




buuctf misc page 2

原创

[~VAS~](#)  已于 2022-03-10 12:45:01 修改  135  收藏 1

分类专栏: [buuctf 笔记 ctf](#) 文章标签: [python](#) [网络安全](#)

于 2022-03-02 11:56:02 首次发布

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/zip471642048/article/details/123226067>

版权



[buuctf](#) 同时被 [3](#) 个专栏收录

5 篇文章 0 订阅

订阅专栏



[笔记](#)

53 篇文章 0 订阅

订阅专栏



[ctf](#)

50 篇文章 1 订阅

订阅专栏

目录

被劫持的神秘礼物

刷新过的图片

snake

[BJDCTF2020]认真你就输了

[BJDCTF2020]藏藏藏

被偷走的文件

[GXYCTF2019]佛系青年

菜刀666

[BJDCTF2020]你猜我是个啥

秘密文件

梅花香之苦寒来

[BJDCTF2020]just_a_rar

[SWPU2019]神奇的二维码

[BJDCTF2020]鸡你太美

[BJDCTF2020]一叶障目

穿越时空的思念

[BJDCTF2020]纳尼

[ACTF新生赛2020]outguess

[SWPU2019]我有一只马里奥

HBNIS2018]excel破解![在这里插入图片描述

谁赢了比赛?

[HBNIS2018]来题中等的吧

[GXYCTF2019]gakki

[WUSTCTF2020]find_me

[ACTF新生赛2020]base64隐写

[SWPU2019]伟大的侦探

[GUET-CTF2019]KO

黑客帝国

[MRCTF2020]你能看懂音符吗

[MRCTF2020]jezmisc

sqltest

[SWPU2019]你有没有好好看网课?

被劫持的神秘礼物

刷新过的图片

F5隐写，解除一个明显是压缩包的东西。

```
(root@kali)-[~/桌面/tools/F5-steganography]
└─# java Extract Misc.jpg -e flag.txt
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Huffman decoding starts
Permutation starts
309504 indices shuffled
Extraction starts
Length of embedded file: 190 bytes
(1, 31, 5) code used

(root@kali)-[~/桌面/tools/F5-steganography]
└─# cat flag.txt
PffL<rEY(flag.txtKIL4KMK1H4206010K361L424047HM PfL<rEY($ flag.txt
0k PKZN

(root@kali)-[~/桌面/tools/F5-steganography]
└─# sudo apt-get install pavucontrol
```

```
PK^C^D^T^@^H^f<86>áL<rEY(^@^@6^@^@H^@^@flag.txtKÉIL`¶4KMK1H420601
0K361`´Lµ4240·47·HM ^E^@PK^A^B^_ ^@^T^@A^@H^@f<86>áL<rEY(^@^@6^@^@H^@$^
^@^@^@^@^@ ^@^@^@^@^@flag.txt
@ ^@^@^@^@A^@X^@É0i@^X^Q0^A^_<9a><88>á^X^Q0^A0k ^G^X^Q0^APK^E^F^@^@^@
A^@A^Z^@^@N^@^@^@^@
~
~
~
~
~
~
~
~
CSDN @~VAS~
```

修改伪加密标志位

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	50	4B	03	04	14	00	00	00	08	00	66	86	E1	4C	3C	72	PK.....ffáL<r
0010h:	45	59	28	00	00	00	26	00	00	00	08	00	00	00	66	6C	EY(...&.....fl
0020h:	61	67	2E	74	78	74	4B	CB	49	4C	AF	B6	34	4B	4D	4B	ag.txtKÉIL`¶4KMK
0030h:	31	48	34	32	30	36	4F	31	30	4B	33	36	31	B4	B4	4C	1H4206010K361`´L
0040h:	B5	34	32	34	30	B7	34	37	B7	48	4D	AD	05	00	50	4B	µ4240·47·HM-..PK
0050h:	01	02	1F	00	14	00	00	00	08	00	66	86	E1	4C	3C	72ffáL<r
0060h:	45	59	28	00	00	00	26	00	00	00	08	00	24	00	00	00	EY(...&.....\$...
0070h:	00	00	00	00	20	00	00	00	00	00	00	00	66	6C	61	67 flag
0080h:	2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	,txt..
0090h:	C9	30	EC	A9	18	11	D4	01	1F	9A	88	AA	18	11	D4	01	É0i@..0..s^a..0.
00A0h:	D8	6B	20	07	18	11	D4	01	50	4B	05	06	00	00	00	00	0k ...0.PK.....
00B0h:	01	00	01	00	5A	00	00	00	4E	00	00	00	00	00	0A	Z...N.....

snake

Serpent – Symmetric Ciphers Online

Grammarly
Works Across Sites and Apps INSTALL
[X 广告](#)

Input type: File

File: C:\fakepath\cipher Browse

Function: SERPENT

Mode: ECB (electronic codebook)

Key: anaconda
(plain)

Plaintext Hex

> Encrypt! > Decrypt!

CSDN @~VAS~

File was uploaded.

Decrypted text:

00000000	43 54 46 7b 77 68 6f 5f 6b 6e 65 77 5f 73 65 72	C T F { w h o _ k n e w _ s e r
00000010	70 65 6e 74 5f 63 69 70 68 65 72 5f 65 78 69 73	p e n t _ c i p h e r _ e x i s
00000020	74 65 64 7d 00 00 00 00 00 00 00 00 00 00 00	t e d }

[\[Download as a binary file\] \[?\]](#) Inactive

[\[BJDCTF2020\]认真你就输了](#)

```
(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/attachment/10]
# ls
'~$10.xls'  10.xls  _10.xls.extracted

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/attachment/10]
# cd _10.xls.extracted/

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/attachment/10/_10.xls.extracted]
# ls
0.zip '[Content_Types].xml' docProps _rels xl

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/attachment/10/_10.xls.extracted]
# grep -r flag
grep: 0.zip: binary file matches
xl/charts/flag.txt:flag{M9eVfi2Pcs#}
xl/sharedStrings.xml:<sst xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main"
count="25" uniqueCount="16"><si><t>Name</t></si><si><t>Text</t></si><si><t>Number</t></si><si><t>Boolean</t></si><si><t>Function</t></si><si><t>a</t></si><si><t>b</t></si><si><t>c</t></si><si><t>x</t></si><si><t>ax^2+bx+c</t></si><si><t>m</t></si><si><t>y</t></si><si><t>slope</t></si><si><t>intercept</t></si><si><t xml:space="preserve">The flag is also right under t
his nicely made chart. </t></si><si><t xml:space="preserve">The flag is under this nicely ma
de chart. </t></si></sst>
```

CSDN @~VAS~

[BJDCTF2020]藏藏藏

```
(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11
# ls
output  藏藏藏.jpg  题目及答案.txt

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11
# cd output/

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11/output
# ls
audit.txt  jpg  zip

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11/output
# cd zip/

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11/output/zip
# ls
00000099.zip

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11/output/zip
# ls
00000099.zip

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11/output/zip
# unzip 00000099.zip
Archive: 00000099.zip
福利.docx: mismatching "local" filename (****.docx),
             continuing with "central" filename version
             inflating: 福利.docx

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11/output/zip
# ls
00000099.zip  福利.docx

(root@DESKTOP-MF98M8E)~/mnt/c/Users/mzq/Downloads/1/11/output/zip
```

CSDN @~VAS~



被偷走的文件

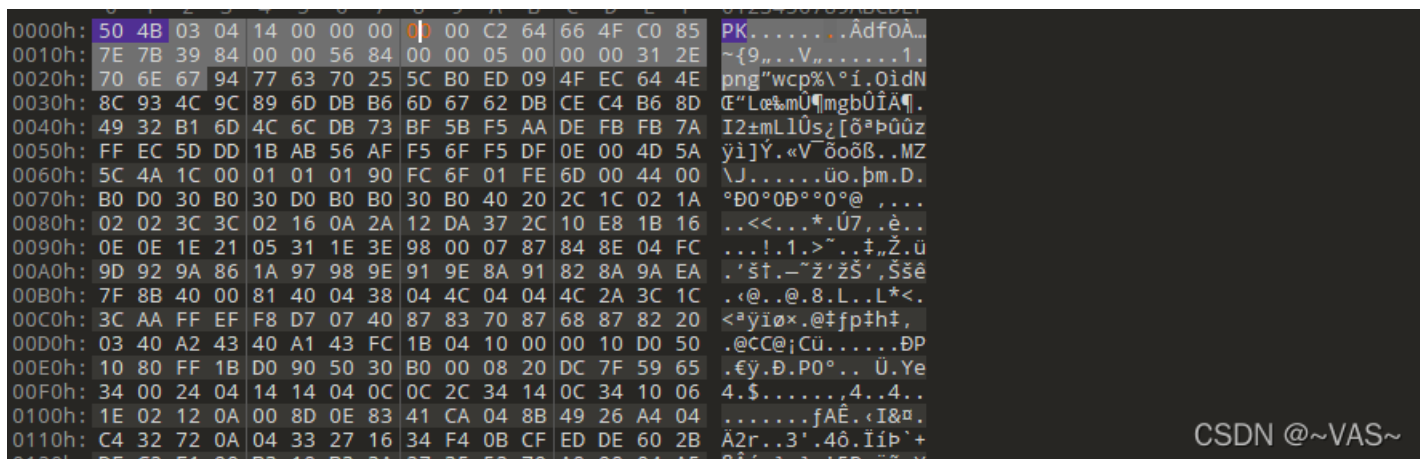
有个rar直接formost，压缩包有密码进行常规密码爆破1-8位

```
PASV
227 Entering Passive Mode (172,16,66,10,56,102).
RETR flag.rar
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete
```

解压得flag



[GXCTF2019]佛系青年



与佛论禅

flag{w0_fo_ci_Be1}

[听佛说宇宙的真谛](#) [参悟佛所言的真意](#) [普度众生](#)

命由己造，相由心生

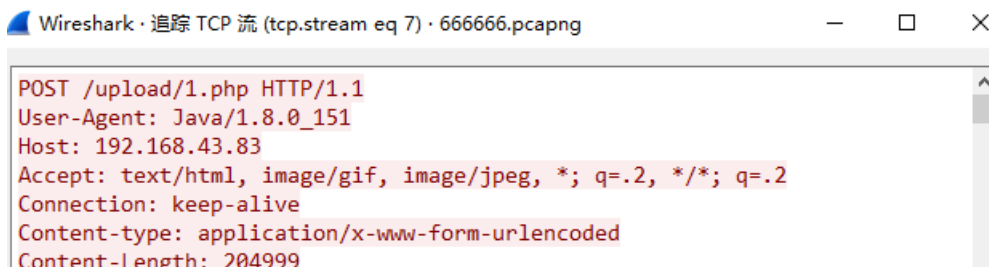
佛曰：遮等諳勝能翳暗諳吟娑梵迦徑羅吟梵者梵禰蘇涅侄室窳真鉢朋能。奢但俱道怯都諳佈梵尼怯一罰心鉢謹
 鉢薩苦奢夢怯帝梵遠那陀諳陀穆諳所納知呈侄以薩怯想夷奢醜數羅怯諳

作者：[蓝色的风之精灵](#)；真米神表示对此工具的非法使用概不负责。
 由 [KeyFansClub 我们的梦想](#) 提供，更多精彩不容错过！

CSDN @~VAS~

菜刀666

在tcp流7里找到一个图片，保存位jpg，打开发现是一个密码，猜测有压缩包




```

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzI
iwiMCIp00BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ21jX3F1b3Rlc19ydW50aw11KDApO2
VjaG8oIi0%2BfCIpOzskZj1iYXN1NjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9QT1NUW
yJ6MiJdOyRjPjXN0c19yZXBsYWN1KCCjccIIsIiIsJGMpOyRjPjXN0c19yZXBsYWN1KCCjcbiIsIi
IsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKtskaSs9MikkYnVmLj11cmxkZWV
vZGUoIiUiLnN1YnN0cigkYywkaS5yKSk7ZWVobYhAZndyaXRlKGVzcGVuKCRmlLj11cmxkZWV
Zik%2FjEiOiIwIiwk702VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDpCd2FtcDY0XHd3d1x
1cGxvYWRcnjY2Ni5qcGc%3D&z2=FFD8FFE000104A46494600010101007800780000FFDB00
43000101010101010101010101010101010101010101010101010101010101010101010101
101010101010101010101010101010101010101010101010101010101010101010101010101
0101010101010101010101010101010101010101010101010101010101010101010101010101
10101010101010101010101010101010101010101010101010101010101010101010101010101
2200021101031101FFC4001F0000010501010101010000000000000000102030405060
708090A0BFFC400B510002010303020403050504040000017D0102030004110512213141
0613516107227114328191A108234281C11552D1F02433627282090A161718191A2526272
8292A3435363738393A434445464748494A535455565758595A636465666768696A737475
767778797A838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B
7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE1E2E3E4E5E6E7E8E9EAF1F2F3F4F5
F6F7F8F9FAFFC4001F010003010101010101010101000000000000102030405060708090
A0BFFC400B51100020102040030407050404000102770001020311040521310612415107
61711322328108144291A1B1C109233352F0156272D10A162434E125F11718191A2627282
92A35363738393A434445464748494A535455565758595A636465666768696A7374757677
78797A82838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B
8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE2E3E4E5E6E7E8E9EAF2F3F4F5F6F7F8
F9FAFFDA000C03010002110311003F00FC18823DB907E62481211D6493F86143D914E012B
CF5E30056C4310192E7D0CC40EFFF30478E3B0DF00FD8F352DA3DBB0AF0769F2C1FF0096
4820600CF2866C0C41CF710E32AD6F187C840F8020A871C672D732780C1D005C0632170FF

```

25 客户端 分組, 0 服务器 分組, 0 turn(s).

整个对话 (206 kB) Show data as ASCII 流 7

查找: 查找下一个 (N)

滤掉此流 打印 另存为... 返回 CSDN @ ~\VAS~



foremost分解pcap得到一个压缩包，输入密码拿到flag

00002778.zip (评估版本)

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)

添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式

00002778.zip - ZIP 压缩文件, 解包大小为 40 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
flag.txt*	40	52	文本文档	2017/12/8 17:28	880CB751

well, you need passwd!

[BJDCTF2020]你猜我是个啥

010editor打开发现是png，修改文件后缀

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 PNG.....IHDR
0010h: 00 00 00 F5 00 00 01 00 08 06 00 00 00 6B 99 30 ...δ.....kʷ0
0020h: 7B 00 00 04 7C 49 44 41 54 78 9C ED DD 41 6E 1B {...}IDATxœIYAn.
0030h: 31 14 05 C1 28 C8 FD AF EC C4 17 10 44 60 7E 48 1..A(Ey`1A.D`~H
0040h: B6 AB B6 01 EC 89 A4 06 37 CF D4 EB EB 9F 5F 40 ¶«¶.i&#.7I0ëëY@
0050h: C6 EF DD 0F 00 3C 4B D4 10 23 6A 88 11 35 C4 88 ÆiY..<K0.#j`.5A^
0060h: 1A 62 44 0D 31 A2 86 18 51 43 8C A8 21 46 D4 10 .bd.1ct.QCCE`!F0.
0070h: 23 6A 88 11 35 C4 FC 79 F7 8F AF D7 EB 7F 3D 47 #j`.5AÛy~.xè.=G
0080h: C2 CA DF C6 4C BD B6 53 7F 9F B3 F2 BC 27 BC 0E ÆÈÈL%[S.Y`ò%`%.
0090h: 55 9F BC B6 4E 6A 88 11 35 C4 88 1A 62 44 0D 31 UY%¶Nj`.5A`.bd.1
00A0h: A2 86 18 51 43 8C A8 21 46 D4 10 23 6A 88 11 35 ct.QCCE`!F0.#j`.5
00B0h: C4 BC 9D 89 AE 28 5F 1F 3E 31 65 3C 61 CE B9 62 Å%.%@(_.>1e<aî`b
00C0h: F7 FB BB FB F7 4F 7A FA 3D 73 52 43 8C A8 21 46 ÷0»U÷Ozú=sRCE`!F
00D0h: D4 10 23 6A 88 11 35 C4 88 1A 62 44 0D 31 A2 86 0.#j`.5A`.bd.1ct
00E0h: 18 51 43 8C A8 21 E6 B1 99 E8 8A 13 6E 90 DC 3D .QCCE`!æ±`èS.n.U=
00F0h: 3B BC 6D CE 39 75 9B E8 84 9F FE F9 72 52 43 8C ;mI9u>è.,YbürRCE
0100h: A8 21 46 D4 10 23 6A 88 11 35 C4 88 1A 62 44 0D `!F0.#j`.5A`.bd.
0110h: 31 A2 86 18 51 43 8C A8 21 66 CB 4C 94 B9 2F 66 1ct.QCCE`!fÈL`!'/f
0120h: BF 6D 7E CA F3 9C D4 10 23 6A 88 11 35 C4 88 1A çm~Èøø0.#j`.5A`.
0130h: 62 44 0D 31 A2 86 18 51 43 8C A8 21 46 D4 10 23 bd.1ct.QCCE`!F0.#
0140h: 6A 88 31 13 8D 71 9B 28 4E 6A 88 11 35 C4 88 1A j`1..q;(Nj`.5A`.
0150h: 62 44 0D 31 A2 86 18 51 43 8C A8 21 46 D4 10 23 bd.1ct.QCCE`!F0.#
0160h: 6A 88 11 35 C4 6C 99 89 9A 11 CE CD 2E A7 7E EE j`.5A1`%s.ÎI.š~i
0170h: 4D EF D9 4D CF 3A C1 49 0D 31 A2 86 18 51 43 8C MiÛMI:AI.1ct.QCCE
0180h: A8 21 46 D4 10 23 6A 88 11 35 C4 88 1A 62 44 0D `!F0.#j`.5A`.bd.
0190h: 31 A2 86 98 C7 66 A2 53 5F 76 CE 19 76 DF 26 EA 1ct`CfCS_vî.vB&é
01A0h: F3 F5 39 27 35 C4 88 1A 62 44 0D 31 A2 86 18 51 ôð9`5A`.bd.1ct.Q
01B0h: 43 8C A8 21 46 D4 10 23 6A 88 11 35 C4 BC BE 7E CCE`!F0.#j`.5A%~
01C0h: FA 2D 6D 17 38 61 4D E5 63 72 0F 27 35 C4 88 1A ú-m.8aMâcr.`5A`.
01D0h: 62 44 0D 31 A2 86 18 51 43 8C A8 21 46 D4 10 23 bd.1ct.QCCE`!F0.#
01E0h: 6A 88 11 35 C4 88 1A 62 DE CE 44 6F FB 0E E5 29 j`.5A`.bbÎDo0.ã)
01F0h: 13 33 CD EA FF EB DB EE 8B 07 A7 5E DB 5B 7A 70 .3IéyèÛi.c.šAÚ[zp
0200h: 52 43 8C A8 21 46 D4 10 23 6A 88 11 35 C4 88 1A RCE`!F0.#j`.5A`.
0210h: 62 44 0D 31 A2 86 18 51 43 8C A8 21 E6 ED F7 53 bd.1ct.QCCE`!æi÷S
0220h: 4F 4D DD 56 9C 30 0F DC 3D E9 BC 69 CE B9 6A F7 OMÛVø0.U=é%iî`j÷
0230h: 4D A9 BB 7F FF 04 27 35 C4 88 1A 62 44 0D 31 A2 Mø».y.`5A`.bd.1c
0240h: 86 18 51 43 8C A8 21 46 D4 10 23 6A 88 11 35 C4 t.QCCE`!F0.#j`.5A
0250h: 88 1A 62 DE CE 44 A7 9C 30 3F 5D F1 E9 33 9C 70 `bbÎD$ø0?]ñé3øp
0260h: A3 EA 4D AF D7 B7 13 A6 AA 35 4E 6A 88 11 35 C4 ÈÈM*x.!.!5Nj`.5A
0270h: 88 1A 62 44 0D 31 A2 86 18 51 43 8C A8 21 46 D4 .bd.1ct.QCCE`!F0

```

CSDN @-VAS-

得到一个二维码，扫码发现并没有flag



搜索flag发现在文件末尾

Wireshark packet capture showing a search for 'flag' in a file. The search results table shows one match at offset 0xBCh with the value 'flag'.

地址	值
0xBCh	flag

找到 1 个 'flag'.

CSDN @~VAS~

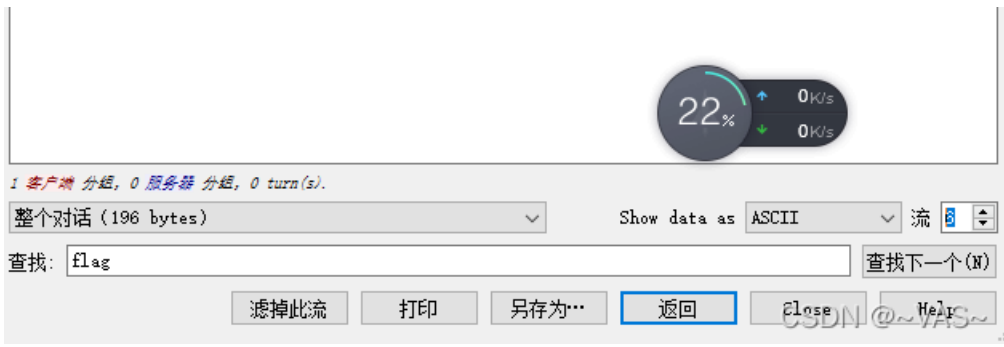
秘密文件

Wireshark packet capture showing a search for 'flag' in a file. The search results table shows one match at offset 0xBCh with the value 'flag'.

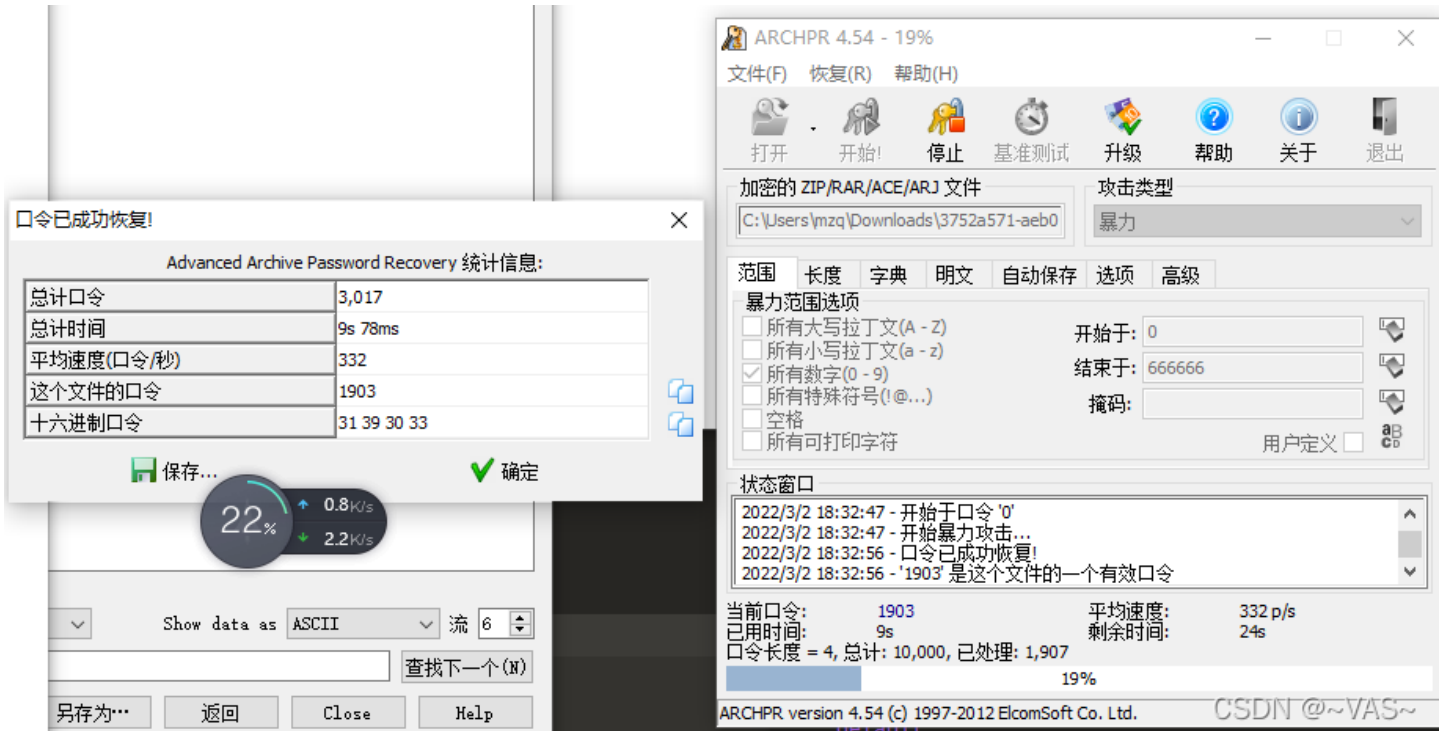
地址	值
0xBCh	flag

找到 1 个 'flag'.

CSDN @~VAS~



foremost分离，爆破拿flag



梅花香之苦寒来

```

a = ""hexdata""
import binascii

def hexStr_to_str(hex_str):
    hex = hex_str.encode('utf-8')
    str_bin = binascii.unhexlify(hex)
    return str_bin.decode('utf-8')

if __name__ == "__main__":
    hex_str = hexStr_to_str(a)
    for i in hex_str.split():

        x,y = eval((i))

        with open('1.txt','a') as f:
            f.write((str(x)+" "+str(y)+"\n"))

```



[\[BJDCTF2020\]just_a_rar](#)



提示4位数进行4位数密码爆破
flag在备注上

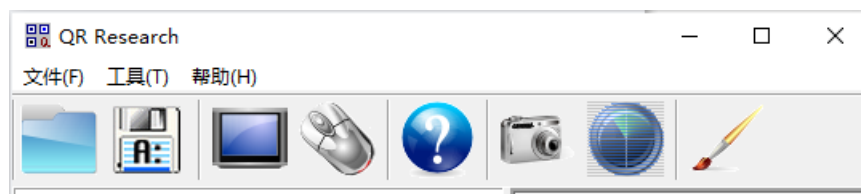
```

ExifTool version Number      : 12.36
File Name                    : flag.jpg
Directory                   : .
File Size                   : 102 KiB
File Modification Date/Time  : 2016:07:27 09:40:10+08:00
File Access Date/Time       : 2022:03:03 08:32:25+08:00
File Inode Change Date/Time : 2022:03:03 08:34:40+08:00
File Permissions            : -rwxrwxrwx
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit             : inches
X Resolution                 : 1
Y Resolution                 : 1
Exif Byte Order             : Big-endian (Motorola, MM)
XP Comment                   : flag{Wadf_123}
Padding                     : (Binary data 2060 bytes, use -b option to extract)
Image Width                 : 580
Image Height                : 868
Encoding Process            : Baseline DCT, Huffman coding
Bits Per Sample             : 8
Color Components            : 3
Y Cb Cr Sub Sampling       : YCbCr4:2:0 (2 2)
Image Size                  : 580x868
Megapixels                  : 0.503
  
```

CSDN @~VAS~

[SWPU2019]神奇的二维码

扫码给了个假的flag





zsteg扫描到存在一个rar文件，进行提取文件

```

└─# zsteg BitcoinPay.png
[?] 163651 bytes of extra data after image end (IEND), offset = 0x7104
extradata:0 .. file: RAR archive data, v5
00000000: 52 61 72 21 1a 07 01 00 33 92 b5 e5 0a 01 05 06 |Rar!....3.....|
00000010: 00 05 01 01 80 80 00 d1 83 d5 03 26 02 03 0b 9c |.....&....|
00000020: 00 04 9c 00 20 97 47 bc ea 80 00 00 0a 65 6e 63 |....G.....enc|
00000030: 6f 64 65 2e 74 78 74 0a 03 02 f1 39 6b fd 93 a9 |ode.txt....9k...|
00000040: d5 01 59 58 4e 6b 5a 6d 64 6f 61 6d 74 73 4d 54 |.YXNkZmdoamtsMT|
00000050: 49 7a 4e 44 55 32 4e 7a 67 35 4d 41 3d 3d 1d 77 |IzNDU2Nzg5MA==.w|
00000060: 56 51 03 05 04 00 52 61 72 21 1a 07 01 00 67 d0 |VQ...Rar!....g.|
00000070: 03 e9 0c 01 05 08 00 07 01 01 83 fc 83 80 00 a7 |.....|
00000080: c8 a4 d9 26 02 03 0b a6 fc 01 04 e1 fe 01 20 d3 |...&.....|
00000090: 05 3b 62 80 03 00 08 66 6c 61 67 2e 6a 70 67 0a |.;b....flag.jpg.|
000000a0: 03 02 ea 7a ef c8 10 a9 d5 01 8f b1 25 41 60 56 |...z.....%A`V|
000000b0: 44 54 23 66 55 50 34 66 a1 16 4d 00 87 11 60 d0 |DT#fUP4f..M...`|
000000c0: 51 61 6a 87 50 d2 1a 43 14 31 48 61 08 7d 16 05 |Qaj.P..C.1Ha.}..|
000000d0: 51 63 a8 69 02 2c 02 2c 0a 2c 3d 02 1a 40 21 2e |Qc.i.,.,.,=.@!..|
000000e0: b7 ce 6b 87 9e fb ad 73 7a d7 5b f9 6f f1 f9 a8 |..k....sz.[o...|
000000f0: aa a9 62 1a ce 73 11 99 89 99 cf e6 7b 86 a6 22 |..b..s.....{.."|

└─(root@DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/神奇的二维码]
└─# zsteg BitcoinPay.png -E 'extradata:0' > 1.RAR

└─(root@DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/神奇的二维码]
└─# ls
1.RAR BitcoinPay.png

```

打开后发现没啥用，binwalk分解图片，有4个压缩包出来了，经过很多次尝试，前两两个应该是混淆用的。

```

└─(root@DESKTOP-MF98M8E)-[/mnt/c/Users/mzq/Downloads/神奇的二维码]
└─# binwalk BitcoinPay.png -e

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         PNG image, 400 x 400, 8-bit/color RGBA, non-interlaced

WARNING: Extractor.execute failed to run external extractor 'unrar e '%e'' : [Errno 2] No such file or directory: 'unrar'
, 'unrar e '%e'' might not be installed correctly

WARNING: Extractor.execute failed to run external extractor 'unrar -x '%e'' : [Errno 2] No such file or directory: 'unrar'
, 'unrar -x '%e'' might not be installed correctly

```



```
'unrar -x %e' might not be installed correctly
28932      0x7104      RAR archive data, version 5.x

WARNING: Extractor.execute failed to run external extractor 'unrar e %e': [Errno 2] No such file or directory: 'unrar'
, 'unrar e %e' might not be installed correctly

WARNING: Extractor.execute failed to run external extractor 'unrar -x %e': [Errno 2] No such file or directory: 'unrar'
, 'unrar -x %e' might not be installed correctly
29034      0x716A      RAR archive data, version 5.x

WARNING: Extractor.execute failed to run external extractor 'unrar e %e': [Errno 2] No such file or directory: 'unrar'
, 'unrar e %e' might not be installed correctly

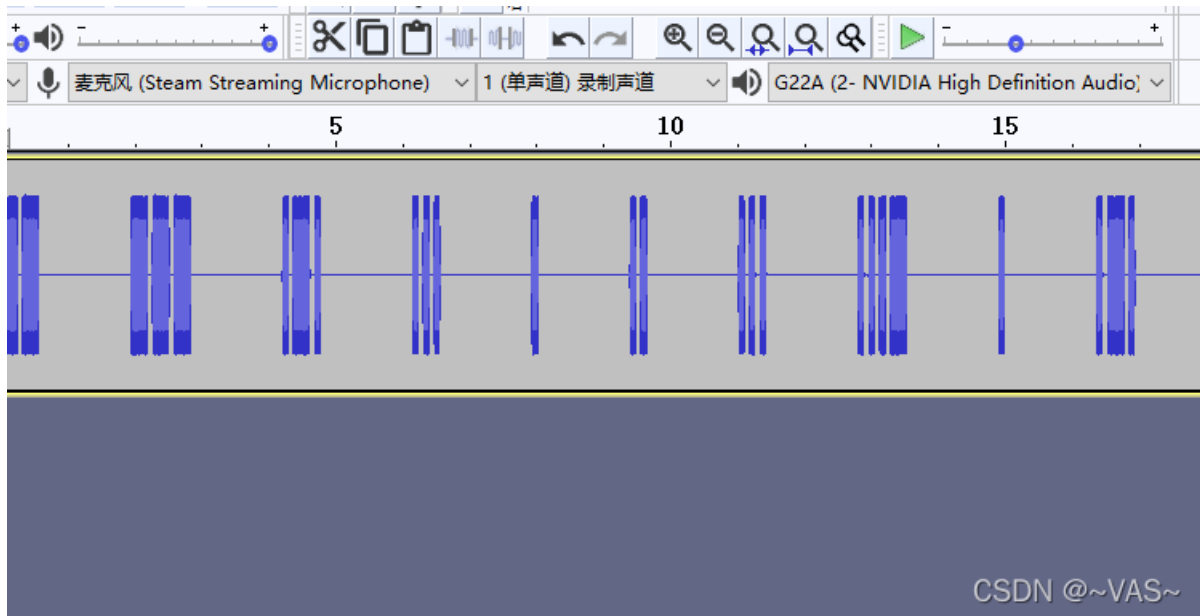
WARNING: Extractor.execute failed to run external extractor 'unrar -x %e': [Errno 2] No such file or directory: 'unrar'
```

CSDN @~VAS~

音频压缩包的密码是docx的base64解密后的

```
b'VjFSSk5XUkdTbFpQVLRsWLRWZDRVvnBHVmtkbFZuQlhWR3hDVmsxcWJGVLVWV1JyWlZad1d6SnFRVDA9'
b'V1RJNWRGSLZPVTlZTVd4UVpGVkdLVnBXVGxCVk1qbFVUVWRrZVZwWFJqQT0='
b'WTI5dFJV0U9YMWxQZfVGeVpWTLBVMjLUTUdkeVpXRjA='
b'Y29tRU90X1lPdUFyZVNPU29TM6dyZWFO'
b'comE0N_Y0uAreS0SoS0great'
Traceback (most recent call last):
```

mp3文件用audi打开发现是摩斯密码



CSDN @~VAS~

flag{小写}

www.mingyue.com 众果搜首页 >> 摩尔斯电码转换

英文字母: MORSEISVERYVERYEASY

转换为摩斯电码 清除 生成摩斯代码的分隔方式: 空格分隔 单斜杠/分隔

摩斯电码: (格式要求: 可用空格或单斜杠/来分隔摩斯电码, 但只可用一种, 不可混用)

转换为英文字母

4核8G 2核2G云服 腾讯云

CSDN @~VAS~ 转换为英文字母

[BJDCTF2020]鸡你太美

修复篮球副本.gif

```
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
h: 47 49 46 38 39 61 68 01 80 02 F7 00 31 00 FF 00 GIF89ah.€.+.1.y.
h: 04 04 0A 0B 09 14 0F 0C 1A 15 21 2C 15 2C 3A 16 .....!.,.:.
h: 10 1B 16 11 21 17 16 21 19 17 28 1B 17 23 1B 17 ...!...!(.##..
h: 28 1B 1C 2D 1C 19 2A 1C 1A 2A 1F 19 2B 20 16 24 (...*..*..+ .$.
h: 20 1D 29 20 1D 2D 21 1D 31 23 20 35 24 22 37 24 .) .-!.# 5$"7$
h: 28 3C 28 20 31 28 23 3B 29 18 22 29 1D 2C 2A 27 (<< 1(##;)."')*
h: 3E 2B 29 34 2D 2C 3F 34 1F 2B 34 26 39 34 31 3A >+)4-.?4.+48941:
h: 35 2D 43 35 36 50 37 36 44 3C 5B 6A 3E 2B 38 3F 5-C56P76D<[j]+8?
h: 32 46 40 3A 51 40 3D 47 42 4A 53 45 3E 53 46 2C 2F@:Q@=GBJSE>SF,
h: 37 49 33 46 4C 56 69 4D 4B 57 4E 3C 47 4F 3E 50 7I3FLViMKWn<GO>P
h: 50 42 59 52 4F 63 53 2F 36 54 4D 59 58 52 64 5F PBYR0cS/6TMYXRd_
h: 48 59 61 79 86 62 50 61 64 57 6D 64 59 62 64 5A HYayibPadWmdYbdZ
h: 68 67 61 6E 68 41 42 69 61 74 6B 65 7A 73 58 5E hganhABiatkezsX^
h: 73 74 7F 74 80 96 75 5D 6B 75 62 68 76 67 79 76 st.t€-u]kubhvgyv
h: 6B 80 77 62 70 77 6C 86 77 75 83 7A 68 6E 7B 76 k€wbpwl1wufzhn{v
h: 87 7B 8F A0 7E 9E B2 80 76 85 80 77 8E 81 62 66 ‡{. ~ž?€v...ewZ,.bf
h: 82 6D 80 82 6E 86 82 7A 95 83 6B 72 83 6C 79 84 ,m€„nt,z•fkrfly„
h: 69 6B 84 7A 8E 84 7A 95 85 73 7F 85 74 87 86 58 ik„zZ„z•...s...t†iX
h: 58 86 7C 96 87 AE BF 89 4C 41 8A 7E 97 8B 76 81 Xt|-†@/LAS~<v.
h: 8B 77 89 8B 78 8E 8C 82 9F 8D 7C 8F 8D 8E A7 8E <w&«xZ€„Y„|.ZšZ
h: 84 90 8F 7F 96 8F BE D4 90 88 99 90 8B A1 91 8C „...-šŒ.™.†j'€
h: A1 91 97 B3 92 85 A1 94 8C A2 95 8C A7 97 83 9B j'~š„„j“€C•€š-f>
h: 98 7F 8D 98 87 9E 98 8B A3 9B 91 AD 9B 94 9E 9C „...“žž“€>'>“žœ
h: 93 A5 9C 94 A8 9E D7 ED 9F 99 AE A0 D8 EE A1 58 “Ÿœ”~žxıY™@ Øi;X
h: 4C A1 85 99 A1 8B 9D A2 99 B5 A3 D7 EF A3 DB F2 Lj...™;†.C™µE×iEUò
h: A4 72 75 A5 65 62 A5 7E 86 A5 C4 DC A6 BD CB A6 pruvëbŸ~†ŸAU!ŸE!
h: D4 E9 A6 D4 EE A6 D6 EC A7 A4 B4 A7 A5 BD A7 DC Ôé!Øi!Øiš¤'šŸŸšŸ
h: F4 A8 70 6B A8 DB F1 A9 99 AE A9 DA F2 AA 61 51 ô“pk”Uñ@™@EUòªaQ
h: AA D1 E9 AA DA EC AB 63 58 AB 7B 78 AB 94 A6 AB aÑé!†j“cX«fX«“†«
```

CSDN @~VAS~



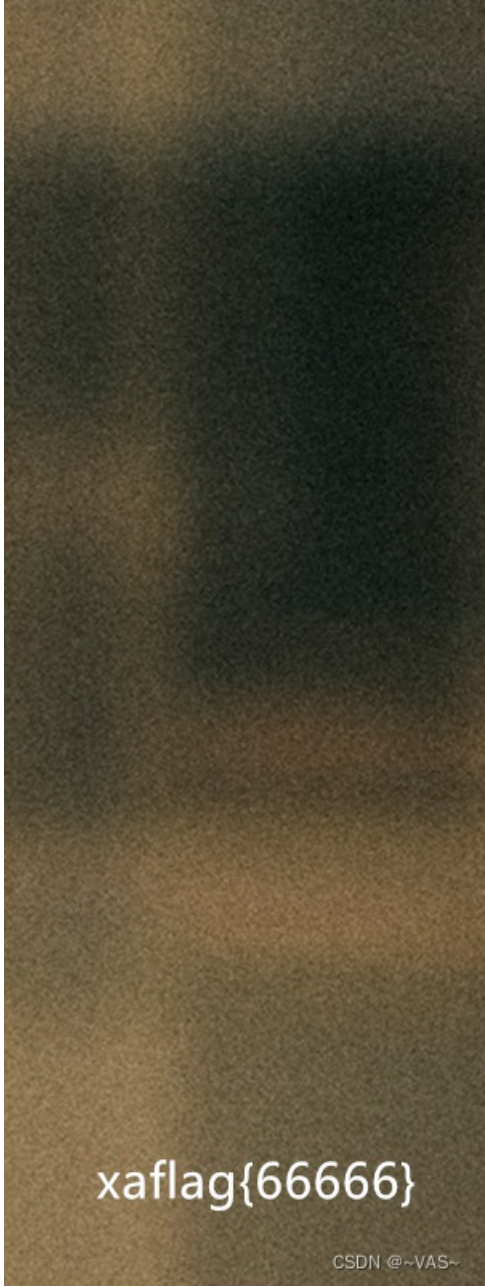
CSDN @~VAS~

[BJDCTF2020]一叶障目

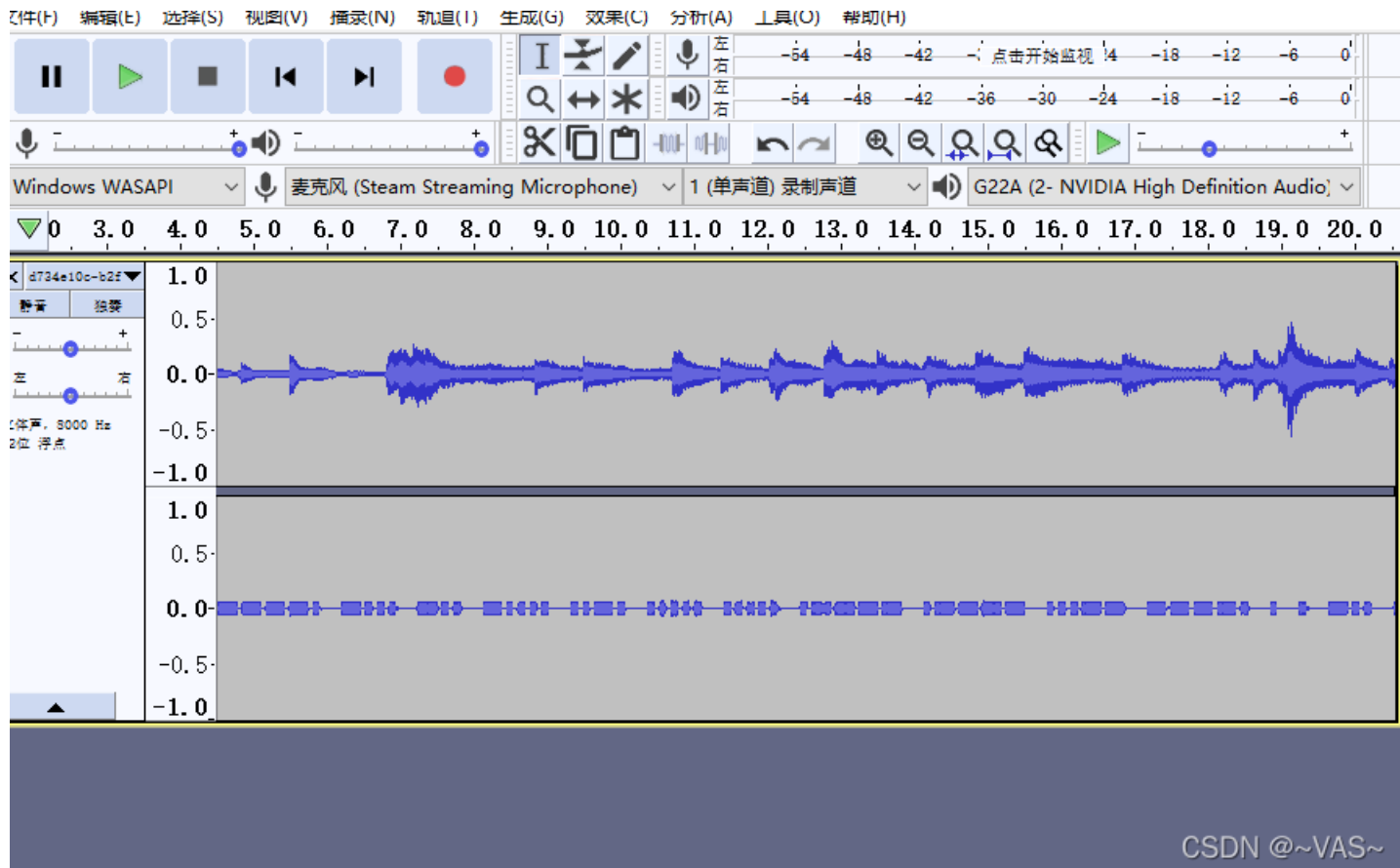
修复图片高度

```
import binascii
import struct
import sys

file = input("图片地址: ")
fr = open(file, 'rb').read()
data = bytearray(fr[0x0c:0x1d])
crc32key = eval('0x'+str(binascii.b2a_hex(fr[0x1d:0x21]))[2:-1])
#原来的代码: crc32key = eval(str(fr[29:33]).replace('\x', '').replace("b'", '0x').replace("'", ''))
n = 4095
for w in range(n):
    width = bytearray(struct.pack('>i', w))
    for h in range(n):
        height = bytearray(struct.pack('>i', h))
        for x in range(4):
            data[x+4] = width[x]
            data[x+8] = height[x]
        crc32result = binascii.crc32(data) & 0xffffffff
        if crc32result == crc32key:
            print(width,height)
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png', 'wb')
            fw.write(newpic)
            fw.close
            sys.exit()
```



穿越时空的思念



众果搜首页 >> 摩尔斯电码转换

英文字母:

生成摩尔斯代码的分隔方式: 空格分隔 单斜杠/分隔

摩尔斯电码: (格式要求: 可用空格或单斜杠/来分隔摩尔斯电码, 但只可用一种, 不可混用)

转换为英

在英文字母输入区域输入英文字母, 单击转换为摩尔斯, 将英文翻译为摩尔斯代码。在摩尔斯电码区域输入摩尔斯电码, 单击转换为英文单词。使用该工具, 可以实现摩尔斯密码的在线翻译, 传递你的神秘信息。摩尔斯代码默认采用空格分隔。

[BJDCTF2020]纳尼

修复文件头

```
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
h: 47 49 46 38 39 61 80 04 88 02 F7 00 00 02 02 02 GIF89a€.^÷.....
h: 0A 01 02 00 09 01 01 02 0B 0A 02 0B 02 0A 09 09 .....
h: 08 0A 11 00 00 12 00 0B 11 08 03 02 02 12 0A 01 .....
h: 13 01 02 1B 02 09 17 2E 06 00 34 01 02 3A 01 01 .....4...
h: 3C 00 0B 38 0F 13 01 02 2C 00 0D 23 01 02 33 08 <..8.....#..3.
h: 00 33 00 09 33 01 01 3C 08 02 3C 45 00 0D 47 01 .3..3..<..<E..G.
h: 03 5D 02 02 59 05 05 4C 12 04 64 01 01 6C 00 01 .]..Y..L..d..l..
h: 62 02 0A 6E 00 0D 67 08 02 71 00 00 75 00 0D 7E b..n..g..q..u..~
h: 43 1B 02 03 42 02 04 4A 06 04 46 03 01 59 01 02 C...B..J..F..Y..
h: 63 02 00 6C 0B 01 66 05 04 75 04 34 7E 00 67 5D c..l..f..u.4~.g]
h: 64 65 46 8C 35 02 8C 3C 01 88 3A 09 93 35 00 94 deF05.0<.^:"5."
h: 3B 02 9A 39 00 9F 36 09 8A 41 08 B5 5F 00 9E 6C ;.š9.Y6.ŠA.µ.žl
h: 00 AD 65 03 AB 6A 00 AE 67 0A B4 65 01 BC 66 02 .-e.«j.@g.'e.¼f.
h: B4 69 01 BB 6A 02 B7 67 0B B2 68 15 B6 71 0C B2 'i.>j.:g.^h.¶q.^
h: 5F 2B B8 67 3A C4 64 02 C8 62 00 C0 60 14 DE 8E _+.g:Äd.Ëb.À'.pŽ
h: 2B CF 8D 36 DB 8C 3A D6 92 3D DA 92 35 E4 8D 2A +İ.6Ü00:0'=Ü'5ä.*
h: E5 95 3A DA 8F 45 DC 92 45 D7 93 4A E1 93 41 FC ä•:Ú.EÜ'E×"Já"Aü
h: B4 5B FA B8 59 FF AE 65 FF AE 6C EC BE 69 ED B6 '[ú.Yy@ey@li%ii¶
h: 66 FD B4 63 FE B8 63 FD B4 6A FF B9 6A FE B6 73 fý'çp,cý'jý'jb¶s
h: EA B5 7F EA C2 7A 01 3B 8A 01 38 85 01 3D 92 02 êµ.éAz.;S.8...='.'
h: 3A 9C 05 37 96 00 41 8F 00 40 90 0C 5B 9B 00 62 :æ.7-.A..@..[>.b
h: AD 05 68 AC 01 65 B3 01 6B B4 01 64 BB 01 6A BC -.CSDN@dVAs~
h: 09 66 B8 13 67 AD 04 69 C6 41 90 8A 3A 87 CC 33 .f..g-.1#A.S:†13
```

用giffame打开

Q1RGe3d

hbmdfYm

FvX3FpYW5n

X2IzX3NhZH0=

Q1RGe3dhbmdfYmFvX3FpYW5nX2IzX3NhZH0=

Base64 Encoding

Encode

Decode

Pattern

Base64

Q1RGe3dhubmdfYmFvX3FpYW5nX2lzX3NhZH0=

CTF{wang_bao_qiang_is_sad}

CSDN @~VAS~

[\[ACTF新生赛2020\]outguess](#)

注释有核心价值观编码

```
File Access Date/Time      : 2022:03:03 10:24:58+08:00
File Inode Change Date/Time : 2022:03:03 10:25:27+08:00
File Permissions          : -rwxrwxrwx
File Type                 : JPEG
File Type Extension       : jpg
MIME Type                 : image/jpeg
JFIF Version              : 1.01
Resolution Unit           : inches
X Resolution              : 96
Y Resolution              : 96
Exif Byte Order           : Big-endian (Motorola, MM)
XP Comment                : 公正民主公正文明公正和谐
Padding                   : (Binary data 2060 bytes, use -b option to extract)
Image Width               : 350
Image Height              : 328
Encoding Process          : Baseline DCT, Huffman coding
Bits Per Sample           : 8
Color Components          : 3
Y Cb Cr Sub Sampling      : YCbCr4:2:0 (2 2)
Image Size                : 350x328
Megapixels                : 0.115

~(root@DESKTOP-MF98M8E)-[~/mnt/c/Users/mzq/Downloads/attachment/tmp/huhuhu] CSDN @~VAS~
```

核心价值观编码

社会主义核心价值观：富强、民主、文明、和谐；自由、平等、公正、法治；爱国、敬业、诚信、友善

abc

编码 解码

公正民主公正文明公正和谐

工具介绍

核心价值观编码 (Core Values Encoder)，经爱党爱国青年sym同意移植本站，旨在通过编程学习党的十八大提出的“社会主义核心价值观”。
联系作者：[github地址](#)
工具地址：<https://sym233.github.io/core-values-encoder/>

CSDN @~VAS~

然后outguess解密

```
~(root@DESKTOP-MF98M8E)-[~/mnt/c/Users/mzq/Downloads/attachment/tmp/huhuhu]
# outguess -k 'abc' -r mmm.jpg 1.txt
Reading mmm.jpg...
Extracting usable bits: 17550 bits
Meg retrieve: seed: 93, len: 23

~(root@DESKTOP-MF98M8E)-[~/mnt/c/Users/mzq/Downloads/attachment/tmp/huhuhu]
```

[SWPU2019]我有一只马里奥

运行exe, 猜测是有文件流隐写

ntfs
flag.txt

CSDN @~VAS~

NtfsStreamsEditor2

NSE NtfsStreamsEditor
Ntfs数据流处理工具

http://blog.sina.com.cn/advnetsoft
advnetsoft@sina.com
by XGQ

搜索 C:\Users\mzq\Downloads\1.txt:flag.txt

选择搜索类型
 全部NTFS磁盘
 自定义磁盘/文件

搜索结果:共6个;用时

* 文件

- C:\Users\mz
- C:\Users\mz
- C:\Users\mz
- C:\Users\mz
- C:\Users\mz [16进制]
- C:\Users\mz

```
00000000| 73 77 75 70 63 74 66 7B 64 64 67 5F 69 73 5F 63 swupctf{ddg_is_c
00000100| 75 74 65 7D ute}
```

删除 - 导出 -> 附加 +/导入 <- 备份 >> 还原 << 导出列表

选择搜索结果, 然后进行处理

CSDN @~VAS~


```
00 00 A8 00 44 02 7A 00 00 00 A3 00 3C 02 F8 D7 .. .D.Z...E.\.bX
00 00 A8 00 48 02 20 00 BE 02 21 00 C0 02 20 00 .. .H. .%.!.A. .
BE 02 21 00 C2 02 B6 00 17 00 43 68 61 6E 67 65 %!.A.¶...Change
53 68 65 65 74 56 69 73 69 62 69 6C 69 74 79 28 SheetVisibility(
29 00 41 00 BC 02 03 00 00 00 69 00 FF FF B8 D7 ).A.%....i.ÿÿ.×
00 00 E0 00 00 00 25 00 66 6C 61 67 20 69 73 20 ..à...%.flag is
68 65 72 65 20 43 54 46 7B 6F 66 66 69 63 65 5F here CTF{office
65 61 73 79 5F 63 72 61 63 6B 65 64 7D 00 00 00 easy_cracked}...
00 00 FF FF FF FF 80 D7 00 00 FF FF FF FF 00 00 ..ÿÿÿÿ€×..ÿÿÿÿ..
01 62 B8 00 41 74 74 72 69 62 75 74 00 65 20 56 .b,.Attribut.e V
42 5F 4E 61 6D 00 65 20 3D 20 22 50 75 62 00 6C B_Nam.e = "Pub.l
69 63 46 75 6E 63 74 00 69 6F 6E 73 22 0D 0A 0D icFunc.tions"...
```

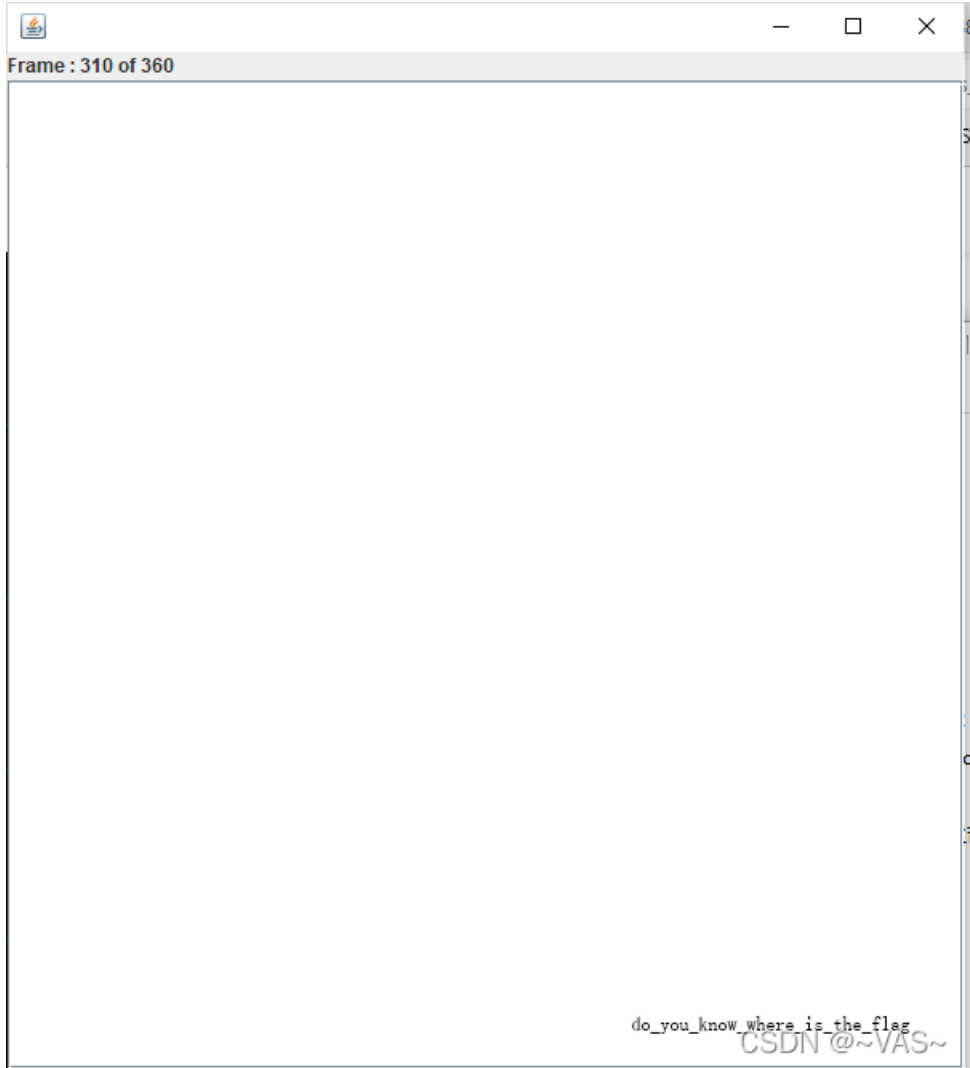
[HBNIS2018]excel破解

谁赢了比赛？

foremost分解图片得到一个rar进行常规爆破

```
(root@DESKTOP-MF98M8E) - [~/mnt/c/Users/mzq/Downloads/cf5d4917-eeaa-42e2-819-
# foremost who_won_the_game.png
Processing: who_won_the_game.png
|*|
```

stegsolve打开frame



在310帧中发现字符，保存，重新观察通道



图片违规！



图片违规！

明显的莫斯密码

莫尔斯电码

Morse code

· · · · · - · · · · · - · · · · · - · · · · ·

编码 解码

alphabet

CSDN @~VAS~

[GXYCTF2019]gakki



一堆无规律字符串，进行词频统计

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
#2V0VI_05X$GygD3*g@gYurMGim#1=D_@Z(JcReVlyGq&N-dgPH8XXSGL{@@}zVmlmxv1vEwbqr)ea!YMI2IznoV_bMrXLbwFrgaiC
j77Ppyn$GsEmoaN6VKJ=j{G#6JHgY(A1$sKX-g9&gigX7d-w*NX&rGN&0tFtQGRkw2j)bh{GPLfZNE=03UmA9nq%FkLH9faebDML
#hz_X*YXxpWW_z03XiDwJzafO(5KI2iJ*2*G5c!{2gSYsw1p$itATG#UGo#O(n^98f-0Y{CPX)ukaakXAte6P)9xkay&8w@fE}p!7uN8g#B
MFacZ3@EQbU(qXG6ig0KGXKWGJJo*J*{kYGVefClpH}uDkDqG2I1YK0rGJjZyqzISR^F%Z5!JG5Y48$*3Y}IG5i9GjYvKaGZo{kXTg0*iG
DYgNX%6!{(F1GSDHq${AXX&VvG*YMA(X)BatC={A}ZN(O7^BoYL6(^F1gySfBlg4mxH=Xy(Z%HwNKB96)cU#qEsS@6W0M%zY!4HI
oNGXP0{5JYXR!{UyOiDIN{s8DBIG4xnrLY^&ORHTpq{G_Z2d)X7yi7j(ou20MKH)FInoecjLkj5_i(X8eR0EZt*RNKZj%u{YOvdv0ppYyrXKI
vi5lzU}La3GZX8uXo-o7sWCs=gyX%5cs!UYh{Y6YI-dliY0{8kdsET3Xna=K_WNjfnv9ia!2y}!#}m1PG!aXwbEGavGK8aX-kxLiPGdlpi8u@
ev{C{4Genn(Y6{gGzX$gYKXg3bGx#qThTKv}iUyXO#L){wNY63zsrflfgYzXGWGaQ7*U*Lkg#x-#@k2wi91im4G)=ll@G)=GkvNYycUuzc
16eQG_vsl1*IUyX{Z^67SO_UX5W^zlrXUA_=CZ{i@O1XENgZf{QiCyW{f}XgA8-$GIDY)X6SYb%Y&Pw)e{7A^i39z^945sNv0YXJ^sUT
T^F%x$hrZ}u%vUjFfX!kyAezAJX(Jrc1P#wjgc#=#NPYcFhem)4XbuBCS3sjYb{GLu&xHsaReYmNFw2i_GZ55g@o1v}XY71^PO#rQ!Y!y
XYdsZ7W}{O}w)u-g#50l66v!GjXPgQ%*zW5g%oe-QesG!@Pas@@cHM=bVOs9K7AGZJilge}{%BeggdfBY^}5XP(HYyeldE#1BrX{h
1$g)=GX(t0{Y4z}Fl&T^iBDsGObey@m8YY63nMWOX5eGY{*eDX*A*}Ylkr3p{JXG0_8=pnbK0jmltKvYufnaxf#kXmVBghUfgaY}*O80l
MFhSfXd&2Y#6D%75f{kga-IRZ{S{QGx}#PYwJvMadDkYUWle^*wo3sE-h=Qr9{9oeG1z8BGdOEd)OE$-^X_#GFKQXg7&W9{nC3Po3!
WXGdaBSVzDg)g0zpNXWcbGgWLAQYo!XNYsGyG6okDzkfFrgKX#Yo{YgX%fOS)Eik&{#alvX-aG*4}UYA{blh^bvMaJ1mYgrHG!^oU
d^Jf@{WGmoNMawD{D#RbRly}Mxh#.ig6g5*ca*qGf{kYD%TYjIX96^aHaaMUaRZXY8zDmj}%WdD7WYiGgG9k1Yak3fYYB3kh0M!
Jb4x3&JZ3izFlifRy-XY6lTP&=(kd1Y-mV!RqGiVWJPi=vAQzVpN9g=ey#{oX5DY!tkP*(GldXHkDgPeG#{4DGUg_4j!Xg&li{Dibdz#7Q!
*{2oDX_@C^kXknk13YC7Cw7yg42Q$SMG6y_qB-GK6r{lU}Gkt(k4E)2g_k*em)k{arW2&aG}XY{7GUR1Jtwx3gqsYpAkOaYJjYRY=dwG{
0okYk#YVYIjKUS$Fh_gXIINc%kzPH}G_{U}7ZggZ-Dy2lgz33jwWYh^a0*eXKckIMggY&UgHBi5&gYlpxQm##nwt$60Hre5(p=kTptipeJ
HAGgqAtYGiilg-eXxNGC0f1d&NeR9X87_rnLalGzt1Z5Q@WlkfAX{Rb1YPnaLXGAWyGagP}}^Hg{ZvOe!udGeGksgF8P}tDf{EkWRB46
YWe{NX^FLgb_R3XGMmewkywzHtn-4cYk$_UvYYaY#i=5s*FM0c-5_Dv3h4AOn&MvVfl22)}#HHcGawmGwta_n)GZmaDqAP{(gWai
y5)oYsMW_2rz$ReDBYGGy@yXo}1w_{^}A{GXfi4ffcr3}Mvlf_H-Gd}jYX5Bs9W5BeEYSWNapkkM0kCkSm_irrKhk{s{DxRawkkYecGNaf
spXF5o=6YGAMwkW6&0oMh39zLxoh%ygGfY{M$XfYLMeiwO@GkJznk2YI%D!2X!s}G^kIKJhiixc6c9u)MKY%K)_&(^{p4e%g0gYX
s1MMMyVi@IkoK{kRmb7YXJXikO_kt-E4sM5WXQgoGetyvpGYZA4SZXr$dJrygs9oW8yhX{yqL1oYUQ({}qa9Muaenk_vwshn)ZkkW4w
t}R{i{Etx{*Mbx4CCA65jYH%eQqkQX{EP}$F**_BWMgT!HpcEPIHa1^y{TiHsElk7G*PBFYMKnYzylG1yqB_Ygg$lfuYx!&HOM)}tX$GL
MQG-#3b{39sP}Yap6*eyqu7Msi&WXeEENgqzQkivx&Yww1AnPG_YSytd=nMRI!Gx1CFknIH^y{iMk8w7xEG(dMXEGY{AI3#itXu-_{tF
P{1T2YWUgslBkqF!VX(zsMXK5MmsJV{xwpgjfwlF8I2FKq14{Xwkm71e%Qp${av_ymleVM)C@5rzY{Q_Y4f@h!1sX6ZYwpwoTcKXNR:
LU6#C9%GtueYyUwSkjP_^}i)Gk4k5iwl@0ig!a@Xk6G*aoCY}iml(^3r3YxgYRNGMxYaaCXAeqnvtYq{Zg{(FY2jD%wC6CPBGp{Zzs(
MYqe7YyeMesjXGDeqT&BBwQN$yIG&!VS8GPHkGu9Aaw6l_0hoY#esYBsBMXewdR3R-kTaataXUw{KG}fl3!kG$KfBzis!gaitXGrT9g2
zuYfw(Bl%yYrk&K@{y-n_ISqzGgVNg-kgvNzY%U1y9{a}{2f!C{pvu5GIYUaokoa1qr3IXgZXhtZalJCyqDfE4$P$*hO%6}&Yb3YgW7d:
InjUhalofH4a*%s9k#asNB5GxDs$)RGD_Gy3iOY4tD0YfwBF3vDwuKzu)*ug%pYtgVd4X0MCeyHY9AKgY&nO_SGc9beHvEkY{Wn
n)yGfPkroAi(LxgHJRXY_GhK{qJrSpb$ARwj)HsvDiXZic8I}iDDDwgFfeiaPOX^QMvxygkicY}=zB&TGS%RpPzatNvkHdteJmiMpXk1
eZsU9N3iUiS)=k^iW!MaksaHab!evM{dxS5@P4oC{pZfBk6JVva2eaOAsop{XkiOrkN&aIYY739ofM&Y80T&Zlro3b58o&Bv! c**OZ6
```

```

# -*- coding:utf-8 -*-
#Author: mochu7
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- =\{\}\[\]"
file_path = input('please input path:')
strings = open(file_path).read()

result = {}
for i in alphabet:
    counts = strings.count(i)
    i = '{0}'.format(i)
    result[i] = counts

res = sorted(result.items(),key=lambda item:item[1],reverse=True)
for data in res:
    print(data)

for i in res:
    flag = str(i[0])
    print(flag[0],end="")

```

```

('b', 1142)
('t', 1141)
('v', 1141)
('r', 1140)
('!', 1058)
('[', 4)
(' ', 1)
('+', 0)
('\ ', 0)
(']', 0)
6XY{gaki_IsMyw1fe}AD0QWJHEKNSUPZ8&*BC249#%^FRTV3@$()-L5670=hoqdujlcmpxzbtvr![ +]
Process finished with exit code 0

```

[\[WUSTCTF2020\]find_me](#)


```

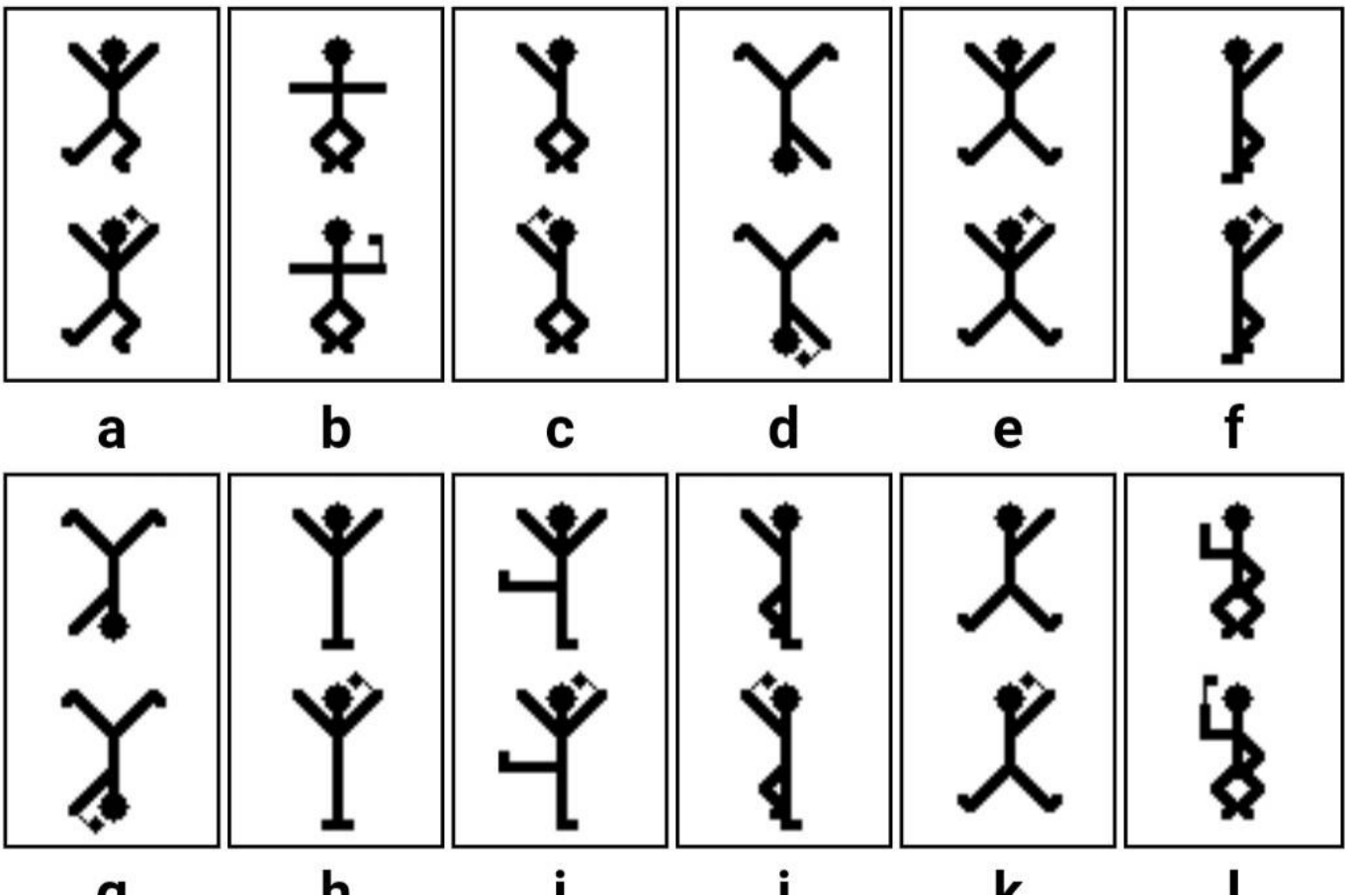
import base64

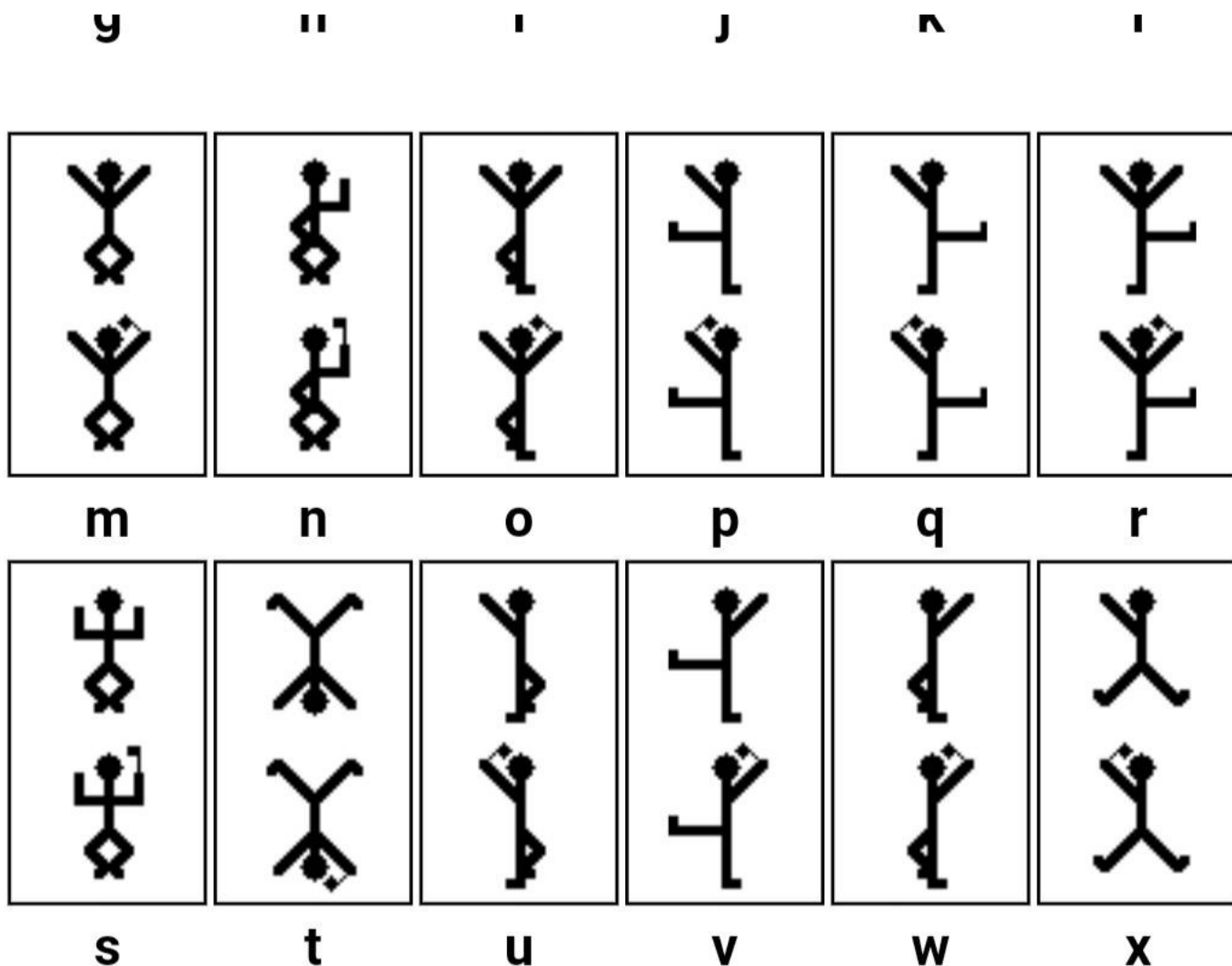
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'

path = input("Path : ")
address = (path[0:(len(path) - len(path.split('\\')[-1]))])
with open(path, 'rb') as f:
    flag = ''
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 = str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")
        offset = abs(b64chars.index(stegb64.replace('=', '')[-1]) - b64chars.index(rowb64.replace('=', '')[-1]))
        equalnum = stegb64.count('=') # no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
            # flag += chr(int(bin(offset)[2:].zfill(equalnum * 2), 2))
            # print(flag) 这样写得不出正确结果
            #print([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)])
        flag = ([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)])
with open(address+'steg_'+path.split('\\')[-1], 'w') as file:
    for i in flag:
        file.write(i)

```

[SWPU2019]伟大的侦探





<https://blog.csdn.net/VAS~>

iloveholmesandwllm

[GUET-CTF2019]KO

Home Projects Services Personal Shop

Search

19

BRAINFUCK/OOK! OBFUSCATION/ENCODING

This tool can run programs written in the [Brainfuck](#) and [Ook!](#) programming languages and display the output.

It can also take a plain text and obfuscate it as source code of a simple program of the above languages.

All the hard work (like actually understanding how those languages work) was done by Daniel Lorch and his [Brainfuck interpreter in PHP](#)

welcome to CTF

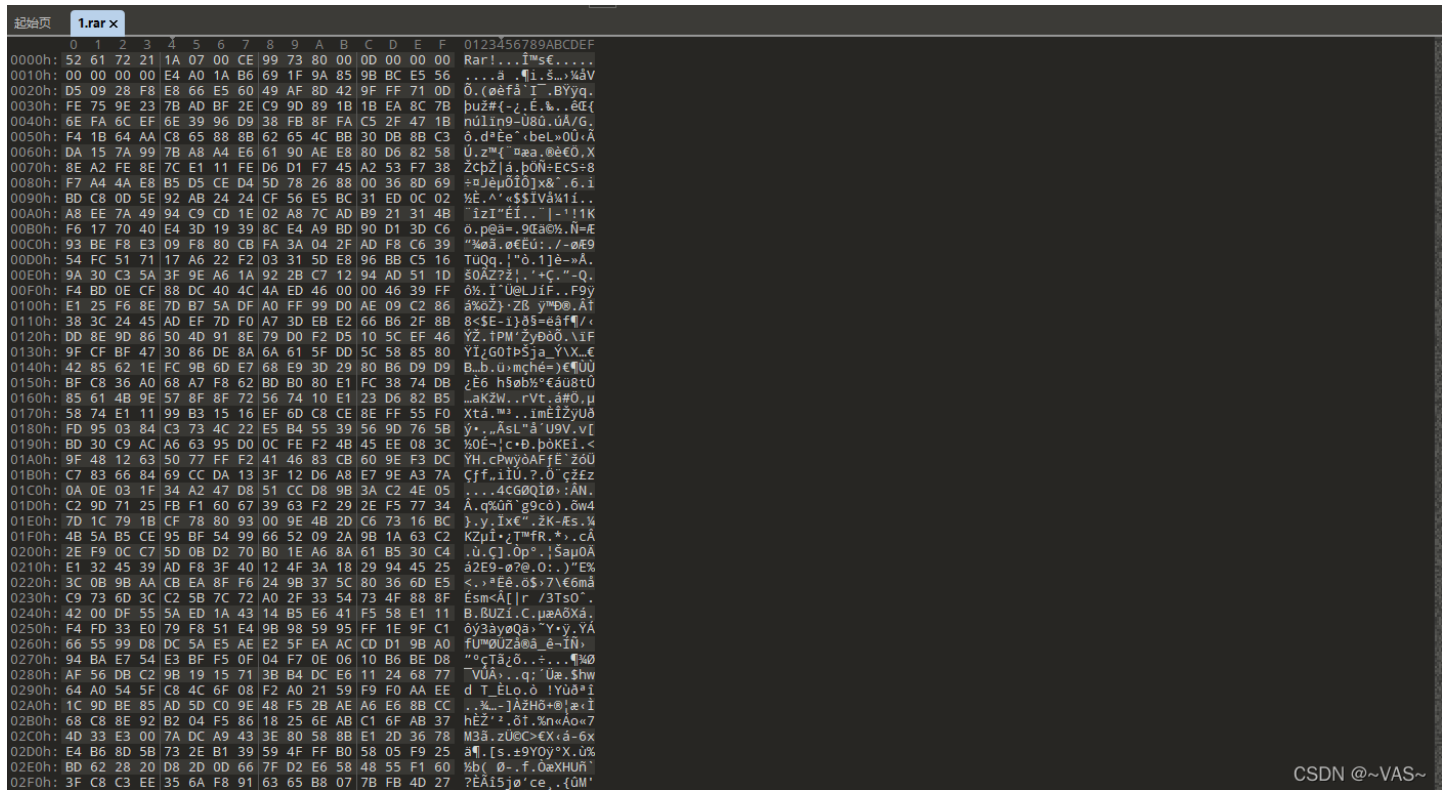
Text to Ook! | Text to short Ook! | Ook! to Text

Text to Brainfuck | Brainfuck to Text

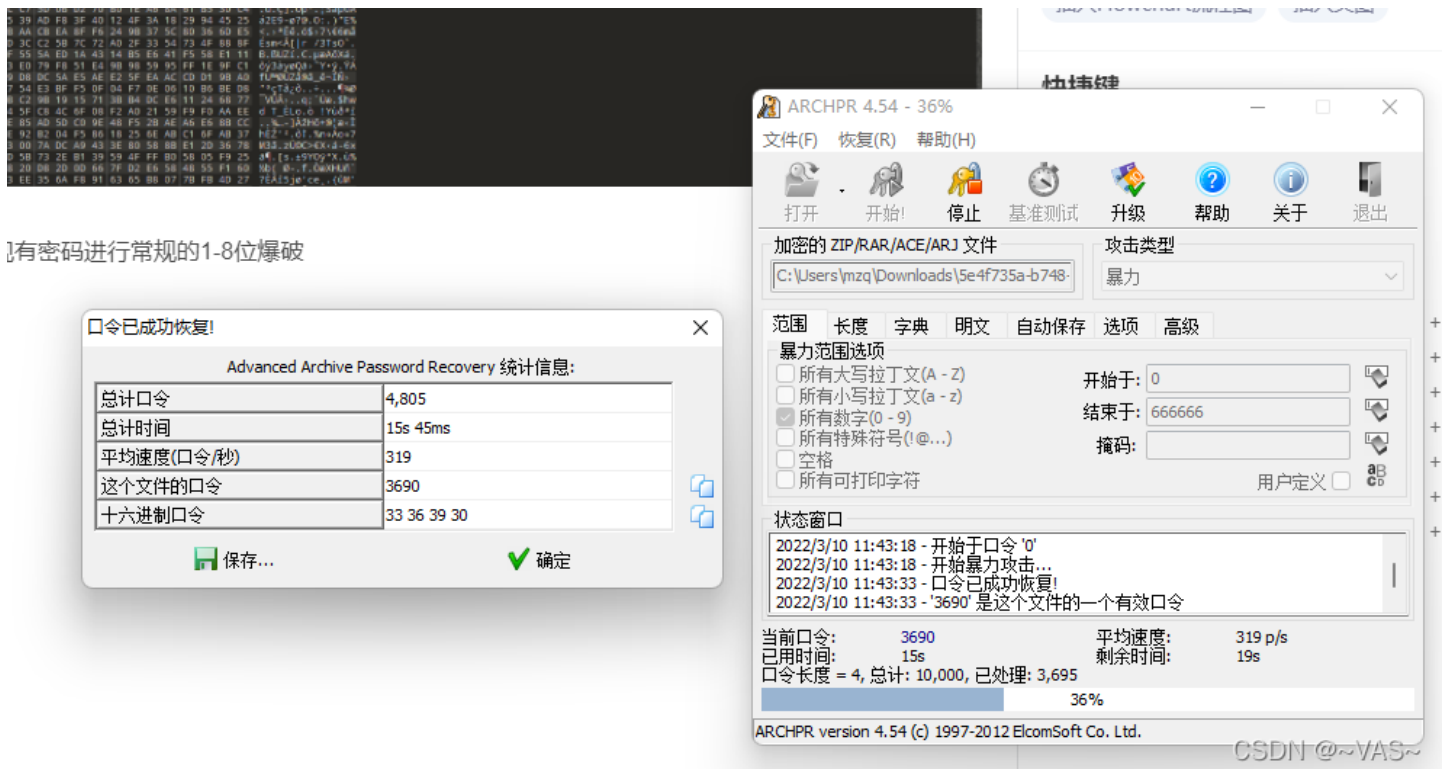
CSDN @-VAS~

黑客帝国

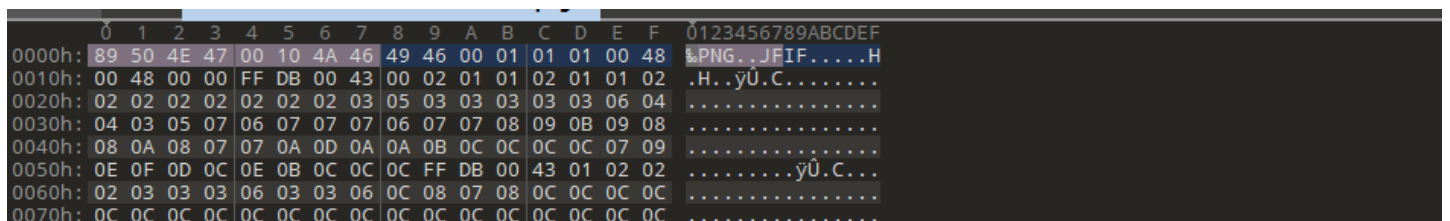
txt的数据头部数据明显是rar的16进制头部，保存为rar



打发现有密码进行常规的1-8位爆破



解压后用010editor打开图片，修改正确的头部



```

0080h: 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C .....
0090h: 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C FF C0 .....ÿÀ
00A0h: 00 11 08 03 06 04 00 03 01 22 00 02 11 01 03 11 .....
00B0h: 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00 .ÿÀ.....
00C0h: 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 .....
00D0h: 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05 ..ÿÀ.µ.....
00E0h: 05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21 .....}.....!
00F0h: 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23 1A..Qa."q.2.'i.#
0100h: 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 B±Á.Rñð$3br,....
0110h: 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A ...%&'()*456789:
0120h: 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJSTUVWXYZ
0130h: 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A cdefghijklstuvwxyz
0140h: 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 f.....t±`%$'""'~™
0150h: 9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 šćčđvy!š`@²³´µ¶·
0160h: B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 ¸¹ºAAAÆÇÈÉÊËÏÐŒ
0170h: D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 Œ×ØÙáâãäåæçèéêñ
0180h: F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03 ôðóôö÷øùÿÿÀ....
0190h: 01 01 01 01 01 01 01 01 01 00 00 00 00 00 00 01

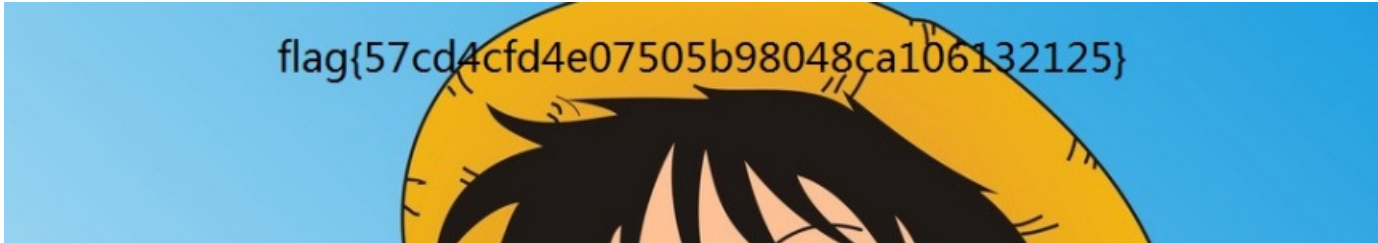
```

CSDN @~VAS~

```

起始页 1:rar 729c4d72a9599a308c04e4015b201.png x QQ图片20220304220015.jpg
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48 y0yà..JFIF....H
0010h: 00 48 00 00 FF DB 00 43 00 02 01 01 02 01 01 02 .H..ÿÜ.C.....
0020h: 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 .....
0030h: 04 03 05 07 06 07 07 07 06 07 07 08 09 0B 09 08 .....
0040h: 08 0A 08 07 07 0A 0D 0A 0A 0B 0C 0C 0C 0C 07 09 .....|. ....
0050h: 0E 0F 0D 0C 0E 0B 0C 0C 0C FF DB 00 43 01 02 02 .....ÿÜ.C...

```



[MRCTF2020]你能看懂音符吗

```

[root@DESKTOP-MF98M8E]~/mnt/c/Users/mzq/Downloads/1/你能看懂音符吗/word
# cat document.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml" xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape" xmlns:wpsCustomData="http://www.wps.cn/officeDocument/2013/wpsCustomData" mc:Ignorable="w14 w15 wp14">
<w:body>
<p>
<pPr>
<w:rPr>
<w:rFonts w:hint="default" w:eastAsiaTheme="minorEastAsia"/>
<w:lang w:val="en-US" w:eastAsia="zh-CN"/>
</w:rPr>
<w:t>呀！一不小心把文档里的东西弄没了.....</w:t>
</w:r>
</w:p>
<w:pPr>
<w:rFonts w:hint="eastAsia"/>
</w:rPr>
<w:p>
<w:pPr>
<w:rPr>
<w:rFonts w:hint="eastAsia"/>
</w:rPr>
<w:p>
<w:pPr>
<w:rPr>
<w:rFonts w:hint="eastAsia"/>
</w:rPr>
<w:p>
<w:pPr>
<w:rPr>
<w:rFonts w:hint="eastAsia" w:eastAsiaTheme="minorEastAsia"/>
<w:vanish/>
</w:rPr>
<w:t>
<w:rPr>
<w:rFonts w:hint="default" w:eastAsiaTheme="minorEastAsia"/>
<w:lang w:val="en-US" w:eastAsia="zh-CN"/>
</w:rPr>
<w:pPr>
<w:rPr>
<w:rFonts w:hint="eastAsia"/>
<w:vanish/>
<w:lang w:val="en-US" w:eastAsia="zh-CN"/>
</w:rPr>
<w:t>这都让你发现了，可是你能看懂吗？</w:t>
</w:r>
</w:p>
<w:bookmarkStart w:id="0" w:name="_GoBack"/>
<w:bookmarkEnd w:id="0"/>
</w:p>
<w:sectPr>
<w:pgSz w:w="11906" w:h="16838"/>
<w:pgMar w:top="1440" w:right="1800" w:bottom="1440" w:left="1800" w:header="851" w:footer="992" w:gutter="0"/>
<w:cols w:space="425" w:num="1"/>
<w:docGrid w:type="lines" w:linePitch="312" w:charSpace="0"/>
</w:sectPr>
</w:body>
</w:document>

```

CSDN @~VAS~

根据盲注判断flag的值，不写这个脚本提取

分组	主机名	内容类型	大小	文件名
156	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>52
166	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>53
176	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20ascii(substr(((select%20count(*)%20from%20information_schema.SCHEMATA)),%201,%201))>53
206	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>100
211	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>100
218	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>100
224	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>100
234	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>100
256	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>50
262	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>50
272	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>50
277	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>50
287	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>50
294	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>25
316	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>25
321	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>25
336	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>25
342	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>25
348	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>12
358	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>12
370	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>12
386	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%203,1))>12
391	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>19
397	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%204,1))>12
404	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>6
410	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>6
436	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%202,1))>9
441	172.16.80.11	text/html	780 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%201,1))>3
448	172.16.80.11	text/html	848 bytes	index.php?act=news&id=1%20and%20length((select%20SCHEMA_name%20from%20information_schema.SCHEMATA%20limit%200,1))>16

CSDN @~VAS~

flag{47edb8300ed5f9b28fc54b0d09ecdef7}

[SWPU2019]你有没有好好看网课?

爆破flag3.zip

The image shows a WinRAR ZIP compression window for 'flag3.zip' (16,317 KB) and the ARCHPR 4.54 password recovery interface. The ARCHPR window shows the file path 'C:\Users\mzq\Downloads\attachment\flag' and the attack type '暴力' (Brute Force). The '暴力范围选项' (Brute Force Range Options) are set to '所有数字(0-9)' (All numbers 0-9). The '状态窗口' (Status Window) shows the progress of the attack, including the current password '183792' and the average speed '16,383,388 p/s'. A progress bar indicates 27% completion.

总计口令	294,901
总计时间	21ms
平均速度(口令/秒)	14,042,904
这个文件的口令	183792
十六进制口令	31 38 33 37 39 32

分析影片，可以得到一个敲击吗和base64是flag2.zip的密码

The image shows a hex dump analysis of a file. The hex data is displayed in columns, with the corresponding ASCII characters shown to the right. The ASCII characters include a Base64 encoded string: '7B 41 32 65 5F 59 30 75 5F 4F 6B 3F 7D 0A 0A 0A'. The Base64 string is '7B4132655F5930755F4F6B3F7D0A0A0A'. The ASCII characters also include a file path: 'C:\Users\mzq\Downloads\attachment\flag'. The Base64 string is decoded to the password '183792'.



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)