# GKCTF X DASCTF应急挑战杯Misc-Writeup

# 原创

本文链接: <u>https://blog.csdn.net/mochu7777777/article/details/118365556</u>

# 版权



<u>CTF\_MISC\_Writeup 专栏收录该内容</u>

246 篇文章 46 订阅 订阅专栏

# 文章目录

# Misc

签到 你知道apng吗

**FireFox Forensics** 

excel 骚操作

0.03

# Misc

签到



#### tcp.stream eq 5 发现 cat /f14g 操作



尝试直接 foremost 分离无果,只能切换为显示Hex数据,然后手动复制出Hex数据,转存为gzip gzip的文件开头Hex为: 1f 8b

hexdata = '1f8b08000000000000003c5d1cb0d80400884e196dcccbf3b528ecffe4b10379e8c57f5f405422601a096b6b3a1660d6d221ca c6fcb0c55599b4094bb226768bbc74be76c504e1d1a3c655fe9d8334b663ee69cda7dbf4ff64afb1d0d4bd5cfe65fb51e4ac6d45be00100

## with open('flag.gz', 'wb') as f: f.write(unhexlify(hexdata))

#### 解压出来还hex数据,转换为字符串是base64,解码base64得到

#### 没啥发现,继续看另外一串Hex数据

#### from binascii import '

hexdata = '1f8b08000000000000000003cd940b8ae4300c44af645b3fe7384927b9ff11f6953b33b0b00c03cb7e609a6e8fe492545572bab57 c798445a5fb88ae735ed123fcf23d766b9ea6789415398a570f8fc9bd3d7b1ed657bcaaf99511f197e245dcc3f3b42d460cefd5fe7cdd1cc 63d3d14e7dbbfe06d280c9ec7ee497f61cdc87be33dbca6ea11bb561c0c265971376155d140ab49ee49b5cb4f30550d549fff2e5e4df35a7 c93b7c30f7ec1d7a31b08192baf710ecdbfb8ca07c71f9c49fd3d326f1b543e89174c7dfab0bc36c123c7ceb9c3f35c9f8ddf437d81df974 fe81c29e4e3ddabcad0513836defa4857a716b8f4cd9f70e9eb97bce0b3ff478fb0da7d9041d331b2c7869f76e8b90ae6ca994b67fbd02bf 2f1e178f32e9fe5cddc1cd1c31edca5dba317fc28d346498f2de1ba0cfe262ed7def14dad6ef0927774b66066607c7f1058be270cabdb51ff 09fabeeeea7f422bee5459dc40fdae34ecf5b095ff32439eadbbfc94bf9916696130e2acf9a780ed7e087e0db99eaa539c8df14cf89e6036 fa97fceb8423dc1a7eaaffe1b74415e6eefbe16b7bf175f7a992d9f4f68cfb5f7f0a9ddffe05def1a5d36bd1f49fee239de3c883f41d2f77 a3fc4b7ee2d3ef03e7bc2bce89eae5d60cfb87b7fdedfa49b78513c4f2219dab6c1fd5cf7aff59e910ff2c17d32f191b9747ba5deaf29ffe 4f1653cf328d59342bc86f88c17cfd65e71ef5effff79aece9e9f3f000ce1e95d90060000'

## with open('flag1.gz', 'wb') as f: f.write(unhexlify(hexdata))

#### 一样的操作, Hex->base64 得到

jMyIjMyIjMyIjMyIjMyIjMyIjMyIjMyIjOQDjACIgACIggDM6EDM6AjMgAzMtMDMtEjM 6AjMgAzMtMDMtEjMwIjO0eZ62ep5K0wKrQWYwVGdv5EItAiM1Aydl5mK6M6jlfpqnrQDt0SLt0SL z0yMw0SMyAjM6Q71pb71mrQDrsCZhBXZ09mTg0CIyUDI3VmbqozoPW+1qeuCN0SLt0SLt0SLt0SL sxWZld1V913e7d2ZhFGbsZmZg0lp9iunbW+Wg0lp9iunbW+Wg0lp9iunbW+WK0wMxoTMwoDMyACM DN0QDN0QD1WazNXMx0Wbf91RGRDNDN0ard0Rf9VZ11WbwADIdRampDKilvFIdRampDKilvVKpM2Y jMyIjMyIjMyIjMyIjMyIjMyIjMyIjMyIjOQDjACIgACIgACIggDM6EDM6AjMgAzMtMDMtEjM 6AjMgAzMtMDMtEjMwIjO0eZ62ep5K0wKrQWYwVGdv5EItAiM1Aydl5mK6M6jlfpqnrQDt0SLt0SL z0yMw0SMyAjM6Q71pb71mrQDrsCZhBXZ09mTg0CIyUDI3VmbqozoPW+1qeuCN0SLt0SLt0SLt0SL sxWZld1V913e7d2ZhFGbsZmZg0lp9iunbW+Wg0lp9iunbW+Wg0lp9iunbW+WK0wMxoTMwoDMyACM DN0QDN0QD1WazNXMx0Wbf91RGRDNDN0ard0Rf9VZ11WbwADIdRampDKilvFIdRampDKilvVKpM2Y ==QIhM0QDN0Q

从base64的填充符位置来看,猜测分了三部分,然后逆序了字符串,所以最终得到

# 你知道apng吗

这里感觉有坑点, flag靠猜测

flag{Welc0me GkC4F m1siCCCCCC!}

第三部分: Y2MpKVvliKDpmaRdIFvliKDpmaRdIDAwbW1lZV9fR0dra0NDNDRGRl9fbW0xMXNzaWlDQ0NDQ0ND MCAyMDowMToxMw0KW+Wbnui9pl0gW+Wbnui9pl0gW+Wbnui9pl0gZmZsbGFhZ2d7e319V1dlZWxs LS0tLS0tLS0tLS0NCueql+WPozoqbmV3IDUyIC0gTm90ZXBhZCsrDQrml7bpl7Q6MjAyMS0wMy0z LS0tLS0tDQrnqpflj6M6Km5ldyA1MiAtIE5vdGVwYWQrKw0K5pe26Ze00jIwMjEtMDMtMzAgMjA6 解码后得到: cc))[删除] [删除] 00mmee\_\_GGkkCC44FF\_\_mm11ssiiCCCCCC0 20:01:13 [回车] [回车] [回车] ffllaagg{{}}WWeell-------窗口:\*new 52 - Notepad++ 时间:2021-03-301:13 [回车] 窗口:\*new 52 - Notepad++ -----21-03-30 20:01:08 # \*\*\*\*\*

20

窗口:\*new 52 - Notepad++ 时间:2021-03-30 20:###########

解码后得到: cc))[删除] [删除] 00mmee\_\_GGkkCC44FF\_\_mm11ssiiCCCCCCC0 20:01:13 [回车] [回车] [回车] ffllaagg{{}}WWeell------窗口:\*new 52 - Notepad++ 时间:2021-03-301:13 [回车]

-----21-03-30 20:01:08

第一部分: Q0NDQ0MhIQ== 解码后得到: CCCCC!!

Challenge	Top 3 Solves	×
	你知道apng <sup>교</sup> 200	3
(flag由flag头	包裹	
🛓 girl.apng		
Flag		Submit



## 改为png只能显示第一帧,wiki上说Firefox支持apng,尝试直接拖入Firefox发现可以显示(我用Chrome也行)



# 我用 ScreenToGif 直接截成Gif, 然后放入 Stegsolve 一帧一帧看

🛃 StegSolve 1.3 by Caesum	- 🗆 X	🗒 QR Research —	D X
File Analyse Help		文件(F) 工具(T) 帮助(H)	
Normal Image		📄 🔛 🔊 📀 🖾 🖉	
		의错等级 H(30%) → 版本 Auto → Auto	館码 Auto 」 て寸 ↓ ↓
		  已解码数据 1:	~
		位置 {17.1,30.4}-{163.4,28.9}-{17.0,174.0}-{163.3,173.6} 颜色正常,正像 版本:3 纠错等级.H,掩码:0 内容: -0327-288a235370ea}	nochu7777

# -0327-288a235370ea}

Frame : 24 of 75		
< > Save	 已解码数据 1: 位置:(177.6.30.4)-(177.6.162.1)-(28.2.30.4)-(28.0.162.1) 颜色反色 谩像 版本:1 别错等级:H,掩码:0 内容: -ad20	^

-ad20

# 🕌 Frame : 39 of 75



这张导出来,用 PS 打开,拉一下就行



# flag{a3c7e4e5



### -9b9d

最终flag为

flag{a3c7e4e5-9b9d-ad20-0327-288a235370ea}

另外也可以使用 APNG Disassembler 来分离出 apng 图片的每一帧 APNG Disassembler: http://apngdis.sourceforge.net

# **FireFox Forensics**

Challenge	Top 3 Solves	×
Fi	reFox Forensics	
	200	
取证大佬说这些	是一份登录凭证文件	
L FireFox_For		
Flag	5	Submit

#### 从文件内容上看应该是 Firefox 的网页登录密码保存加密文件,给了key

此	电脑 > 下载 > FireFox_Forensics			
•	~ 名称	修改日期	类型	大小
	🗟 key4.db	2021/5/8 18:39	Data Base File	288 KB
	0 logins.json	2021/5/8 18:53	JSON Source File	1 KB

#### Google找一下有没有工具

~



https://github.com/lclevy/firepwd

```
PS D:\Tools\Misc\firepwd-master> python .\firepwd.py -d C:\Users\Administrator\Downloads\FireFox_Forensics
globalSalt: b'1e26e84b2f01da28d865e7258f9003d16b9c43f2'
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
    SEQUENCE {
      SEQUENCE {
        OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
        SEQUENCE {
          OCTETSTRING b'66a735e17767b37d83d464126b36d4269243f9e0c99405ccd68f442798f83129'
          INTEGER b'01'
          INTEGER b'20'
          SEQUENCE {
            OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
      SEQUENCE {
        OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
        OCTETSTRING b'24eb241594de7ab37ec379d9ba06'
  OCTETSTRING b'946322a2b2978db6601e449e1bdf7c4d'
clearText b'70617373776f72642d636865636b0202'
password check? True
SEQUENCE {
  SEQUENCE {
    OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
    SEQUENCE {
      SEQUENCE {
        OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
        SEQUENCE {
          OCTETSTRING b'56722302469f529a29dc73f28d6af3ed0ee483cceff05772e96e2313336816fd'
          INTEGER b'01'
          INTEGER b'20'
          SEQUENCE {
            OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
      SEQUENCE {
        OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
        OCTETSTRING b'ef6a4df3e5fd7608c97df9e22092
  OCTETSTRING b'51b24cd6a2672c312255d7f2dddeb67336fd56973b4302bb2eacf2270c251d41'
 }
clearText b'673dec57458fb95bd50bdc9198541038970e5b3d518973a40808080808080808
decrypting login/password pairs
https://ctf.g1nkg0.com:b'admin',b'GKCTF{9cf21dda-34be-4f6c-a629-9c4647981ad7}'
PS D:\Tools\Misc\firepwd-master>
```

GKCTF{9cf21dda-34be-4f6c-a629-9c4647981ad7}

excel 骚操作

Challenge	Top 3 Solves	
	excel 骚操作	
你直的了解exc	200 el吗(flag中flag头包裹	
tlag.xlsx		
Flag		Submit

https://blog.csdn.net/mochu7777777



 $\times$ 

某些单元格设置了只有双击击才能显示内容的格式, Ctrl+A 全选然后右键, 选择 清楚内容->格式

	N22		¥	Q	fx																													
4 A		8	с	D		F	G	н		1		L			0	P	0	R	s	т	U	V				z	AA	AB	AC	AD	AE	AF	AG	AH
<ol> <li>1 我看见</li> </ol>	flag 7.	你呢?																																
2	1	1	1	1	3		1 1				1	1				1	1				1		1				1	1	1	1	1	1	1	
3	1								1	1			1						1		1			1	1								1	
4	1		1	1	3		1 1			1							1	1	1	1		1		1			1	1	1	1	1		1	
s	1		1						1			1	1	1			1		1				1	1							1		1	
6	1		1		3		1 1		1					1				1		1		1			1		1	1	1		1		1	
7	1		1		3		1 1			1				1						1		1		1	1		1	1	1		1		1	
8	1		1		1		1 1	L	1		1			1		1	1	1							1		1	1	1		1		1	
9									1							1		1	1	1			1		1									
10										1			1				1 1						1			1	1							
11									1		1	1	1	1			1 1		1		1	1			1			1			1			
12									1	1	1		1	1		1	1	1	1		1	1	1	1	1	1			1	1	1		1	
12												1					1					1		1				1	1	1	1	1		
14								1	1	1		1	1	1			1 1	1		1		1	1		1		1	1			1	1	1	
15									1		1	1	1				1		1	1	1				1			1		1	1	1	1	
16								1	1	1	1		1	1		1	1	1	1						1	1	1	1	1	1	1	1	1	
17	1	1	1		3		3	1	1	1								1	1				1	1	1		1	1			1			
18	1	1	1	1	1		1 1	1	1		. 1	1	1	1		1	1 1					1	1		1	1				1			1	
19																	1		1	1	1	1	1	1	1			1						
20	1																1		1		1	1		1				1	1		1	1		
21				1	3		1 1	1	1								1	1	1	1		1			1	1	1				1			
22	1	1	1		1		1										1	1			1	1	1	1	1		1	1	1	1	1	1		
23	1	1	1	1			1 1	1	1								1		1	1	1		1		1	1		1	1		1	1		
24	1		1	1			1 1										1		1		1	1		1	1					1			1	
25	1	1		1	1		1 1	1	1								1				1	1		1	1		1	1		1		1	1	
26							1	1									1	1		1	1		1				1		1	1				
27									1			1				1	1	1		1	1		1		1									
28	1	1	1	1	1		1 1		1	1	1	1	1	1			1	1			1	1	1		1		1	1	1		1		1	
29							1		1		1			1			1	1				1	1	1			1	1	1		1		1	
30	1	1	1	1	3		3		1	1	1	1	1	1			1	1	1	1		1	1		1		1	1	1		1		1	
31					3		1						1	1			1	1		1	1				1						1		1	
32	1	1	1		3		3						1	1			1			1		1		1			1	1	1	1	1		1	
33	1	1	1		3		3		1	1	1	1					1	1	1				1		1								1	
24	1	1	1		3		3				1		1	1		1	1	1	1	1	1	1	1	1			1	1	1	1	1	1	1	
25																																		
35																																		
37																																		
28																																		
~																																		
42																																		
42																																		
44																																		
45																																		
46																																		
47																																		

## 只有 空单元格 和 内容为1的单元格,猜测为二维码,修改行高列宽相等

	ABCDEFG	H I J K	LMN	OPQ	RSTU	VWXYZA	AABACADAEAFAG	Α
1	我看见flag了,你呢?							

2	1	1	1	1	1	1	1				1	1			1		1				1		1				1	1	1	1	1	1	1	
3	1								1	1			1						1		1			1	1								1	
4	1		1	1	1	1	1			1							1	1	1	1		1		1			1	1	1	1	1		1	
5	1		1						1			1	1	1			1		1				1	1							1		1	
6	1		1		1	1	1		1					1				1		1		1			1		1	1	1		1		1	
7	1		1		1	1	1			1				1						1		1		1	1		1	1	1		1		1	
8	1		1		1	1	1		1		1			1	1	1		1							1		1	1	1		1		1	
9									1						1			1	1	1			1		1									
10										1			1			1	1						1			1	1							
11									1		1	1	1	1		1	1		1		1	1			1			1			1			
12									1	1	1		1	1	1		1	1	1		1	1	1	1	1	1			1	1	1		1	
13												1					1					1		1				1	1	1	1	1		
14								1	1	1		1	1	1		1	1	1		1		1	1		1		1	1			1	1	1	
15									1		1	1	1				1		1	1	1				1			1		1	1	1	1	
16								1	1	1	1		1	1	1	1		1	1						1	1	1	1	1	1	1	1	1	
17	1	1	1		1		1	1	1	1								1	1				1	1	1		1	1			1			
18	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					1	1		1	1				1			1	
19																	1		1	1	1	1	1	1	1			1						
20	1																1		1		1	1		1				1	1		1	1		
21				1	1	1	1	1	1								1	1	1	1		1			1	1	1				1			
22	1	1	1		1	1											1	1			1	1	1	1	1		1	1	1	1	1	1		
23	1	1	1	1		1	1		1								1		1	1	1		1		1	1		1	1		1	1		
24	1		1	1		1	1										1		1		1	1		1	1					1			1	
25	1	1		1	1	1	1	1	1								1				1	1		1	1		1	1		1		1	1	
26							1	1									1	1		1	1		1				1		1	1				
27									1			1			1		1	1		1	1		1		1									
28	1	1	1	1	1	1	1		1	1	1	1	1	1			1	1			1	1	1		1		1	1	1		1		1	
29							1		1		1			1			1	1				1	1	1			1	1	1		1		1	
30	1	1	1	1	1		1		1	1	1	1	1	1			1	1	1	1		1	1		1		1	1	1		1		1	
31					1		1						1	1			1	1		1	1				1						1		1	
32	1	1	1		1		1						1	1			1			1		1		1			1	1	1	1	1		1	
33	1	1	1		1		1		1	1	1	1					1	1	1			_	1	_	1		_			_			1	
34	1	1	1		1		1				1		1	1	1		1	1	1	1	1	1	1	1			1	1	1	1	1	1	1	
35											_				_				_			f I	ups	2.771	ло	j.ci	SCII	1.11	301	101	2110	11	11	FFF

# 选中该范围 Ctrl+H 替换,替换为框点击 格式,选择 背景颜色选择一个黑色单元格

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z AAABACADAFAFAG	AH AI AI AK AI AM AN AO AP AO AP AS AT AI
我看见flag了,你呢?	
1111111 11 11 1 1 1 1111111	
1 11 1 1 1 1 1 1	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
1 1 1 1 1 1 1 1 1 1 1 1	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
1 1 1 1 1 1 1	
1 1 1 1 1 1 1 1 1 1 1 1 1 1	
2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
3 1 1 1 1 1 1 1 1 1 1 1	
4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	曾视为(b): (IIIII(m)) * (IIIII(m)) *
9 1 1 1 1 1 1 1 1 1	范围(H): 工作表 · □ 区分大小写(C) 设置格式(F)
D 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	###(C) 協行 ▼ □ 単元格匹配(O) 从単元格远程格式:
2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	查扰范围(1): 公式 ▼ □ 区分全/半角(B)
3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	● 字体颜色(T)
4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	◎ 操作技巧 全部替换(A) 替换(R) 查找全部(I) 查找上一个(V) 查找上一个(F) 同 背影与字体颜色(A)
5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
6 11 11 11 1 1 11	(Es Stabutul)
7 1 1 1 1 1 1 1 1	3666世纪4月2日8日
8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
5	
6	
8	

## 替换之后发现为 汉信码

AJ3 - ©, fx														
A B C D E F G H I J K I	LMNOPQRS	TUVWXYZA	AABACADAEAFAG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	A
1 我看见flag了, 你呢?														
2														

4 5 6 7 8 9 10	۳ł								
11									
12			5 替接	ł.					×
14									
15			查找	(D) 替换(F	∧/pc 耒柊			×	
16			查找P	内容(N): 1					各式(M) ▼
17				WPS	表格 已经完成了搜索并	+进行了 503 셏	替换。		
18			替換注	5(E):				1	各式(M) ▼
19			范围(	H): T/E			确定		
20			+9.45				WEAL		
			138.8%	5): 1921 J					
21				-				2	ETE(T)
21 22 23			查找》	ē围(L): 公式 ▼ □	区分全/半角(B)			i	5项(T) < <
21 22 23 24			查找	ē围(L): 公式 ▼ □	区分全/半角(B)			1	š项(T) < <
21 22 23 24 25			· · · · · · · · · · · · · · · · · · ·	范围(L): 公式 ▼ □ 作技巧 全部替换	区分全/半角(B) (A) 替换(R) 查	找全部(I) 查找	线上一个(V) 查找	〕 を下个(F)	频(T) < < 关闭
21 22 23 24 25 26			· 查找 · · · · · · · · · · · · · · · · · · ·	范围(L):公式 ▼ □ (指技巧 全部替换)	区分全/半角(B) (A)	找全部(I) 查封	乾上一个(V) 直部	፤ (F) ←→(F)	频(T) << 关闭
21 22 23 24 25 26 27			· 章叔 () 操	范围(L): 公式 ▼ □	区分全/半角(B) (A) 替换(R) 查	找全部(I) 查封	乾上一个(V)   查找	፤ (¶)↑—₮\$	频(T) << 关闭
21 22 23 24 25 26 27 28			· · · · · · · · · · · · · · · · · · ·	范围(L): 公式 ▼ □	区分全/半角(B) (A) 替换(R) 查	找全部(I) 查排	ጲ上一个(V) _ 查找	≵ (F)—⊤3	频(T) < < 关闭
21 22 23 24 25 26 27 28 29				范围(L): 公式 ▼ □	区分全/半角(B) (A)   替换(R)	找全部(I) 查排	ŝ上─个(V) _ 查找	ž (¶)^—7β	5项(T) << 关闭
21 22 23 24 25 26 27 28 29 30				2週(L): 公式	区分全/半角(B) (A) 替换(R) 查	找全部(I) 查打	ŝ上─个(V)	≵ (F)	频(T) << 关闭
21 22 23 24 25 26 27 28 29 30 31		y F		8調(l): 公式 ▼ □	区分全/半角(B) (A)   替换(R)	找全部(I) 宣	€上一个(V) _ 查找	х 8Ћ—^(F)	频(T) << 关闭
21 22 23 24 25 26 27 28 29 30 31 32				8週(1): 公式	区分全/半角(B) (A)   替换(R)	找全部(I) 查拉	₹重 (/)/~	غ (F) (F) (F)	频(T) << 关闭
21 22 23 24 25 26 27 27 28 29 30 31 32 33				5團(L): 公式 ▼ □	区分全/半角(B) (A) 替换(R) 雪	找全部(1) 查打	&上一个(V) │ 査歩	£ ₹ <b>₽</b> - <b>↑</b> (₽)	频(T) << 关闭
21 22 23 24 25 26 27 28 29 30 31 32 32 33 34				5團(1): 公式 ▼ □	区分全/半角(B) (A) 替换(R) 查	找全部(I) ) 查	2上一个(V)	₹ 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	频项(T) << 关闭
21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 56				6團(l): 公式 ▼ □	区分全/半角(B) (A)   替换(R)   查	找全部()) 查打	ź上一个(V)   查挂	± 8∓—∧(F)	城(I) << 关闭 出

### 在线的汉信码站用不了了: http://www.efittech.com/hxdec.html

## 但是在网上看到有一个叫 中国物品编码中心 的APP可以扫描识别

#### 中国物品编码中心研发的"汉信码"手机识读软件上线啦!

发布时间: 2013-10-16 | 信息来源: 中国自动识别网 | 文章作者: | 点击数: 3083

中国物品编码中心研发的"汉信码"手机识读软件上线啦!

目前支持以下功能:

1.快速的汉信码识读,包括多种信息格式(文本、网址、名片等);

2.扫描二维码名片添加到本地通讯录;

3.扫描汉信码上网服务;

4.扫描结果通过邮箱和好友一起分享;

5.扫描历史的保存。

"汉信码"手机识读软件分为iOS版和Android版,分别适用于苹果公司iPhone4、4S、5等系列手机(以及iPad系列和iPod Touch 4、iPod Touch 5)以及三星、HTC等公司的Android系列手机。

iPhone安装: 对于iPhone手机,请各位登录苹果商店(APP Store),搜索"汉信二维码"(注意是汉信二维码,不是汉信码),在搜索结果排名第一的就 是该软件,或者用苹果设备访问以下网址:https://itunes.apple.com/us/app/han-xin-er-wei-ma/id665768613?mt=8 点击下载即可下载安装。

三星、HTC等Android系统手机安装:

对于三星、HTC等手机用户,请各位访问安智市场(http://www.anzhi.com/soft\_969237.html#,这个链接可以下载),或者安卓市场 (http://apk.hiapk.com/html/2013/07/1662908.html?module=256&info=SWzhTwF4,这个链接可以下载);或在安智、安卓市场搜索"汉信 码",排名第一的就是该软件,用手机访问时,点击下载即可下载安装,用电脑等设备访问时,可以下载到电脑上,用豌豆荚、91助手等手机软件工具帮助 安装,也可以用腾讯手机管家一键安装。



**应用详情:**中国编码APP是集商品条码的注册、续展、变 更、数据通报等功能为一体的综合型的移动版客户端,企 业用户可办理中国物品编码中心所有基础业务,同时对大 众用户开放扫一扫功能,用户通过扫描可对市面上常见的 各种码制进行解析,并通过中心的庞大的数据体系,为用 户展示更为详实的商品条码数据服务。

新版本特性:本软件包括六大基础业务模块、六类特色 服务模块、四个条码小工具,集成了条码注册、数据采 集、咨询服务、二维码应用、扫码查信息等多种应用服 务。同时,本软件为消费者提供商品条码、食品安全追溯 码、物联网统一编码Ecode、快递单号、图书码等编码的 信息查询,支持EAN-13、EAN-8、UPC-A、UPC-E、 Code128、Code39、Code93、GS1 DataBar、ITF等 一维码码制和QR码、汉信码、PDF417、Data Matrix、 Azte

https://blog.csdn.net/mochu77/11777

<	扫描结果
扫描内容	smsto:13511100000:flag{9e e0cb62-f443-4a72-e9a3-4 3c0b910757e}
码制	HANXIN
条码知识	
汉信码是由中国物 一个制定了国家标	品编码中心研制开发,是我国第 准的自主知识产权的二维码,具

有知识产权免费、汉字编码能力强、预污损、预畸 变、信息容量大等特点。2007年8月23日,国家标 准化管理委员会发布了GB/T 21049《汉信码》国 家标准。和其他二维码相比,汉信码更适合汉字信 息的表示,其支持GB 18030中规定的160万个汉字 信息字符,具有高度的汉字表达能力和汉字压缩效 率;具有很强的纠错能力、抗污损和畸变能力,支 持加密技术。

#### https://blog.csdn.net/mochu7777777

flag{9ee0cb62-f443-4a72-e9a3-43c0b910757e}

# 0.03



链接: https://pan.baidu.com/s/1OXIYfEr0s\_zd\_ZXdz48XKg密码: bian

https://gkctf20201-1251267611.file.myqcloud.com/0.03.rar

View Hint Flag Submit

https://blog.csdn.net/mochu7777777

🝰 flag_in_the_disk.zip	2021/6/11 9:58	ZIP 压缩文件	358,400 KB
🗾 secret.txt	2021/6/22 10:20	TXT 文件	1 KB

C:\Users\Administrator\Downloads\0.03\secret.txt - Sublime Text (UNREGISTERED)





但是看大小猜测可能为 虚拟系统文件,可能需要挂载,经过多次尝试发现当密码为: 31122331331311212231231231311 时 VeraCrypt 可以挂载。

🗴 VeraCrypt	— — X
Volumes System Favorites Tools Settings	Help Homepage
Drive Volume S A: B: E:	Size Encryption Algorithm Type
F: G: Enter password for C:\Users\Administrat H:	or\Downloads\0.03\flag_in_the_disk.zip
Password: 3112233133131121223123	312313311 ОК
K: PKCS-5 PRF: Autodetection	TrueCrypt Mode     Cancel
Use PIM Cache passwords and ke Display password	yfiles in memory
Use keyfiles	Keyfiles Mount Options
C: Users (Administrator (Downloads (0.03)	flag_in_the_disk.zip V Select File
VeraCrypt Vever save history	Volume Tools Select Device
Mount Auto-Mount Devices	Dismount All Exit

名称	^				修改日期	]	i	类型		大小		
🗾 ohhhhh	hhh.txt				2021/6/	5 19:39	1	TXT 文(	件		1 KB	
E F:\oh	hhhhhhhh.txt -	Sublim	ne Text	(UNRE	GISTERE	D)						
File Edi	hhhhhhh.txt - it Selection	Sublim Find	ne Text View	(UNRE) Goto	GISTERE Tools	D) Project	Prefere	ences	Help			
File Edi	hhhhhhh.txt - it Selection phhhhhhhh.txt	Sublim	ne Text View ×	(UNRE) Goto	GISTERE Tools	D) Project	Prefer	ences	Help			
File Edi	hhhhhhh.txt - it Selection hhhhhhhh.txt flag i	Find S no	view View ×	(UNREC Goto	GISTERE Tools	D) Project	Prefer	ences	Help			
File Edi	ihhhhhhh.txt - it Selection phhhhhhhh.txt flag i	Find S NO	view View ×	(UNREC Goto	GISTERE Tools	D) Project	Prefere	ences	Help			

VeraCrypt 对于同一个文件可以用不同密码挂载,得到不同内容。需要找到真的密码, secret.txt 中的信息都试了不行,当看 到 0.03.rar 是RAR的压缩包时猜测可能存在 NTFS文件流隐写。



### 扫描一下发现确实存在NTFS文件流隐写

NSE	NtfsStreamsEditor2			_		×
N	se NtfsStreamsEdito	h h	ttp://blog.sina. ad	.com.cn/adv vnetsoft@si	netsof na.con	t n
• •	Ntfs数据流处理工具	Į			by XG	Q
	捜索 💮 编辑 📄 记录 😧 信息					
选:	圣搜索类型 数据流行	3称匹配		_		
0	●全部NTFS磁盘 ●自定义磁盘/文件(夹) C:\Users\Administrator\Download	~ 🎾 搜索	停止			
搜索	结果:共1个;用时0.000 s					
*	文件	数据流名称	大小 <b>(</b> 字节)	可疑度 <mark>(0-5</mark>	)	
⊡	C:\Users\Administrator\Downloads\0.03\secret.txt:whatyoumaywant	whatyoumaywant	37	1		
1						
						1777





看着有点像 <mark>敲击码</mark>,联合 secret.txt 中的那串数字确实类似敲击码中的坐标,但是如果只有 x,y,那只能定位到三个一组的字 符串,经过尝试发现这样得到字符串并不是正确的密码。所以怀疑是 x,y,z 三位一组的坐标,一组坐标定位一个字符串。最后一 位数字定位 x,y 坐标得到的三个字符串中的前后顺序。密码的真实坐标如下:

31 E	1 223 313 313 112 122 312 312 B C C A F D D C E	2 313 311		
得	到密码: EBCCAFDDCE			
此目	l脑 → 本地磁盘 (F:)			
	名称	∨ 修改日期	类型	大小
	🗾 flag.txt	2021/6/11 9:35	TXT 文件	1 KB
	F:\flag.txt - Sublime Text (UNREGIS	STERED)		
	File Edit Selection Find View G	Goto Tools Project Prefer	ences Help	
	I flag.txt ×			
l E	1 flag{85ec0e23-e	ebbe-4fa7-9c8c-e8	8b743d0d85c https://blog.cs	} sdn.net/mochu7777777

flag{85ec0e23-ebbe-4fa7-9c8c-e8b743d0d85c}