

【buuctf-misc】--writeup

原创

[「已注销」](#) 于 2022-01-06 16:55:40 发布 2129 收藏

分类专栏: [BUUCTF](#) 文章标签: [安全](#) [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/qq_41152432/article/details/122347949

版权



[BUUCTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

藏藏藏

binwalk查看隐藏文件:

```
(kali@kali)-[~/tmp]
└─$ binwalk dd.jpg
```

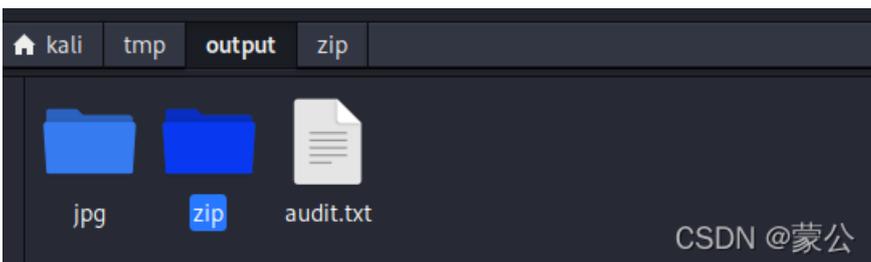
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
63967	0xF9DF	End of Zip archive, footer length: 22

CSDN @蒙公

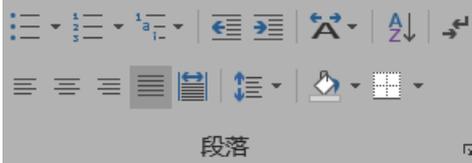
有一个zip文件, 分离: foremost

```
(kali@kali)-[~/tmp]
└─$ foremost dd.jpg
Processing: dd.jpg
|foundat=福利.docx\T\8'CPww
.v$]z]vV
;83(u@ rGq
*|
```

CSDN @蒙公



压缩包里有个福利.docx, 扫描获得flag。



AaBbC AaBb AaBbC AaBbC AaBbCcDd AaBbC
标题 标题 1 标题 2 副标题 强调 要点



↪ CSDN @蒙公

ezmisc

题目

解题快手榜



[MRCTF2020]ezmisc

1

得到的flag请包上flag{}提交。
感谢Galaxy师傅供题。

attachment...

Flag

提交
CSDN@蒙公

更改图片的高度即可。

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00	00	01	F4	00	00	02	4F	08	02	00	00	00	37	0C	8F	...ó...O.....7..
0B	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00sRGB.öî.é..
00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA...±...üa...
00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	..pHYs...Û...Û.Ç
6F	A8	64	00	00	26	C5	49	44	41	54	78	5E	ED	DA	DD	o`d...&AIDATx^iUÝ
99	C4	B6	B1	45	51	C5	A5	80	F4	EC	50	14	8D	93	71	»Ä±EQÄveçiP.."q
00	0E	C3	9E	39	DC	18	91	4D	B2	9B	04	C1	61	13	BD	..Ûz9Ü.'M±.áa.±
D7	CB	D5	1C	14	0A	FC	EB	92	7D	3F	FF	F1	3F	49	52	*ËÖ...üé')?yn?IR

Where is
the Flag???

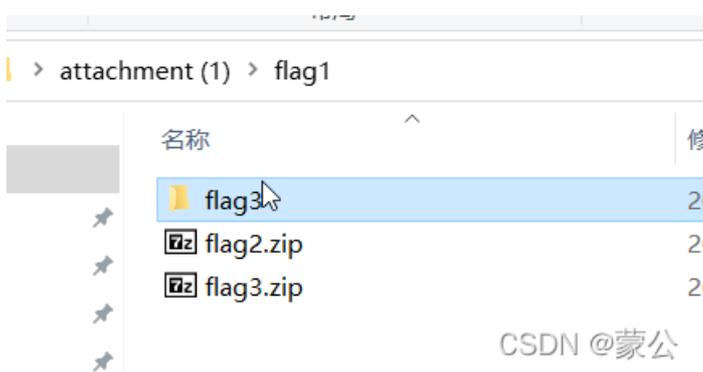
MRCTF{1ts_vEryyyyyy_ez!}

CSDN @蒙公

把MRCTF换成flag提交。

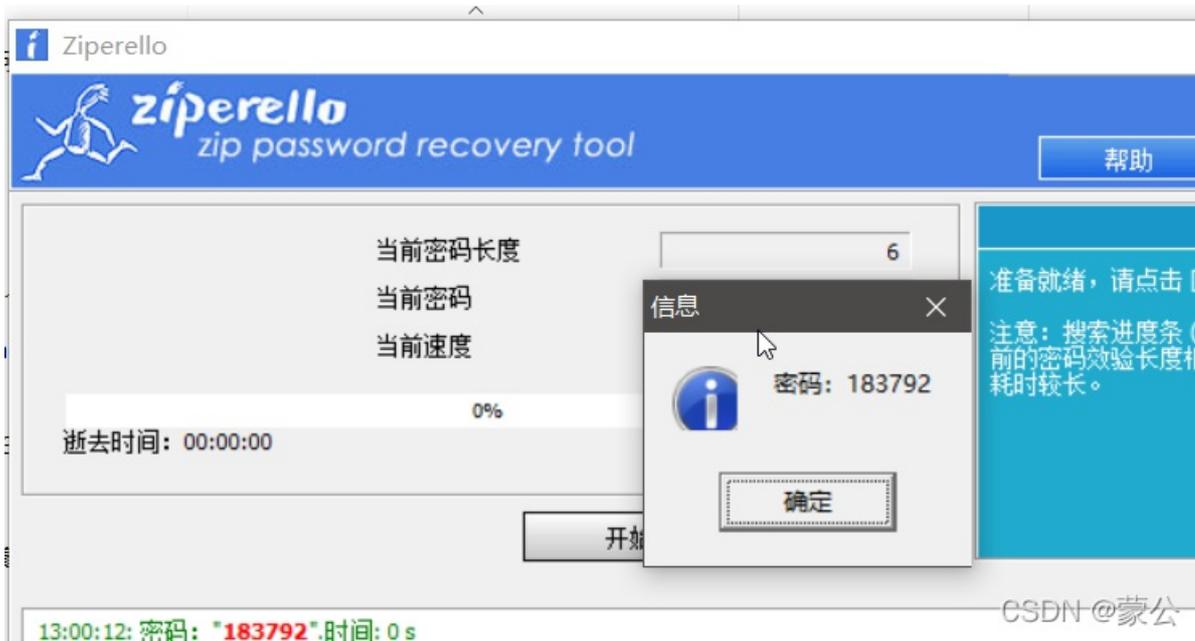
你有没有好好看网课？

给了两个加密的zip, flag2.zip, flag3.zip

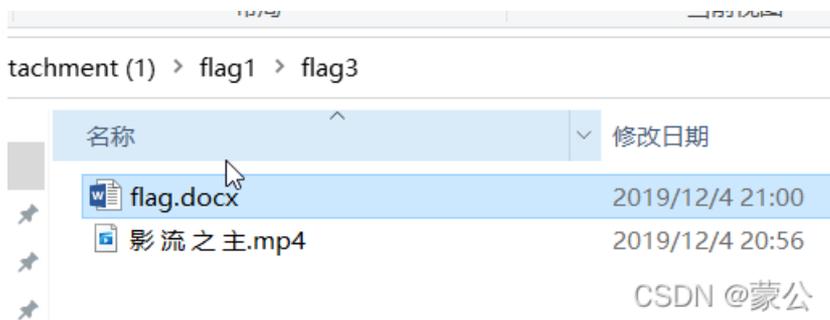


CSDN @蒙公

flag2解密不出来, flag3可以跑出来。



flag3解密出来是一个docx和一个mp4。



flag3应该就是找到flag2的密码的关键。

从小 5 就 20 列文虎克,

我每年的 7 月 11 日的生日愿望就是拥有一个🔍

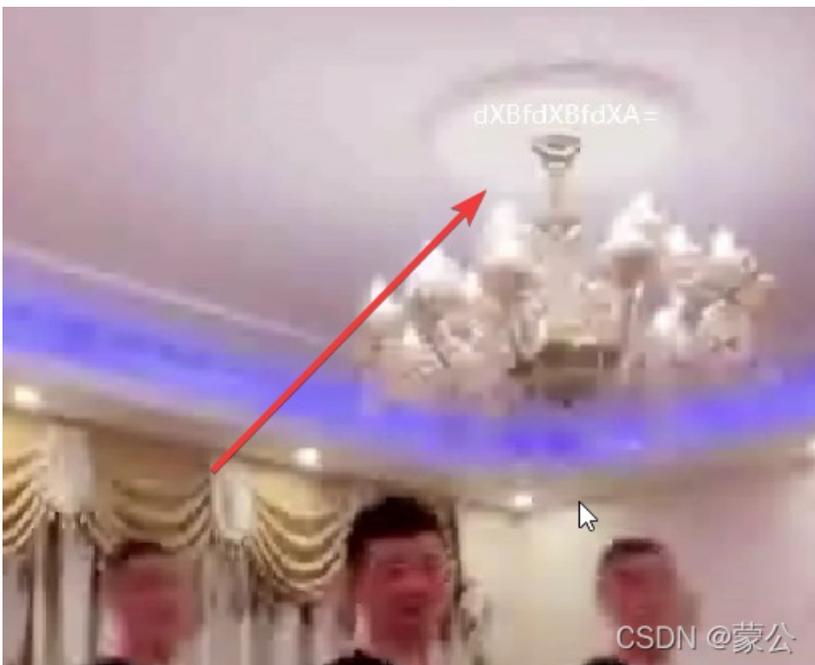


然而，520711并不是flag2的密码，要不然肯定可以爆出来。

那这串数字是什么意思？

根据题目，是要看网课，即那个mp4的视频。实际上，520711就是在视频的5.20s和7.11s的时候，有提示，

不过要非常仔细，不然真发现不了。



第一个以为是摩斯电码，实际上并不是，是敲击码，解密：[CTF在线工具-在线敲击码|敲击码编码|敲击码算法|tap code](#)

敲击码是一个5X5矩阵。

	1	2	3	4	5
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

CSDN @蒙公

k整合到了c里。敲击码以/作为分隔。所以题目中的...../.../.../.../...../

就是52313132，数点数即可。

[在线工具](#)

[买SSL证书](#)

[SSL在线工具](#)

[工具网](#)

敲击码

tap code

52313132

查询

反查

w(W) 1(L) 1(L) m(M)

CSDN @蒙公

所以解密出来是wllm。

第二个是base64。


```
C:\Users\n0rland3r\Desktop>volatility.exe -f mem.dump imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility debug : Determining profile based on KDBG search..
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Users\n0rland3r\Desktop\mem.dump)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80003e02110L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80003e03d00L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2019-11-13 08:39:44 UTC+0000
Image local date and time : 2019-11-13 16:39:44 +0800
C:\Users\n0rland3r\Desktop>
```

CSDN @蒙公

一般选择建议profile的第一个，准确性更高。

第二步看cmd命令历史cmdscan。

```
C:\Users\n0rland3r\Desktop>volatility.exe -f mem.dump --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: conhost.exe Pid: 2632
CommandHistory: 0x242350 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x2229d0: flag.ccx_password_is_same_with_Administrator
*****
CommandProcess: conhost.exe Pid: 2748
CommandHistory: 0x2926d0 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
C:\Users\n0rland3r\Desktop>
```

CSDN @蒙公

发现有flag.ccx文件，而且提示密码和administor账户的密码一样。

第三步查看特定文件filesan。如flag

```
C:\Users\n0rland3r\Desktop>volatility.exe -f mem.dump --profile=Win7SP1x64 filesan |findstr flag
Volatility Foundation Volatility Framework 2.6
0x000000003e435890 15 0 R-rw- \Device\HarddiskVolume2\Users\Administrator\Desktop\flag.ccx
C:\Users\n0rland3r\Desktop>
```

CSDN @蒙公

第四步，把特殊文件down到本地dumpfiles。

```
C:\Users\n0rland3r\Desktop>volatility.exe -f mem.dump --profile=Win7SP1x64 dumpfiles -Q 0x000000003e435890 --dump-dir=./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3e435890 None \Device\HarddiskVolume2\Users\Administrator\Desktop\flag.ccx
C:\Users\n0rland3r\Desktop>
```

CSDN @蒙公

提示说密码和administrator的密码一样，说明这个文件是加密的。需要找到administrator的密码。

第五步，查找注册表用户hivelist。

```
C:\Users\n0rland3r\Desktop>volatility.exe -f mem.dump --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual          Physical          Name
-----
0xfffff8a001cfd010 0x0000000039828010 \??\C:\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.
0xfffff8a002fa2010 0x0000000013a3f010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a00000f010 0x0000000023385010 [no name]
0xfffff8a000024010 0x0000000023510010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000064010 0x0000000023552010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0000e7410 0x0000000011bcc410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000100360 0x0000000015346360 \SystemRoot\System32\Config\SECURITY
0xfffff8a0003f4410 0x000000001527d410 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0007ae010 0x000000001d867010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0012d4010 0x000000001c938010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a001590010 0x000000001151a010 \SystemRoot\System32\Config\SAM
0xfffff8a0015ca010 0x00000000111a3010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001c34010 0x0000000039803010 \??\C:\Users\Administrator\ntuser.dat
```

CSDN @蒙公

因为需要administrator的密码，所以只需要关注system用户。把此用户的hash显示出来hashdump。

```
C:\Users\n0rland3r\Desktop>volatility.exe -f mem.dump --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010
Volatility Foundation Volatility Framework 2.6
Administrator:500:6377a2fdb0151e35b75e0c8d76954a50:0d546438b1f4c396753b4fc8c8565d5b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

CSDN @蒙公

然后解密hash。解密后面那段就行。



所以flag.ccx的密码是ABCabc123，但是并不知道是什么加密。

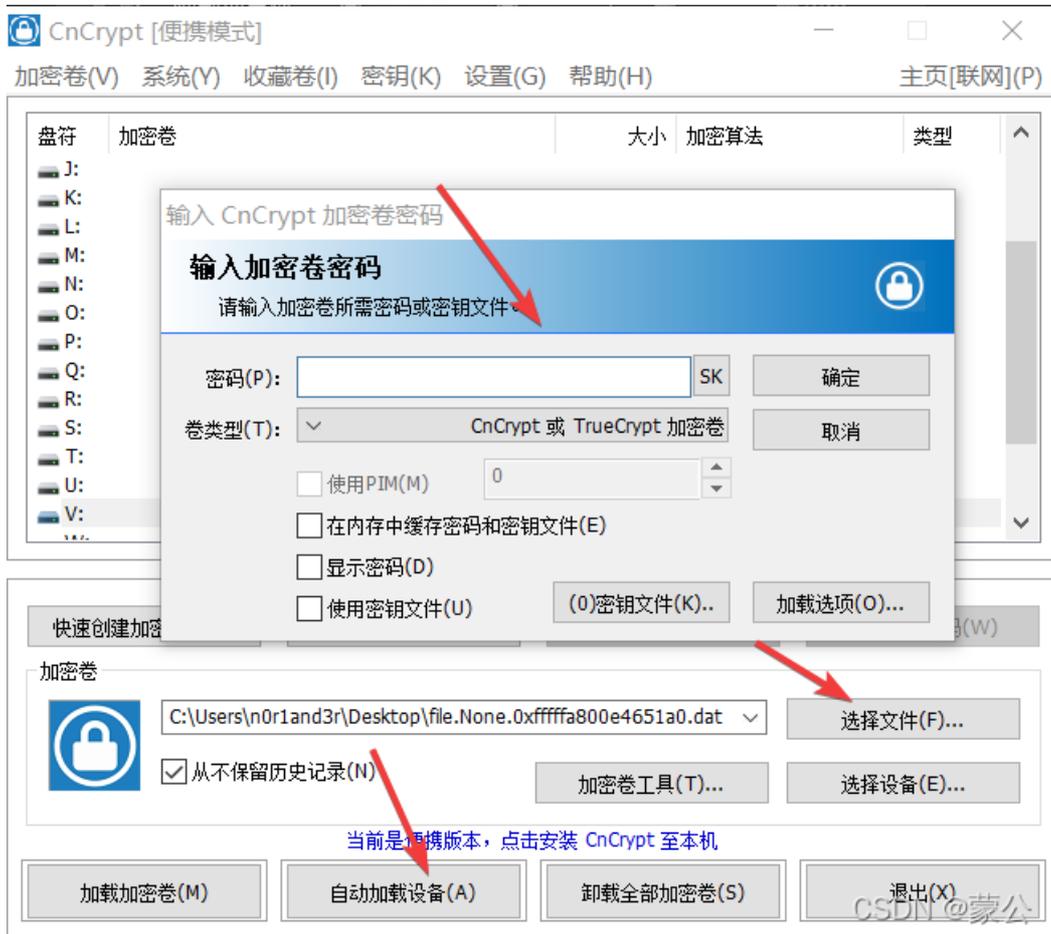
第六步，列举进程pslist。

0xfffffa800e991b10	taskhost.exe	2208	500	10	264	1	0	2019-11-13	08:31:56
0xfffffa800e44a7a0	dwm.exe	2268	816	7	144	1	0	2019-11-13	08:31:57
0xfffffa800e9b8b10	explorer.exe	2316	2260	25	699	1	0	2019-11-13	08:31:57
0xfffffa800ea4f060	vm3dservice.ex	2472	2316	2	40	1	0	2019-11-13	08:31:57
0xfffffa800ea54b10	vmtoolsd.exe	2480	2316	9	188	1	0	2019-11-13	08:31:57
0xfffffa800ea9ab10	rundll132.exe	2968	2620	6	611	1	1	2019-11-13	08:32:02
0xfffffa800e8b59c0	WmiPrvSE.exe	2764	608	11	316	0	0	2019-11-13	08:32:13
0xfffffa800ea75b10	cmd.exe	2260	2316	1	20	1	0	2019-11-13	08:33:45
0xfffffa800e687330	conhost.exe	2632	404	2	63	1	0	2019-11-13	08:33:45
0xfffffa800e41db10	WmiApSrv.exe	2792	500	4	113	0	0	2019-11-13	08:34:27
0xfffffa800ed68840	CnCrypt.exe	1608	2316	4	115	1	1	2019-11-13	08:34:40
0xfffffa800e4a5b10	audiodg.exe	2100	768	6	130	0	0	2019-11-13	08:39:29
0xfffffa800ea57b10	DumpIt.exe	1072	2316	1	26	1	1	2019-11-13	08:39:43
0xfffffa800ealc060	conhost.exe	2748	404	2	62	1	0	2019-11-13	08:39:43

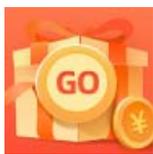
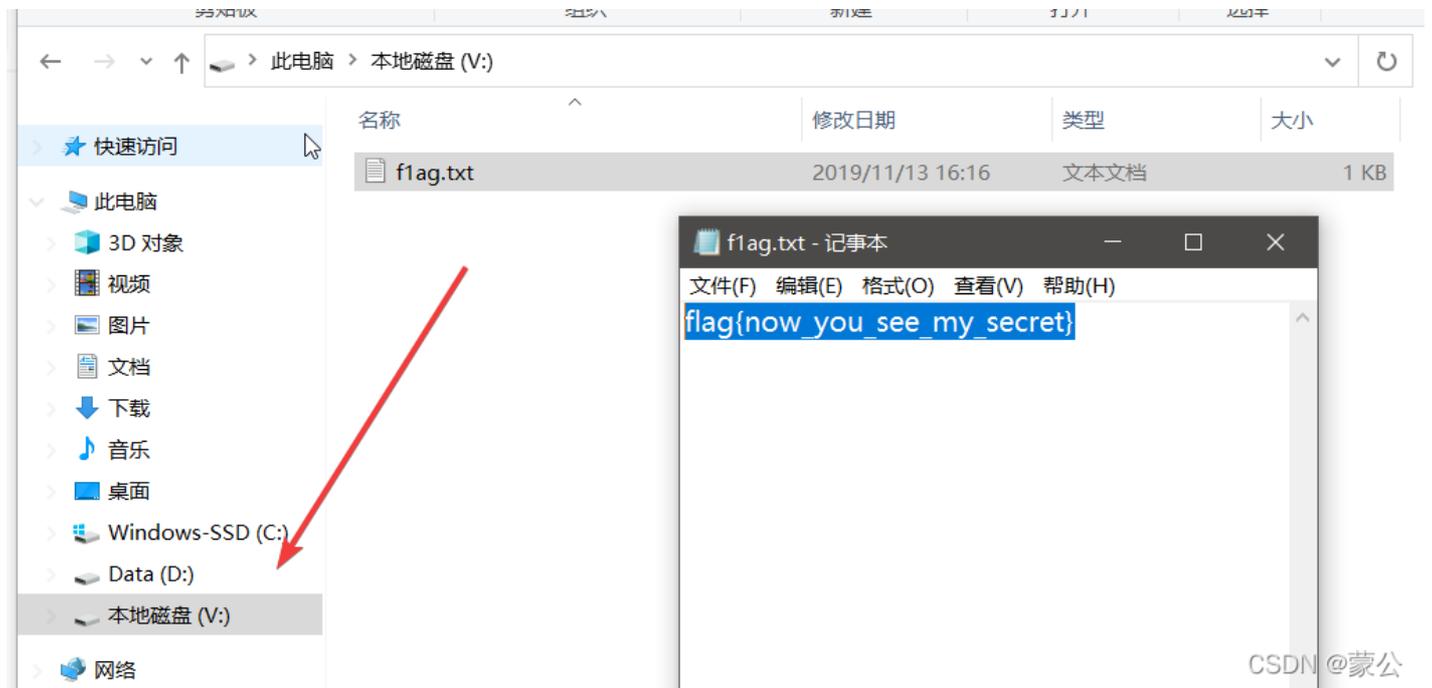
CSDN @蒙公

发现cncrypt，这就是它的加密工具。可以使用cncrypt工具解密。





先把文件加载进来, 然后点击加载加密卷, 然后输入密码, 就能把加密卷加载到你的本地。



[创作打卡挑战赛](#)
赢取流量/现金/CSDN周边激励大奖