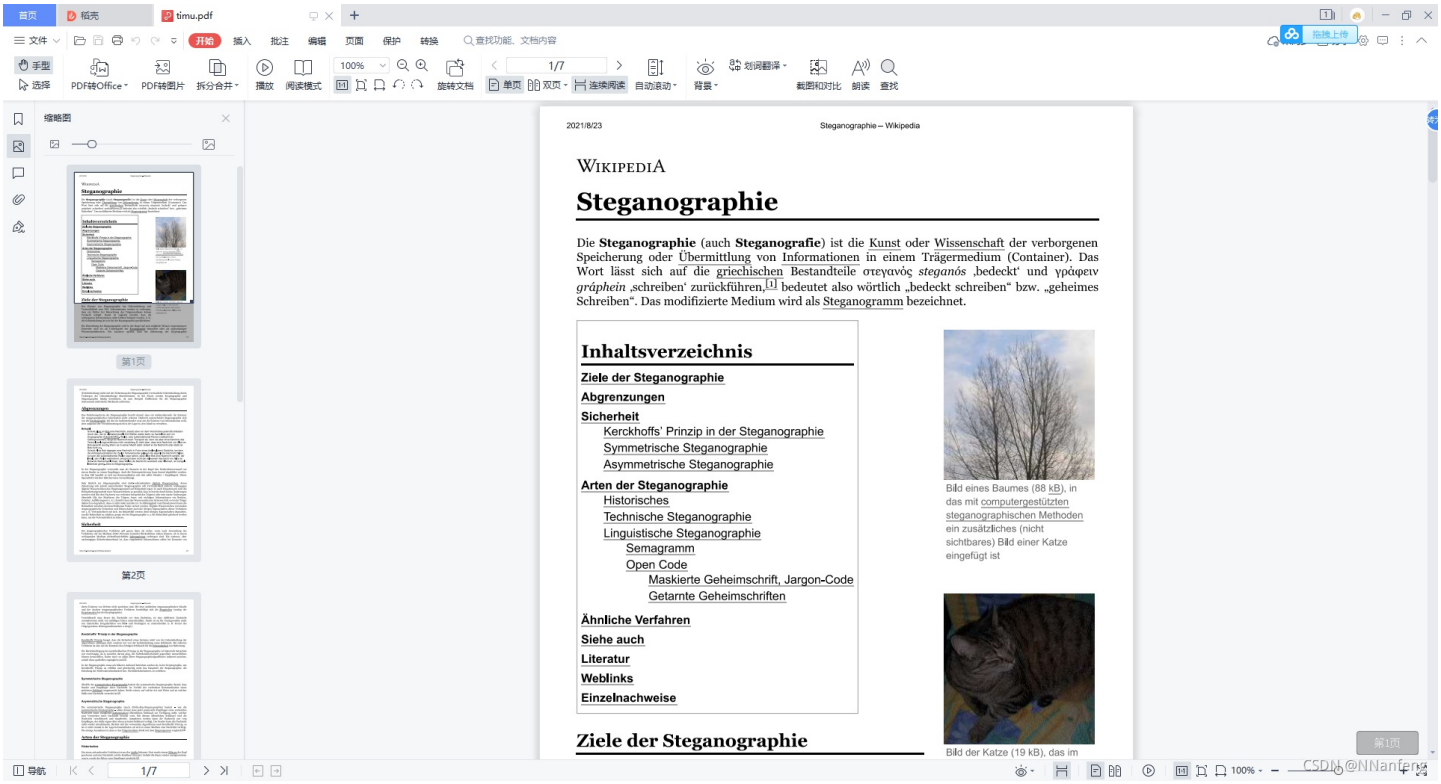
2 篇文章 0 订阅

订阅专栏

MISC

1.NEW MISC

下载文件，是一个pdf文件



打开pdf，有俄文看不懂，因为是一道杂项题考虑隐写，百度“ctf pdf 隐写”

http://blog.sina.com.cn/s/blog_6dc0c58b0102x9zd.html

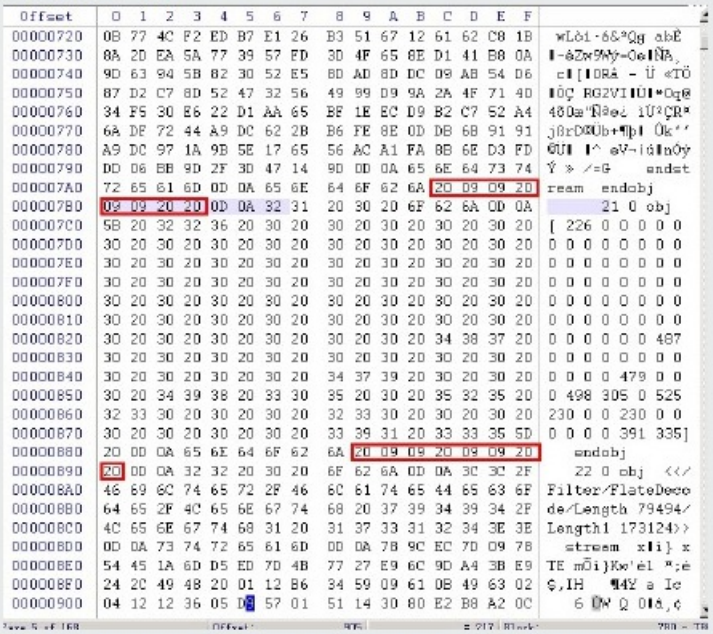
找到了这位师傅写的总结，pdf两种隐写方式，如下图：

1.wbStego4.3open

wbStego4.3open可以把文件隐藏到BMP、TXT、HTM和PDF文件中。

使用方法略，很简单.

2.WinHex查看



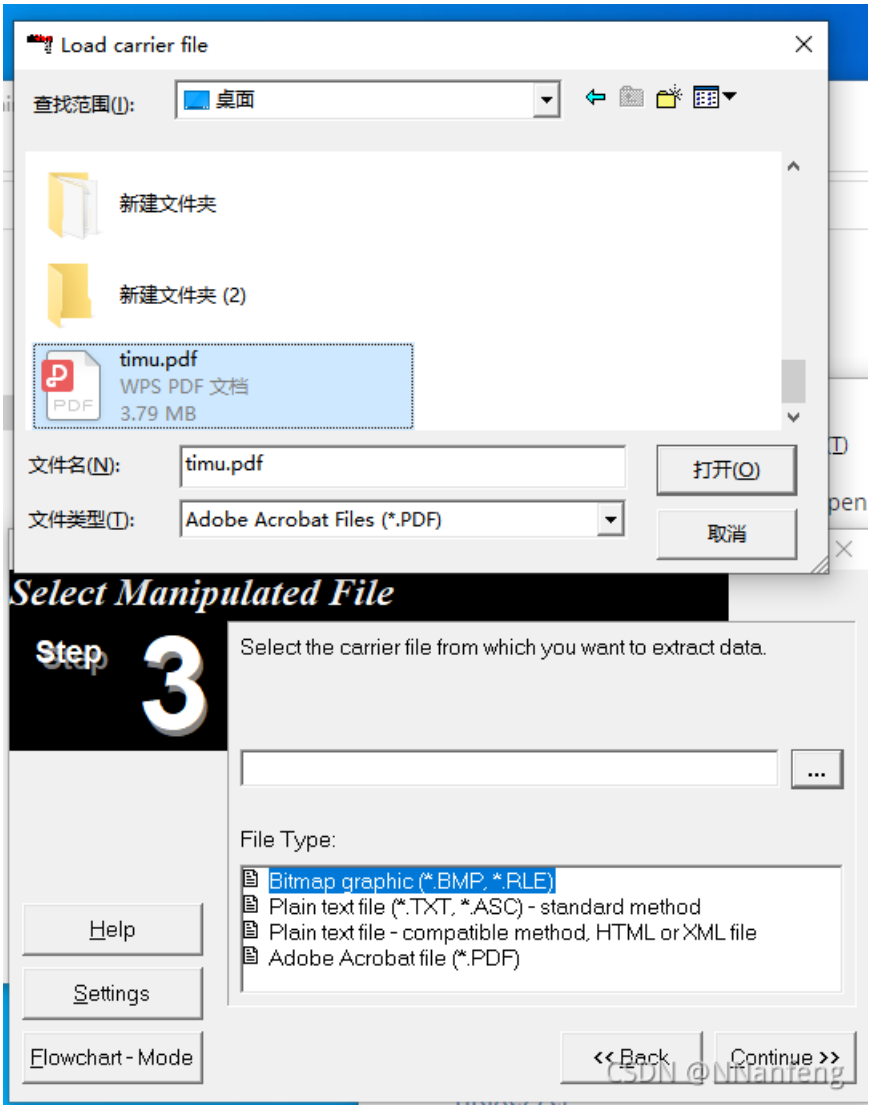
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000720	0B	77	4C	F2	ED	B7	E1	26	B3	51	67	12	61	62	C8	1B	wLòí·á&³Qg abÈ
00000730	8A	2D	EA	5A	77	39	57	FD	3D	4F	65	8E	D1	41	B8	0A	Š-êZw9Wý=OeŽÑA¸
00000740	9D	63	94	5B	82	30	52	E5	BD	AD	8D	DC	D9	AB	54	D6	c"[‚0Rå Ü «TÖ
00000750	87	D2	C7	8D	52	47	32	56	49	99	D9	9A	2A	4F	71	4D	‡ÒÇ RG2VI™Ùš*OqM
00000760	34	F5	30	E6	22	D1	AA	65	BF	1E	EC	D9	B2	C7	52	A4	4õ0æ"ÑªeÀ ìÙ²ÇR¤
00000770	6A	DF	72	44	A9	DC	62	2B	B6	FE	8E	0D	DB	6B	91	91	jßrD©Üb+¶þŽ ÛK‘‘
00000780	A9	DC	97	1A	9B	5E	17	65	56	AC	A1	FA	BB	6E	D3	FD	©Ü— ›^ eV¬¡ú»nÓý
00000790	DD	06	BB	9D	2F	3D	47	14	9D	0D	0A	65	6E	64	73	74	Ý »/=G endst
000007A0	72	65	61	6D	0D	0A	65	6E	64	6F	62	6A	20	09	09	20	ream endobj
000007B0	09	09	20	20	0D	0A	32	31	20	30	20	6F	62	6A	0D	0A	21 0 obj
000007C0	5B	20	32	32	36	20	30	20	30	20	30	20	30	20	30	20	[226 0 0 0 0 0
000007D0	30	20	30	20	30	20	30	20	30	20	30	20	30	20	30	20	0 0 0 0 0 0 0 0
000007E0	30	20	30	20	30	20	30	20	30	20	30	20	30	20	30	20	0 0 0 0 0 0 0 0
000007F0	30	20	30	20	30	20	30	20	30	20	30	20	30	20	30	20	0 0 0 0 0 0 0 0
00000800	30	20	30	20	30	20	30	20	30	20	30	20	30	20	30	20	0 0 0 0 0 0 0 0
00000810	30	20	30	20	30	20	30	20	30	20	30	20	30	20	30	20	0 0 0 0 0 0 0 0
00000820	30	20	30	20	30	20	30	20	30	20	30	20	34	38	37	20	0 0 0 0 0 0 0 487
00000830	30	20	30	20	30	20	30	20	30	20	30	20	30	20	30	20	0 0 0 0 0 0 0 0
00000840	30	20	30	20	30	20	30	20	34	37	39	20	30	20	30	20	0 0 0 0 479 0 0
00000850	30	20	34	39	38	20	33	30	35	20	30	20	35	32	35	20	0 498 305 0 525
00000860	32	33	30	20	30	20	30	20	32	33	30	20	30	20	30	20	230 0 0 230 0 0
00000870	30	20	30	20	30	20	30	20	33	39	31	20	33	33	35	5D	0 0 0 0 391 335]
00000880	20	0D	0A	65	6E	64	6F	62	6A	20	09	09	20	09	09	20	endobj
00000890	20	0D	0A	32	32	20	30	20	6F	62	6A	0D	0A	3C	3C	2F	22 0 obj <</
000008A0	46	69	6C	74	65	72	2F	46	6C	61	74	65	44	65	63	6F	Filter/FlateDeco
000008B0	64	65	2F	4C	65	6E	67	74	68	20	37	39	34	39	34	2F	de/Length 79494/
000008C0	4C	65	6E	67	74	68	31	20	31	37	33	31	32	34	3E	3E	Length1 173124>>
000008D0	0D	0A	73	74	72	65	61	6D	0D	0A	78	9C	EC	7D	09	78	stream x\ì} x
000008E0	54	45	1A	6D	D5	ED	7D	4B	77	27	E9	6C	9D	A4	3B	E9	TE mÕí}Kw'él ¤;é
000008F0	24	2C	49	48	20	01	12	B6	34	59	09	61	0B	49	63	02	$,IH ¶4Y a Ic
00000900	04	12	12	36	05	D8	57	01	51	14	30	80	E2	B8	A2	0C	6 ØW Q 0€â¸¢

用WinHex打开生成文件123.pdf，其中混入了许多由20和09组成的8位字节,将这些8位字节提取出来之后取其最低有效位，组合得其所代表的ASCII码的二进制形式，再把二进制码转换成ASCII码就可以得到信息（20代表0，09代表1）。

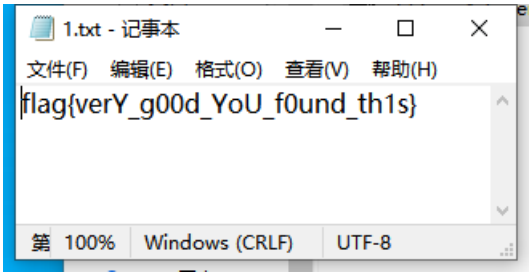
找工具：wbStego4.3open

找不到工具的师傅可以去我分享的链接下载：链接：https://pan.baidu.com/s/1S-w-W8YcAZVU4hKJXez7cg
提取码：da4l
–来自百度网盘超级会员V1的分享

打开软件 点击continue 选择 decode 点continue 选择文件timu.pdf



之后再点continue（空密码，弱密码破解） 输入 输出的文件名字 得到txt文件



flag{verY_g00d_YoU_f0und_th1s}

2.A_MISC

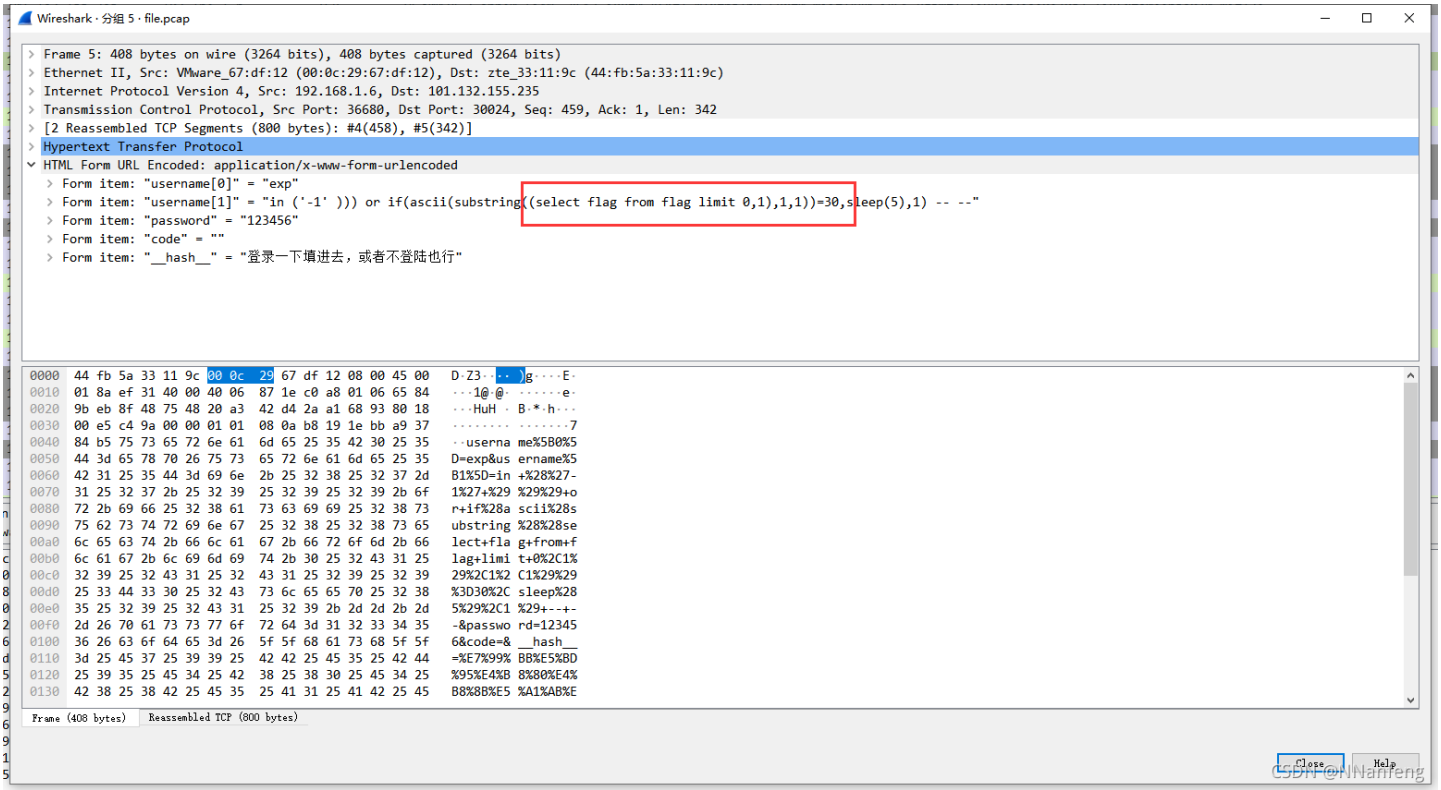
下载文件，压缩包文件有密码，跑词典跑出密码是qwer

得到一个图片文件

给了一个百度云盘分享链接https://pan.baidu.com/s/1cG2QvYy3khpQGLfjfbYevg，打开需要输入 要提取码，改图片高度得到提取码

下载得到file.pcap文件，又是流量分析

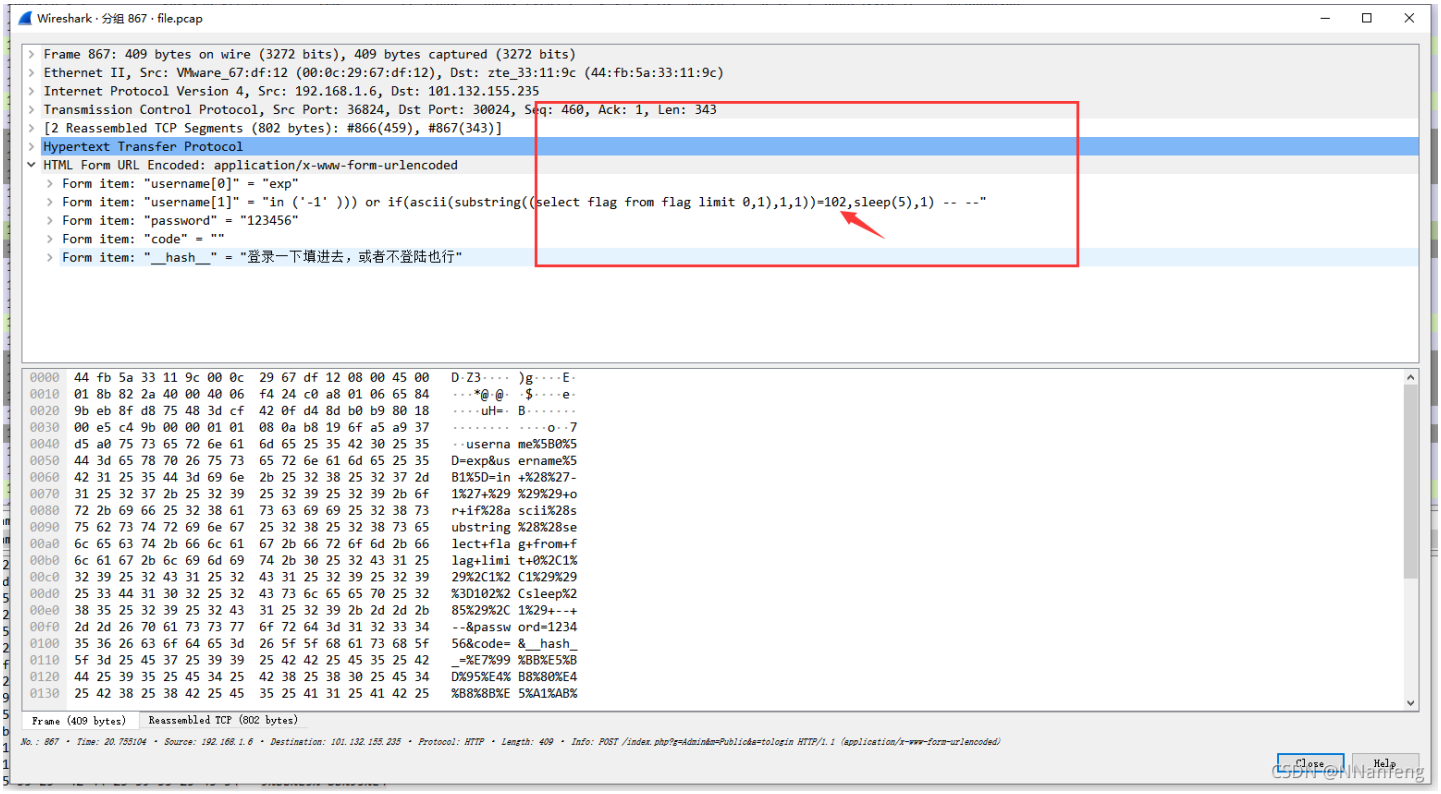
用wireshark打开文件分析



可以分析这一句语句应该是在盲注，这里推荐一个师傅的博客，有盲注分析

https://blog.csdn.net/qq_45555226/article/details/102809032

（不会写脚本一步一步的搜字符串“,XX,1”，比如要得到第一个字符就搜索",2,1",则往前看一个http协 议的详细信息



得到ASCII码为102，为f，依次进行，得到最终的ASCII码：102 108 97 103 123 99 100 50 99 51 101 50 102 101 97 52 54 51 100 101 100 57 97 102 56 48 48 100 55 49 53 53 98 101 55 97 113 125——最后的flag：f l a g { c d 2 c 3 e 2 f e a 4 6 3 d e d 9 a f 8 0 0 d 7 1 5 5 b e 7 a q }，去掉空 格提交正确)

CRYPTO

1.EAZY_CRYPTO

下载附件打开内容（公正公正公正诚信文明公正民主公正法治法治诚信民主自由敬业公正友善公正平等平等法治民主平等平等和谐敬业自由诚信平等和谐平等公正法治法治平等平等爱国和谐公正平等敬业公正敬业自由敬业平等自由法治和谐平等文明自由诚信自由平等富强公正敬业平等民主公正诚信和谐公正文明公正爱国自由诚信自由平等文明公正诚信富强自由法治法治平等平等自由平等富强法治诚信和谐），曾经做过的24字核心价值观编码，解码网站“http://www.hiencode.com/cvencode.html”

得到flag：flag{lIUqU9O5guX6YiITsRNPiQmbhNRjGuTP}