# buuoj re逆向前32题writeup(截图+c++源码+过程)

原创

weixin_51275728 于 2021-12-06 01:41:44 发布 2073 收藏 1

分类专栏： ctfre 文章标签： c++ unctf 安全 信息安全

本文链接：https://blog.csdn.net/weixin_51275728/article/details/121738646

版权

ctfre 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

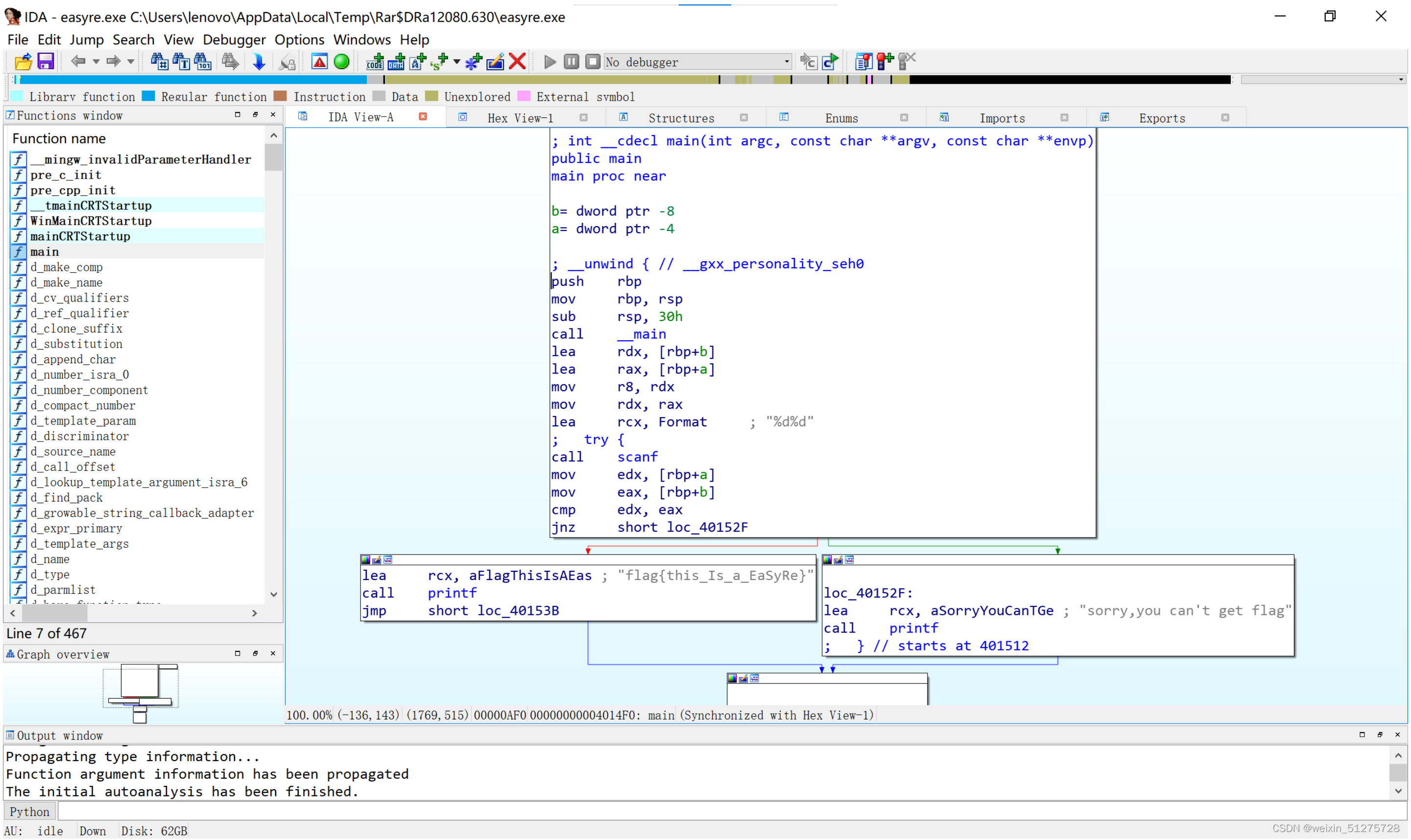
**萌新第一次写这玩意，如有错误，请多指教。**

### RE

## 1-32

# 1 easyre

1、easyre 明码


IDA - easyre.exe C:\Users\lenovo\AppData\Local\Temp\Rar$DRa12080.630\easyre.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Function name
Line 7 of 467
Graph overview
Output window
Python

```
__mingw_invalidParameterHandler
pre_c_init
pre_cpp_init
__tmainCRTStartup
WinMainCRTStartup
mainCRTStartup
main
d_make_comp
d_make_name
d_cv_qualifiers
d_ref_qualifier
d_clone_suffix
d_substitution
d_append_char
d_number_isra_0
d_number_component
d_compact_number
d_template_param
d_discriminator
d_source_name
d_call_offset
d_lookup_template_argument_isra_6
d_find_pack
d_growable_string_callback_adapter
d_expr_primary
d_template_args
d_name
d_type
d_parmlist
```

```
; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near

b= dword ptr -8
a= dword ptr -4

; __unwind { // __gxx_personality_seh0
push    rbp
mov     rbp, rsp
sub     rsp, 30h
call    __main
lea     rdx, [rbp+b]
lea     rax, [rbp+a]
mov     r8, rdx
mov     rdx, rax
lea     rcx, Format     ; "%d%d"
;   try {
call    scanf
mov     edx, [rbp+a]
mov     eax, [rbp+b]
cmp     edx, eax
jnz     short loc_40152F
```

```
lea     rcx, aFlagThisIsAEas ; "flag{this_Is_a_EaSyRe}"
call    printf
jmp     short loc_40153B
```

```
loc_40152F:
lea     rcx, aSorryYouCanTGe ; "sorry,you can't get flag"
call    printf
;   } // starts at 401512
```

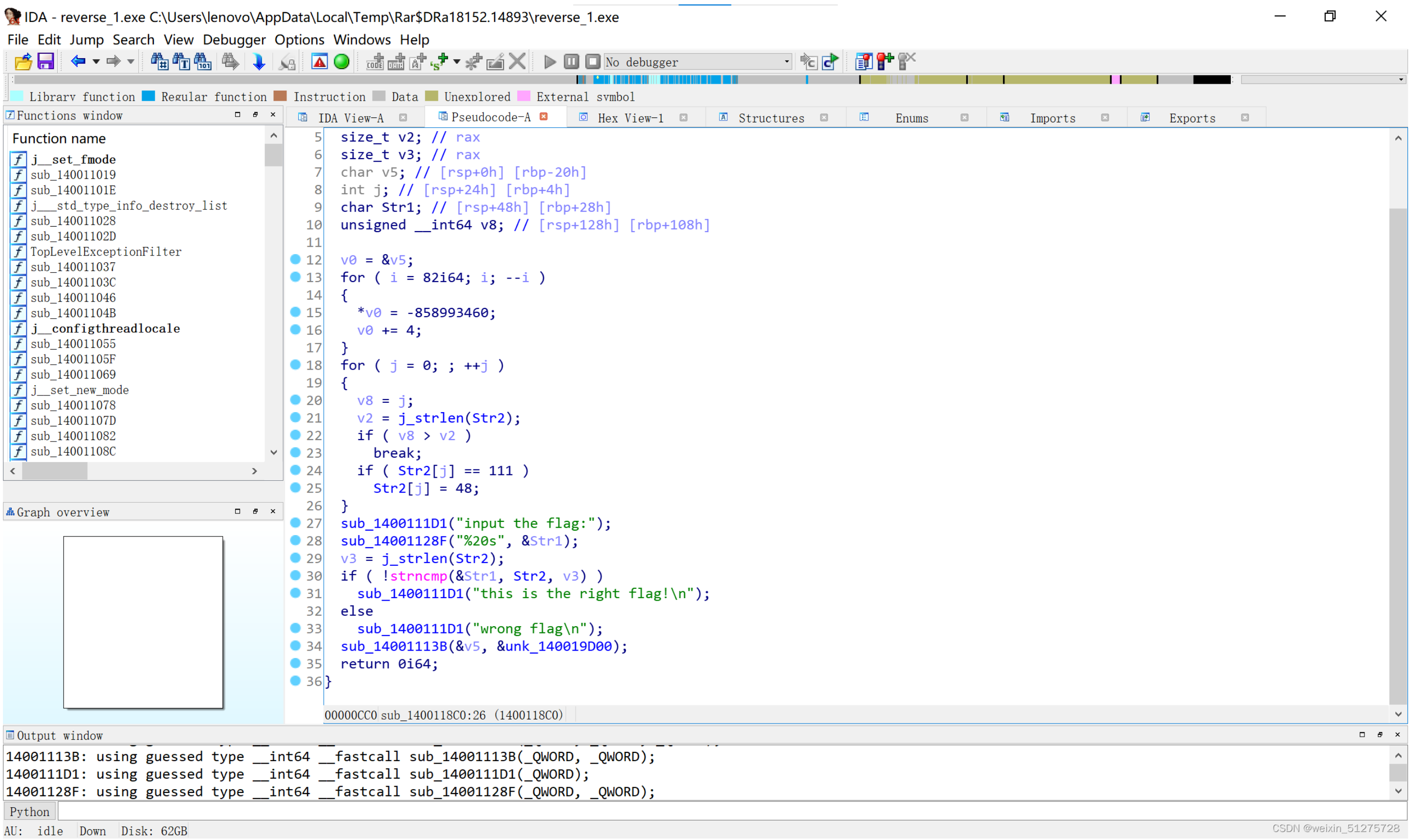
```
100.00% (-136,143) (1769,515) 00000AF0 00000000004014F0: main (Synchronized with Hex View-1)
```

```
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle   Down   Disk: 62GB
```

## 2 Reverse1

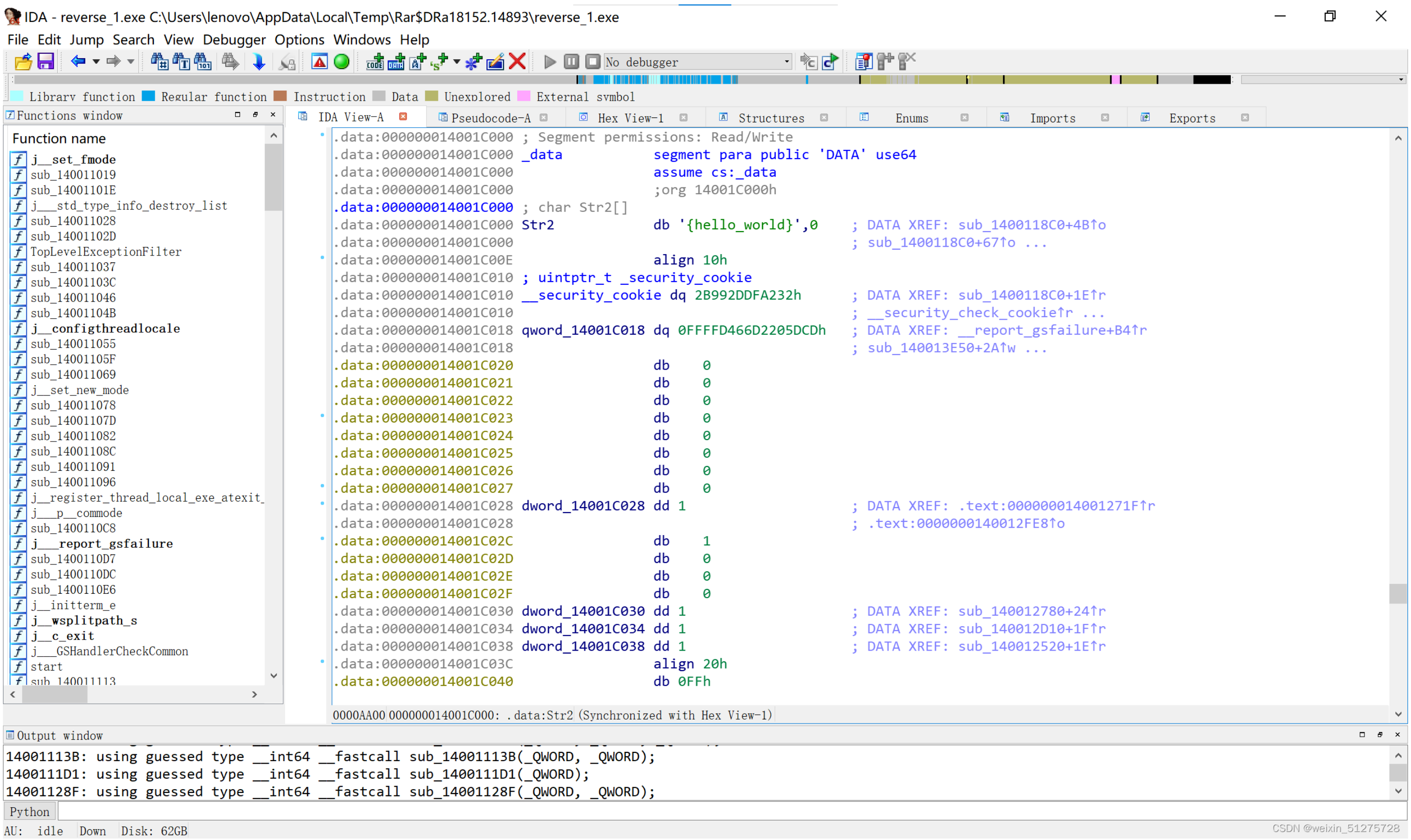
## 2、Reverse1明码



```
  size_t v2; // rax
  size_t v3; // rax
  char v5; // [rsp+0h] [rbp-20h]
  int j; // [rsp+24h] [rbp+4h]
  char Str1; // [rsp+48h] [rbp+28h]
  unsigned __int64 v8; // [rsp+128h] [rbp+108h]

  v0 = &v5;
  for ( i = 82i64; i; --i )
  {
    *v0 = -858993460;
    v0 += 4;
  }
  for ( j = 0; ; ++j )
  {
    v8 = j;
    v2 = j_strlen(Str2);
    if ( v8 > v2 )
      break;
    if ( Str2[j] == 111 )
      Str2[j] = 48;
  }
  sub_1400111D1("input the flag:");
  sub_14001128F("%20s", &Str1);
  v3 = j_strlen(Str2);
  if ( !strncmp(&Str1, Str2, v3) )
    sub_1400111D1("this is the right flag!\n");
  else
    sub_1400111D1("wrong flag\n");
  sub_14001113B(&v5, &unk_140019D00);
  return 0i64;
}
```

```
00000CC0 sub_1400118C0:26 (1400118C0)
```

```
14001113B: using guessed type __int64 __fastcall sub_14001113B(_QWORD, _QWORD);
1400111D1: using guessed type __int64 __fastcall sub_1400111D1(_QWORD);
14001128F: using guessed type __int64 __fastcall sub_14001128F(_QWORD, _QWORD);
```



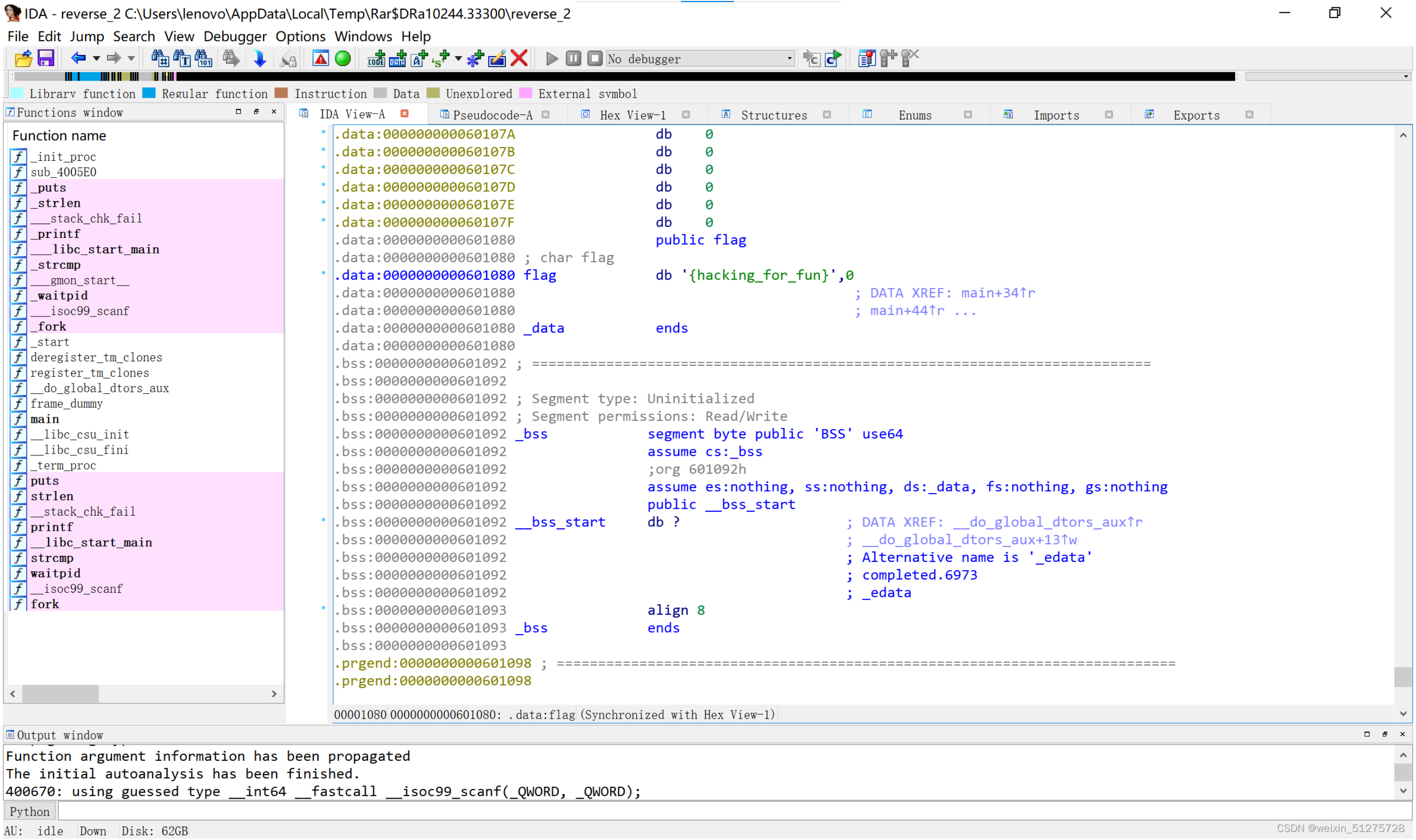
```
.data:000000014001C000 ; Segment permissions: Read/Write
.data:000000014001C000 _data           segment para public 'DATA' use64
.data:000000014001C000                 assume cs:_data
.data:000000014001C000                 ;org 14001C000h
.data:000000014001C000 ; char Str2[]
.data:000000014001C000 Str2            db '{hello_world}',0    ; DATA XREF: sub_1400118C0+4B↑o
.data:000000014001C000                                         ; sub_1400118C0+67↑o ...
.data:000000014001C00E                 align 10h
.data:000000014001C010 ; uintptr_t _security_cookie
.data:000000014001C010 __security_cookie dq 2B992DDFA232h      ; DATA XREF: sub_1400118C0+1E↑r
.data:000000014001C010                                         ; __security_check_cookie↑r ...
.data:000000014001C018 qword_14001C018 dq 0FFFFD466D2205DCDh   ; DATA XREF: __report_gsfailure+B4↑r
.data:000000014001C018                                         ; sub_140013E50+2A↑w ...
.data:000000014001C020                 db    0
.data:000000014001C021                 db    0
.data:000000014001C022                 db    0
.data:000000014001C023                 db    0
.data:000000014001C024                 db    0
.data:000000014001C025                 db    0
.data:000000014001C026                 db    0
.data:000000014001C027                 db    0
.data:000000014001C028 dword_14001C028 dd 1                    ; DATA XREF: .text:000000014001271F↑r
.data:000000014001C028                                         ; .text:0000000140012FE8↑o
.data:000000014001C02C                 db    1
.data:000000014001C02D                 db    0
.data:000000014001C02E                 db    0
.data:000000014001C02F                 db    0
.data:000000014001C030 dword_14001C030 dd 1                    ; DATA XREF: sub_140012780+24↑r
.data:000000014001C034 dword_14001C034 dd 1                    ; DATA XREF: sub_140012D10+1F↑r
.data:000000014001C038 dword_14001C038 dd 1                    ; DATA XREF: sub_140012520+1E↑r
.data:000000014001C03C                 align 20h
.data:000000014001C040                 db 0FFh
```

```
0000AA00 000000014001C000: .data:Str2 (Synchronized with Hex View-1)
```

```
14001113B: using guessed type __int64 __fastcall sub_14001113B(_QWORD, _QWORD);
1400111D1: using guessed type __int64 __fastcall sub_1400111D1(_QWORD);
14001128F: using guessed type __int64 __fastcall sub_14001128F(_QWORD, _QWORD);
```

## 3 Reverse2

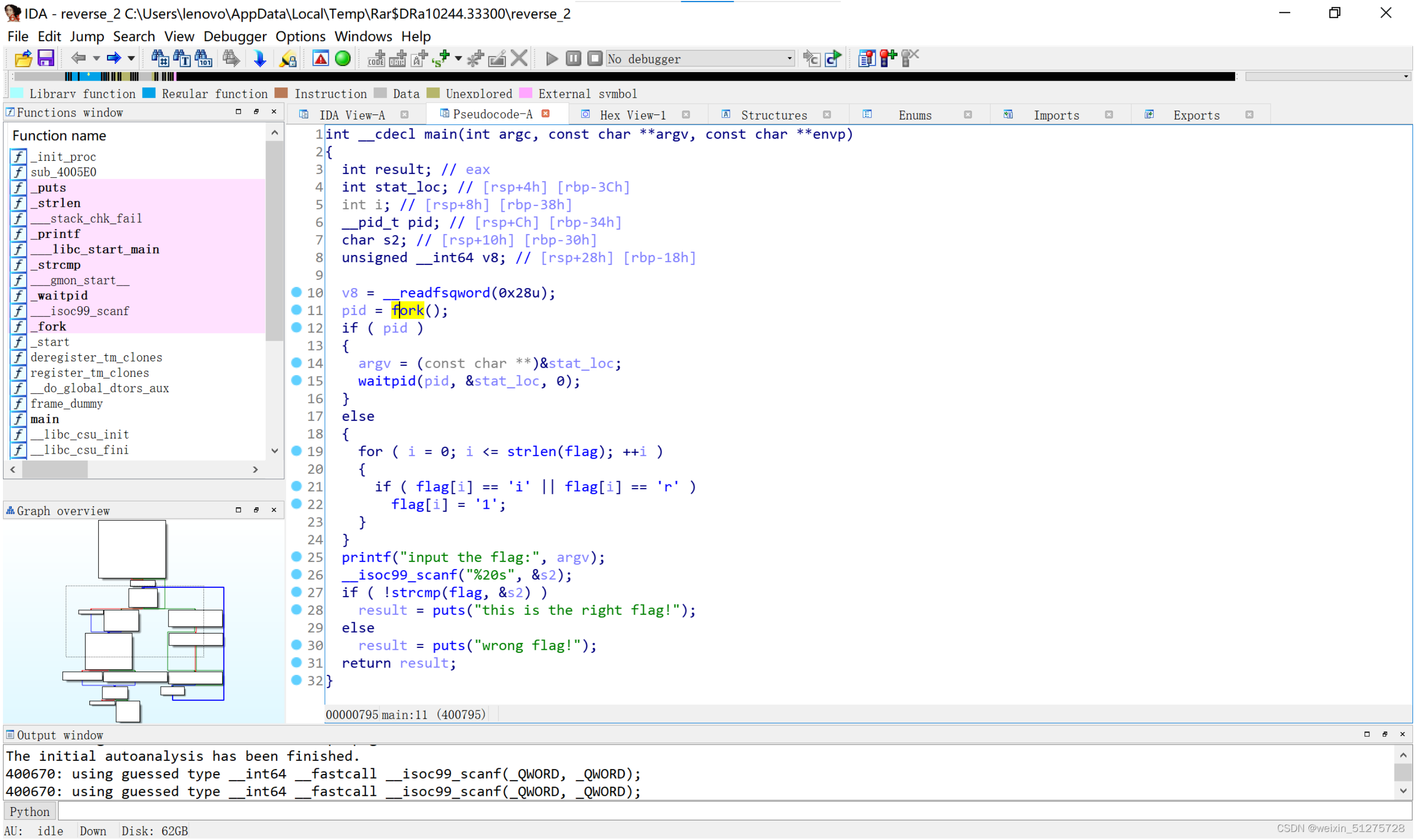
## 3、Reverse2 几乎明码


IDA - reverse_2 C:\Users\lenovo\AppData\Local\Temp\Rar$DRa10244.33300\reverse_2
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
Output window
Python
AU: idle Down Disk: 62GB

```
Function name
_init_proc
sub_4005E0
_puts
_strlen
___stack_chk_fail
_printf
___libc_start_main
_strcmp
__gmon_start__
_waitpid
___isoc99_scanf
_fork
_start
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
frame_dummy
main
__libc_csu_init
__libc_csu_fini
_term_proc
puts
strlen
__stack_chk_fail
printf
__libc_start_main
strcmp
waitpid
__isoc99_scanf
fork
```

```
.data:000000000060107A                 db    0
.data:000000000060107B                 db    0
.data:000000000060107C                 db    0
.data:000000000060107D                 db    0
.data:000000000060107E                 db    0
.data:000000000060107F                 db    0
.data:0000000000601080                 public flag
.data:0000000000601080 ; char flag
.data:0000000000601080 flag            db '{hacking_for_fun}',0
.data:0000000000601080                                         ; DATA XREF: main+34↑r
.data:0000000000601080                                         ; main+44↑r ...
.data:0000000000601080 _data           ends
.data:0000000000601080
.bss:0000000000601092 ; ===========================================================================
.bss:0000000000601092
.bss:0000000000601092 ; Segment type: Uninitialized
.bss:0000000000601092 ; Segment permissions: Read/Write
.bss:0000000000601092 _bss            segment byte public 'BSS' use64
.bss:0000000000601092                 assume cs:_bss
.bss:0000000000601092                 ;org 601092h
.bss:0000000000601092                 assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.bss:0000000000601092                 public __bss_start
.bss:0000000000601092 __bss_start     db ?                    ; DATA XREF: __do_global_dtors_aux↑r
.bss:0000000000601092                                         ; __do_global_dtors_aux+13↑w
.bss:0000000000601092                                         ; Alternative name is '_edata'
.bss:0000000000601092                                         ; completed.6973
.bss:0000000000601092                                         ; _edata
.bss:0000000000601093                 align 8
.bss:0000000000601093 _bss            ends
.bss:0000000000601093
.prgend:0000000000601098 ; ===========================================================================
.prgend:0000000000601098
00001080 0000000000601080: .data:flag (Synchronized with Hex View-1)
```

```
Function argument information has been propagated
The initial autoanalysis has been finished.
400670: using guessed type __int64 __fastcall __isoc99_scanf(_QWORD, _QWORD);
```


IDA - reverse_2 C:\Users\lenovo\AppData\Local\Temp\Rar$DRa10244.33300\reverse_2
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
Graph overview
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
Output window
Python
AU: idle Down Disk: 62GB

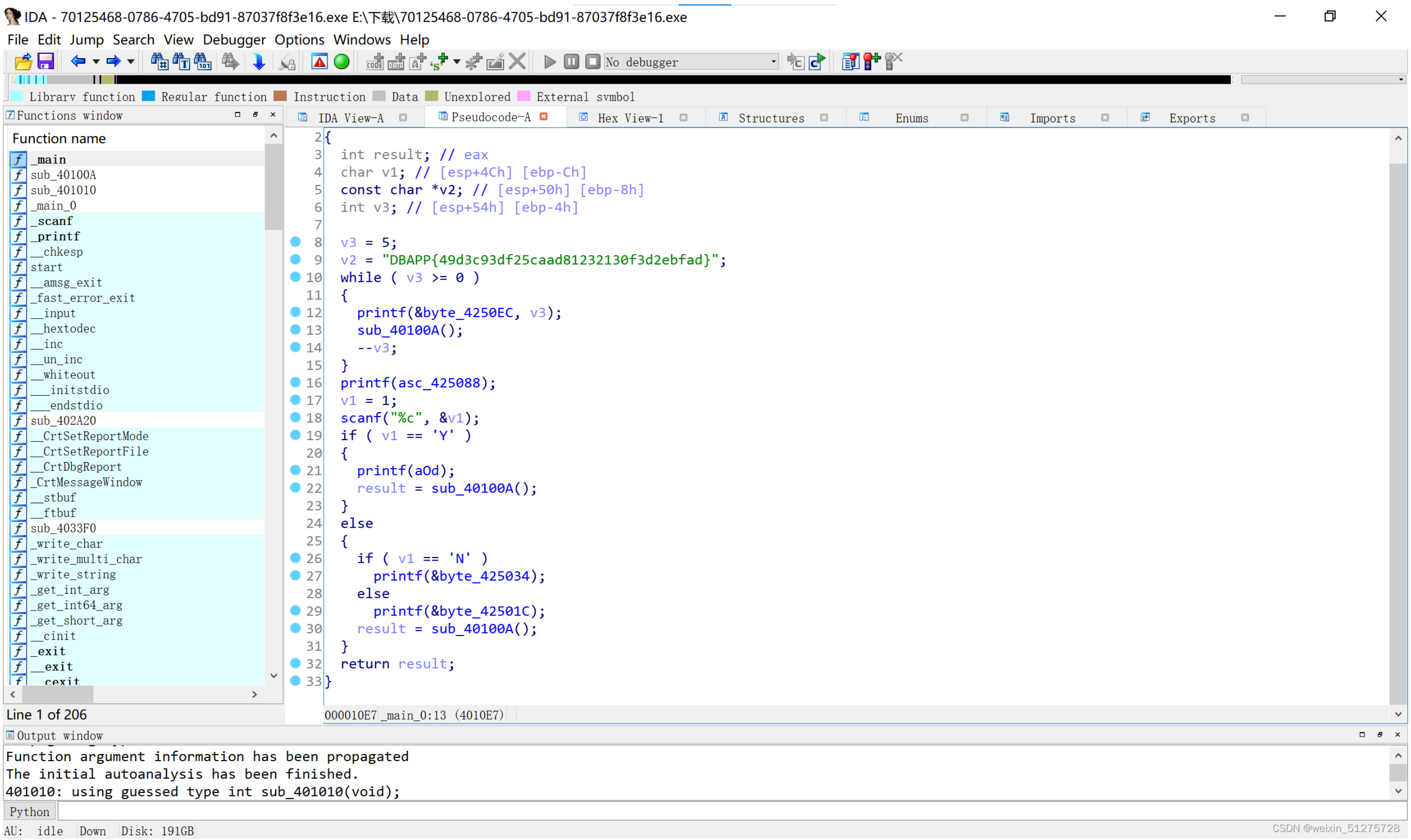
```
Function name
_init_proc
sub_4005E0
_puts
_strlen
___stack_chk_fail
_printf
___libc_start_main
_strcmp
__gmon_start__
_waitpid
___isoc99_scanf
_fork
_start
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
frame_dummy
main
__libc_csu_init
__libc_csu_fini
```

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int result; // eax
  int stat_loc; // [rsp+4h] [rbp-3Ch]
  int i; // [rsp+8h] [rbp-38h]
  __pid_t pid; // [rsp+Ch] [rbp-34h]
  char s2; // [rsp+10h] [rbp-30h]
  unsigned __int64 v8; // [rsp+28h] [rbp-18h]

  v8 = __readfsqword(0x28u);
  pid = fork();
  if ( pid )
  {
    argv = (const char **)&stat_loc;
    waitpid(pid, &stat_loc, 0);
  }
  else
  {
    for ( i = 0; i <= strlen(flag); ++i )
    {
      if ( flag[i] == 'i' || flag[i] == 'r' )
        flag[i] = '1';
    }
  }
  printf("input the flag:", argv);
  __isoc99_scanf("%20s", &s2);
  if ( !strcmp(flag, &s2) )
    result = puts("this is the right flag!");
  else
    result = puts("wrong flag!");
  return result;
}
00000795 main:11 (400795)
```

```
The initial autoanalysis has been finished.
400670: using guessed type __int64 __fastcall __isoc99_scanf(_QWORD, _QWORD);
400670: using guessed type __int64 __fastcall __isoc99_scanf(_QWORD, _QWORD);
```

## 4 内涵的软件

4、内涵的软件 明码

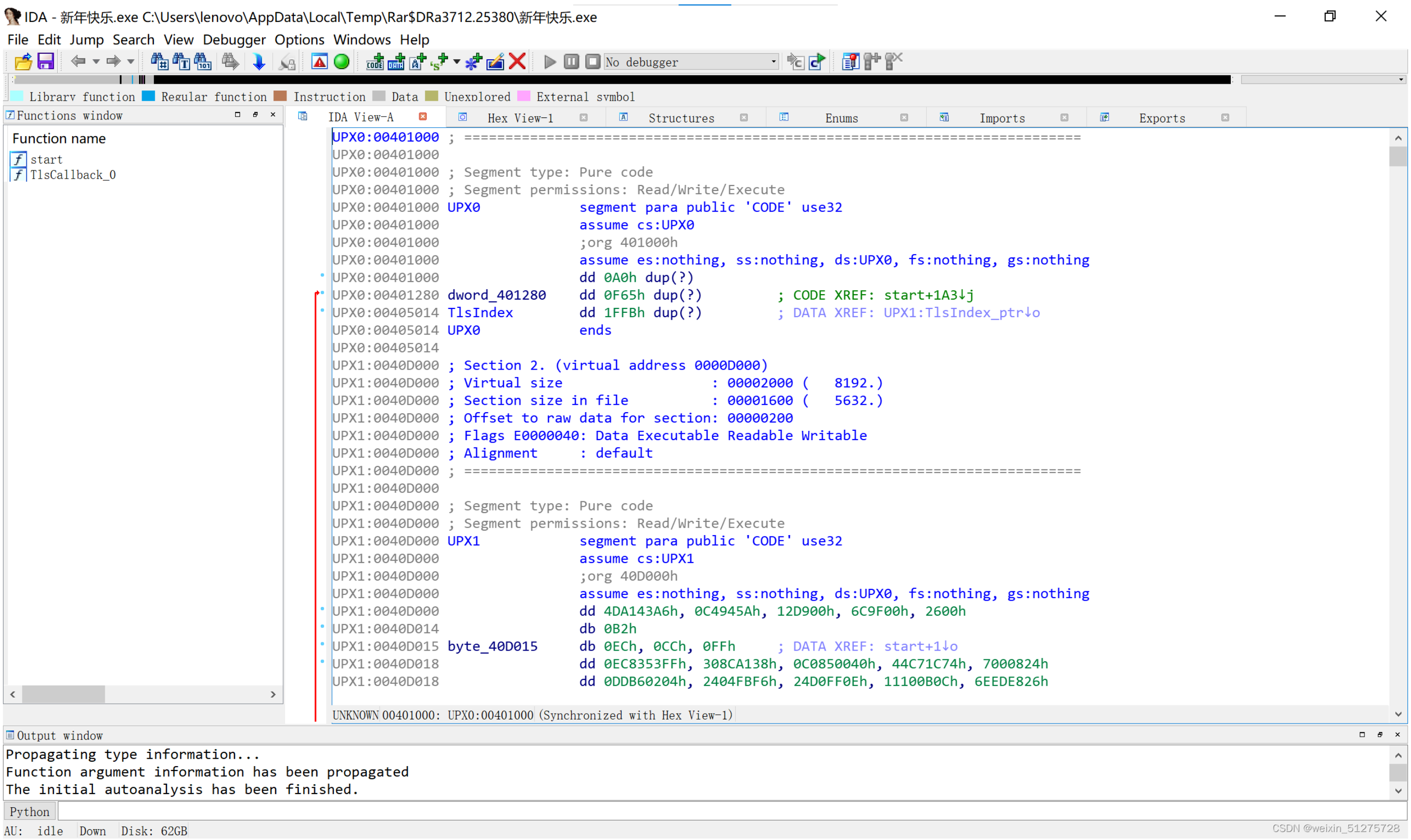


```
{
  int result; // eax
  char v1; // [esp+4Ch] [ebp-Ch]
  const char *v2; // [esp+50h] [ebp-8h]
  int v3; // [esp+54h] [ebp-4h]

  v3 = 5;
  v2 = "DBAPP{49d3c93df25caad81232130f3d2ebfad}";
  while ( v3 >= 0 )
  {
    printf(&byte_4250EC, v3);
    sub_40100A();
    --v3;
  }
  printf(asc_425088);
  v1 = 1;
  scanf("%c", &v1);
  if ( v1 == 'Y' )
  {
    printf(aOd);
    result = sub_40100A();
  }
  else
  {
    if ( v1 == 'N' )
      printf(&byte_425034);
    else
      printf(&byte_42501C);
    result = sub_40100A();
  }
  return result;
}
```

```
Function argument information has been propagated
The initial autoanalysis has been finished.
401010: using guessed type int sub_401010(void);
```

## 5 新年快乐

## 5、新年快乐 有壳先脱壳,之后是明码



IDA - 新年快乐.exe C:\Users\lenovo\AppData\Local\Temp\Rar$DRa3712.25380\新年快乐.exe

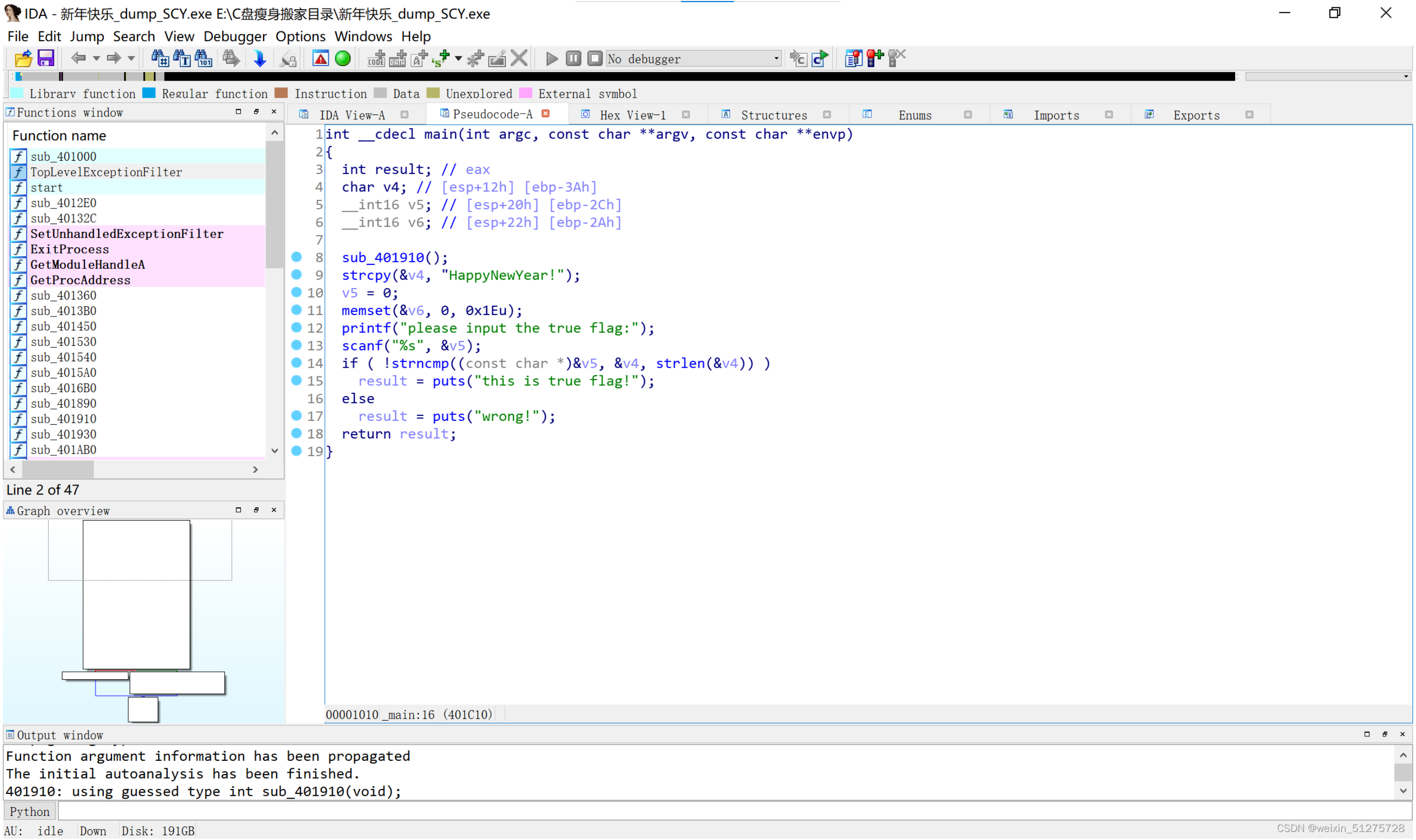
Function name
start
TlsCallback_0

```
UPX0:00401000 ; ===========================================================================
UPX0:00401000
UPX0:00401000 ; Segment type: Pure code
UPX0:00401000 ; Segment permissions: Read/Write/Execute
UPX0:00401000 UPX0            segment para public 'CODE' use32
UPX0:00401000                 assume cs:UPX0
UPX0:00401000                 ;org 401000h
UPX0:00401000                 assume es:nothing, ss:nothing, ds:UPX0, fs:nothing, gs:nothing
UPX0:00401000                 dd 0A0h dup(?)
UPX0:00401280 dword_401280    dd 0F65h dup(?)         ; CODE XREF: start+1A3↓j
UPX0:00405014 TlsIndex        dd 1FFBh dup(?)         ; DATA XREF: UPX1:TlsIndex_ptr↓o
UPX0:00405014 UPX0            ends
UPX0:00405014
UPX1:0040D000 ; Section 2. (virtual address 0000D000)
UPX1:0040D000 ; Virtual size                  : 00002000 (   8192.)
UPX1:0040D000 ; Section size in file          : 00001600 (   5632.)
UPX1:0040D000 ; Offset to raw data for section: 00000200
UPX1:0040D000 ; Flags E0000040: Data Executable Readable Writable
UPX1:0040D000 ; Alignment     : default
UPX1:0040D000 ; ===========================================================================
UPX1:0040D000
UPX1:0040D000 ; Segment type: Pure code
UPX1:0040D000 ; Segment permissions: Read/Write/Execute
UPX1:0040D000 UPX1            segment para public 'CODE' use32
UPX1:0040D000                 assume cs:UPX1
UPX1:0040D000                 ;org 40D000h
UPX1:0040D000                 assume es:nothing, ss:nothing, ds:UPX0, fs:nothing, gs:nothing
UPX1:0040D000                 dd 4DA143A6h, 0C4945Ah, 12D900h, 6C9F00h, 2600h
UPX1:0040D014                 db 0B2h
UPX1:0040D015 byte_40D015     db 0ECh, 0CCh, 0FFh     ; DATA XREF: start+1↓o
UPX1:0040D018                 dd 0EC8353FFh, 308CA138h, 0C0850040h, 44C71C74h, 7000824h
UPX1:0040D018                 dd 0DDB60204h, 2404FBF6h, 24D0FF0Eh, 11100B0Ch, 6EEDE826h
```

UNKNOWN 00401000: UPX0:00401000 (Synchronized with Hex View-1)

```
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 62GB



IDA - 新年快乐_dump_SCY.exe E:\C盘瘦身搬家目录\新年快乐_dump_SCY.exe

Function name
sub_401000
TopLevelExceptionFilter
start
sub_4012E0
sub_40132C
SetUnhandledExceptionFilter
ExitProcess
GetModuleHandleA
GetProcAddress
sub_401360
sub_4013B0
sub_401450
sub_401530
sub_401540
sub_4015A0
sub_4016B0
sub_401890
sub_401910
sub_401930
sub_401AB0

Line 2 of 47

```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int result; // eax
  char v4; // [esp+12h] [ebp-3Ah]
  __int16 v5; // [esp+20h] [ebp-2Ch]
  __int16 v6; // [esp+22h] [ebp-2Ah]

  sub_401910();
  strcpy(&v4, "HappyNewYear!");
  v5 = 0;
  memset(&v6, 0, 0x1Eu);
  printf("please input the true flag:");
  scanf("%s", &v5);
  if ( !strncmp((const char *)&v5, &v4, strlen(&v4)) )
    result = puts("this is true flag!");
  else
    result = puts("wrong!");
  return result;
}
```

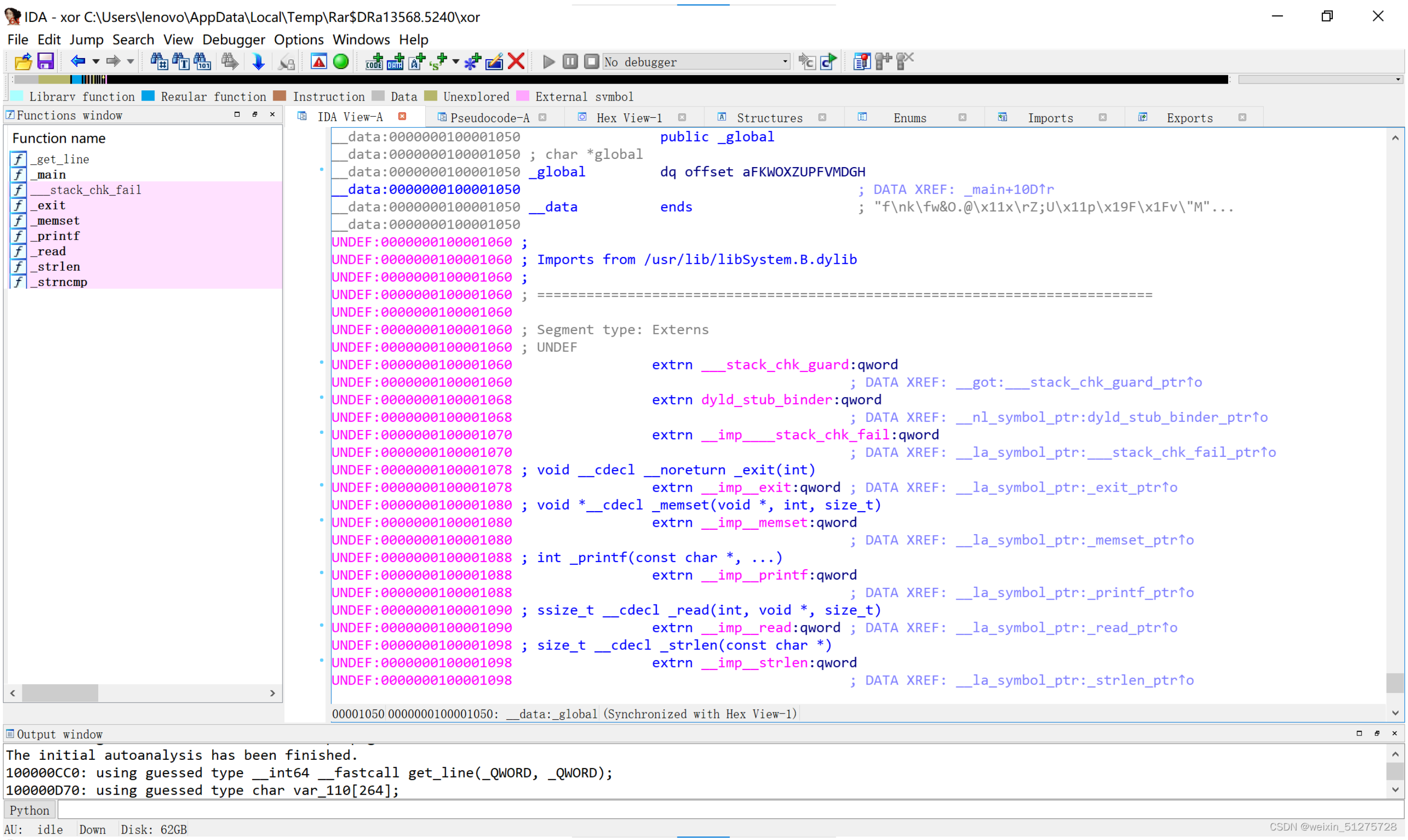
00001010 _main:16 (401C10)

```
Function argument information has been propagated
The initial autoanalysis has been finished.
401910: using guessed type int sub_401910(void);
```

AU: idle Down Disk: 191GB

## 6 Xor

## 6、Xor 就是简单的异或



IDA - xor C:\Users\lenovo\AppData\Local\Temp\Rar$DRa13568.5240\xor

Function name
- _get_line
- _main
- ___stack_chk_fail
- _exit
- _memset
- _printf
- _read
- _strlen
- _strncmp

```
__data:0000000100001050                 public _global
__data:0000000100001050 ; char *global
__data:0000000100001050 _global         dq offset aFKWOXZUPFVMDGH
__data:0000000100001050                                         ; DATA XREF: _main+10D↑r
__data:0000000100001050 __data          ends                    ; "f\nk\fw&O.@\x11x\rZ;U\x11p\x19F\x1Fv\"M"...
__data:0000000100001050
UNDEF:0000000100001060 ;
UNDEF:0000000100001060 ; Imports from /usr/lib/libSystem.B.dylib
UNDEF:0000000100001060 ;
UNDEF:0000000100001060 ; ===========================================================================
UNDEF:0000000100001060
UNDEF:0000000100001060 ; Segment type: Externs
UNDEF:0000000100001060 ; UNDEF
UNDEF:0000000100001060                 extrn ___stack_chk_guard:qword
UNDEF:0000000100001060                                         ; DATA XREF: __got:___stack_chk_guard_ptr↑o
UNDEF:0000000100001068                 extrn dyld_stub_binder:qword
UNDEF:0000000100001068                                         ; DATA XREF: __nl_symbol_ptr:dyld_stub_binder_ptr↑o
UNDEF:0000000100001070                 extrn __imp____stack_chk_fail:qword
UNDEF:0000000100001070                                         ; DATA XREF: __la_symbol_ptr:___stack_chk_fail_ptr↑o
UNDEF:0000000100001078 ; void __cdecl __noreturn _exit(int)
UNDEF:0000000100001078                 extrn __imp__exit:qword ; DATA XREF: __la_symbol_ptr:_exit_ptr↑o
UNDEF:0000000100001080 ; void *__cdecl _memset(void *, int, size_t)
UNDEF:0000000100001080                 extrn __imp__memset:qword
UNDEF:0000000100001080                                         ; DATA XREF: __la_symbol_ptr:_memset_ptr↑o
UNDEF:0000000100001088 ; int _printf(const char *, ...)
UNDEF:0000000100001088                 extrn __imp__printf:qword
UNDEF:0000000100001088                                         ; DATA XREF: __la_symbol_ptr:_printf_ptr↑o
UNDEF:0000000100001090 ; ssize_t __cdecl _read(int, void *, size_t)
UNDEF:0000000100001090                 extrn __imp__read:qword ; DATA XREF: __la_symbol_ptr:_read_ptr↑o
UNDEF:0000000100001098 ; size_t __cdecl _strlen(const char *)
UNDEF:0000000100001098                 extrn __imp__strlen:qword
UNDEF:0000000100001098                                         ; DATA XREF: __la_symbol_ptr:_strlen_ptr↑o
```

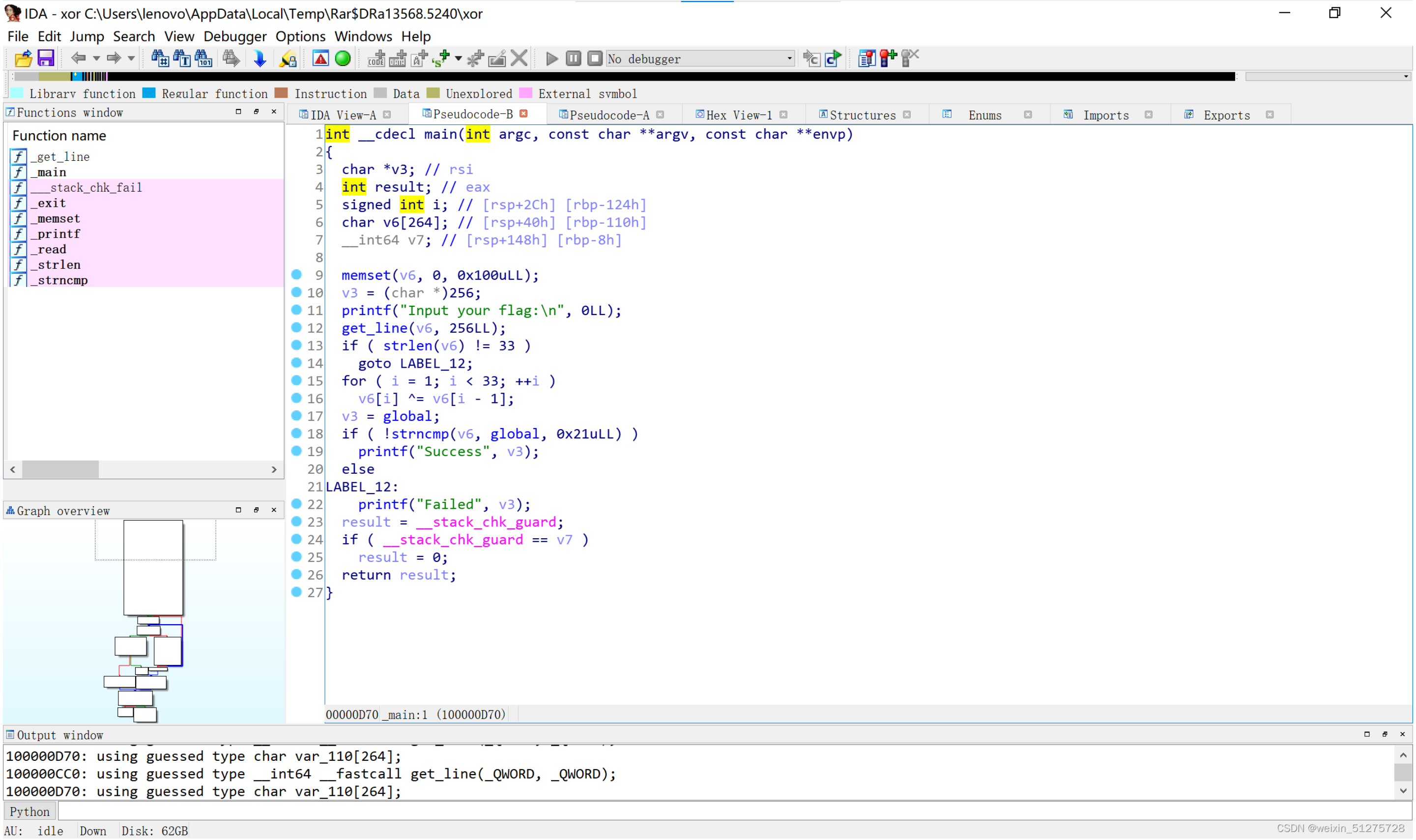
00001050 0000000100001050: __data:_global (Synchronized with Hex View-1)

Output window

```
The initial autoanalysis has been finished.
100000CC0: using guessed type __int64 __fastcall get_line(_QWORD, _QWORD);
100000D70: using guessed type char var_110[264];
```

AU: idle Down Disk: 62GB

CSDN @weixin_51275728



IDA - xor C:\Users\lenovo\AppData\Local\Temp\Rar$DRa13568.5240\xor

Function name
- _get_line
- _main
- ___stack_chk_fail
- _exit
- _memset
- _printf
- _read
- _strlen
- _strncmp

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *v3; // rsi
  int result; // eax
  signed int i; // [rsp+2Ch] [rbp-124h]
  char v6[264]; // [rsp+40h] [rbp-110h]
  __int64 v7; // [rsp+148h] [rbp-8h]

  memset(v6, 0, 0x100uLL);
  v3 = (char *)256;
  printf("Input your flag:\n", 0LL);
  get_line(v6, 256LL);
  if ( strlen(v6) != 33 )
    goto LABEL_12;
  for ( i = 1; i < 33; ++i )
    v6[i] ^= v6[i - 1];
  v3 = global;
  if ( !strncmp(v6, global, 0x21uLL) )
    printf("Success", v3);
  else
LABEL_12:
    printf("Failed", v3);
  result = __stack_chk_guard;
  if ( __stack_chk_guard == v7 )
    result = 0;
  return result;
}
```

00000D70 _main:1 (100000D70)

Output window

```
100000D70: using guessed type char var_110[264];
100000CC0: using guessed type __int64 __fastcall get_line(_QWORD, _QWORD);
100000D70: using guessed type char var_110[264];
```

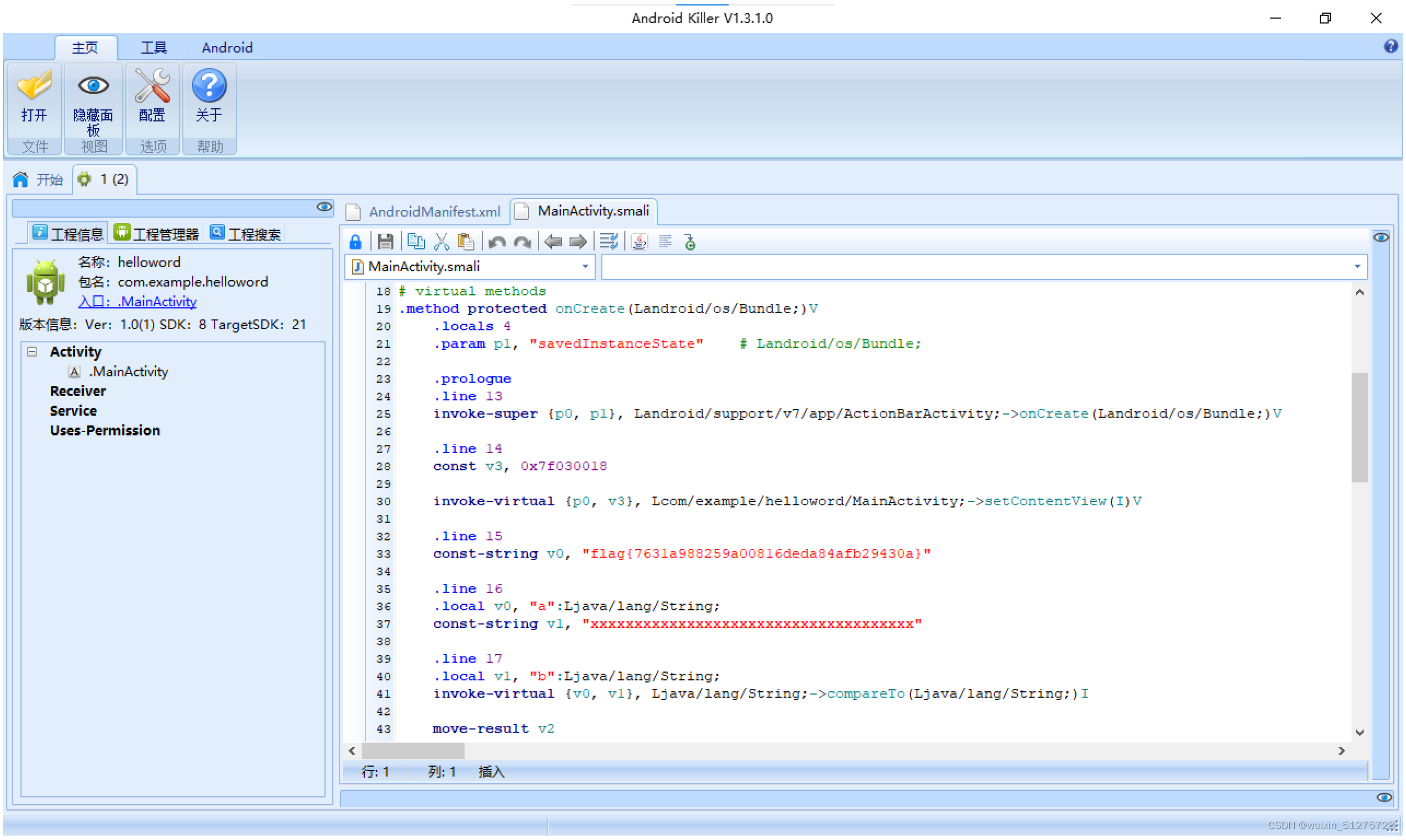
AU: idle Down Disk: 62GB

CSDN @weixin_51275728

```
#include < iostream>
using namespace std;
int main(){
char miwen[34] =
{
  0x66, 0x0A, 0x6B, 0x0C, 0x77, 0x26, 0x4F, 0x2E, 0x40, 0x11,
  0x78, 0x0D, 0x5A, 0x3B, 0x55, 0x11, 0x70, 0x19, 0x46, 0x1F,
  0x76, 0x22, 0x4D, 0x23, 0x44, 0x0E, 0x67, 0x06, 0x68, 0x0F,
  0x47, 0x32, 0x4F, 0x00
};
for(int i=0;i<33;i++)
{char p=miwen[i]^miwen[i+1];
cout<<p;
}}
```

## 7 helloworld

7、helloworld 明码



名称：helloword
包名：com.example.helloword
入口：.MainActivity
版本信息：Ver：1.0(1) SDK：8 TargetSDK：21

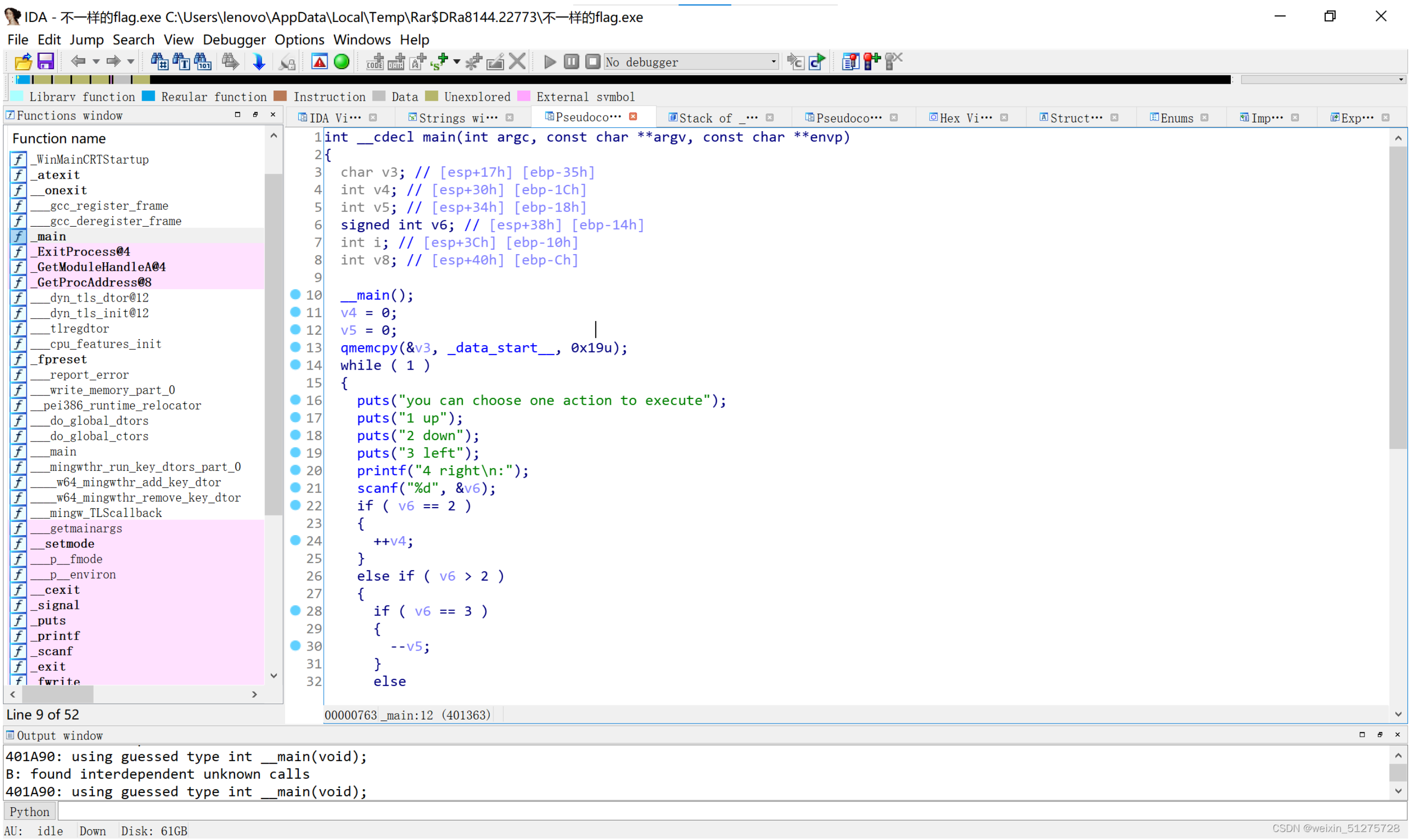
Activity
.MainActivity
Receiver
Service
Uses-Permission

```
# virtual methods
.method protected onCreate(Landroid/os/Bundle;)V
    .locals 4
    .param p1, "savedInstanceState"    # Landroid/os/Bundle;

    .prologue
    .line 13
    invoke-super {p0, p1}, Landroid/support/v7/app/ActionBarActivity;->onCreate(Landroid/os/Bundle;)V

    .line 14
    const v3, 0x7f030018

    invoke-virtual {p0, v3}, Lcom/example/helloword/MainActivity;->setContentView(I)V

    .line 15
    const-string v0, "flag{7631a988259a00816deda84afb29430a}"

    .line 16
    .local v0, "a":Ljava/lang/String;
    const-string v1, "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

    .line 17
    .local v1, "b":Ljava/lang/String;
    invoke-virtual {v0, v1}, Ljava/lang/String;->compareTo(Ljava/lang/String;)I

    move-result v2
```

行: 1　列: 1　插入

## 9 不一样的flag

## 9不一样的flag 迷宫



IDA - 不一样的flag.exe C:\Users\lenovo\AppData\Local\Temp\Rar$DRa8144.22773\不一样的flag.exe

```
_WinMainCRTStartup
_atexit
__onexit
___gcc_register_frame
___gcc_deregister_frame
_main
_ExitProcess@4
_GetModuleHandleA@4
_GetProcAddress@8
___dyn_tls_dtor@12
___dyn_tls_init@12
___tlregdtor
___cpu_features_init
_fpreset
__report_error
___write_memory_part_0
__pei386_runtime_relocator
___do_global_dtors
___do_global_ctors
___main
___mingwthr_run_key_dtors_part_0
____w64_mingwthr_add_key_dtor
____w64_mingwthr_remove_key_dtor
___mingw_TLScallback
___getmainargs
__setmode
___p__fmode
___p__environ
__cexit
_signal
_puts
_printf
_scanf
_exit
_fwrite
```

Line 9 of 52

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char v3; // [esp+17h] [ebp-35h]
  int v4; // [esp+30h] [ebp-1Ch]
  int v5; // [esp+34h] [ebp-18h]
  signed int v6; // [esp+38h] [ebp-14h]
  int i; // [esp+3Ch] [ebp-10h]
  int v8; // [esp+40h] [ebp-Ch]

  __main();
  v4 = 0;
  v5 = 0;
  qmemcpy(&v3, _data_start__, 0x19u);
  while ( 1 )
  {
    puts("you can choose one action to execute");
    puts("1 up");
    puts("2 down");
    puts("3 left");
    printf("4 right\n:");
    scanf("%d", &v6);
    if ( v6 == 2 )
    {
      ++v4;
    }
    else if ( v6 > 2 )
    {
      if ( v6 == 3 )
      {
        --v5;
      }
      else
```

00000763 _main:12 (401363)

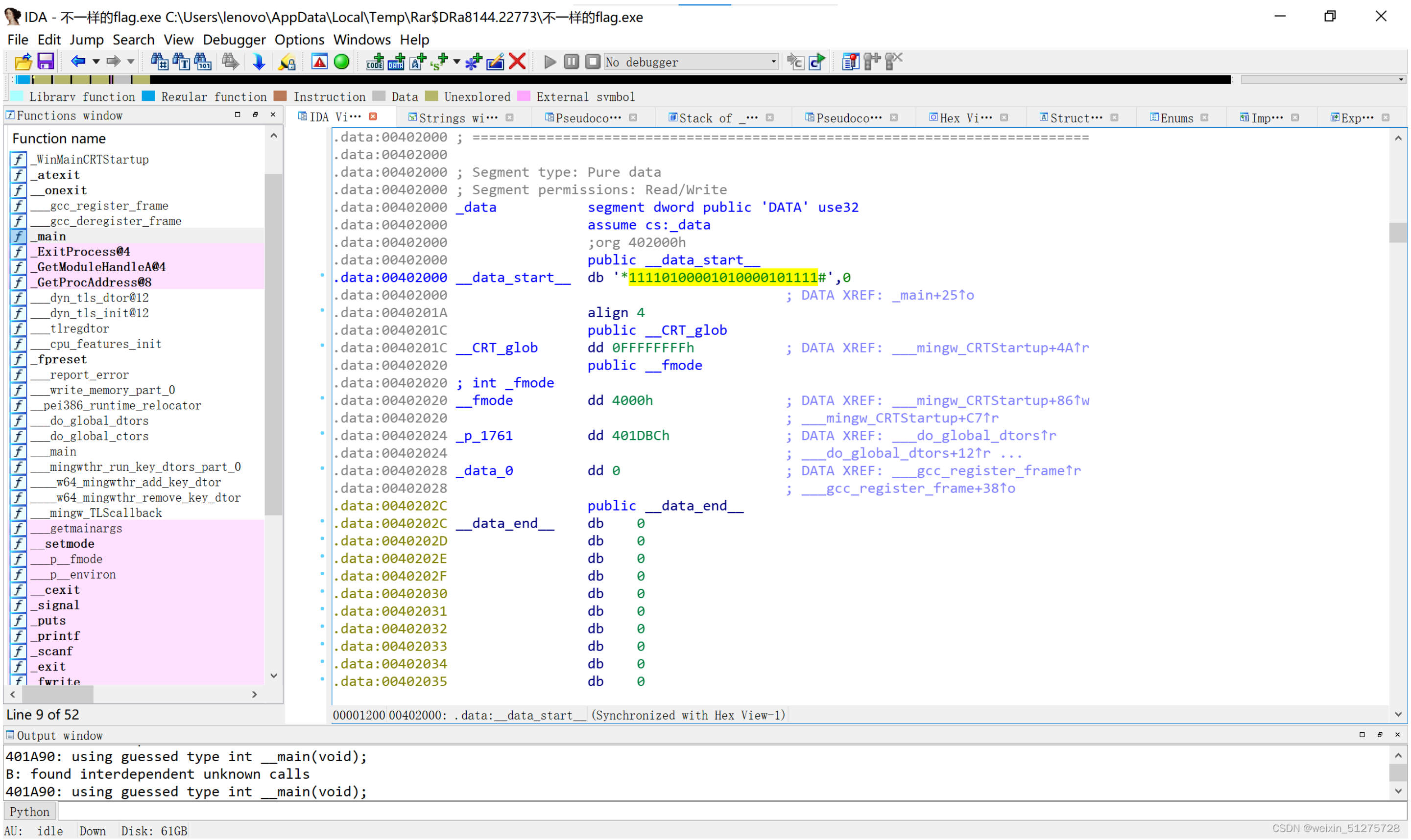
Output window

```
401A90: using guessed type int __main(void);
B: found interdependent unknown calls
401A90: using guessed type int __main(void);
```

Python

AU: idle Down Disk: 61GB

CSDN @weixin_51275728



IDA - 不一样的flag.exe C:\Users\lenovo\AppData\Local\Temp\Rar$DRa8144.22773\不一样的flag.exe

```
_WinMainCRTStartup
_atexit
__onexit
___gcc_register_frame
___gcc_deregister_frame
_main
_ExitProcess@4
_GetModuleHandleA@4
_GetProcAddress@8
___dyn_tls_dtor@12
___dyn_tls_init@12
___tlregdtor
___cpu_features_init
_fpreset
__report_error
___write_memory_part_0
__pei386_runtime_relocator
___do_global_dtors
___do_global_ctors
___main
___mingwthr_run_key_dtors_part_0
____w64_mingwthr_add_key_dtor
____w64_mingwthr_remove_key_dtor
___mingw_TLScallback
___getmainargs
__setmode
___p__fmode
___p__environ
__cexit
_signal
_puts
_printf
_scanf
_exit
_fwrite
```

Line 9 of 52

```
.data:00402000 ; ===========================================================================
.data:00402000
.data:00402000 ; Segment type: Pure data
.data:00402000 ; Segment permissions: Read/Write
.data:00402000 _data           segment dword public 'DATA' use32
.data:00402000                 assume cs:_data
.data:00402000                 ;org 402000h
.data:00402000                 public __data_start__
.data:00402000 __data_start__  db '*11110100001010000101111#',0
.data:00402000                                         ; DATA XREF: _main+25↑o
.data:0040201A                 align 4
.data:0040201C                 public __CRT_glob
.data:0040201C __CRT_glob      dd 0FFFFFFFFh           ; DATA XREF: ___mingw_CRTStartup+4A↑r
.data:00402020                 public __fmode
.data:00402020 ; int _fmode
.data:00402020 __fmode         dd 4000h                ; DATA XREF: ___mingw_CRTStartup+86↑w
.data:00402020                                         ; ___mingw_CRTStartup+C7↑r
.data:00402024 _p_1761         dd 401DBCh              ; DATA XREF: ___do_global_dtors↑r
.data:00402024                                         ; ___do_global_dtors+12↑r ...
.data:00402028 _data_0         dd 0                    ; DATA XREF: ___gcc_register_frame↑r
.data:00402028                                         ; ___gcc_register_frame+38↑o
.data:0040202C                 public __data_end__
.data:0040202C __data_end__    db    0
.data:0040202D                 db    0
.data:0040202E                 db    0
.data:0040202F                 db    0
.data:00402030                 db    0
.data:00402031                 db    0
.data:00402032                 db    0
.data:00402033                 db    0
.data:00402034                 db    0
.data:00402035                 db    0
```

00001200 00402000: .data:__data_start__ (Synchronized with Hex View-1)

Output window

```
401A90: using guessed type int __main(void);
B: found interdependent unknown calls
401A90: using guessed type int __main(void);
```

Python

AU: idle Down Disk: 61GB

CSDN @weixin_51275728

1 上 2 下 3 左 4 右

*1111

01000

01010

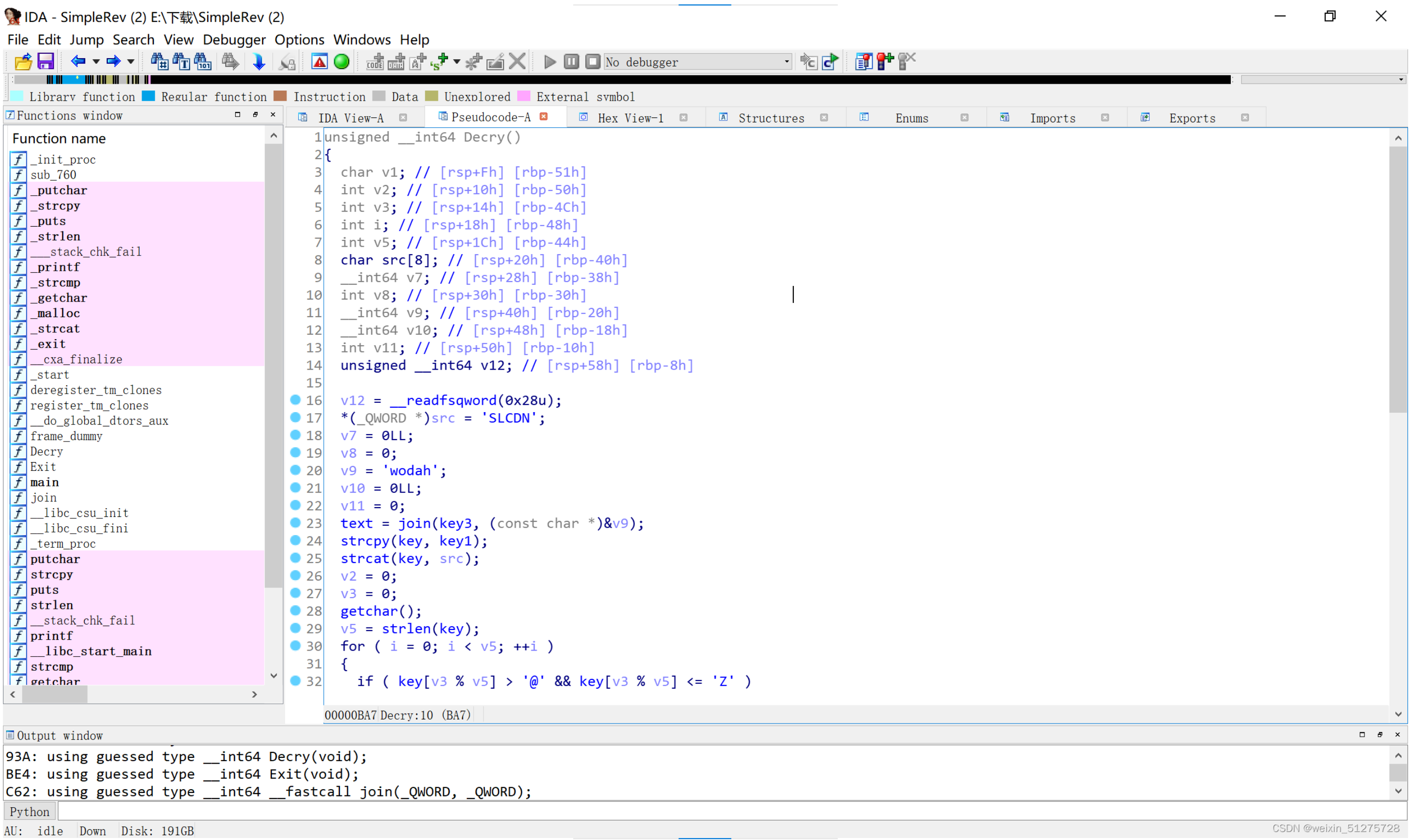
00010

1111#

222441144222

# 10 simplerev

10SimpleRev

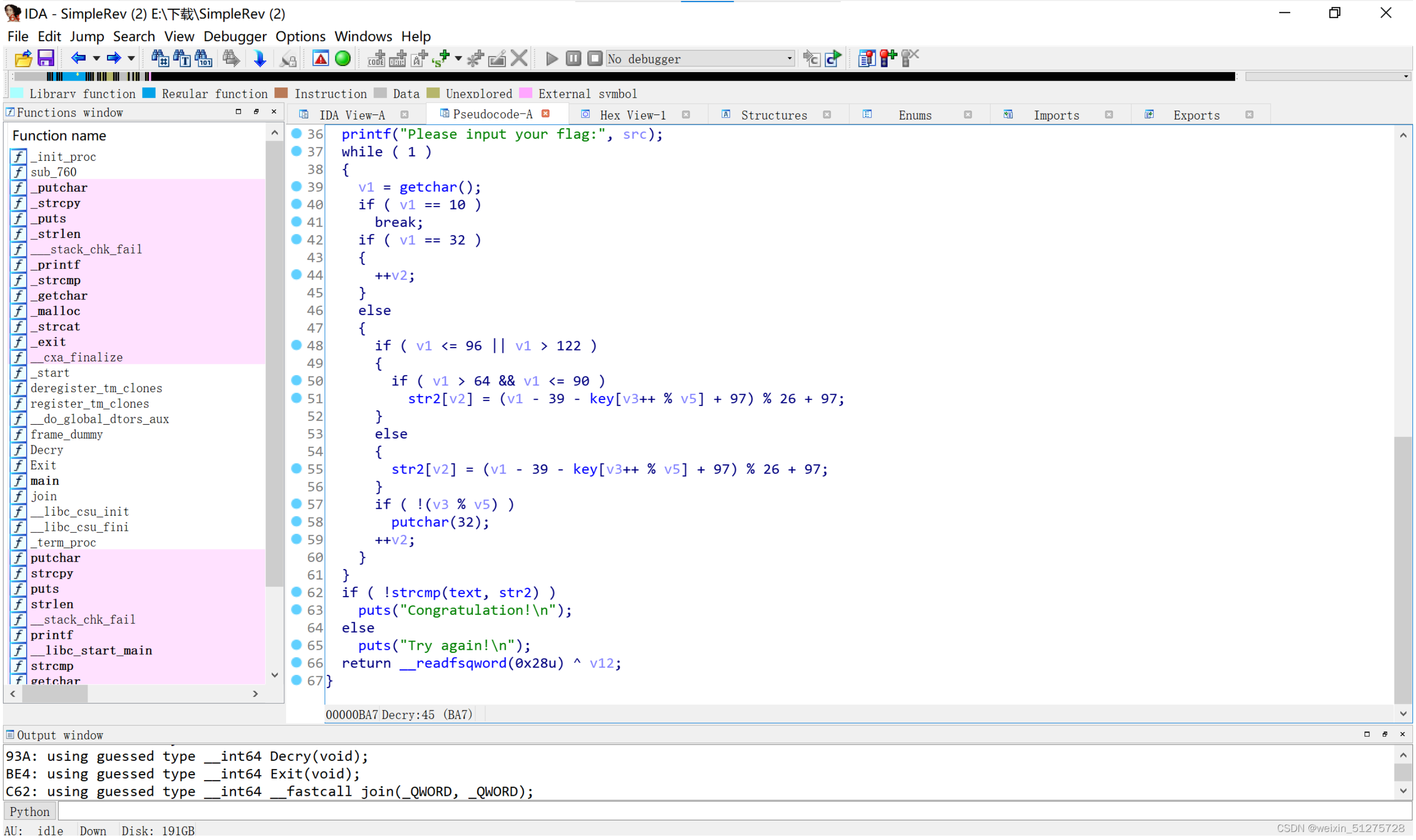


```
unsigned __int64 Decry()
{
  char v1; // [rsp+Fh] [rbp-51h]
  int v2; // [rsp+10h] [rbp-50h]
  int v3; // [rsp+14h] [rbp-4Ch]
  int i; // [rsp+18h] [rbp-48h]
  int v5; // [rsp+1Ch] [rbp-44h]
  char src[8]; // [rsp+20h] [rbp-40h]
  __int64 v7; // [rsp+28h] [rbp-38h]
  int v8; // [rsp+30h] [rbp-30h]
  __int64 v9; // [rsp+40h] [rbp-20h]
  __int64 v10; // [rsp+48h] [rbp-18h]
  int v11; // [rsp+50h] [rbp-10h]
  unsigned __int64 v12; // [rsp+58h] [rbp-8h]

  v12 = __readfsqword(0x28u);
  *(_QWORD *)src = 'SLCDN';
  v7 = 0LL;
  v8 = 0;
  v9 = 'wodah';
  v10 = 0LL;
  v11 = 0;
  text = join(key3, (const char *)&v9);
  strcpy(key, key1);
  strcat(key, src);
  v2 = 0;
  v3 = 0;
  getchar();
  v5 = strlen(key);
  for ( i = 0; i < v5; ++i )
  {
    if ( key[v3 % v5] > '@' && key[v3 % v5] <= 'Z' )
```

```
00000BA7 Decry:10 (BA7)
```

```
93A: using guessed type __int64 Decry(void);
BE4: using guessed type __int64 Exit(void);
C62: using guessed type __int64 __fastcall join(_QWORD, _QWORD);
```

```
AU:  idle   Down   Disk: 191GB
```

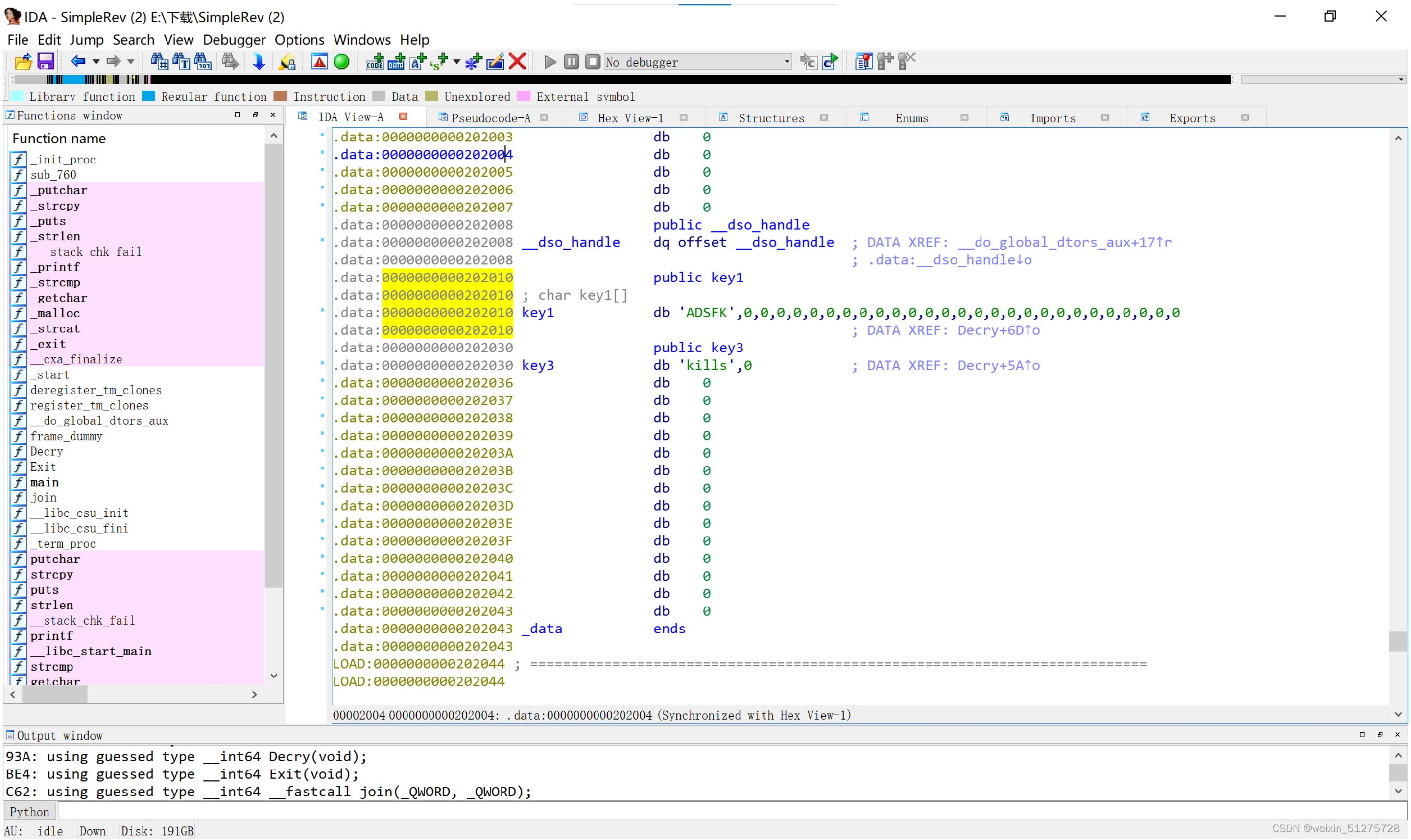


```
  printf("Please input your flag:", src);
  while ( 1 )
  {
    v1 = getchar();
    if ( v1 == 10 )
      break;
    if ( v1 == 32 )
    {
      ++v2;
    }
    else
    {
      if ( v1 <= 96 || v1 > 122 )
      {
        if ( v1 > 64 && v1 <= 90 )
          str2[v2] = (v1 - 39 - key[v3++ % v5] + 97) % 26 + 97;
      }
      else
      {
        str2[v2] = (v1 - 39 - key[v3++ % v5] + 97) % 26 + 97;
      }
      if ( !(v3 % v5) )
        putchar(32);
      ++v2;
    }
  }
  if ( !strcmp(text, str2) )
    puts("Congratulation!\n");
  else
    puts("Try again!\n");
  return __readfsqword(0x28u) ^ v12;
}
```

```
00000BA7 Decry:45 (BA7)
```

```
93A: using guessed type __int64 Decry(void);
BE4: using guessed type __int64 Exit(void);
C62: using guessed type __int64 __fastcall join(_QWORD, _QWORD);
```

```
AU:  idle   Down   Disk: 191GB
```



IDA - SimpleRev (2) E:\下载\SimpleRev (2)
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
Output window
Python
AU: idle Down Disk: 191GB

```
Function name
_init_proc
sub_760
_putchar
_strcpy
_puts
_strlen
___stack_chk_fail
_printf
_strcmp
_getchar
_malloc
_strcat
_exit
__cxa_finalize
_start
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
frame_dummy
Decry
Exit
main
join
__libc_csu_init
__libc_csu_fini
_term_proc
putchar
strcpy
puts
strlen
__stack_chk_fail
printf
__libc_start_main
strcmp
getchar
```

```
.data:0000000000202003                 db    0
.data:0000000000202004                 db    0
.data:0000000000202005                 db    0
.data:0000000000202006                 db    0
.data:0000000000202007                 db    0
.data:0000000000202008                 public __dso_handle
.data:0000000000202008 __dso_handle    dq offset __dso_handle  ; DATA XREF: __do_global_dtors_aux+17↑r
.data:0000000000202008                                         ; .data:__dso_handle↓o
.data:0000000000202010                 public key1
.data:0000000000202010 ; char key1[]
.data:0000000000202010 key1            db 'ADSFK',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
.data:0000000000202010                                         ; DATA XREF: Decry+6D↑o
.data:0000000000202030                 public key3
.data:0000000000202030 key3            db 'kills',0            ; DATA XREF: Decry+5A↑o
.data:0000000000202036                 db    0
.data:0000000000202037                 db    0
.data:0000000000202038                 db    0
.data:0000000000202039                 db    0
.data:000000000020203A                 db    0
.data:000000000020203B                 db    0
.data:000000000020203C                 db    0
.data:000000000020203D                 db    0
.data:000000000020203E                 db    0
.data:000000000020203F                 db    0
.data:0000000000202040                 db    0
.data:0000000000202041                 db    0
.data:0000000000202042                 db    0
.data:0000000000202043                 db    0
.data:0000000000202043 _data           ends
.data:0000000000202043
LOAD:0000000000202044 ; ===========================================================================
LOAD:0000000000202044
00002004 0000000000202004: .data:0000000000202004 (Synchronized with Hex View-1)
```

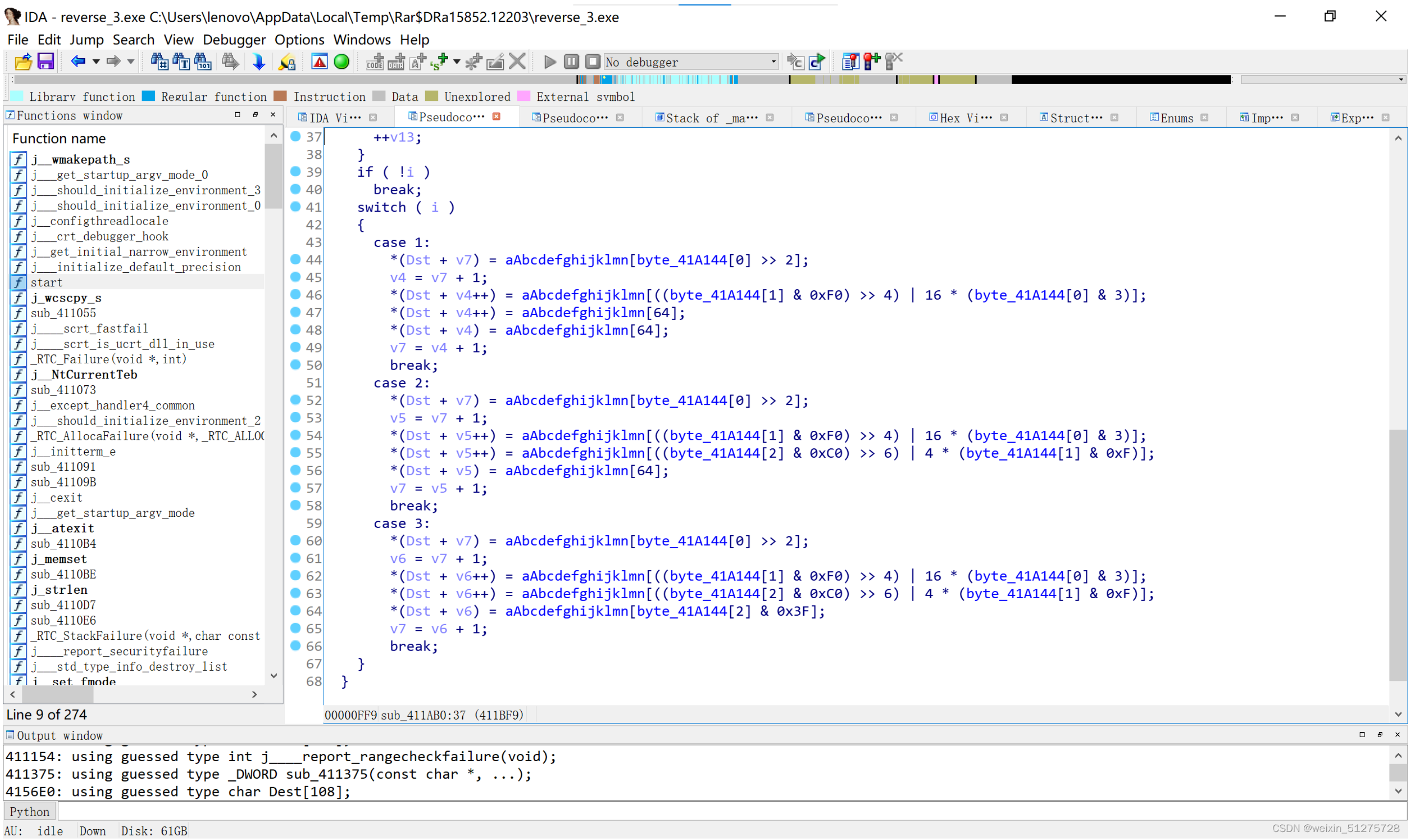
```
93A: using guessed type __int64 Decry(void);
BE4: using guessed type __int64 Exit(void);
C62: using guessed type __int64 __fastcall join(_QWORD, _QWORD);
```

key拼接src ADSFKNDCLS text也是 killshadow(小端) 然后key转小写

```cpp
#include <iostream>
using namespace std;
int main(){
 string p="killshadow";
 string key="adsfkndcls";
 for(int i=0;i<10;i++)
 {for(int j=1;j<128;j++){
  if((j>'a'&&j<'z')||(j>'A'&&j<'Z'))
  {if(p[i]==(j-39-key[i]+97)%26+97)
  {char pp=j;
  cout<<pp;
  break;}}}}
```

# 8 reverse3

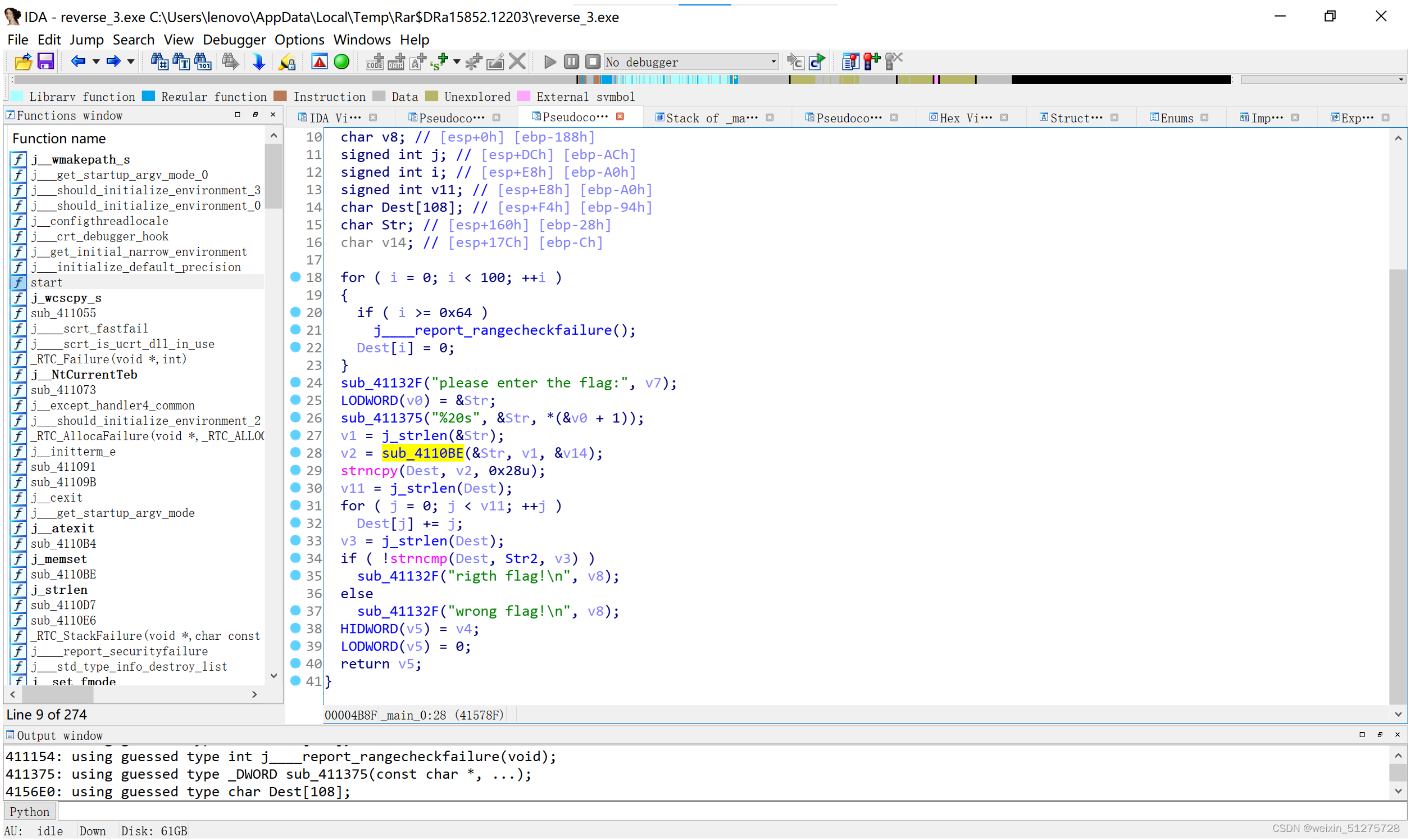
8 reverse3 先base64 再每位数加上自己的位数


IDA - reverse_3.exe C:\Users\lenovo\AppData\Local\Temp\Rar$DRa15852.12203\reverse_3.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function
Regular function
Instruction
Data
Unexplored
External symbol
Functions window
IDA Vi…
Pseudoco…
Pseudoco…
Stack of _ma…
Pseudoco…
Hex Vi…
Struct…
Enums
Imp…
Exp…
Function name
j__wmakepath_s
j___get_startup_argv_mode_0
j___should_initialize_environment_3
j___should_initialize_environment_0
j__configthreadlocale
j___crt_debugger_hook
j___get_initial_narrow_environment
j___initialize_default_precision
start
j_wcscpy_s
sub_411055
j____scrt_fastfail
j____scrt_is_ucrt_dll_in_use
_RTC_Failure(void *,int)
j_NtCurrentTeb
sub_411073
j__except_handler4_common
j___should_initialize_environment_2
_RTC_AllocaFailure(void *,_RTC_ALLO(
j__initterm_e
sub_411091
sub_41109B
j__cexit
j___get_startup_argv_mode
j__atexit
sub_4110B4
j_memset
sub_4110BE
j_strlen
sub_4110D7
sub_4110E6
_RTC_StackFailure(void *,char const
j____report_securityfailure
j___std_type_info_destroy_list
j__set_fmode
Line 9 of 274
Output window
Python
AU: idle Down Disk: 61GB
CSDN @weixin_51275728

```
      ++v13;
    }
    if ( !i )
      break;
    switch ( i )
    {
      case 1:
        *(Dst + v7) = aAbcdefghijklmn[byte_41A144[0] >> 2];
        v4 = v7 + 1;
        *(Dst + v4++) = aAbcdefghijklmn[((byte_41A144[1] & 0xF0) >> 4) | 16 * (byte_41A144[0] & 3)];
        *(Dst + v4++) = aAbcdefghijklmn[64];
        *(Dst + v4) = aAbcdefghijklmn[64];
        v7 = v4 + 1;
        break;
      case 2:
        *(Dst + v7) = aAbcdefghijklmn[byte_41A144[0] >> 2];
        v5 = v7 + 1;
        *(Dst + v5++) = aAbcdefghijklmn[((byte_41A144[1] & 0xF0) >> 4) | 16 * (byte_41A144[0] & 3)];
        *(Dst + v5++) = aAbcdefghijklmn[((byte_41A144[2] & 0xC0) >> 6) | 4 * (byte_41A144[1] & 0xF)];
        *(Dst + v5) = aAbcdefghijklmn[64];
        v7 = v5 + 1;
        break;
      case 3:
        *(Dst + v7) = aAbcdefghijklmn[byte_41A144[0] >> 2];
        v6 = v7 + 1;
        *(Dst + v6++) = aAbcdefghijklmn[((byte_41A144[1] & 0xF0) >> 4) | 16 * (byte_41A144[0] & 3)];
        *(Dst + v6++) = aAbcdefghijklmn[((byte_41A144[2] & 0xC0) >> 6) | 4 * (byte_41A144[1] & 0xF)];
        *(Dst + v6) = aAbcdefghijklmn[byte_41A144[2] & 0x3F];
        v7 = v6 + 1;
        break;
    }
  }
```

```
00000FF9 sub_411AB0:37 (411BF9)
```

```
411154: using guessed type int j____report_rangecheckfailure(void);
411375: using guessed type _DWORD sub_411375(const char *, ...);
4156E0: using guessed type char Dest[108];
```


IDA - reverse_3.exe C:\Users\lenovo\AppData\Local\Temp\Rar$DRa15852.12203\reverse_3.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function
Regular function
Instruction
Data
Unexplored
External symbol
Functions window
IDA Vi…
Pseudoco…
Pseudoco…
Stack of _ma…
Pseudoco…
Hex Vi…
Struct…
Enums
Imp…
Exp…
Function name
j__wmakepath_s
j___get_startup_argv_mode_0
j___should_initialize_environment_3
j___should_initialize_environment_0
j__configthreadlocale
j___crt_debugger_hook
j___get_initial_narrow_environment
j___initialize_default_precision
start
j_wcscpy_s
sub_411055
j____scrt_fastfail
j____scrt_is_ucrt_dll_in_use
_RTC_Failure(void *,int)
j_NtCurrentTeb
sub_411073
j__except_handler4_common
j___should_initialize_environment_2
_RTC_AllocaFailure(void *,_RTC_ALLO(
j__initterm_e
sub_411091
sub_41109B
j__cexit
j___get_startup_argv_mode
j__atexit
sub_4110B4
j_memset
sub_4110BE
j_strlen
sub_4110D7
sub_4110E6
_RTC_StackFailure(void *,char const
j____report_securityfailure
j___std_type_info_destroy_list
j__set_fmode
Line 9 of 274
Output window
Python
AU: idle Down Disk: 61GB
CSDN @weixin_51275728

```
  char v8; // [esp+0h] [ebp-188h]
  signed int j; // [esp+DCh] [ebp-ACh]
  signed int i; // [esp+E8h] [ebp-A0h]
  signed int v11; // [esp+E8h] [ebp-A0h]
  char Dest[108]; // [esp+F4h] [ebp-94h]
  char Str; // [esp+160h] [ebp-28h]
  char v14; // [esp+17Ch] [ebp-Ch]

  for ( i = 0; i < 100; ++i )
  {
    if ( i >= 0x64 )
      j____report_rangecheckfailure();
    Dest[i] = 0;
  }
  sub_41132F("please enter the flag:", v7);
  LODWORD(v0) = &Str;
  sub_411375("%20s", &Str, *(&v0 + 1));
  v1 = j_strlen(&Str);
  v2 = sub_4110BE(&Str, v1, &v14);
  strncpy(Dest, v2, 0x28u);
  v11 = j_strlen(Dest);
  for ( j = 0; j < v11; ++j )
    Dest[j] += j;
  v3 = j_strlen(Dest);
  if ( !strncmp(Dest, Str2, v3) )
    sub_41132F("rigth flag!\n", v8);
  else
    sub_41132F("wrong flag!\n", v8);
  HIDWORD(v5) = v4;
  LODWORD(v5) = 0;
  return v5;
}
```

```
00004B8F _main_0:28 (41578F)
```

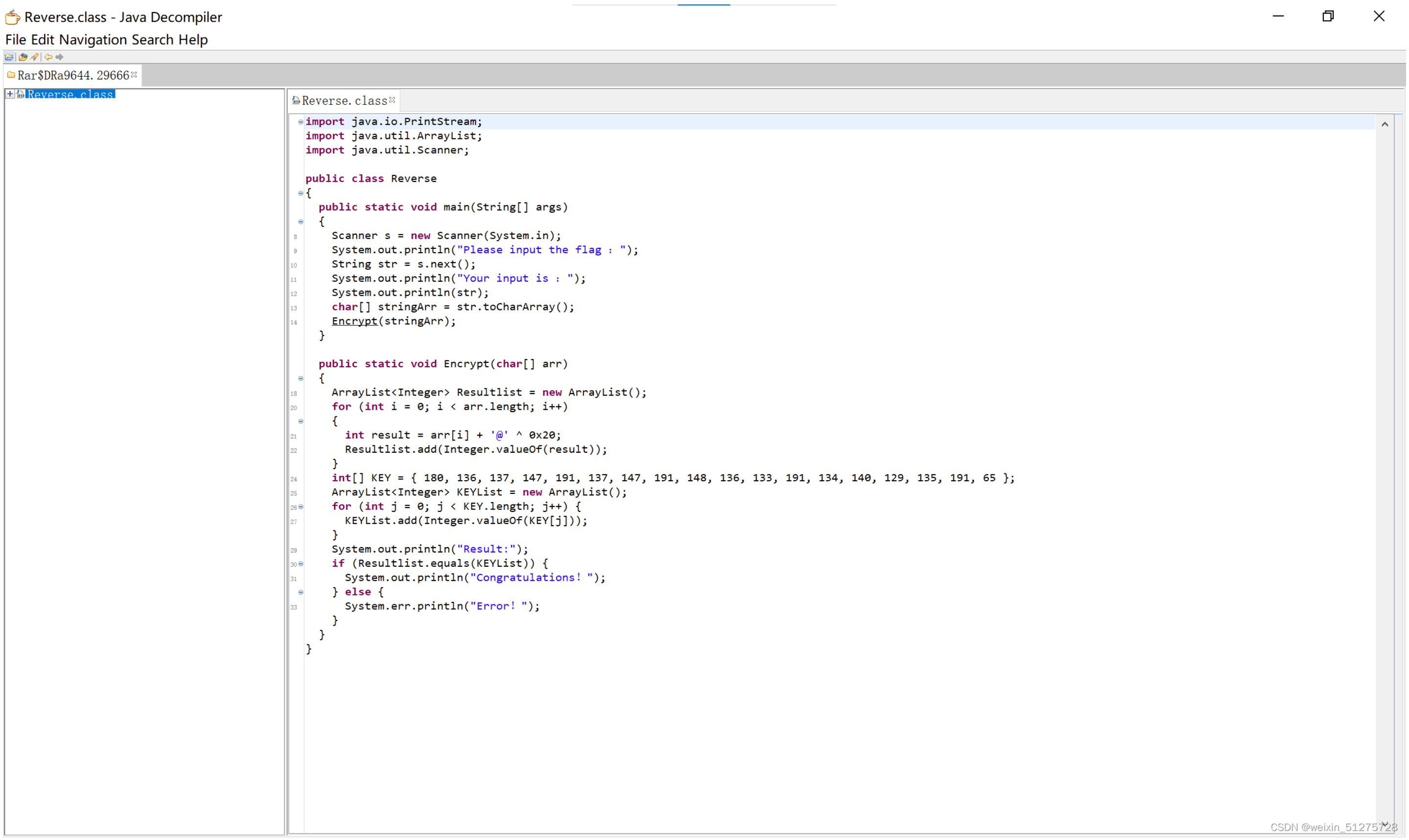
```
411154: using guessed type int j____report_rangecheckfailure(void);
411375: using guessed type _DWORD sub_411375(const char *, ...);
4156E0: using guessed type char Dest[108];
```

```
#include <iostream>
using namespace std;
int main(){
 string p="e3nifIH9b_C@n@dH";
 for(int i=0;i<p.length();i++)
 p[i]-=i;
 cout<<p;
}
```

再base64 解码即可

## 11 java

11 java 逆向解密密，用gui

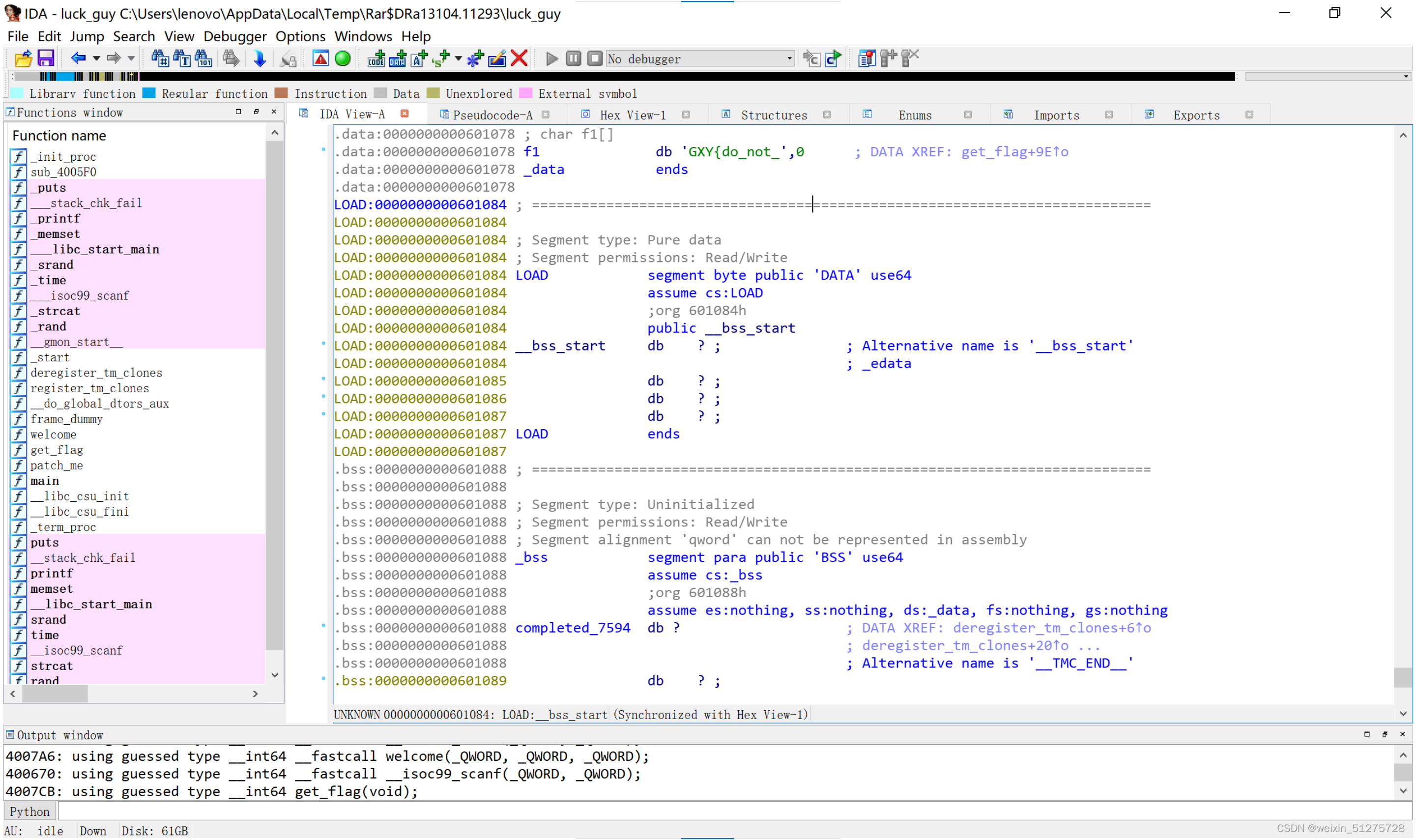


```
import java.io.PrintStream;
import java.util.ArrayList;
import java.util.Scanner;

public class Reverse
{
  public static void main(String[] args)
  {
    Scanner s = new Scanner(System.in);
    System.out.println("Please input the flag : ");
    String str = s.next();
    System.out.println("Your input is : ");
    System.out.println(str);
    char[] stringArr = str.toCharArray();
    Encrypt(stringArr);
  }

  public static void Encrypt(char[] arr)
  {
    ArrayList<Integer> Resultlist = new ArrayList();
    for (int i = 0; i < arr.length; i++)
    {
      int result = arr[i] + '@' ^ 0x20;
      Resultlist.add(Integer.valueOf(result));
    }
    int[] KEY = { 180, 136, 137, 147, 191, 137, 147, 191, 148, 136, 133, 191, 134, 140, 129, 135, 191, 65 };
    ArrayList<Integer> KEYList = new ArrayList();
    for (int j = 0; j < KEY.length; j++) {
      KEYList.add(Integer.valueOf(KEY[j]));
    }
    System.out.println("Result:");
    if (Resultlist.equals(KEYList)) {
      System.out.println("Congratulations! ");
    } else {
      System.err.println("Error! ");
    }
  }
}
```

```
#include < iostream>
using namespace std;
int main(){
 int key[] = { 180, 136, 137, 147, 191, 137, 147, 191, 148, 136, 133, 191, 134, 140, 129, 135, 191, 65 };
 for(int i=0;i<18;i++){
  char p=key[i]-'@'^0x20;
  cout<<p;
 }
```

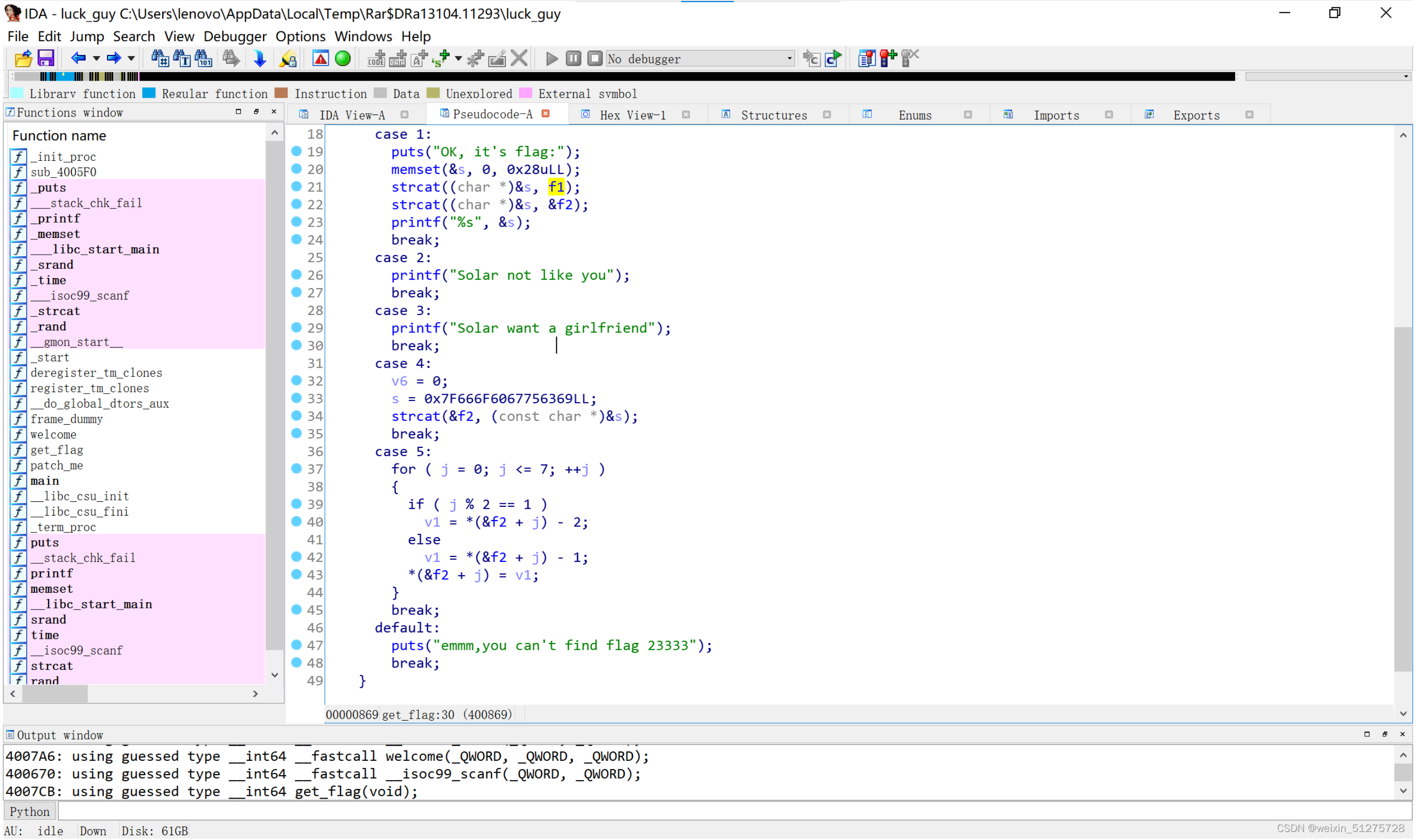
## 12 luckgay

12luckgay



```
.data:0000000000601078 ; char f1[]
.data:0000000000601078 f1              db 'GXY{do_not_',0      ; DATA XREF: get_flag+9E↑o
.data:0000000000601078 _data           ends
.data:0000000000601078
LOAD:0000000000601084 ; ===========================================================================
LOAD:0000000000601084
LOAD:0000000000601084 ; Segment type: Pure data
LOAD:0000000000601084 ; Segment permissions: Read/Write
LOAD:0000000000601084 LOAD            segment byte public 'DATA' use64
LOAD:0000000000601084                 assume cs:LOAD
LOAD:0000000000601084                 ;org 601084h
LOAD:0000000000601084                 public __bss_start
LOAD:0000000000601084 __bss_start     db    ? ;               ; Alternative name is '__bss_start'
LOAD:0000000000601084                                         ; _edata
LOAD:0000000000601085                 db    ? ;
LOAD:0000000000601086                 db    ? ;
LOAD:0000000000601087                 db    ? ;
LOAD:0000000000601087 LOAD            ends
LOAD:0000000000601087
.bss:0000000000601088 ; ===========================================================================
.bss:0000000000601088
.bss:0000000000601088 ; Segment type: Uninitialized
.bss:0000000000601088 ; Segment permissions: Read/Write
.bss:0000000000601088 ; Segment alignment 'qword' can not be represented in assembly
.bss:0000000000601088 _bss            segment para public 'BSS' use64
.bss:0000000000601088                 assume cs:_bss
.bss:0000000000601088                 ;org 601088h
.bss:0000000000601088                 assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.bss:0000000000601088 completed_7594  db ?                    ; DATA XREF: deregister_tm_clones+6↑o
.bss:0000000000601088                                         ; deregister_tm_clones+20↑o ...
.bss:0000000000601088                                         ; Alternative name is '__TMC_END__'
.bss:0000000000601089                 db    ? ;
UNKNOWN 0000000000601084: LOAD:__bss_start (Synchronized with Hex View-1)
```

```
4007A6: using guessed type __int64 __fastcall welcome(_QWORD, _QWORD, _QWORD);
400670: using guessed type __int64 __fastcall __isoc99_scanf(_QWORD, _QWORD);
4007CB: using guessed type __int64 get_flag(void);
```



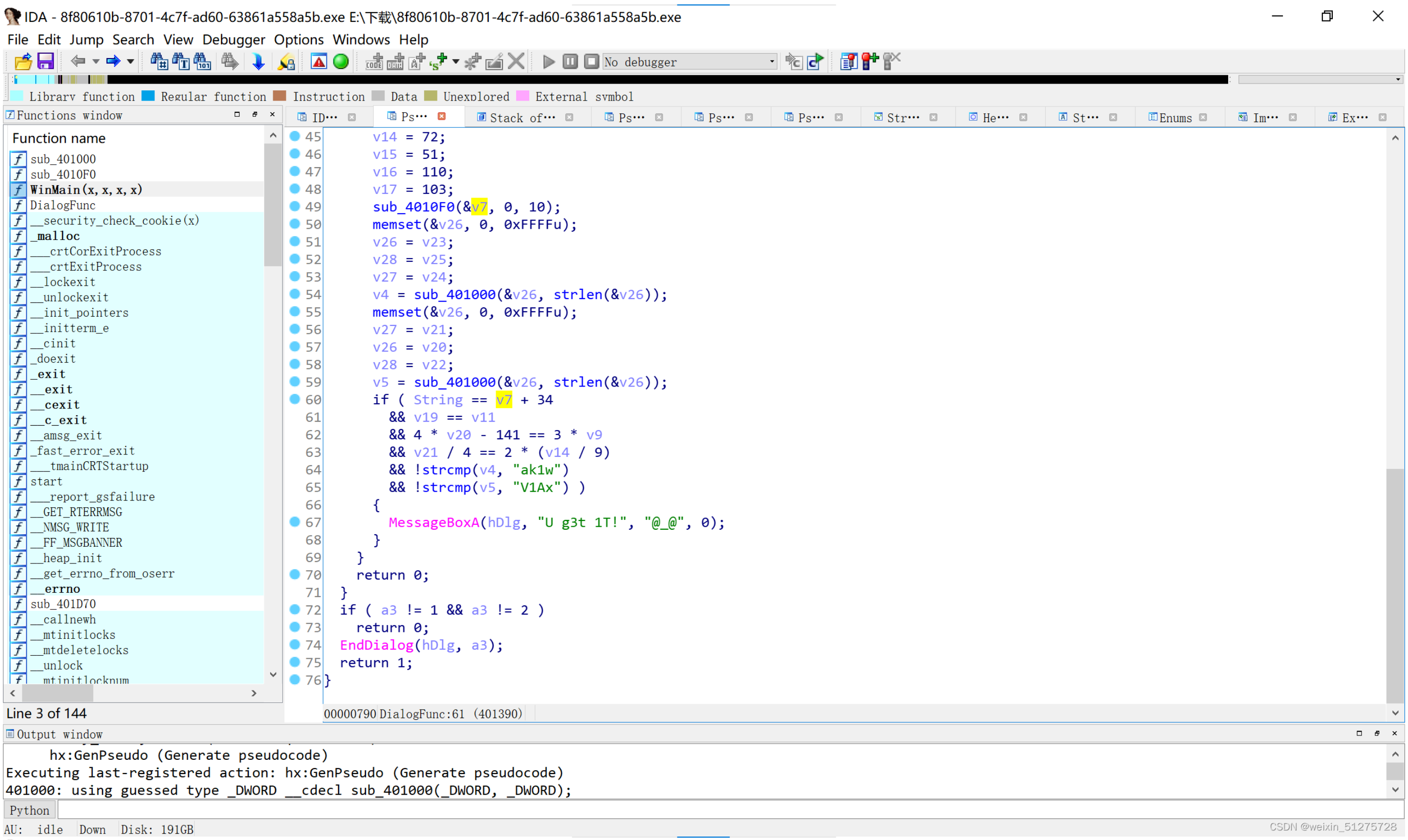
```
    case 1:
      puts("OK, it's flag:");
      memset(&s, 0, 0x28uLL);
      strcat((char *)&s, f1);
      strcat((char *)&s, &f2);
      printf("%s", &s);
      break;
    case 2:
      printf("Solar not like you");
      break;
    case 3:
      printf("Solar want a girlfriend");
      break;
    case 4:
      v6 = 0;
      s = 0x7F666F6067756369LL;
      strcat(&f2, (const char *)&s);
      break;
    case 5:
      for ( j = 0; j <= 7; ++j )
      {
        if ( j % 2 == 1 )
          v1 = *(&f2 + j) - 2;
        else
          v1 = *(&f2 + j) - 1;
        *(&f2 + j) = v1;
      }
      break;
    default:
      puts("emmm,you can't find flag 23333");
      break;
  }
00000869 get_flag:30 (400869)
```

```
4007A6: using guessed type __int64 __fastcall welcome(_QWORD, _QWORD, _QWORD);
400670: using guessed type __int64 __fastcall __isoc99_scanf(_QWORD, _QWORD);
4007CB: using guessed type __int64 get_flag(void);
```

```
#include <iostream>
using namespace std;
int main(){
 int p[]={0x69,0x63,0x75,0x67,0x60,0x6f,0x66,0x7f};
 for(int i=0;i<8;i++){
  if(i%2==1)
  p[i]-=2;
  else p[i]-=1;
  char x=p[i];
  cout<<x;
 }
}
```

## 13 刮开有奖

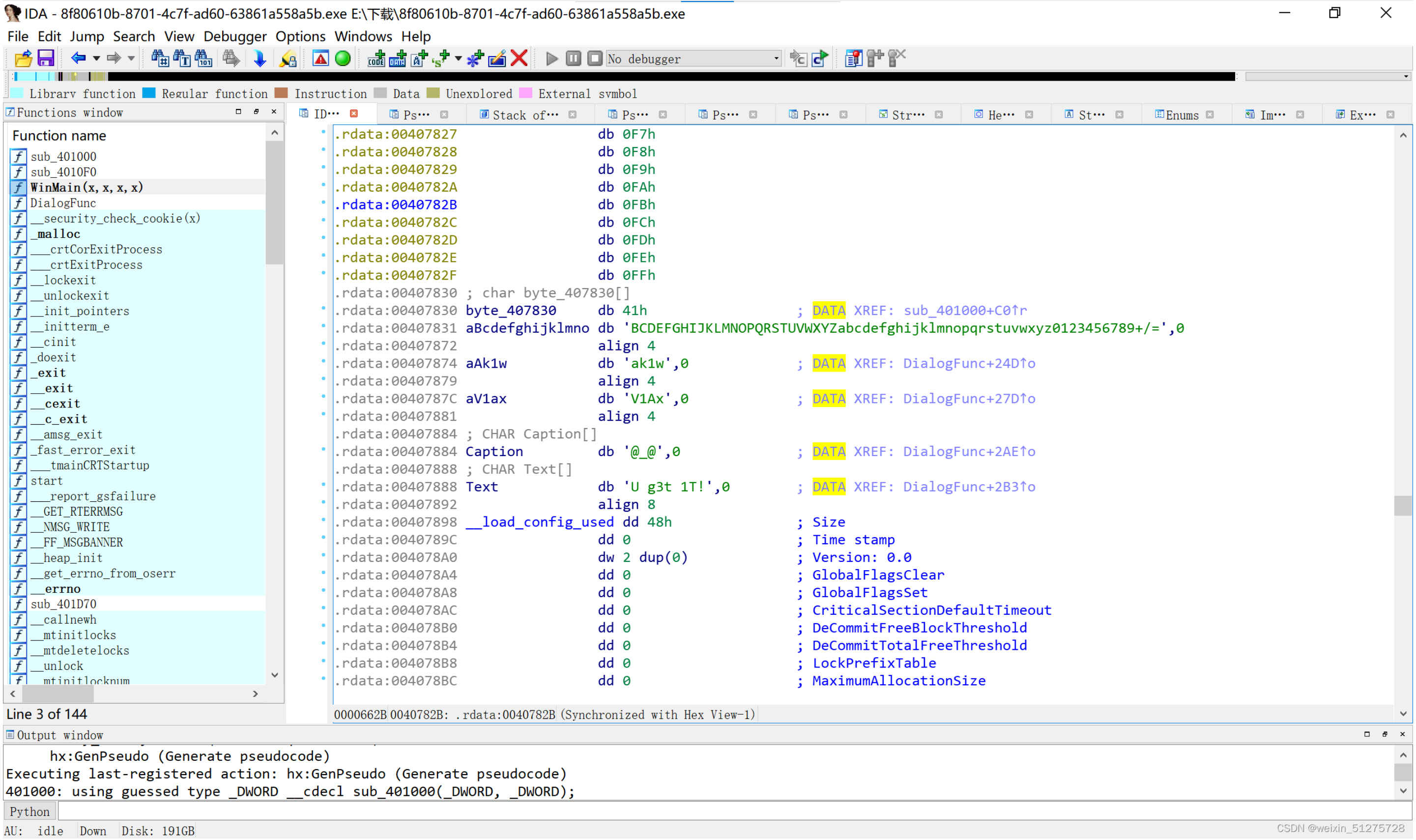
## 13 刮开有奖


IDA - 8f80610b-8701-4c7f-ad60-63861a558a5b.exe E:\下载\8f80610b-8701-4c7f-ad60-63861a558a5b.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
Function name
sub_401000
sub_4010F0
WinMain(x, x, x, x)
DialogFunc
Line 3 of 144
Output window
Python
AU: idle Down Disk: 191GB
CSDN @weixin_51275728

```
      v14 = 72;
      v15 = 51;
      v16 = 110;
      v17 = 103;
      sub_4010F0(&v7, 0, 10);
      memset(&v26, 0, 0xFFFFu);
      v26 = v23;
      v28 = v25;
      v27 = v24;
      v4 = sub_401000(&v26, strlen(&v26));
      memset(&v26, 0, 0xFFFFu);
      v27 = v21;
      v26 = v20;
      v28 = v22;
      v5 = sub_401000(&v26, strlen(&v26));
      if ( String == v7 + 34
        && v19 == v11
        && 4 * v20 - 141 == 3 * v9
        && v21 / 4 == 2 * (v14 / 9)
        && !strcmp(v4, "ak1w")
        && !strcmp(v5, "V1Ax") )
      {
        MessageBoxA(hDlg, "U g3t 1T!", "@_@", 0);
      }
    }
    return 0;
  }
  if ( a3 != 1 && a3 != 2 )
    return 0;
  EndDialog(hDlg, a3);
  return 1;
}
```

00000790 DialogFunc:61 (401390)

```
    hx:GenPseudo (Generate pseudocode)
Executing last-registered action: hx:GenPseudo (Generate pseudocode)
401000: using guessed type _DWORD __cdecl sub_401000(_DWORD, _DWORD);
```


IDA - 8f80610b-8701-4c7f-ad60-63861a558a5b.exe E:\下载\8f80610b-8701-4c7f-ad60-63861a558a5b.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
Function name
sub_401000
sub_4010F0
WinMain(x, x, x, x)
DialogFunc
Line 3 of 144
Output window
Python
AU: idle Down Disk: 191GB
CSDN @weixin_51275728

```
.rdata:00407827                 db 0F7h
.rdata:00407828                 db 0F8h
.rdata:00407829                 db 0F9h
.rdata:0040782A                 db 0FAh
.rdata:0040782B                 db 0FBh
.rdata:0040782C                 db 0FCh
.rdata:0040782D                 db 0FDh
.rdata:0040782E                 db 0FEh
.rdata:0040782F                 db 0FFh
.rdata:00407830 ; char byte_407830[]
.rdata:00407830 byte_407830     db 41h                  ; DATA XREF: sub_401000+C0↑r
.rdata:00407831 aBcdefghijklmno db 'BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=',0
.rdata:00407872                 align 4
.rdata:00407874 aAk1w           db 'ak1w',0             ; DATA XREF: DialogFunc+24D↑o
.rdata:00407879                 align 4
.rdata:0040787C aV1ax           db 'V1Ax',0             ; DATA XREF: DialogFunc+27D↑o
.rdata:00407881                 align 4
.rdata:00407884 ; CHAR Caption[]
.rdata:00407884 Caption         db '@_@',0              ; DATA XREF: DialogFunc+2AE↑o
.rdata:00407888 ; CHAR Text[]
.rdata:00407888 Text            db 'U g3t 1T!',0        ; DATA XREF: DialogFunc+2B3↑o
.rdata:00407892                 align 8
.rdata:00407898 __load_config_used dd 48h               ; Size
.rdata:0040789C                 dd 0                    ; Time stamp
.rdata:004078A0                 dw 2 dup(0)             ; Version: 0.0
.rdata:004078A4                 dd 0                    ; GlobalFlagsClear
.rdata:004078A8                 dd 0                    ; GlobalFlagsSet
.rdata:004078AC                 dd 0                    ; CriticalSectionDefaultTimeout
.rdata:004078B0                 dd 0                    ; DeCommitFreeBlockThreshold
.rdata:004078B4                 dd 0                    ; DeCommitTotalFreeThreshold
.rdata:004078B8                 dd 0                    ; LockPrefixTable
.rdata:004078BC                 dd 0                    ; MaximumAllocationSize
```

0000662B 0040782B: .rdata:0040782B (Synchronized with Hex View-1)

```
    hx:GenPseudo (Generate pseudocode)
Executing last-registered action: hx:GenPseudo (Generate pseudocode)
401000: using guessed type _DWORD __cdecl sub_401000(_DWORD, _DWORD);
```

程序处理+base64

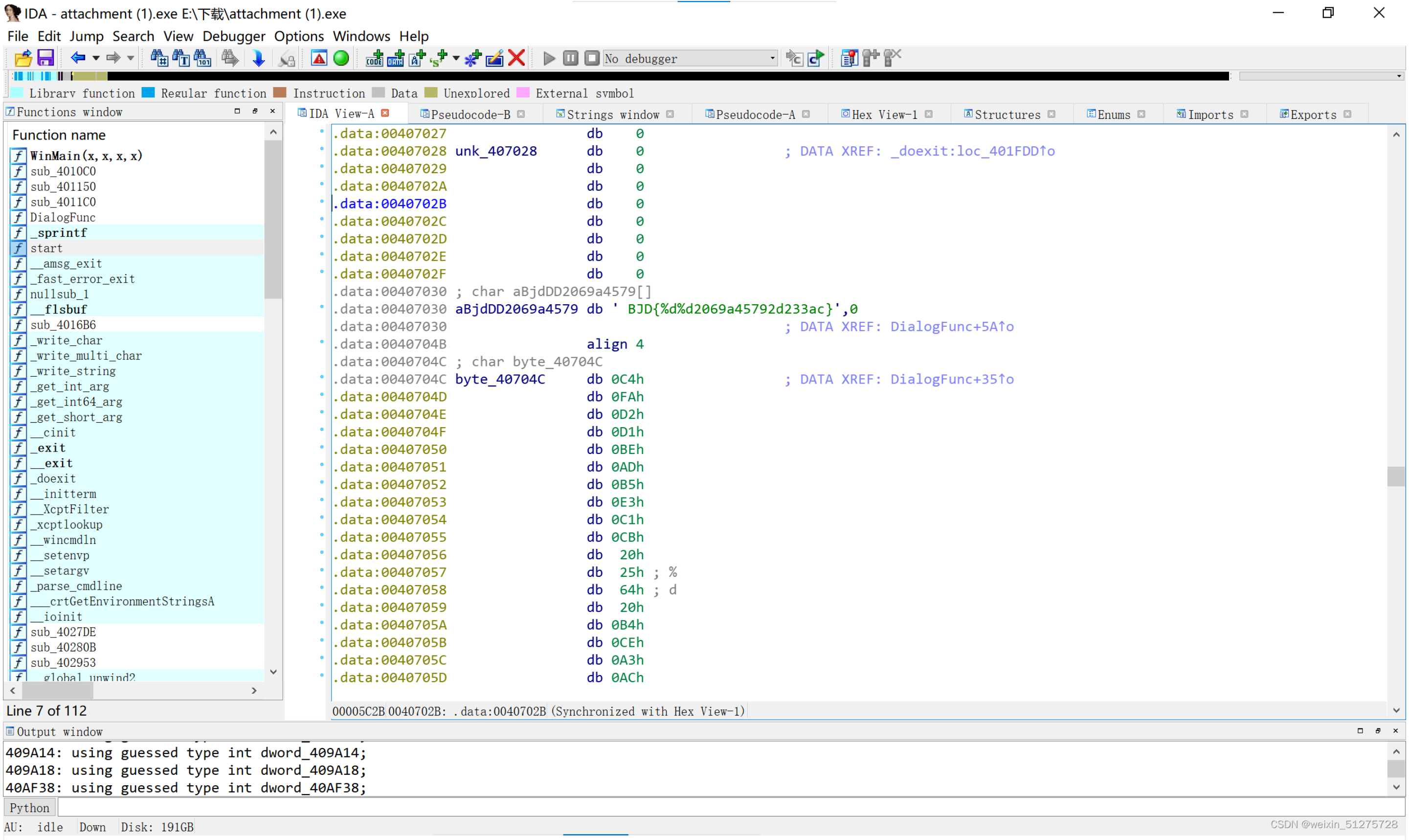
sub_4010c0

```
#include<stdio.h>
#include<iostream>

using namespace std;

int  sub(char a1[], int a2, int a3)
```

```
{
  int result; // eax
  int i; // esi
  int v5; // ecx
  int v6; // edx

  result = a3;
  for ( i = a2; i <= a3; a2 = i )
  {
    v5 = i;
    //v6 = *(DWORD *)(4 * i + a1);
    v6 = a1[i];
    if ( a2 < result && i < result )
    {
      do
      {
        //if ( v6 > *(DWORD *)(a1 + 4 * result) )
        if ( v6 > a1[result] )
        {
          if ( i >= result )
            break;
          ++i;
          //*(DWORD *)(v5 + a1) = *(DWORD *)(a1 + 4 * result);
          a1[v5] = a1[result];
          if ( i >= result )
            break;
          //while ( *(DWORD *)(a1 + 4 * i) <= v6 )
          while ( a1[i] <= v6 )
          {
            if ( ++i >= result )
              goto LABEL_13;
          }
          if ( i >= result )
            break;
          v5 = i;
          //*(DWORD *)(a1 + 4 * result) = *(DWORD *)(4 * i + a1);
          a1[result] = a1[i];
        }
        --result;
      }
      while ( i < result );
    }
LABEL_13:
    //*(DWORD *)(a1 + 4 * result) = v6;
    a1[result]= v6;
    sub(a1, a2, i - 1);
    result = a3;
    ++i;
  }
  return result;
}

int main()
{
    char a[11]={90,74,83,69,67,97,78,72,51,110,103};
    cout<<">>>>sub"<<endl;
    sub(a,0,10);
    for (int i=0;i<11;i++)
    {
        cout<<"a["<<i+7<<"]"<<a[i]<<" "<<int(a[i])<<endl;
        cout<<"a["<<i<<"]"<<a[i]<<" "<<int(a[i])<<endl;
        //cout<<a[i]<<" ";
    }
}
```

# 14 JustRE

14 JustRE先开始以为是直接的明码，发现不是，动调爆破



IDA - attachment (1).exe E:\下载\attachment (1).exe

Function name

```
WinMain(x, x, x, x)
sub_4010C0
sub_401150
sub_4011C0
DialogFunc
_sprintf
start
__amsg_exit
_fast_error_exit
nullsub_1
__flsbuf
sub_4016B6
_write_char
_write_multi_char
_write_string
_get_int_arg
_get_int64_arg
_get_short_arg
__cinit
_exit
__exit
_doexit
__initterm
__XcptFilter
_xcptlookup
__wincmdln
__setenvp
__setargv
_parse_cmdline
___crtGetEnvironmentStringsA
__ioinit
sub_4027DE
sub_40280B
sub_402953
__global_unwind2
```

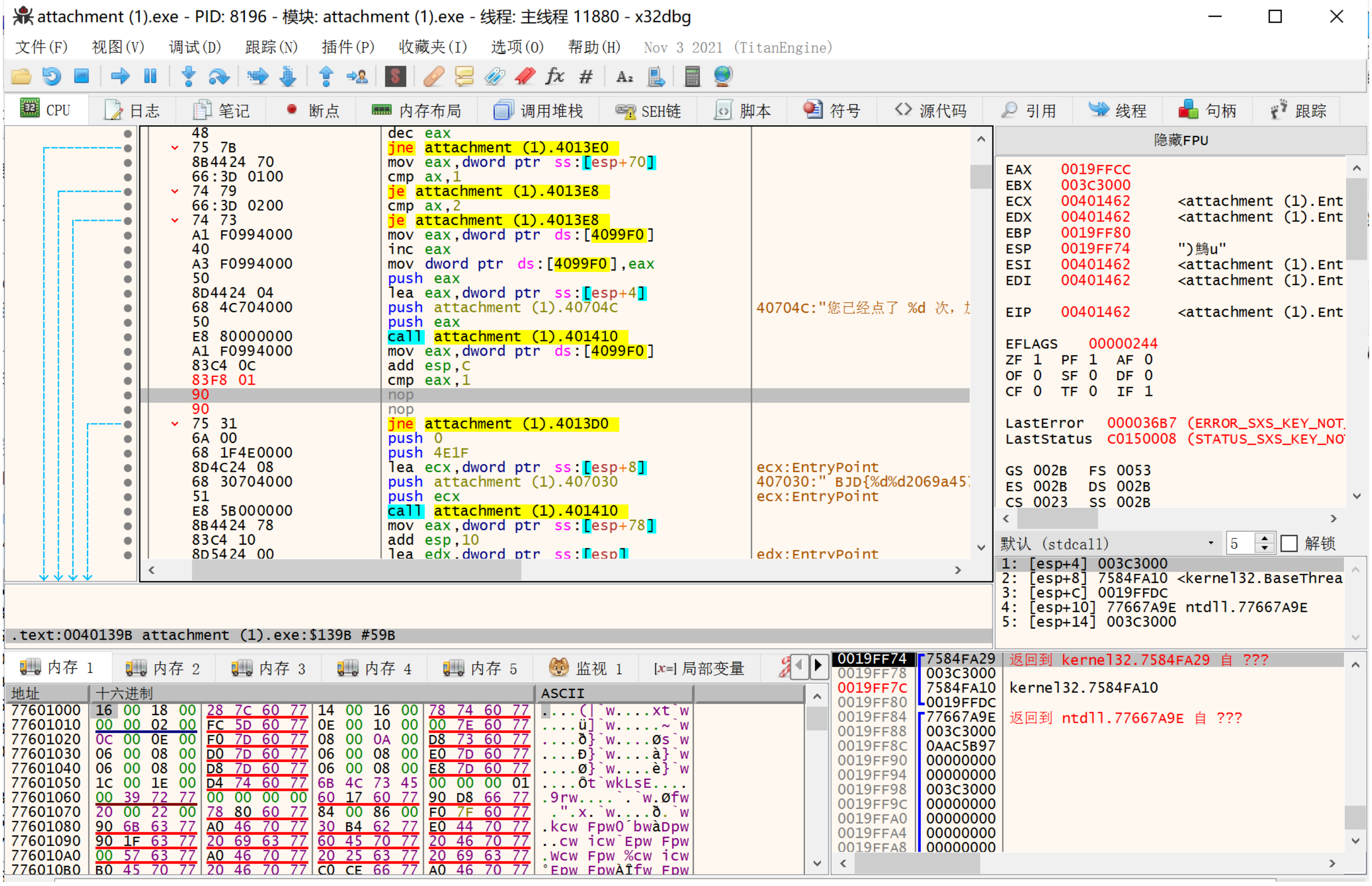
Line 7 of 112

```
.data:00407027                 db    0
.data:00407028 unk_407028      db    0               ; DATA XREF: _doexit:loc_401FDD↑o
.data:00407029                 db    0
.data:0040702A                 db    0
.data:0040702B                 db    0
.data:0040702C                 db    0
.data:0040702D                 db    0
.data:0040702E                 db    0
.data:0040702F                 db    0
.data:00407030 ; char aBjdDD2069a4579[]
.data:00407030 aBjdDD2069a4579 db ' BJD{%d%d2069a45792d233ac}',0
.data:00407030                                         ; DATA XREF: DialogFunc+5A↑o
.data:0040704B                 align 4
.data:0040704C ; char byte_40704C
.data:0040704C byte_40704C     db 0C4h                 ; DATA XREF: DialogFunc+35↑o
.data:0040704D                 db 0FAh
.data:0040704E                 db 0D2h
.data:0040704F                 db 0D1h
.data:00407050                 db 0BEh
.data:00407051                 db 0ADh
.data:00407052                 db 0B5h
.data:00407053                 db 0E3h
.data:00407054                 db 0C1h
.data:00407055                 db 0CBh
.data:00407056                 db  20h
.data:00407057                 db  25h ; %
.data:00407058                 db  64h ; d
.data:00407059                 db  20h
.data:0040705A                 db 0B4h
.data:0040705B                 db 0CEh
.data:0040705C                 db 0A3h
.data:0040705D                 db 0ACh
00005C2B 0040702B: .data:0040702B (Synchronized with Hex View-1)
```

Output window

```
409A14: using guessed type int dword_409A14;
409A18: using guessed type int dword_409A18;
40AF38: using guessed type int dword_40AF38;
```

AU: idle Down Disk: 191GB



attachment (1).exe - PID: 8196 - 模块: attachment (1).exe - 线程: 主线程 11880 - x32dbg

```
48                dec eax
75 7B             jne attachment (1).4013E0
8B4424 70         mov eax,dword ptr ss:[esp+70]
66:3D 0100        cmp ax,1
74 79             je attachment (1).4013E8
66:3D 0200        cmp ax,2
74 73             je attachment (1).4013E8
A1 F0994000       mov eax,dword ptr ds:[4099F0]
40                inc eax
A3 F0994000       mov dword ptr ds:[4099F0],eax
50                push eax
8D4424 04         lea eax,dword ptr ss:[esp+4]
68 4C704000       push attachment (1).40704C        40704C:"您已经点了 %d 次，
50                push eax
E8 80000000       call attachment (1).401410
A1 F0994000       mov eax,dword ptr ds:[4099F0]
83C4 0C           add esp,C
83F8 01           cmp eax,1
90                nop
90                nop
75 31             jne attachment (1).4013D0
6A 00             push 0
68 1F4E0000       push 4E1F
8D4C24 08         lea ecx,dword ptr ss:[esp+8]      ecx:EntryPoint
68 30704000       push attachment (1).407030        407030:" BJD{%d%d2069a45
51                push ecx                          ecx:EntryPoint
E8 5B000000       call attachment (1).401410
8B4424 78         mov eax,dword ptr ss:[esp+78]
83C4 10           add esp,10
8D5424 00         lea edx,dword ptr ss:[esp]        edx:EntryPoint

.text:0040139B attachment (1).exe:$139B #59B
```

```
EAX     0019FFCC
EBX     003C3000
ECX     00401462      <attachment (1).Ent
EDX     00401462      <attachment (1).Ent
EBP     0019FF80
ESP     0019FF74      ")鵜u"
ESI     00401462      <attachment (1).Ent
EDI     00401462      <attachment (1).Ent

EIP     00401462      <attachment (1).Ent

EFLAGS    00000244
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1

LastError   000036B7 (ERROR_SXS_KEY_NOT_
LastStatus  C0150008 (STATUS_SXS_KEY_NO

GS 002B   FS 0053
ES 002B   DS 002B
CS 0023   SS 002B
```

默认 (stdcall) 5 □ 解锁

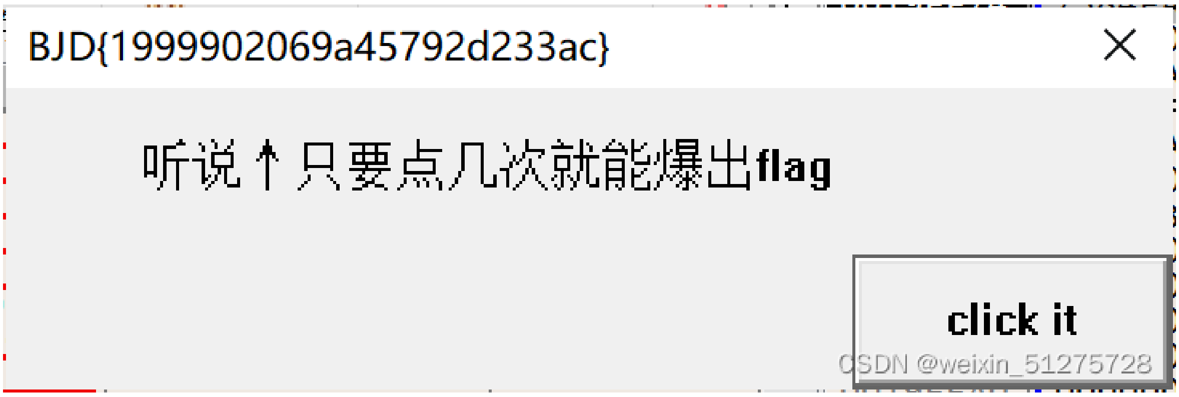
```
1: [esp+4] 003C3000
2: [esp+8] 7584FA10 <kernel32.BaseThrea
3: [esp+C] 0019FFDC
4: [esp+10] 77667A9E ntdll.77667A9E
5: [esp+14] 003C3000
```

```
地址      十六进制                                          ASCII
77601000  16 00 18 00 28 7C 60 77 14 00 16 00 78 74 60 77  ....(|`w....xt`w
77601010  00 00 02 00 FC 5D 60 77 0E 00 10 00 00 7E 60 77  ....ü]`w.....~`w
77601020  0C 00 0E 00 F0 7D 60 77 08 00 0A 00 D8 73 60 77  ....ð}`w....Øs`w
77601030  06 00 08 00 D0 7D 60 77 06 00 08 00 E0 7D 60 77  ....Ð}`w....à}`w
77601040  06 00 08 00 D8 7D 60 77 06 00 08 00 E8 7D 60 77  ....Ø}`w....è}`w
77601050  1C 00 1E 00 D4 74 60 77 6B 4C 73 45 00 00 00 01  ....Ôt`wkLsE....
77601060  00 39 72 77 00 00 00 00 60 17 60 77 90 D8 66 77  .9rw....`.`w.Øfw
77601070  20 00 22 00 78 80 60 77 84 00 86 00 F0 7F 60 77   .".x.`w....ð.`w
77601080  90 6B 63 77 A0 46 70 77 30 B4 62 77 E0 44 70 77  .kcw Fpw0´bwàDpw
77601090  90 1F 63 77 20 69 63 77 60 45 70 77 20 46 70 77  ..cw icw`Epw Fpw
776010A0  00 57 63 77 A0 46 70 77 20 25 63 77 20 69 63 77  .Wcw Fpw %cw icw
776010B0  B0 45 70 77 20 46 70 77 C0 CE 66 77 A0 46 70 77  °Epw FpwÀÎfw Fpw
```

```
0019FF74  7584FA29  返回到 kernel32.7584FA29 自 ???
0019FF78  003C3000
0019FF7C  7584FA10  kernel32.7584FA10
0019FF80  0019FFDC
0019FF84  77667A9E  返回到 ntdll.77667A9E 自 ???
0019FF88  003C3000
0019FF8C  0AAC5B97
0019FF90  00000000
0019FF94  00000000
0019FF98  003C3000
0019FF9C  00000000
0019FFA0  00000000
0019FFA4  00000000
0019FFA8  00000000
```

搜索到 10271 个字符串于 4485 毫秒内

已调试时间 0:11:23:28



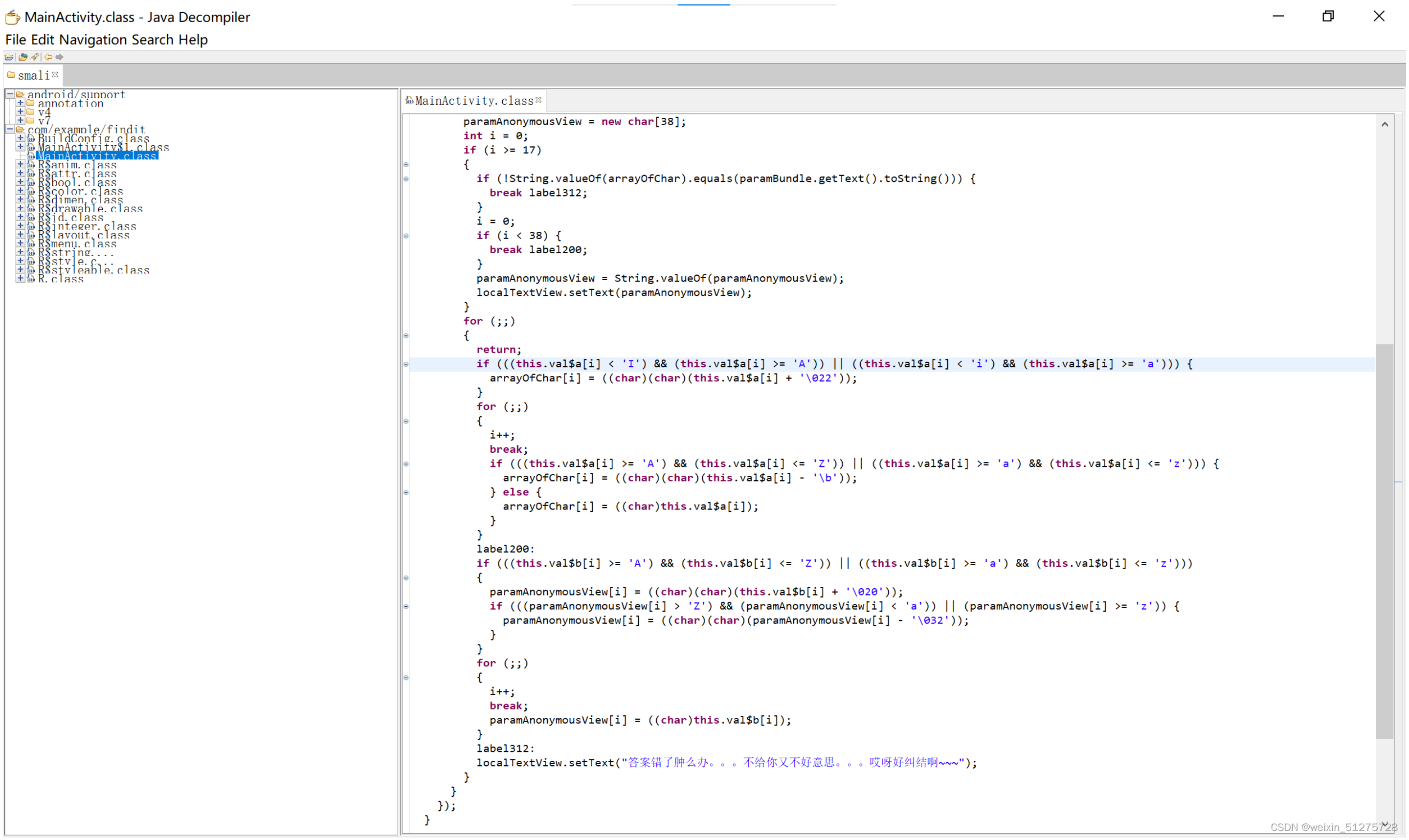
BJD{1999902069a45792d233ac}

听说↑只要点几次就能爆出flag

（不爆破按19999下也行）打开即可

## 15 findit

15 findit



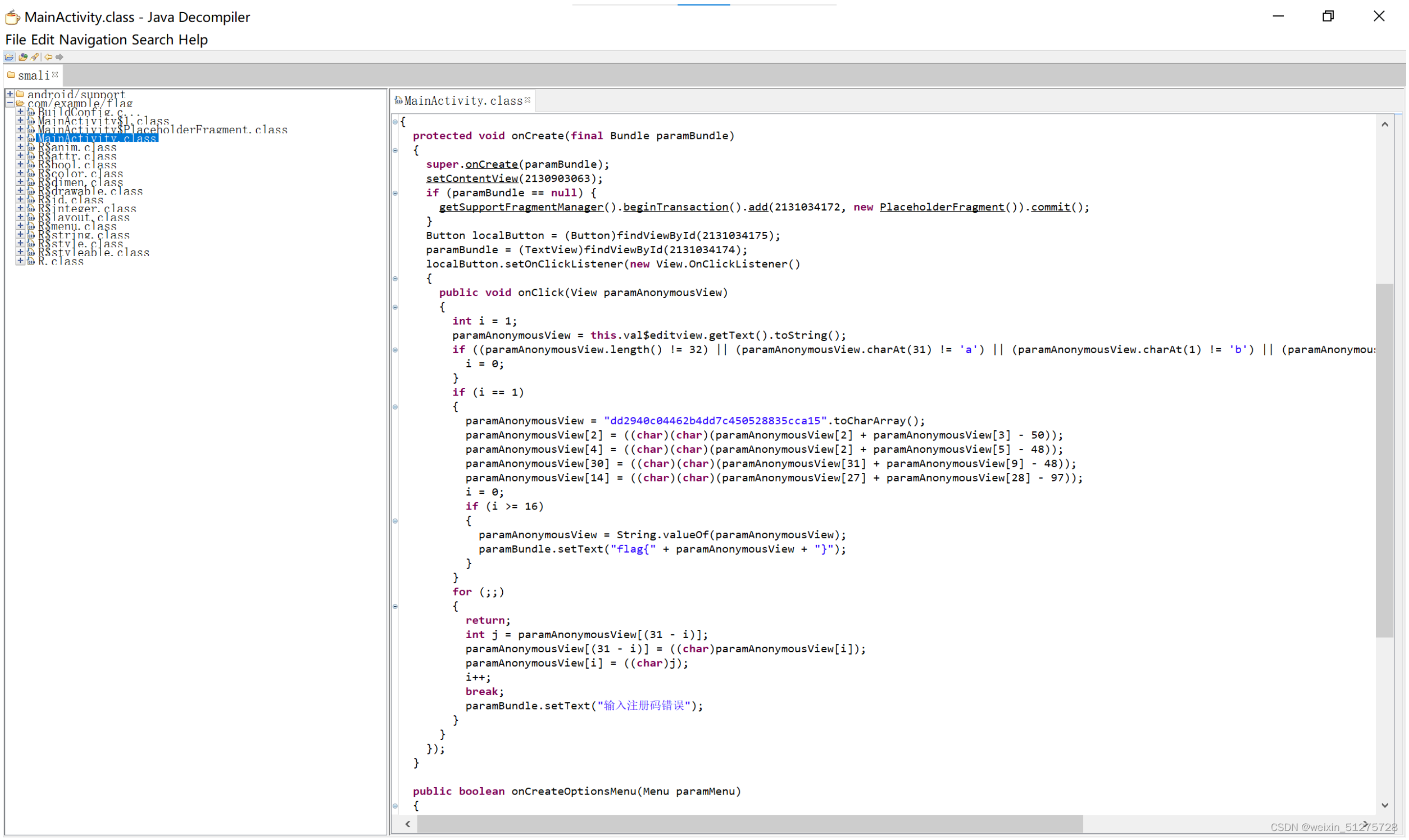
```java
          paramAnonymousView = new char[38];
          int i = 0;
          if (i >= 17)
          {
            if (!String.valueOf(arrayOfChar).equals(paramBundle.getText().toString())) {
              break label312;
            }
            i = 0;
            if (i < 38) {
              break label200;
            }
            paramAnonymousView = String.valueOf(paramAnonymousView);
            localTextView.setText(paramAnonymousView);
          }
          for (;;)
          {
            return;
            if (((this.val$a[i] < 'I') && (this.val$a[i] >= 'A')) || ((this.val$a[i] < 'i') && (this.val$a[i] >= 'a'))) {
              arrayOfChar[i] = ((char)(char)(this.val$a[i] + '\022'));
            }
            for (;;)
            {
              i++;
              break;
              if (((this.val$a[i] >= 'A') && (this.val$a[i] <= 'Z')) || ((this.val$a[i] >= 'a') && (this.val$a[i] <= 'z'))) {
                arrayOfChar[i] = ((char)(char)(this.val$a[i] - '\b'));
              } else {
                arrayOfChar[i] = ((char)this.val$a[i]);
              }
            }
            label200:
            if (((this.val$b[i] >= 'A') && (this.val$b[i] <= 'Z')) || ((this.val$b[i] >= 'a') && (this.val$b[i] <= 'z')))
            {
              paramAnonymousView[i] = ((char)(char)(this.val$b[i] + '\020'));
              if (((paramAnonymousView[i] > 'Z') && (paramAnonymousView[i] < 'a')) || (paramAnonymousView[i] >= 'z')) {
                paramAnonymousView[i] = ((char)(char)(paramAnonymousView[i] - '\032'));
              }
            }
            for (;;)
            {
              i++;
              break;
              paramAnonymousView[i] = ((char)this.val$b[i]);
            }
            label312:
            localTextView.setText("答案错了肿么办。。。不给你又不好意思。。。哎呀好纠结啊~~~");
          }
        }
      });
    }
```

```cpp
#include < iostream>
using namespace std;
int main(){
char a[]={0x70,0x76,0x6b,0x71, 0x7b, 0x6d, 0x31,0x36,0x34, 0x36,0x37,0x35,0x32,0x36,0x32,0x30, 0x33,0x33,0x6c,0x34,0x6d,0x34,0x39,0x6c,0x6e,0x70,0x37,0x70,0x39,0x6d,0x6e,0x6b,0x32,0x38,0x6b,0x37,0x35,0x7d};
        for(int i=0;i<38;i++){
         cout<<a[i]; }
}
```

然后凯撒（看1第一个字符与第四个字符是否相邻，是则基本上就是凯撒）

## 16 简单注册器

16 简单注册器



```
{
  protected void onCreate(final Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    setContentView(2130903063);
    if (paramBundle == null) {
      getSupportFragmentManager().beginTransaction().add(2131034172, new PlaceholderFragment()).commit();
    }
    Button localButton = (Button)findViewById(2131034175);
    paramBundle = (TextView)findViewById(2131034174);
    localButton.setOnClickListener(new View.OnClickListener()
    {
      public void onClick(View paramAnonymousView)
      {
        int i = 1;
        paramAnonymousView = this.val$editview.getText().toString();
        if ((paramAnonymousView.length() != 32) || (paramAnonymousView.charAt(31) != 'a') || (paramAnonymousView.charAt(1) != 'b') || (paramAnonymou
          i = 0;
        }
        if (i == 1)
        {
          paramAnonymousView = "dd2940c04462b4dd7c450528835cca15".toCharArray();
          paramAnonymousView[2] = ((char)(char)(paramAnonymousView[2] + paramAnonymousView[3] - 50));
          paramAnonymousView[4] = ((char)(char)(paramAnonymousView[2] + paramAnonymousView[5] - 48));
          paramAnonymousView[30] = ((char)(char)(paramAnonymousView[31] + paramAnonymousView[9] - 48));
          paramAnonymousView[14] = ((char)(char)(paramAnonymousView[27] + paramAnonymousView[28] - 97));
          i = 0;
          if (i >= 16)
          {
            paramAnonymousView = String.valueOf(paramAnonymousView);
            paramBundle.setText("flag{" + paramAnonymousView + "}");
          }
        }
        for (;;)
        {
          return;
          int j = paramAnonymousView[(31 - i)];
          paramAnonymousView[(31 - i)] = ((char)paramAnonymousView[i]);
          paramAnonymousView[i] = ((char)j);
          i++;
          break;
          paramBundle.setText("输入注册码错误");
        }
      }
    });
  }

  public boolean onCreateOptionsMenu(Menu paramMenu)
  {
```

```
#include < iostream>
using namespace std;
int main(){
string p="dd2940c04462b4dd7c450528835cca15";
p[2]=p[2]+p[3]-50;
p[4]=p[2]+p[5]-48;
p[30]=p[31]+p[9]-48;
p[14]=p[27]+p[28]-97;
cout<<p;
}
```

## 17 pyre

17 pyre python反编译 - 在线工具 (tool.lu)

#!/usr/bin/env python

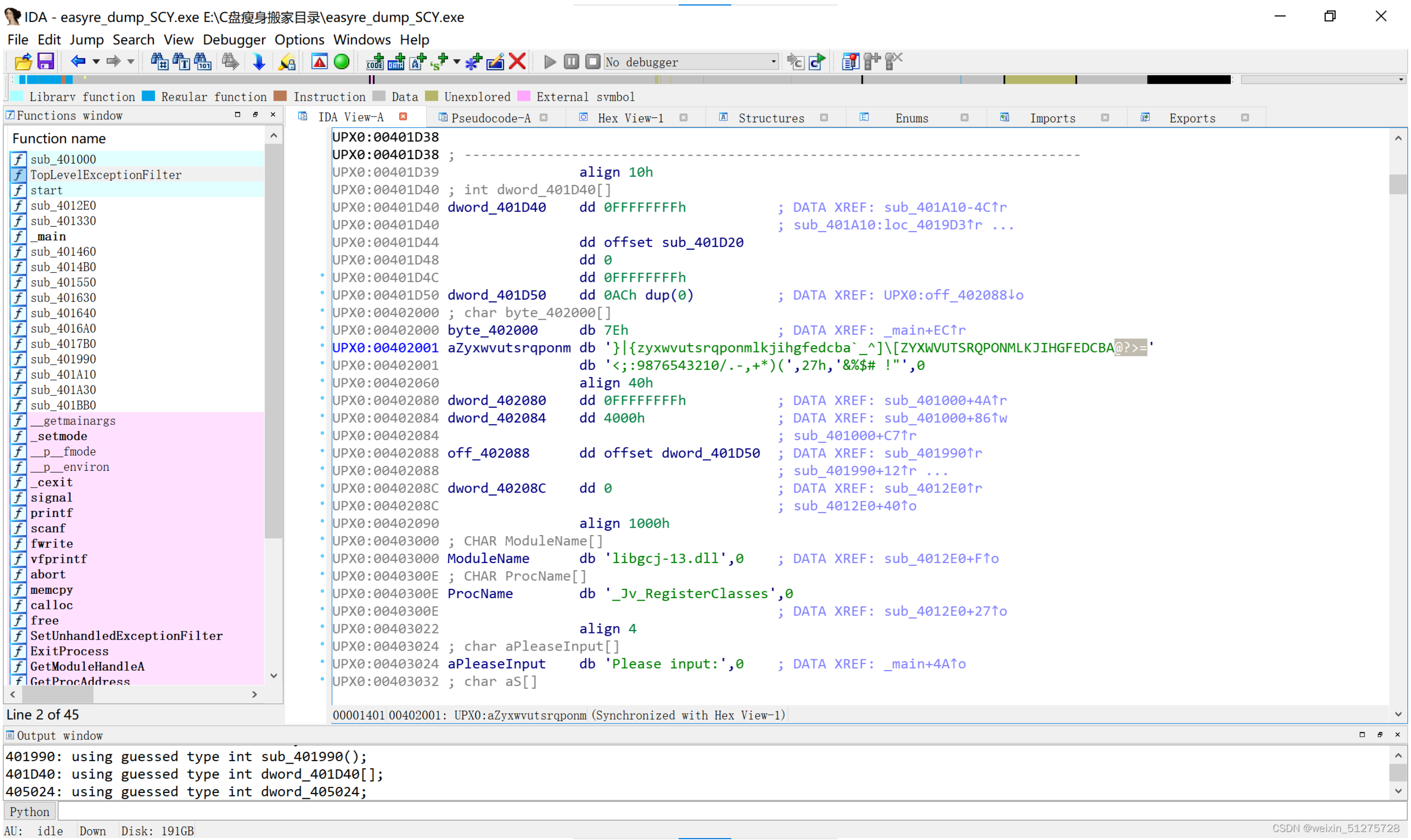
https://tool.lu/pyc/ for more information

```
print 'Welcome to Re World!'
print 'Your input1 is your flag~'
l = len(input1)
for i in range(l):
    num = ((input1[i] + i) % 128 + 128) % 128
    code += num

for i in range(l - 1):
    code[i] = code[i] ^ code[i + 1]

print code
code = [
    '\x1f',
    '\x12',
    '\x1d',
    '(',
    '0',
    '4',
    '\x01',
    '\x06',
    '\x14',
    '4',
    ',',
    '\x1b',
    'U',
    '?',
    'o',
    '6',
    '*',
    ':',
    '\x01',
    'D',
    ';',
'%',’0x13’]
```

```
#include <iostream>
using namespace std;
int main(){
char coder[]={0x13,'%',';','D',0x01,':','*','6','o','?','U',0x1b,',','4',0x14,0x06,0x01,'4','0','(',0x1d,0x12,0x1f};
char code[23];
for(int i=0;i<23;i++)
code[i]=coder[22-i];
for(int i=22;i>0;i--)
 code[i-1]^=code[i];
 for(int i=0;i<23;i++){
  code[i]=(code[i]-i)&0xff;
  cout<<code[i]; }
}
```

## 18 easyre

18.easyre 有壳，脱壳,壳没有完美脱出，但够看了。

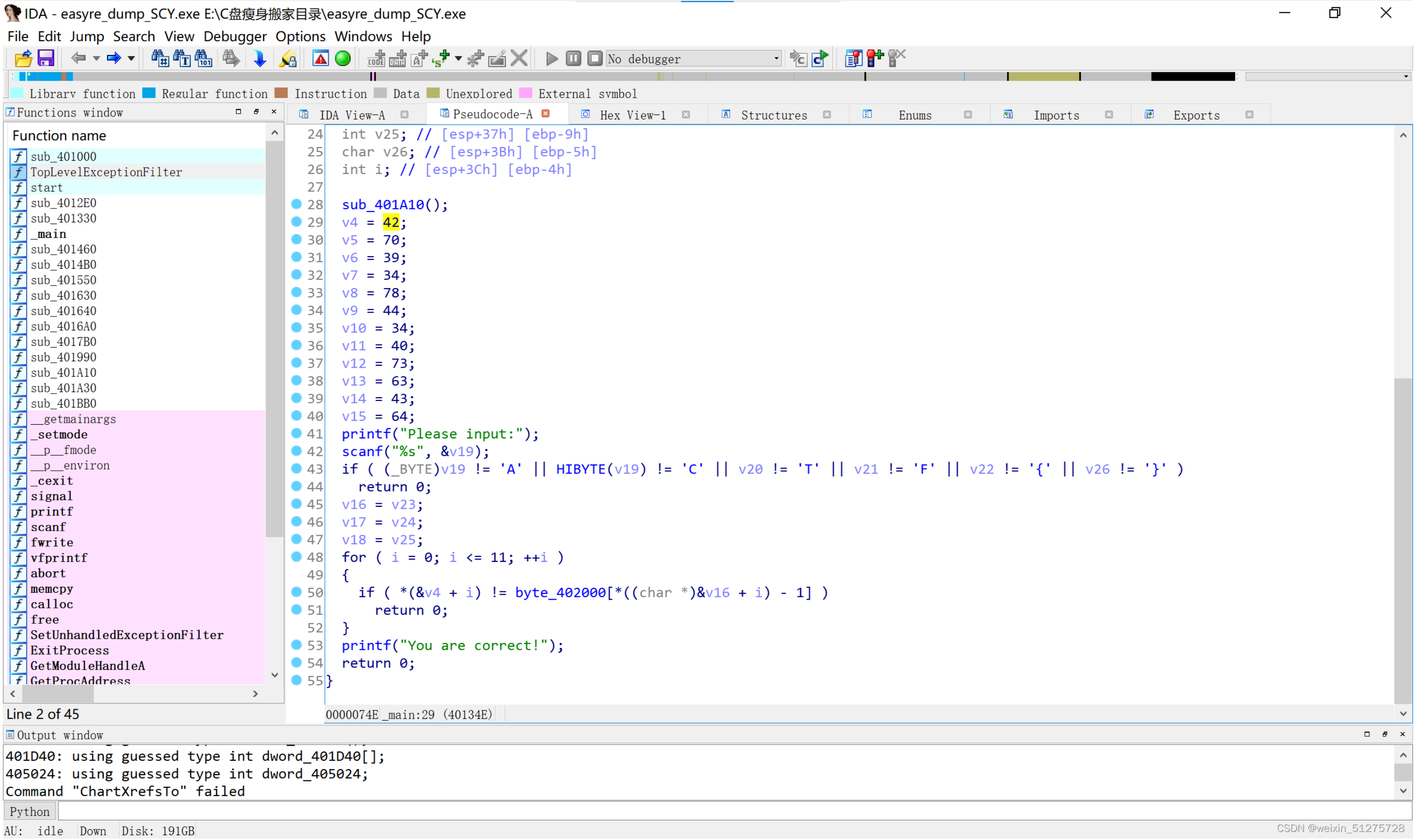

IDA - easyre_dump_SCY.exe E:\C盘瘦身搬家目录\easyre_dump_SCY.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
Function name
Line 2 of 45
Output window
Python
AU: idle Down Disk: 191GB

```
sub_401000
TopLevelExceptionFilter
start
sub_4012E0
sub_401330
_main
sub_401460
sub_4014B0
sub_401550
sub_401630
sub_401640
sub_4016A0
sub_4017B0
sub_401990
sub_401A10
sub_401A30
sub_401BB0
__getmainargs
_setmode
__p__fmode
__p__environ
_cexit
signal
printf
scanf
fwrite
vfprintf
abort
memcpy
calloc
free
SetUnhandledExceptionFilter
ExitProcess
GetModuleHandleA
GetProcAddress
```

```
UPX0:00401D38
UPX0:00401D38 ; ---------------------------------------------------------------------------
UPX0:00401D39                 align 10h
UPX0:00401D40 ; int dword_401D40[]
UPX0:00401D40 dword_401D40    dd 0FFFFFFFFh           ; DATA XREF: sub_401A10-4C↑r
UPX0:00401D40                                         ; sub_401A10:loc_4019D3↑r ...
UPX0:00401D44                 dd offset sub_401D20
UPX0:00401D48                 dd 0
UPX0:00401D4C                 dd 0FFFFFFFFh
UPX0:00401D50 dword_401D50    dd 0ACh dup(0)          ; DATA XREF: UPX0:off_402088↓o
UPX0:00402000 ; char byte_402000[]
UPX0:00402000 byte_402000     db 7Eh                  ; DATA XREF: _main+EC↑r
UPX0:00402001 aZyxwvutsrqponm db '}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>='
UPX0:00402001                 db '<;:9876543210/.-,+*)(',27h,'&%$# !"',0
UPX0:00402060                 align 40h
UPX0:00402080 dword_402080    dd 0FFFFFFFFh           ; DATA XREF: sub_401000+4A↑r
UPX0:00402084 dword_402084    dd 4000h                ; DATA XREF: sub_401000+86↑w
UPX0:00402084                                         ; sub_401000+C7↑r
UPX0:00402088 off_402088      dd offset dword_401D50  ; DATA XREF: sub_401990↑r
UPX0:00402088                                         ; sub_401990+12↑r ...
UPX0:0040208C dword_40208C    dd 0                    ; DATA XREF: sub_4012E0↑r
UPX0:0040208C                                         ; sub_4012E0+40↑o
UPX0:00402090                 align 1000h
UPX0:00403000 ; CHAR ModuleName[]
UPX0:00403000 ModuleName      db 'libgcj-13.dll',0    ; DATA XREF: sub_4012E0+F↑o
UPX0:0040300E ; CHAR ProcName[]
UPX0:0040300E ProcName        db '_Jv_RegisterClasses',0
UPX0:0040300E                                         ; DATA XREF: sub_4012E0+27↑o
UPX0:00403022                 align 4
UPX0:00403024 ; char aPleaseInput[]
UPX0:00403024 aPleaseInput    db 'Please input:',0    ; DATA XREF: _main+4A↑o
UPX0:00403032 ; char aS[]
```

00001401 00402001: UPX0:aZyxwvutsrqponm (Synchronized with Hex View-1)

```
401990: using guessed type int sub_401990();
401D40: using guessed type int dword_401D40[];
405024: using guessed type int dword_405024;
```


IDA - easyre_dump_SCY.exe E:\C盘瘦身搬家目录\easyre_dump_SCY.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
Function name
Line 2 of 45
Output window
Python
AU: idle Down Disk: 191GB

```
sub_401000
TopLevelExceptionFilter
start
sub_4012E0
sub_401330
_main
sub_401460
sub_4014B0
sub_401550
sub_401630
sub_401640
sub_4016A0
sub_4017B0
sub_401990
sub_401A10
sub_401A30
sub_401BB0
__getmainargs
_setmode
__p__fmode
__p__environ
_cexit
signal
printf
scanf
fwrite
vfprintf
abort
memcpy
calloc
free
SetUnhandledExceptionFilter
ExitProcess
GetModuleHandleA
GetProcAddress
```

```c
  int v25; // [esp+37h] [ebp-9h]
  char v26; // [esp+3Bh] [ebp-5h]
  int i; // [esp+3Ch] [ebp-4h]

  sub_401A10();
  v4 = 42;
  v5 = 70;
  v6 = 39;
  v7 = 34;
  v8 = 78;
  v9 = 44;
  v10 = 34;
  v11 = 40;
  v12 = 73;
  v13 = 63;
  v14 = 43;
  v15 = 64;
  printf("Please input:");
  scanf("%s", &v19);
  if ( (_BYTE)v19 != 'A' || HIBYTE(v19) != 'C' || v20 != 'T' || v21 != 'F' || v22 != '{' || v26 != '}' )
    return 0;
  v16 = v23;
  v17 = v24;
  v18 = v25;
  for ( i = 0; i <= 11; ++i )
  {
    if ( *(&v4 + i) != byte_402000[*((char *)&v16 + i) - 1] )
      return 0;
  }
  printf("You are correct!");
  return 0;
}
```

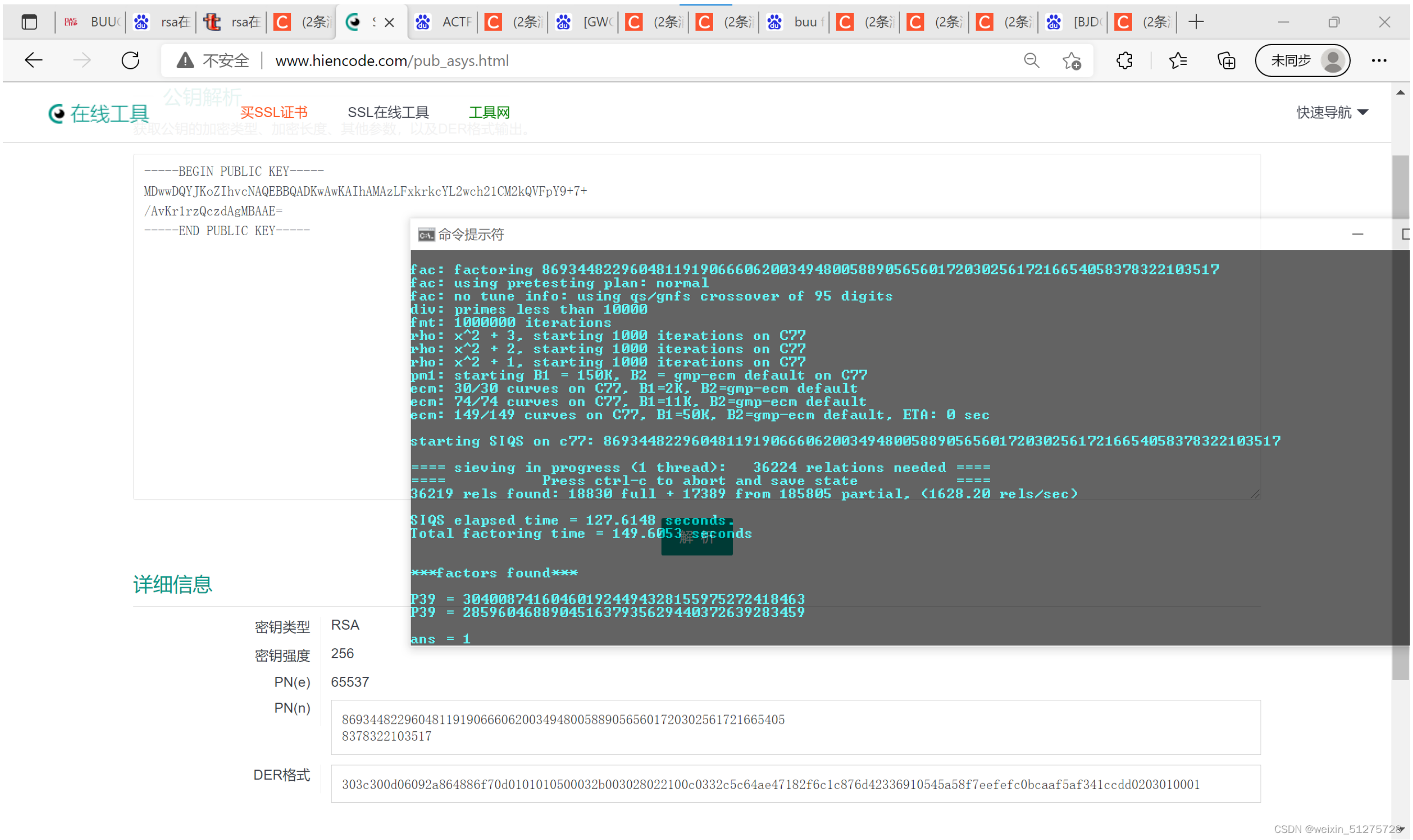
0000074E _main:29 (40134E)

```
401D40: using guessed type int dword_401D40[];
405024: using guessed type int dword_405024;
Command "ChartXrefsTo" failed
```

```
#include < iostream>
using namespace std;
int main(){
string p="~}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)('&%$# !\"";
 int v4 [12]={ 42,70,39,34,78,44,34,40,73,63,43,64};
 for(int i=0;i<12;i++)
{for(int j=0;j<p.length();j++){
 if(p[j]==v4[i]){
  char pp=j+2;
  cout<<pp;
  break;
 }}}}
```

## 19 rsa

## 19.Rsa算法



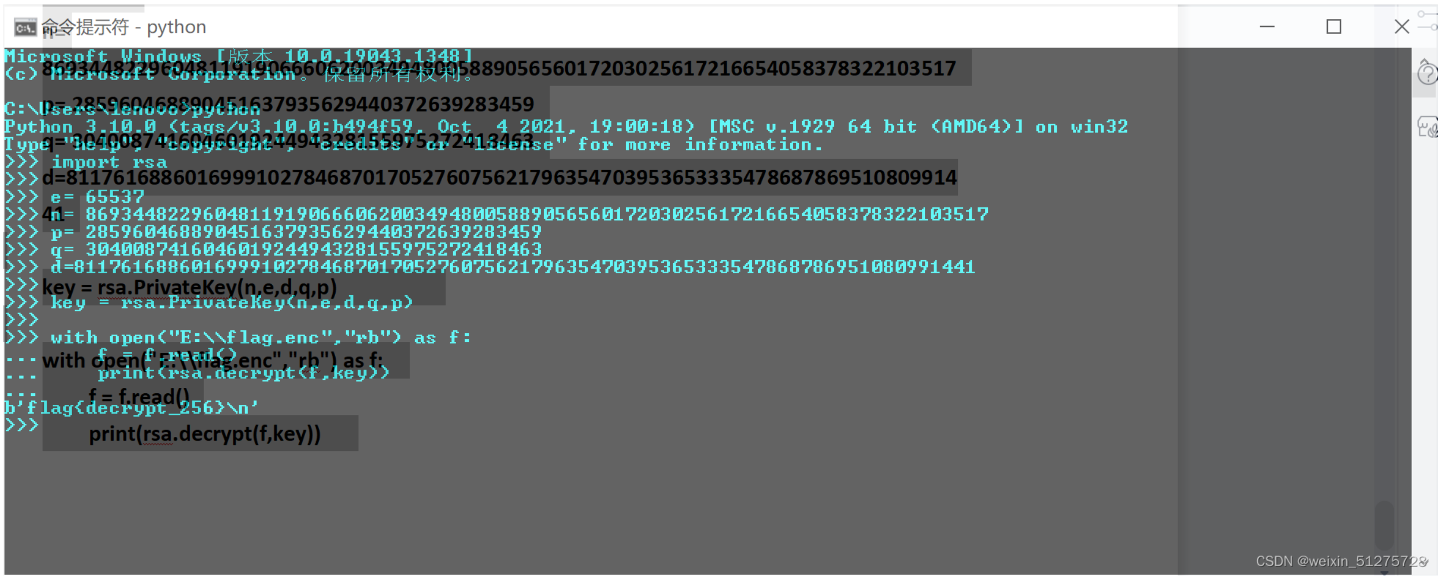
```
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFpY9+7+
/AvKr1rzQczdAgMBAAE=
-----END PUBLIC KEY-----
```

```
fac: factoring 86934482296048119190666062003494800588905656017203025617216654058378322103517
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits
div: primes less than 10000
fmt: 1000000 iterations
rho: x^2 + 3, starting 1000 iterations on C77
rho: x^2 + 2, starting 1000 iterations on C77
rho: x^2 + 1, starting 1000 iterations on C77
pm1: starting B1 = 150K, B2 = gmp-ecm default on C77
ecm: 30/30 curves on C77, B1=2K, B2=gmp-ecm default
ecm: 74/74 curves on C77, B1=11K, B2=gmp-ecm default
ecm: 149/149 curves on C77, B1=50K, B2=gmp-ecm default, ETA: 0 sec

starting SIQS on c77: 86934482296048119190666062003494800588905656017203025617216654058378322103517

==== sieving in progress (1 thread):   36224 relations needed ====
====           Press ctrl-c to abort and save state           ====
36219 rels found: 18830 full + 17389 from 185805 partial, (1628.20 rels/sec)

SIQS elapsed time = 127.6148 seconds.
Total factoring time = 149.6053 seconds


***factors found***

P39 = 304008741604601924494328155975272418463
P39 = 285960468890451637935629440372639283459

ans = 1
```

详细信息

| | |
|---|---|
| 密钥类型 | RSA |
| 密钥强度 | 256 |
| PN(e) | 65537 |
| PN(n) | 86934482296048119190666062003494800588905656017203025617216654058378322103517 |
| DER格式 | 303c300d06092a864886f70d0101010500032b003028022100c0332c5c64ae47182f6c1c876d42336910545a58f7eefefc0bcaaf5af341ccdd0203010001 |

CSDN @weixin_51275728



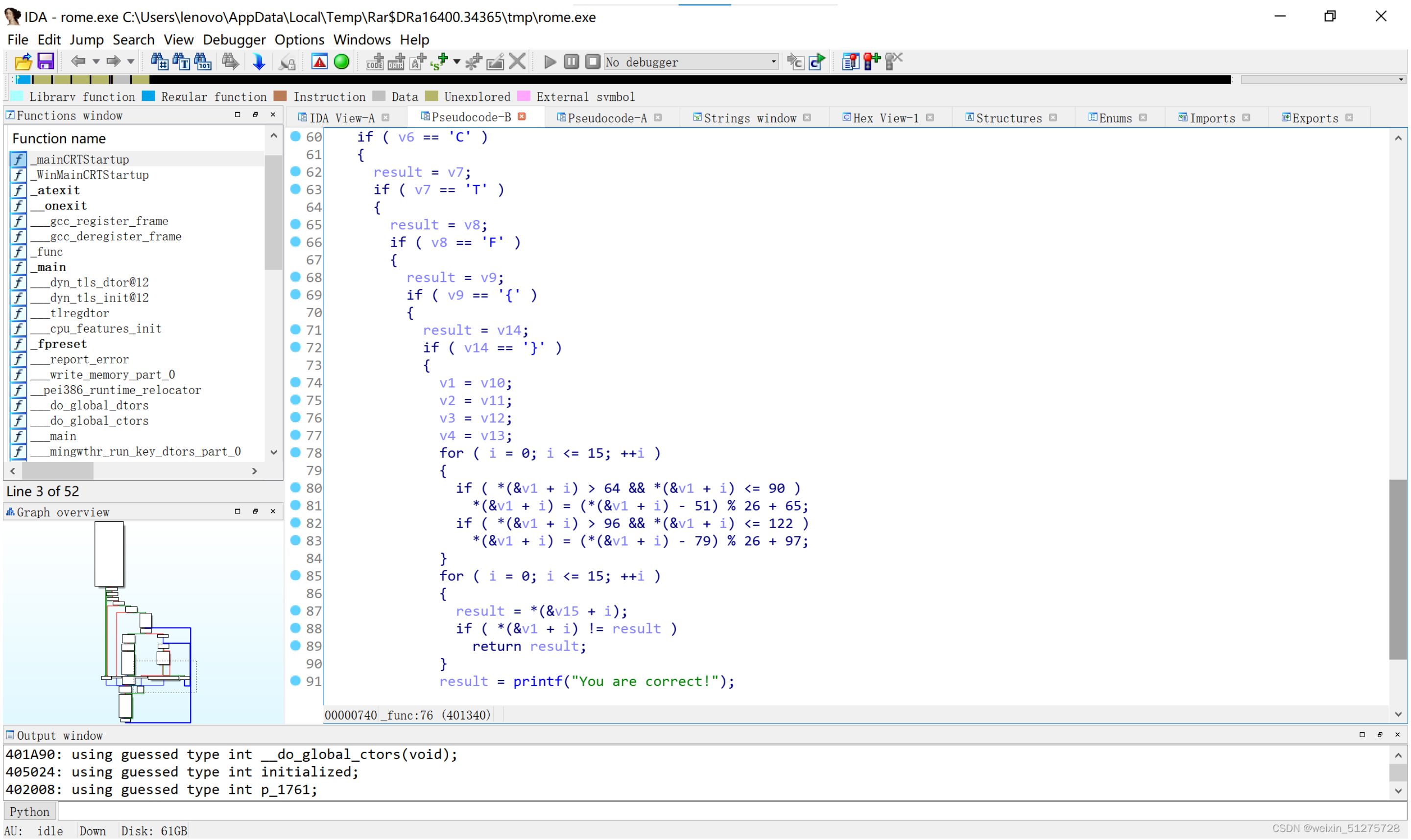
```
Microsoft Windows [版本 10.0.19043.1348]
(c) Microsoft Corporation。保留所有权利。

C:\Users\lenovo>python
Python 3.10.0 (tags/v3.10.0:b494f59, Oct  4 2021, 19:00:18) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import rsa
>>>
>>> e= 65537
>>> n= 86934482296048119190666062003494800588905656017203025617216654058378322103517
>>> p= 285960468890451637935629440372639283459
>>> q= 304008741604601924494328155975272418463
>>> d=81176168860169991027846870170527607562179635470395365333547868786951080991441
>>>
>>> key = rsa.PrivateKey(n,e,d,q,p)
>>>
>>> with open("E:\\flag.enc","rb") as f:
...     f = f.read()
...     print(rsa.decrypt(f,key))
...
b'flag{decrypt_256}\n'
>>>
```

CSDN @weixin_51275728

```
import rsa
e= 65537
n= 86934482296048119190666062003494800588905656017203025617216654058378322103517
p= 285960468890451637935629440372639283459
q= 304008741604601924494328155975272418463
d=81176168860169991027846870170527607562179635470395365333547868786951080991441

key = rsa.PrivateKey(n,e,d,q,p)

with open("E:\\flag.enc","rb") as f:
    f = f.read()
print(rsa.decrypt(f,key))
```

## 20 rome

20 rome



```
if ( v6 == 'C' )
{
  result = v7;
  if ( v7 == 'T' )
  {
    result = v8;
    if ( v8 == 'F' )
    {
      result = v9;
      if ( v9 == '{' )
      {
        result = v14;
        if ( v14 == '}' )
        {
          v1 = v10;
          v2 = v11;
          v3 = v12;
          v4 = v13;
          for ( i = 0; i <= 15; ++i )
          {
            if ( *(&v1 + i) > 64 && *(&v1 + i) <= 90 )
              *(&v1 + i) = (*(&v1 + i) - 51) % 26 + 65;
            if ( *(&v1 + i) > 96 && *(&v1 + i) <= 122 )
              *(&v1 + i) = (*(&v1 + i) - 79) % 26 + 97;
          }
          for ( i = 0; i <= 15; ++i )
          {
            result = *(&v15 + i);
            if ( *(&v1 + i) != result )
              return result;
          }
          result = printf("You are correct!");
```

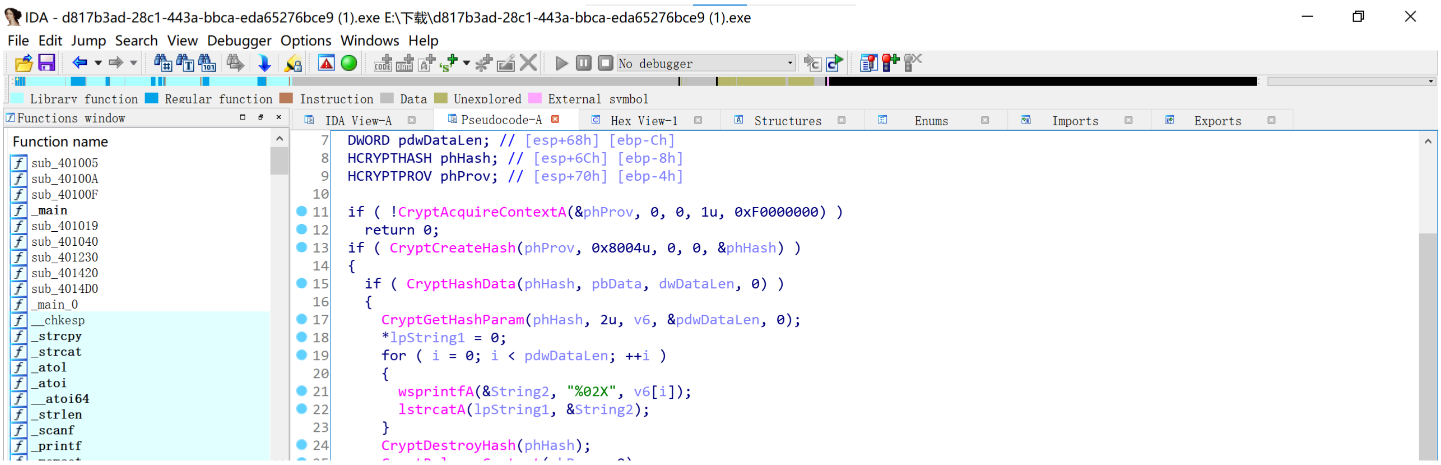
```
00000740 _func:76 (401340)
```

```
401A90: using guessed type int __do_global_ctors(void);
405024: using guessed type int initialized;
402008: using guessed type int p_1761;
```

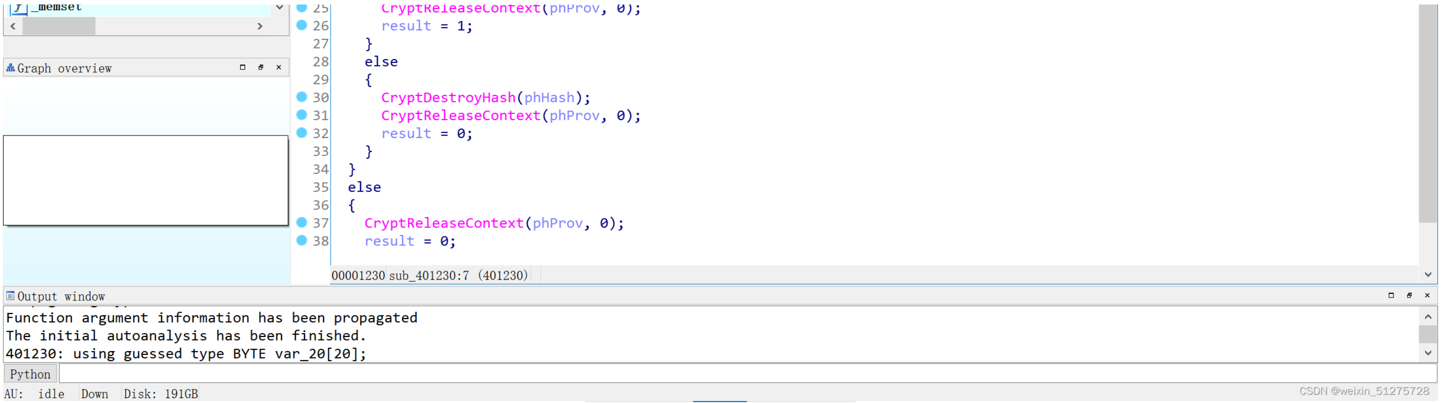
```
#include < iostream>
using namespace std;
int main(){
 int v15[16]={81,115,119,51,115,106,95,108,122,52,95,85,106,119,64,108};
 for(int i=0;i<=15;i++){
 for(int j=1;j<128;j++){
  int k=j;
 if ( j> 64 && j <= 90 )
 k = (k - 51) % 26 + 65;
if ( j > 96 && j <= 122 )
 k = (k - 79) % 26 + 97;
 if(k==v15[i]) {
  char p=j;
  cout<<p;
  break;
 }}}}
```

# 21 crackrtf

21 crackrtf cryptcreatehash 上网查其参数的含义



```
DWORD pdwDataLen; // [esp+68h] [ebp-Ch]
HCRYPTHASH phHash; // [esp+6Ch] [ebp-8h]
HCRYPTPROV phProv; // [esp+70h] [ebp-4h]

if ( !CryptAcquireContextA(&phProv, 0, 0, 1u, 0xF0000000) )
  return 0;
if ( CryptCreateHash(phProv, 0x8004u, 0, 0, &phHash) )
{
  if ( CryptHashData(phHash, pbData, dwDataLen, 0) )
  {
    CryptGetHashParam(phHash, 2u, v6, &pdwDataLen, 0);
    *lpString1 = 0;
    for ( i = 0; i < pdwDataLen; ++i )
    {
      wsprintfA(&String2, "%02X", v6[i]);
      lstrcatA(lpString1, &String2);
    }
    CryptDestroyHash(phHash);
```

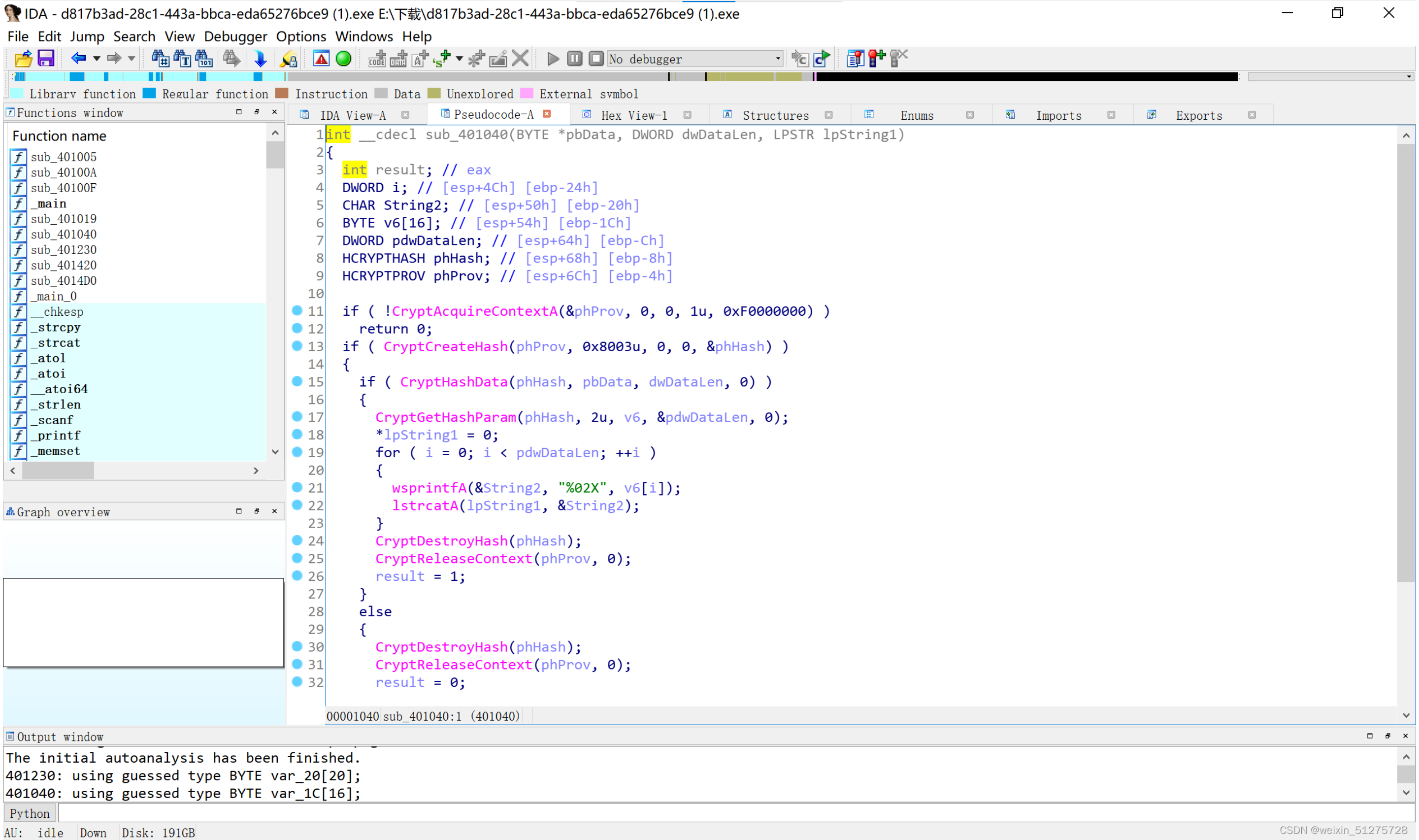


```
      CryptReleaseContext(phProv, 0);
      result = 1;
    }
    else
    {
      CryptDestroyHash(phHash);
      CryptReleaseContext(phProv, 0);
      result = 0;
    }
  }
  else
  {
    CryptReleaseContext(phProv, 0);
    result = 0;
```

```
00001230 sub_401230:7 (401230)
```

```
Function argument information has been propagated
The initial autoanalysis has been finished.
401230: using guessed type BYTE var_20[20];
```

```
AU:  idle   Down   Disk: 191GB
```

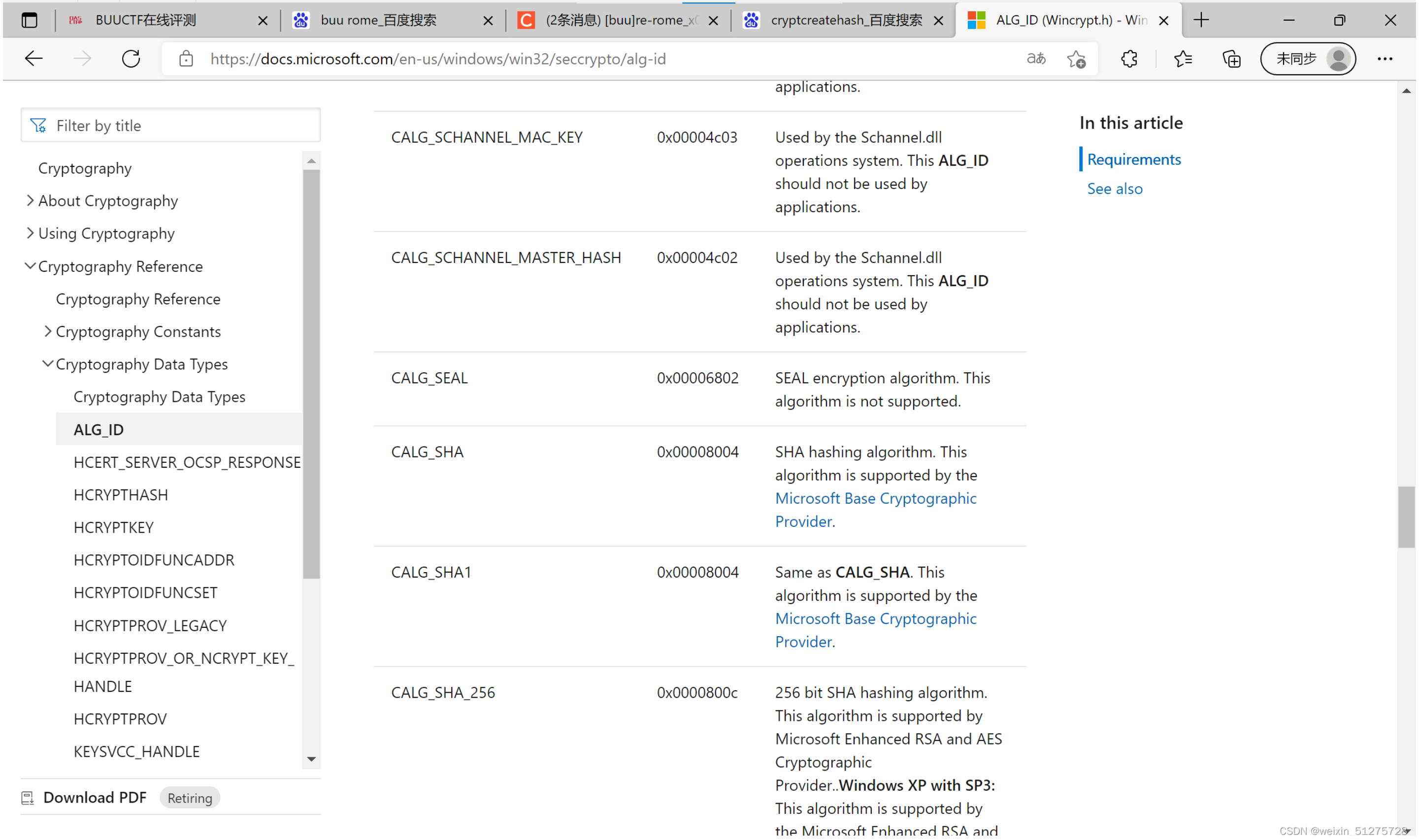


```
int __cdecl sub_401040(BYTE *pbData, DWORD dwDataLen, LPSTR lpString1)
{
  int result; // eax
  DWORD i; // [esp+4Ch] [ebp-24h]
  CHAR String2; // [esp+50h] [ebp-20h]
  BYTE v6[16]; // [esp+54h] [ebp-1Ch]
  DWORD pdwDataLen; // [esp+64h] [ebp-Ch]
  HCRYPTHASH phHash; // [esp+68h] [ebp-8h]
  HCRYPTPROV phProv; // [esp+6Ch] [ebp-4h]

  if ( !CryptAcquireContextA(&phProv, 0, 0, 1u, 0xF0000000) )
    return 0;
  if ( CryptCreateHash(phProv, 0x8003u, 0, 0, &phHash) )
  {
    if ( CryptHashData(phHash, pbData, dwDataLen, 0) )
    {
      CryptGetHashParam(phHash, 2u, v6, &pdwDataLen, 0);
      *lpString1 = 0;
      for ( i = 0; i < pdwDataLen; ++i )
      {
        wsprintfA(&String2, "%02X", v6[i]);
        lstrcatA(lpString1, &String2);
      }
      CryptDestroyHash(phHash);
      CryptReleaseContext(phProv, 0);
      result = 1;
    }
    else
    {
      CryptDestroyHash(phHash);
      CryptReleaseContext(phProv, 0);
      result = 0;
```

```
00001040 sub_401040:1 (401040)
```

```
The initial autoanalysis has been finished.
401230: using guessed type BYTE var_20[20];
401040: using guessed type BYTE var_1C[16];
```

```
AU:  idle   Down   Disk: 191GB
```



applications.

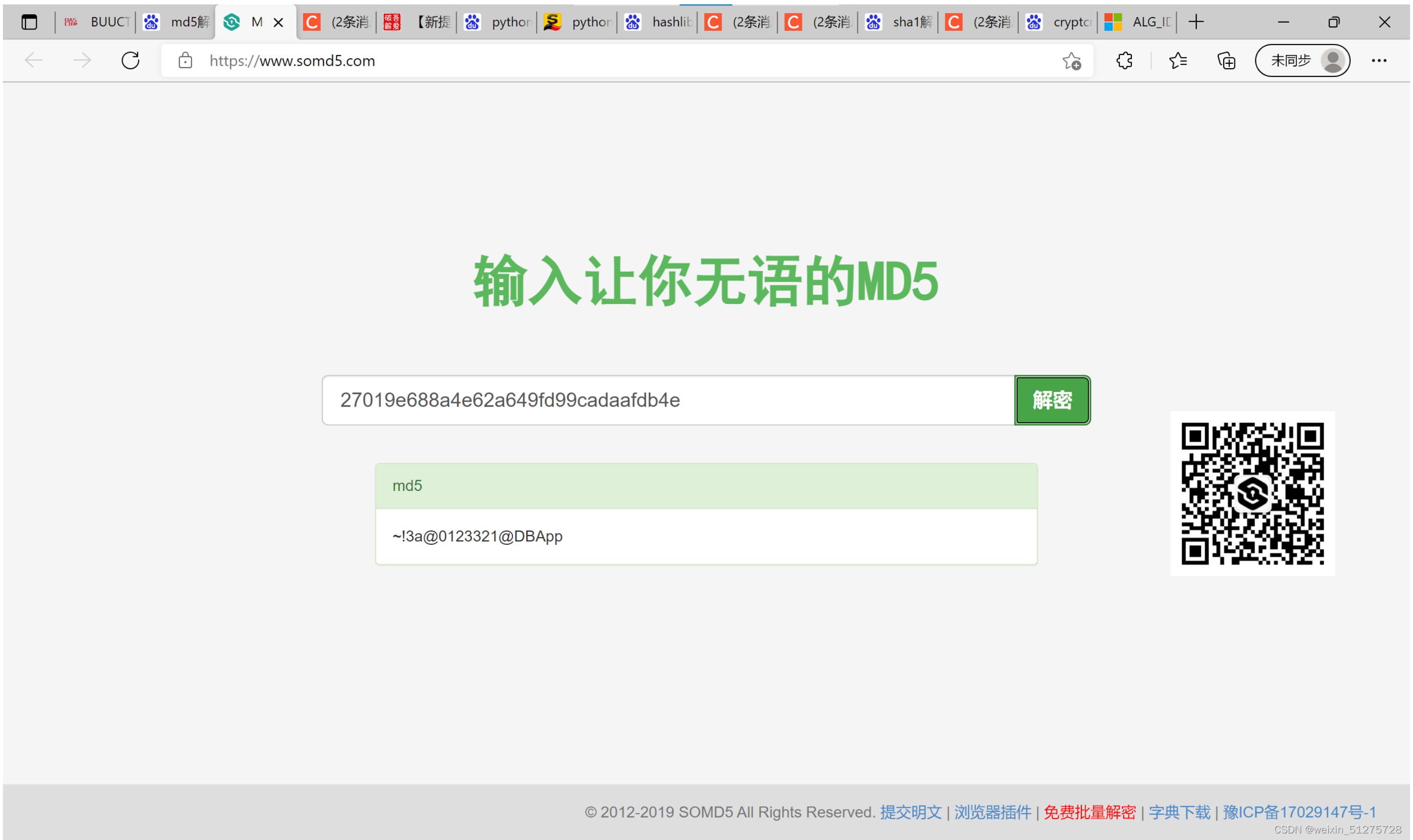
| | | |
|---|---|---|
| CALG_SCHANNEL_MAC_KEY | 0x00004c03 | Used by the Schannel.dll operations system. This **ALG_ID** should not be used by applications. |
| CALG_SCHANNEL_MASTER_HASH | 0x00004c02 | Used by the Schannel.dll operations system. This **ALG_ID** should not be used by applications. |
| CALG_SEAL | 0x00006802 | SEAL encryption algorithm. This algorithm is not supported. |
| CALG_SHA | 0x00008004 | SHA hashing algorithm. This algorithm is supported by the Microsoft Base Cryptographic Provider. |
| CALG_SHA1 | 0x00008004 | Same as **CALG_SHA**. This algorithm is supported by the Microsoft Base Cryptographic Provider. |
| CALG_SHA_256 | 0x0000800c | 256 bit SHA hashing algorithm. This algorithm is supported by Microsoft Enhanced RSA and AES Cryptographic Provider..**Windows XP with SP3:** This algorithm is supported by the Microsoft Enhanced RSA and |

the Microsoft Enhanced RSA and

这个代码在网上找的，有点问题

```
import hashlib
flags = "@DBApp"
h2=""
for i in range(100000,999999):
    h2 = hashlib.sha1((str(i)+flags).encode())
    flags = h2.hexdigest()
    if "6e32d0943418c2c33385bc35a1470250dd8923a9" == flags:
            print (str(i)+flags)
            print (i)
```

也可以在网上找sha1破解
就算不行也没关系的，看，直接就出两步的结果



输入让你无语的MD5

27019e688a4e62a649fd99cadaafdb4e

md5

~!3a@0123321@DBApp

© 2012-2019 SOMD5 All Rights Reserved. 提交明文 | 浏览器插件 | 免费批量解密 | 字典下载 | 豫ICP备17029147号-1

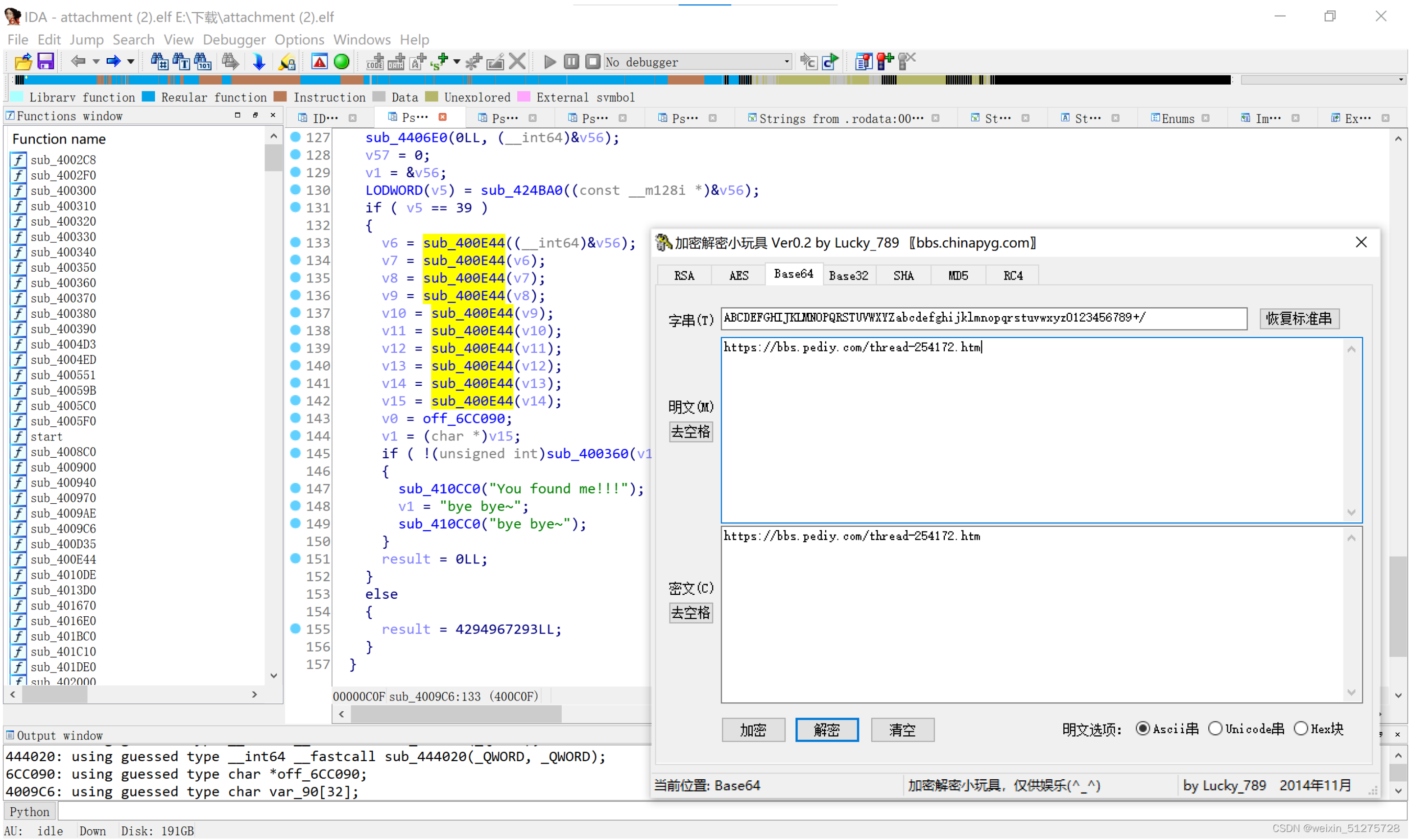
CSDN @weixin_51275728

有个AAA文件，并且要进行异或操作，但不知道怎么异或

但是一看自己目录，有rtf文件了，打开就有flag ,感情是白忙了一小时！淦！看别人writeup
这里是文件前五个字符与头部指针{\rtfl异或，答案与第二个字符串相同。

## 22 easyre

## 22 easyre base64 10次 发现被坑了



```
  sub_4406E0(0LL, (__int64)&v56);
  v57 = 0;
  v1 = &v56;
  LODWORD(v5) = sub_424BA0((const __m128i *)&v56);
  if ( v5 == 39 )
  {
    v6 = sub_400E44((__int64)&v56);
    v7 = sub_400E44(v6);
    v8 = sub_400E44(v7);
    v9 = sub_400E44(v8);
    v10 = sub_400E44(v9);
    v11 = sub_400E44(v10);
    v12 = sub_400E44(v11);
    v13 = sub_400E44(v12);
    v14 = sub_400E44(v13);
    v15 = sub_400E44(v14);
    v0 = off_6CC090;
    v1 = (char *)v15;
    if ( !(unsigned int)sub_400360(v1
    {
      sub_410CC0("You found me!!!");
      v1 = "bye bye~";
      sub_410CC0("bye bye~");
    }
    result = 0LL;
  }
  else
  {
    result = 4294967293LL;
  }
}
```

00000C0F sub_4009C6:133 (400C0F)

```
444020: using guessed type __int64 __fastcall sub_444020(_QWORD, _QWORD);
6CC090: using guessed type char *off_6CC090;
4009C6: using guessed type char var_90[32];
```

加密解密小玩具 Ver0.2 by Lucky_789 〖bbs.chinapyg.com〗

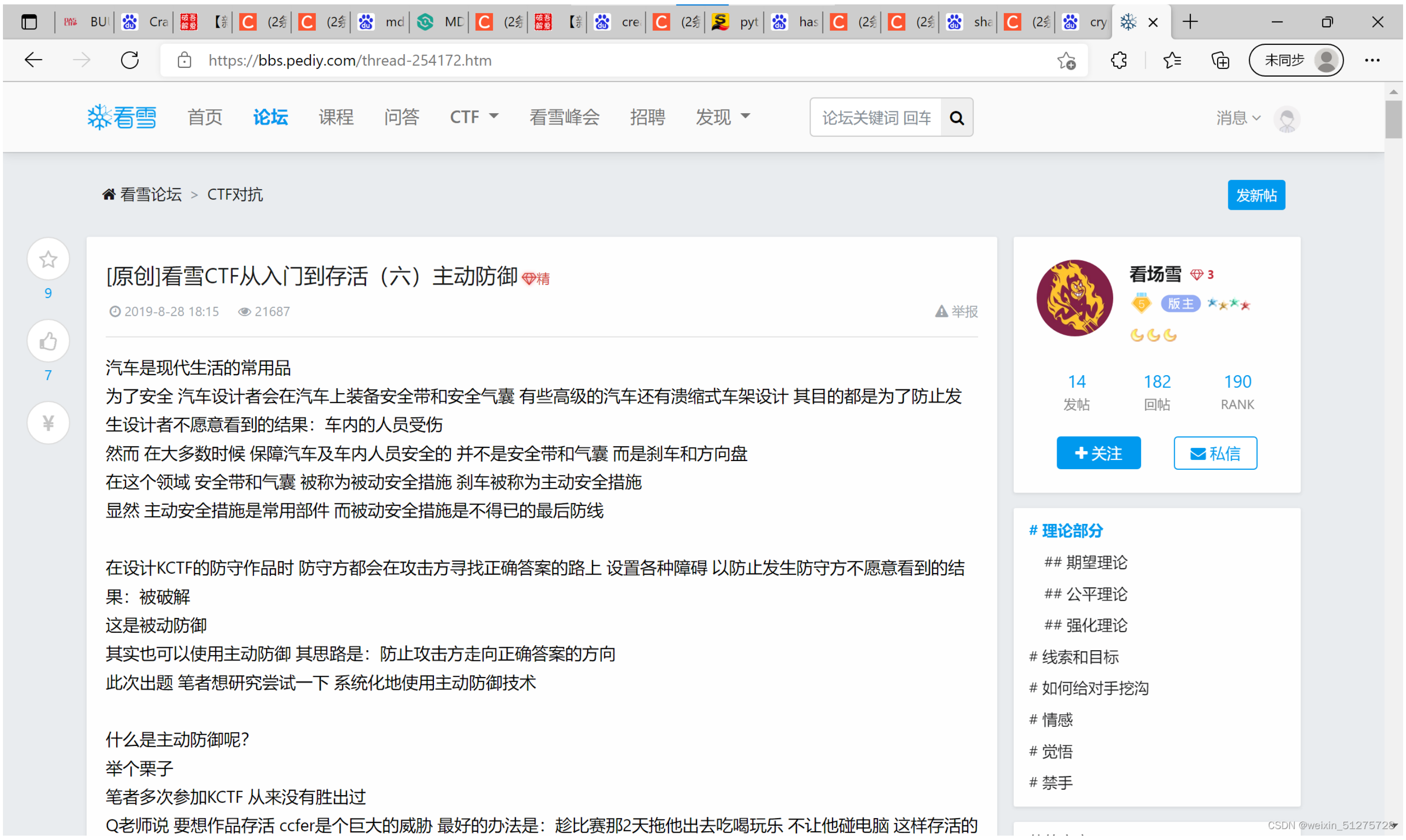
字串(T) ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

明文(M) https://bbs.pediy.com/thread-254172.htm

密文(C) https://bbs.pediy.com/thread-254172.htm

明文选项: ● Ascii串 ○ Unicode串 ○ Hex块

当前位置: Base64 加密解密小玩具，仅供娱乐(^_^) by Lucky_789 2014年11月



https://bbs.pediy.com/thread-254172.htm

看雪论坛 > CTF对抗

[原创]看雪CTF从入门到存活（六）主动防御

2019-8-28 18:15 21687

汽车是现代生活的常用品
为了安全 汽车设计者会在汽车上装备安全带和安全气囊 有些高级的汽车还有溃缩式车架设计 其目的都是为了防止发生设计者不愿意看到的结果：车内的人员受伤
然而 在大多数时候 保障汽车及车内人员安全的 并不是安全带和气囊 而是刹车和方向盘
在这个领域 安全带和气囊 被称为被动安全措施 刹车被称为主动安全措施
显然 主动安全措施是常用部件 而被动安全措施是不得已的最后防线

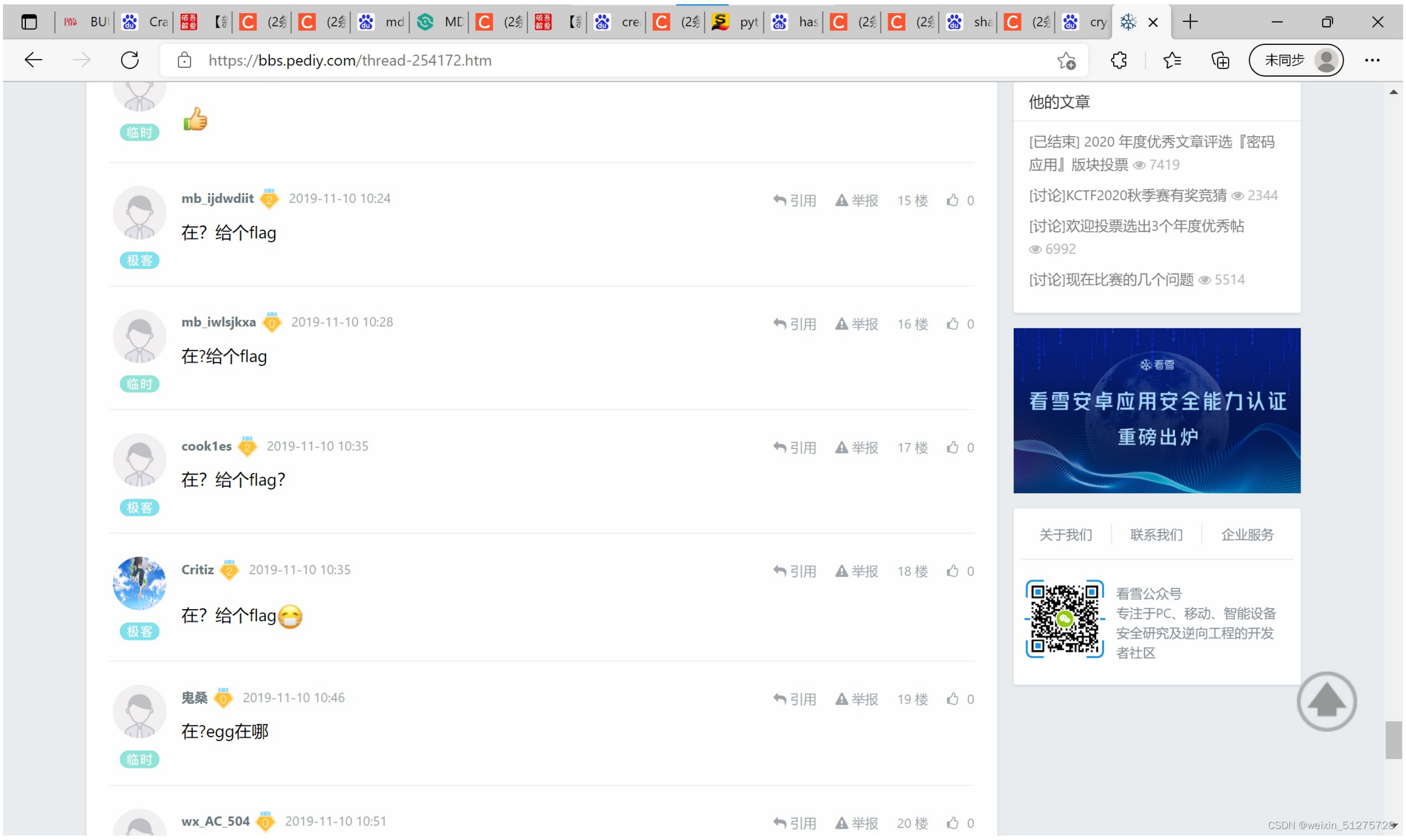
在设计KCTF的防守作品时 防守方都会在攻击方寻找正确答案的路上 设置各种障碍 以防止发生防守方不愿意看到的结果：被破解
这是被动防御
其实也可以使用主动防御 其思路是：防止攻击方走向正确答案的方向
此次出题 笔者想研究尝试一下 系统化地使用主动防御技术

什么是主动防御呢?
举个栗子
笔者多次参加KCTF 从来没有胜出过
Q老师说 要想作品存活 ccfer是个巨大的威胁 最好的办法是：趁比赛那2天拖他出去吃喝玩乐 不让他碰电脑 这样存活的

看场雪 3
版主
14 发帖
182 回帖
190 RANK

# 理论部分
## 期望理论
## 公平理论
## 强化理论
# 线索和目标
# 如何给对手挖沟
# 情感
# 觉悟
# 禁手

一般你做题得到看到这篇帖子的网址时候，你就被坑了，你看那清一色的评论



临时

mb_ijdwdiit 2019-11-10 10:24 引用 举报 15 楼 0

在？给个flag

极客

mb_iwlsjkxa 2019-11-10 10:28 引用 举报 16 楼 0

在?给个flag

临时

cook1es 2019-11-10 10:35 引用 举报 17 楼 0

在？给个flag?

极客

Critiz 2019-11-10 10:35 引用 举报 18 楼 0

在？给个flag

极客

鬼桑 2019-11-10 10:46 引用 举报 19 楼 0

在?egg在哪

临时

wx_AC_504 2019-11-10 10:51 引用 举报 20 楼 0

他的文章

[已结束] 2020 年度优秀文章评选『密码应用』版块投票 7419

[讨论]KCTF2020秋季赛有奖竞猜 2344

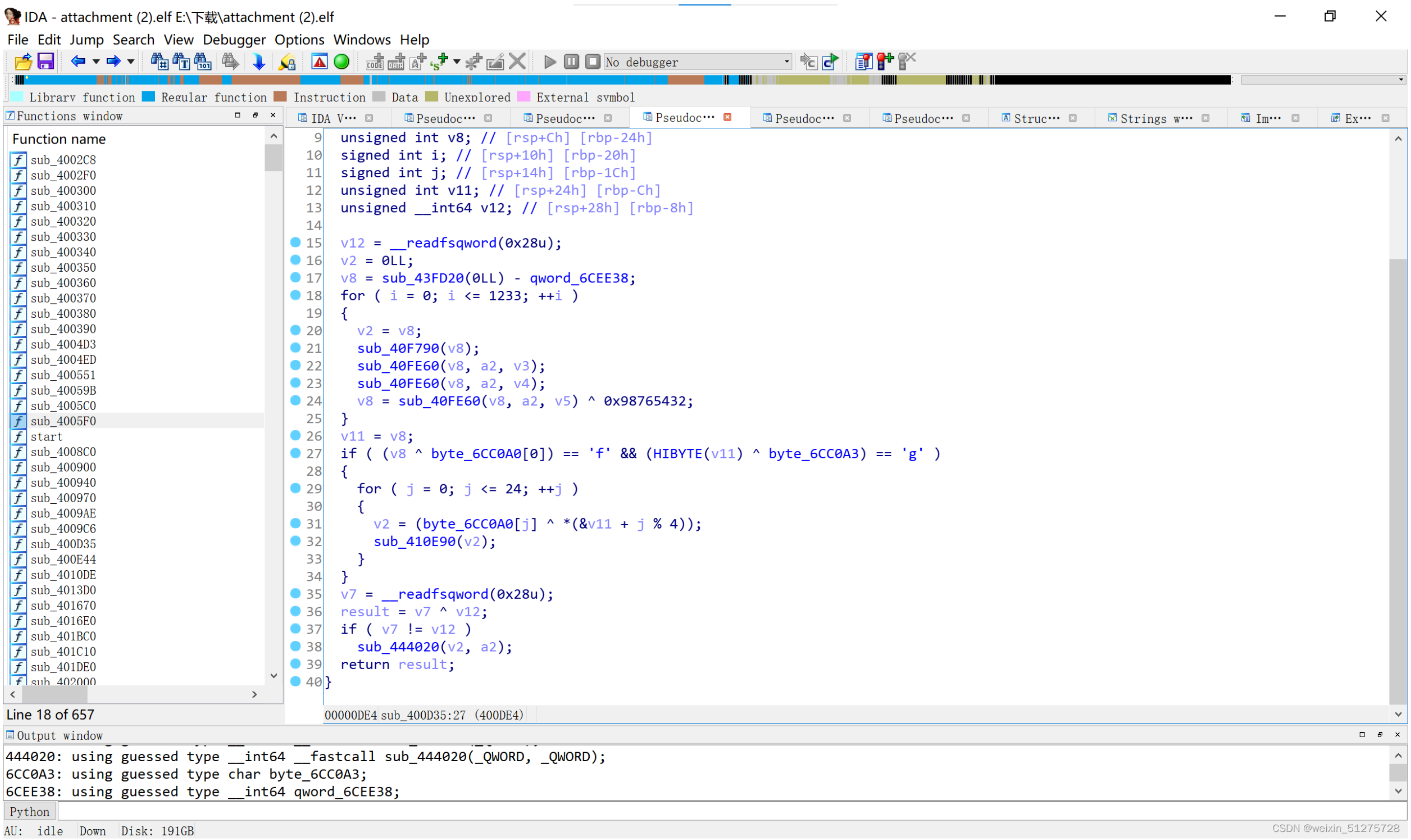
[讨论]欢迎投票选出3个年度优秀帖 6992

[讨论]现在比赛的几个问题 5514

关于我们 联系我们 企业服务

看雪公众号
专注于PC、移动、智能设备安全研究及逆向工程的开发者社区

下面也什么都没有了，看fini_array，指向三个函数，第二个有价值。



```
sub_4002C8
sub_4002F0
sub_400300
sub_400310
sub_400320
sub_400330
sub_400340
sub_400350
sub_400360
sub_400370
sub_400380
sub_400390
sub_4004D3
sub_4004ED
sub_400551
sub_40059B
sub_4005C0
sub_4005F0
start
sub_4008C0
sub_400900
sub_400940
sub_400970
sub_4009AE
sub_4009C6
sub_400D35
sub_400E44
sub_4010DE
sub_4013D0
sub_401670
sub_4016E0
sub_401BC0
sub_401C10
sub_401DE0
sub_402000
```

Line 18 of 657

```c
  unsigned int v8; // [rsp+Ch] [rbp-24h]
  signed int i; // [rsp+10h] [rbp-20h]
  signed int j; // [rsp+14h] [rbp-1Ch]
  unsigned int v11; // [rsp+24h] [rbp-Ch]
  unsigned __int64 v12; // [rsp+28h] [rbp-8h]

  v12 = __readfsqword(0x28u);
  v2 = 0LL;
  v8 = sub_43FD20(0LL) - qword_6CEE38;
  for ( i = 0; i <= 1233; ++i )
  {
    v2 = v8;
    sub_40F790(v8);
    sub_40FE60(v8, a2, v3);
    sub_40FE60(v8, a2, v4);
    v8 = sub_40FE60(v8, a2, v5) ^ 0x98765432;
  }
  v11 = v8;
  if ( (v8 ^ byte_6CC0A0[0]) == 'f' && (HIBYTE(v11) ^ byte_6CC0A3) == 'g' )
  {
    for ( j = 0; j <= 24; ++j )
    {
      v2 = (byte_6CC0A0[j] ^ *(&v11 + j % 4));
      sub_410E90(v2);
    }
  }
  v7 = __readfsqword(0x28u);
  result = v7 ^ v12;
  if ( v7 != v12 )
    sub_444020(v2, a2);
  return result;
}
```

00000DE4 sub_400D35:27 (400DE4)

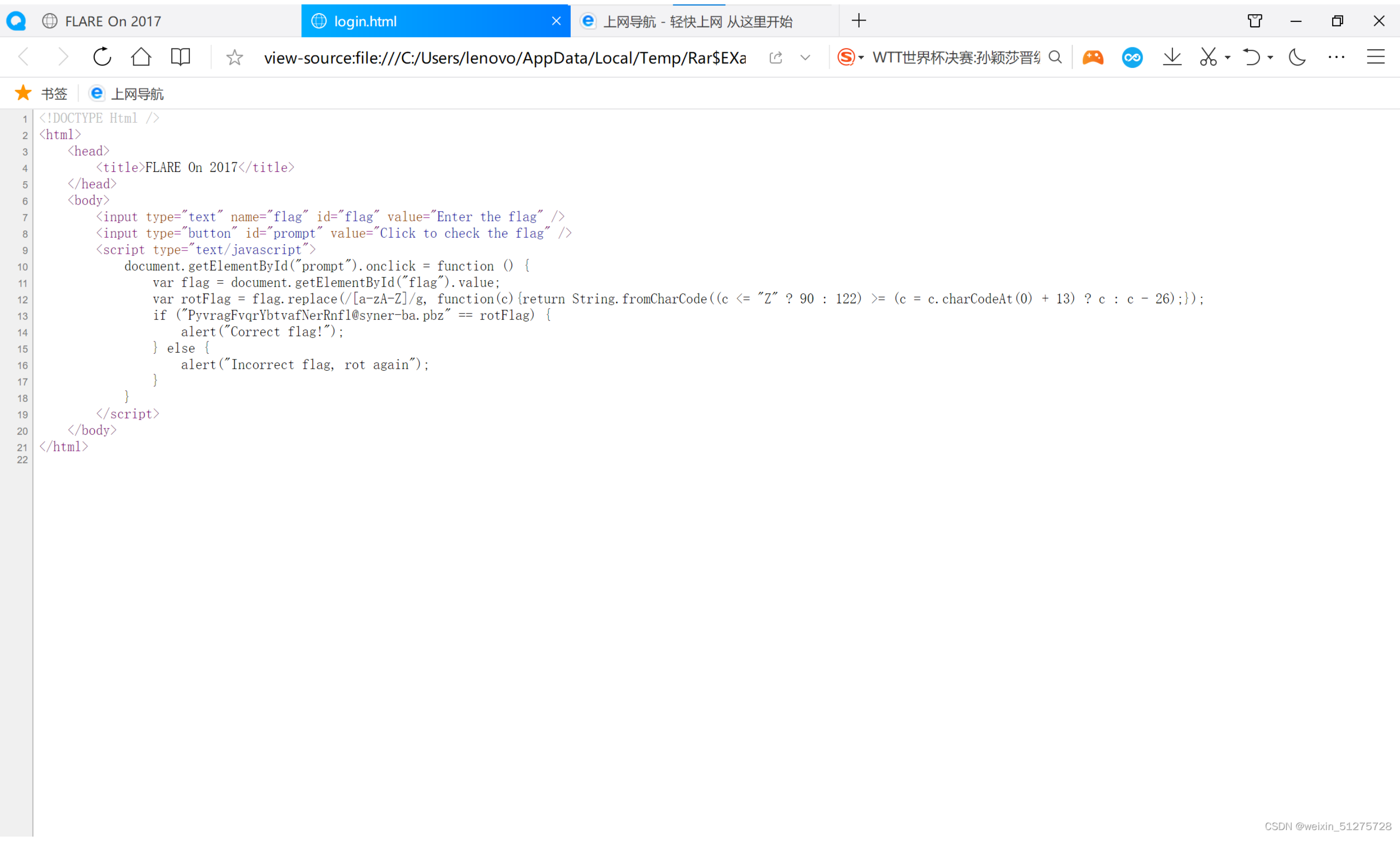
```
444020: using guessed type __int64 __fastcall sub_444020(_QWORD, _QWORD);
6CC0A3: using guessed type char byte_6CC0A3;
6CEE38: using guessed type __int64 qword_6CEE38;
```

AU: idle Down Disk: 191GB

```
#include < iostream>
using namespace std;
int main(){
int v17[]={73,111,100,108,62,81,110,98,40,111,99,121,127,121,46,105,127,100,96,51,119,125,119,101,107,57,123,105
,121,61,126,121,76,64,69,67};
for(int i=0;i<=35;i++)
 {v17[i]^=i;
 char p=v17[i];
 cout<<p;
 }
 cout<<endl;
unsigned char ida_chars[] =
{
  0x40, 0x35, 0x20, 0x56, 0x5D, 0x18, 0x22, 0x45, 0x17, 0x2F,
  0x24, 0x6E, 0x62, 0x3C, 0x27, 0x54, 0x48, 0x6C, 0x24, 0x6E,
  0x72, 0x3C, 0x32, 0x45, 0x5B
}; string f="flag";
for(int i=0;i<4;i++){
 f[i]^=ida_chars[i];
}
 for(int i=0;i<25;i++){
  ida_chars[i]^=f[i%4];
  cout<<ida_chars[i];
 }
}
```

## 23 login

23 login 感觉是web题，结果是披着web外套的re


FLARE On 2017
login.html
上网导航 - 轻快上网 从这里开始
view-source:file:///C:/Users/lenovo/AppData/Local/Temp/Rar$EXa
WTT世界杯决赛:孙颖莎晋级
书签
上网导航

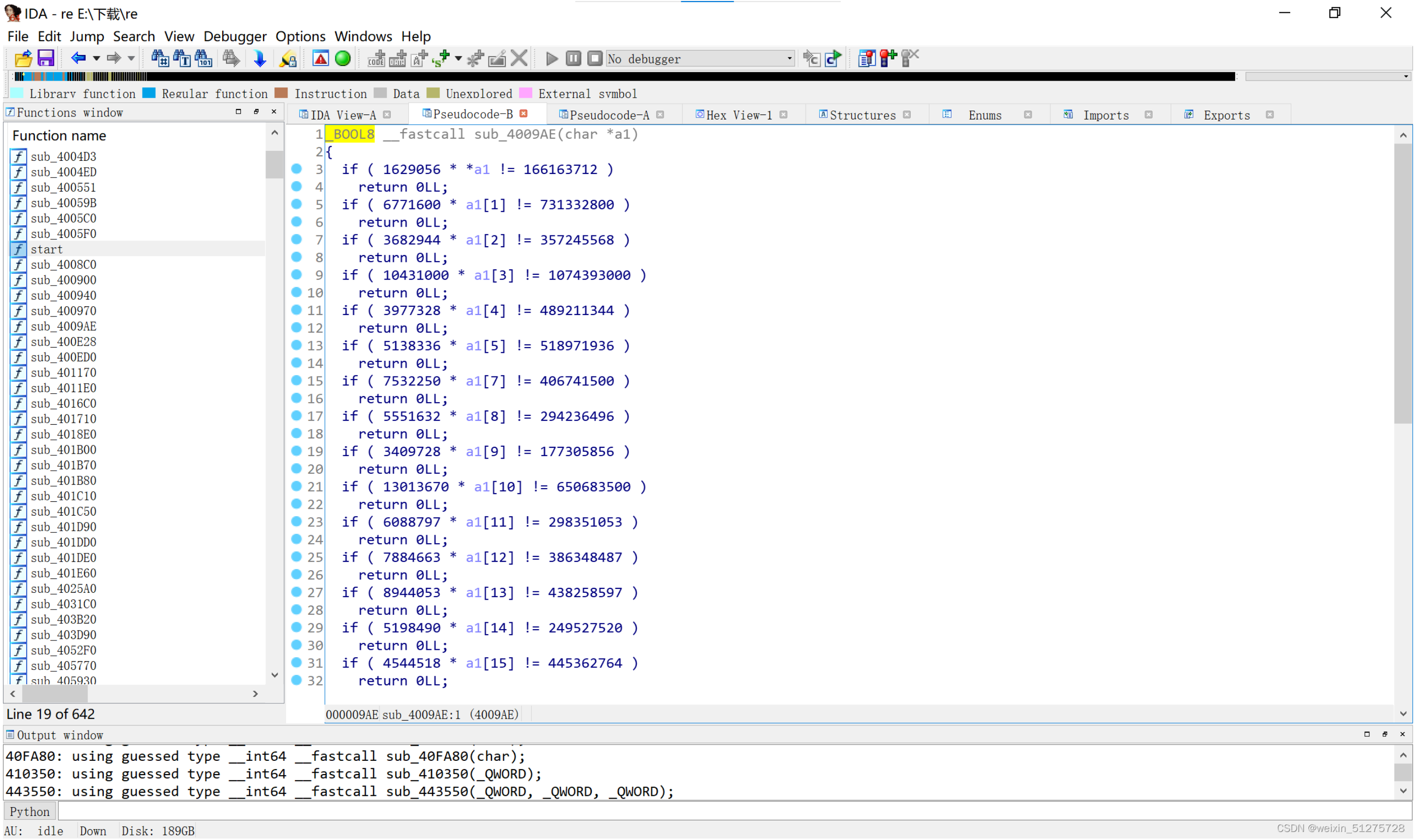
```
<!DOCTYPE Html />
<html>
    <head>
        <title>FLARE On 2017</title>
    </head>
    <body>
        <input type="text" name="flag" id="flag" value="Enter the flag" />
        <input type="button" id="prompt" value="Click to check the flag" />
        <script type="text/javascript">
            document.getElementById("prompt").onclick = function () {
                var flag = document.getElementById("flag").value;
                var rotFlag = flag.replace(/[a-zA-Z]/g, function(c){return String.fromCharCode((c <= "Z" ? 90 : 122) >= (c = c.charCodeAt(0) + 13) ? c : c - 26);});
                if ("PyvragFvqrYbtvafNerRnfl@syner-ba.pbz" == rotFlag) {
                    alert("Correct flag!");
                } else {
                    alert("Incorrect flag, rot again");
                }
            }
        </script>
    </body>
</html>
```

```
#include < iostream>
using namespace std;
int main(){
 string p="PyvragFvqrYbtvafNerRnfl@syner-ba.pbz";
 for(int i=0;i<p.length();i++){
  if(p[i]>='a'&&p[i]<='z'){
   if(p[i]-13<97)
   p[i]+=13;
   else p[i]-=13;
  }
  else if(p[i]>='A'&&p[i]<='Z'){
   if(p[i]-13<65)
   p[i]+=13;
   else p[i]-=13;
  }
  cout<<p[i]; }
}
```

## 24 re

24 re 在kali虚拟机中脱壳，upx -d 文件名 然后进ida(不知道怎么把虚拟机中的文件传到电脑上，就用在虚拟机上用qq小号以邮箱途径发给大号，正确用法是用ubantu，但有点复杂，不想搞)

解密



```
sub_4004D3
sub_4004ED
sub_400551
sub_40059B
sub_4005C0
sub_4005F0
start
sub_4008C0
sub_400900
sub_400940
sub_400970
sub_4009AE
sub_400E28
sub_400ED0
sub_401170
sub_4011E0
sub_4016C0
sub_401710
sub_4018E0
sub_401B00
sub_401B70
sub_401B80
sub_401C10
sub_401C50
sub_401D90
sub_401DD0
sub_401DE0
sub_401E60
sub_4025A0
sub_4031C0
sub_403B20
sub_403D90
sub_4052F0
sub_405770
sub_405930
```

```
_BOOL8 __fastcall sub_4009AE(char *a1)
{
  if ( 1629056 * *a1 != 166163712 )
    return 0LL;
  if ( 6771600 * a1[1] != 731332800 )
    return 0LL;
  if ( 3682944 * a1[2] != 357245568 )
    return 0LL;
  if ( 10431000 * a1[3] != 1074393000 )
    return 0LL;
  if ( 3977328 * a1[4] != 489211344 )
    return 0LL;
  if ( 5138336 * a1[5] != 518971936 )
    return 0LL;
  if ( 7532250 * a1[7] != 406741500 )
    return 0LL;
  if ( 5551632 * a1[8] != 294236496 )
    return 0LL;
  if ( 3409728 * a1[9] != 177305856 )
    return 0LL;
  if ( 13013670 * a1[10] != 650683500 )
    return 0LL;
  if ( 6088797 * a1[11] != 298351053 )
    return 0LL;
  if ( 7884663 * a1[12] != 386348487 )
    return 0LL;
  if ( 8944053 * a1[13] != 438258597 )
    return 0LL;
  if ( 5198490 * a1[14] != 249527520 )
    return 0LL;
  if ( 4544518 * a1[15] != 445362764 )
    return 0LL;
```

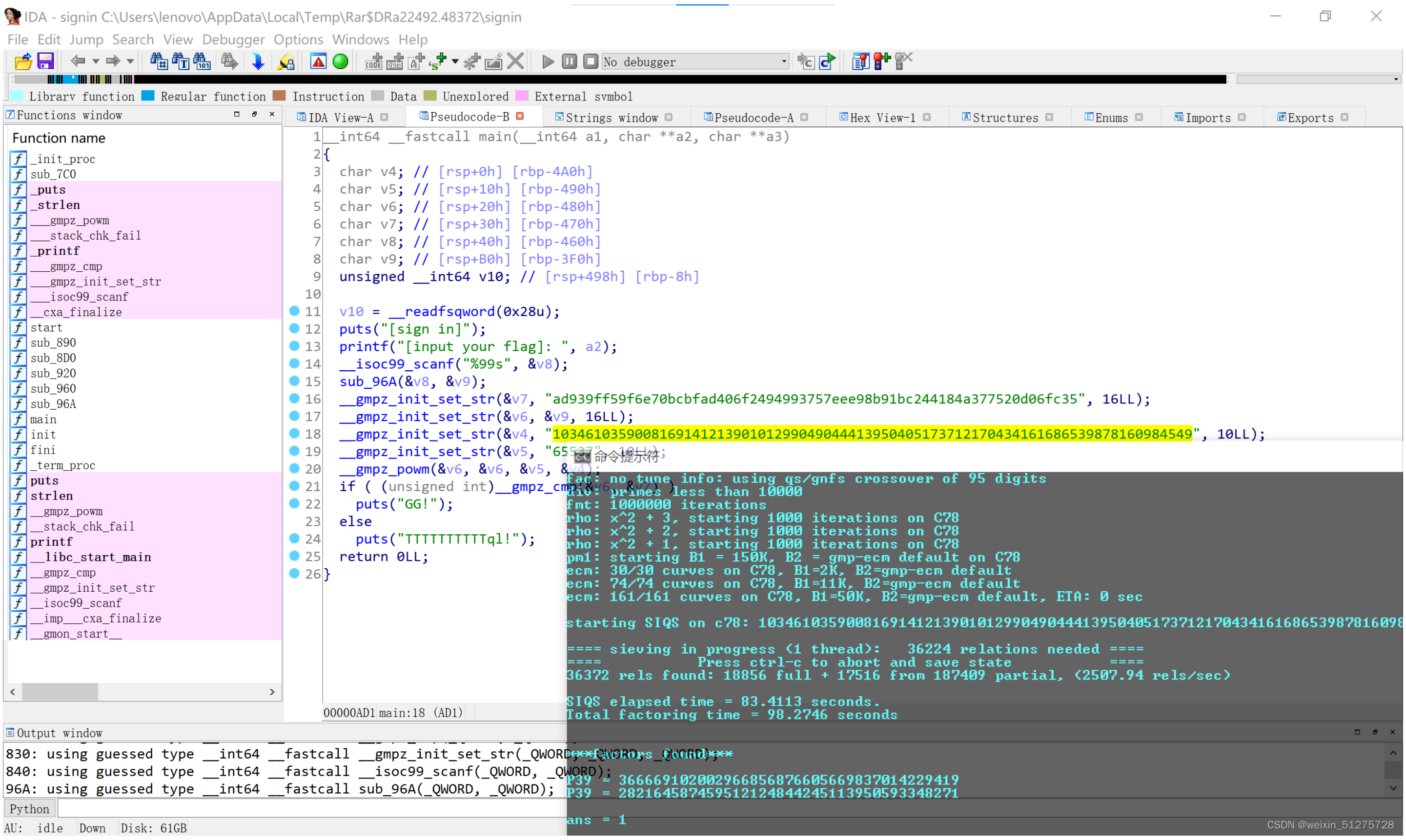
000009AE sub_4009AE:1 (4009AE)

```
40FA80: using guessed type __int64 __fastcall sub_40FA80(char);
410350: using guessed type __int64 __fastcall sub_410350(_QWORD);
443550: using guessed type __int64 __fastcall sub_443550(_QWORD, _QWORD, _QWORD);
```

```
#include < iostream>
using namespace std;
int main(){
char a1[32];
a1[0] = 166163712/ 1629056 ;
    a1[1] = 731332800 / 6771600;
   a1[2] = 357245568 /   3682944  ;
    a1[3] = 1074393000/  10431000  ;
  a1[4] = 489211344/3977328 ;
   a1[5] = 518971936/5138336 ;
   a1[6]='0';
 a1[7] = 406741500/7532250  ;
   a1[8] = 294236496/ 5551632 ;
 a1[9] = 177305856/ 3409728  ;
  a1[10] = 650683500/ 13013670  ;
   a1[11] = 298351053 / 6088797 ;
a1[12] = 386348487 /7884663;
 a1[13] = 438258597/8944053 ;
 a1[14] = 249527520/5198490 ;
  a1[15] = 445362764 /  4544518;
 a1[17] = 174988800/3645600 ;
a1[16] = 981182160 /10115280 ;
  a1[18] = 493042704 / 9667504;
     a1[19] = 257493600/5364450 ;
    a1[20] = 767478780/13464540 ;
 a1[21] = 312840624/5488432 ;
  a1[22] = 1404511500/14479500 ;
   a1[23] = 316139670/  6451830 ;
  a1[24] = 619005024/6252576 ;
  a1[25] = 372641472/7763364 ;
  a1[26] = 373693320/7327320 ;
 a1[27] = 498266640 / 8741520;
  a1[28] = 452465676/8871876 ;
  a1[29] = 208422720/ 4086720 ;
 a1[30] = 515592000/9374400 ;
   a1[31] = 719890500/5759124 ;
   cout<<a1;
}//a1[6]不知道，爆破的。
```

## 25 signin

25signin,rsa



```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  char v4; // [rsp+0h] [rbp-4A0h]
  char v5; // [rsp+10h] [rbp-490h]
  char v6; // [rsp+20h] [rbp-480h]
  char v7; // [rsp+30h] [rbp-470h]
  char v8; // [rsp+40h] [rbp-460h]
  char v9; // [rsp+B0h] [rbp-3F0h]
  unsigned __int64 v10; // [rsp+498h] [rbp-8h]

  v10 = __readfsqword(0x28u);
  puts("[sign in]");
  printf("[input your flag]: ", a2);
  __isoc99_scanf("%99s", &v8);
  sub_96A(&v8, &v9);
  __gmpz_init_set_str(&v7, "ad939ff59f6e70bcbfad406f2494993757eee98b91bc244184a377520d06fc35", 16LL);
  __gmpz_init_set_str(&v6, &v9, 16LL);
  __gmpz_init_set_str(&v4, "103461035900816914121390101299049044413950405173712170434161686539878160984549", 10LL);
  __gmpz_init_set_str(&v5, "65
  __gmpz_powm(&v6, &v6, &v5, &
  if ( (unsigned int)__gmpz_cm
    puts("GG!");
  else
    puts("TTTTTTTTTTql!");
  return 0LL;
}
```

```
830: using guessed type __int64 __fastcall __gmpz_init_set_str(_QWORD
840: using guessed type __int64 __fastcall __isoc99_scanf(_QWORD, _QWORD);
96A: using guessed type __int64 __fastcall sub_96A(_QWORD, _QWORD);
```

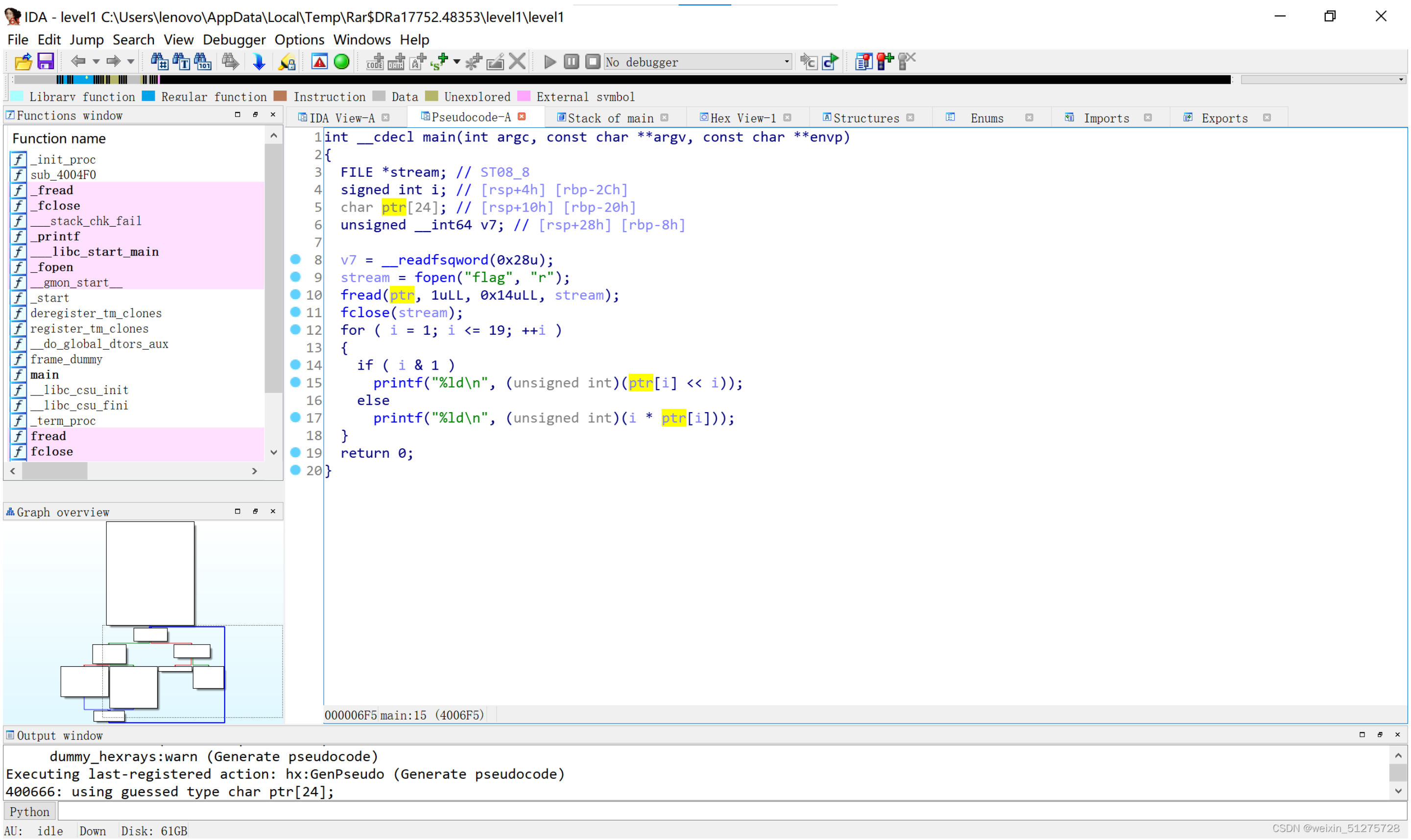
```
fac: no tune info: using qs/gnfs crossover of 95 digits
div: primes less than 10000
fmt: 1000000 iterations
rho: x^2 + 3, starting 1000 iterations on C78
rho: x^2 + 2, starting 1000 iterations on C78
rho: x^2 + 1, starting 1000 iterations on C78
pm1: starting B1 = 150K, B2 = gmp-ecm default on C78
ecm: 30/30 curves on C78, B1=2K, B2=gmp-ecm default
ecm: 74/74 curves on C78, B1=11K, B2=gmp-ecm default
ecm: 161/161 curves on C78, B1=50K, B2=gmp-ecm default, ETA: 0 sec

starting SIQS on c78: 10346103590081691412139010129904904441395040517371217043416168653987816098

==== sieving in progress (1 thread):   36224 relations needed ====
====            Press ctrl-c to abort and save state           ====
36372 rels found: 18856 full + 17516 from 187409 partial, (2507.94 rels/sec)

SIQS elapsed time = 83.4113 seconds.
Total factoring time = 98.2746 seconds

***factors found***

P39 = 366669102002966856876605669837014229419
P39 = 282164587459512124844245113950593348271

ans = 1
```

借网上的代码。。。 当时不会安gmpy2的库，方法可见安装angr库时遇到的问题及解决方法https://blog.csdn.net/weixin_51275728/article/details/122137833?spm=1001.2014.3001.5501

```
import gmpy2
import binascii

p = 282164587459512124844245113950593348271
q = 366669102002966856876605669837014229419
e = 65537
c = 0xad939ff59f6e70bcbfad406f2494993757eee98b91bc244184a377520d06fc35
n = 103461035900816914121390101299049044413950405173712170434161686539878160984549
d = gmpy2.invert(e, (p-1) * (q-1))
//48FFDA96436D1CC92E4415DE8C4D14FA4B6FD5D36D94B390D2308ADC1234CCCFBE38B158D8087
m = gmpy2.powmod(c, d, n)

print(binascii.unhexlify(hex(m)[2:]).decode(encoding="utf-8"))
```

## 26 level1

26level1



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  FILE *stream; // ST08_8
  signed int i; // [rsp+4h] [rbp-2Ch]
  char ptr[24]; // [rsp+10h] [rbp-20h]
  unsigned __int64 v7; // [rsp+28h] [rbp-8h]

  v7 = __readfsqword(0x28u);
  stream = fopen("flag", "r");
  fread(ptr, 1uLL, 0x14uLL, stream);
  fclose(stream);
  for ( i = 1; i <= 19; ++i )
  {
    if ( i & 1 )
      printf("%ld\n", (unsigned int)(ptr[i] << i));
    else
      printf("%ld\n", (unsigned int)(i * ptr[i]));
  }
  return 0;
}
```

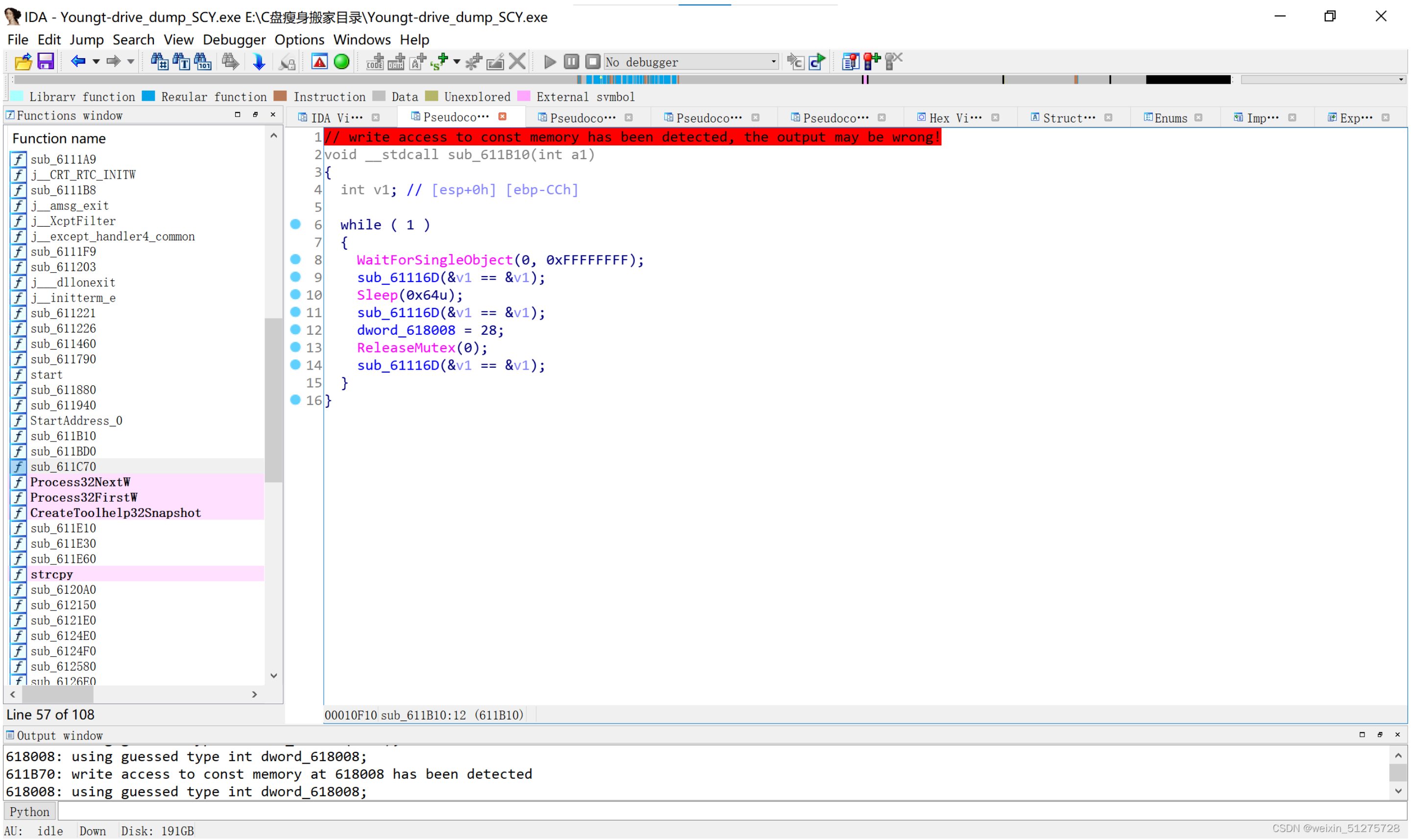
```
     dummy_hexrays:warn (Generate pseudocode)
Executing last-registered action: hx:GenPseudo (Generate pseudocode)
400666: using guessed type char ptr[24];
```

```
#include < iostream>
using namespace std;
int main(){
long long int a[20]={0,198,232,816,200,1536,300,6144,984,51200,570,92160,1200,565248,756,1474560,800,6291456,1782,65536000};
 for(int i=1;i<20;i++)
 {if(i&1)
 a[i]=a[i]>>i;
 else a[i]/=i;
 }
 for(int i=0;i<20;i++){
 char p=a[i];
 cout<<p;}
}
```

## 27 youghterdriver

27youghterdriver 有壳，脱壳，还是说一下，脱壳不一定要脱的很好，只要ida能识别其中的函数及数据就行。但我这次脱的太差了，函数都识别错了，一个反面教材。

创建了两个线程，得依次分析



Function name
sub_6111A9
j__CRT_RTC_INITW
sub_6111B8
j__amsg_exit
j__XcptFilter
j__except_handler4_common
sub_6111F9
sub_611203
j__dllonexit
j__initterm_e
sub_611221
sub_611226
sub_611460
sub_611790
start
sub_611880
sub_611940
StartAddress_0
sub_611B10
sub_611BD0
sub_611C70
Process32NextW
Process32FirstW
CreateToolhelp32Snapshot
sub_611E10
sub_611E30
sub_611E60
strcpy
sub_6120A0
sub_612150
sub_6121E0
sub_6124E0
sub_6124F0
sub_612580
sub_6126F0

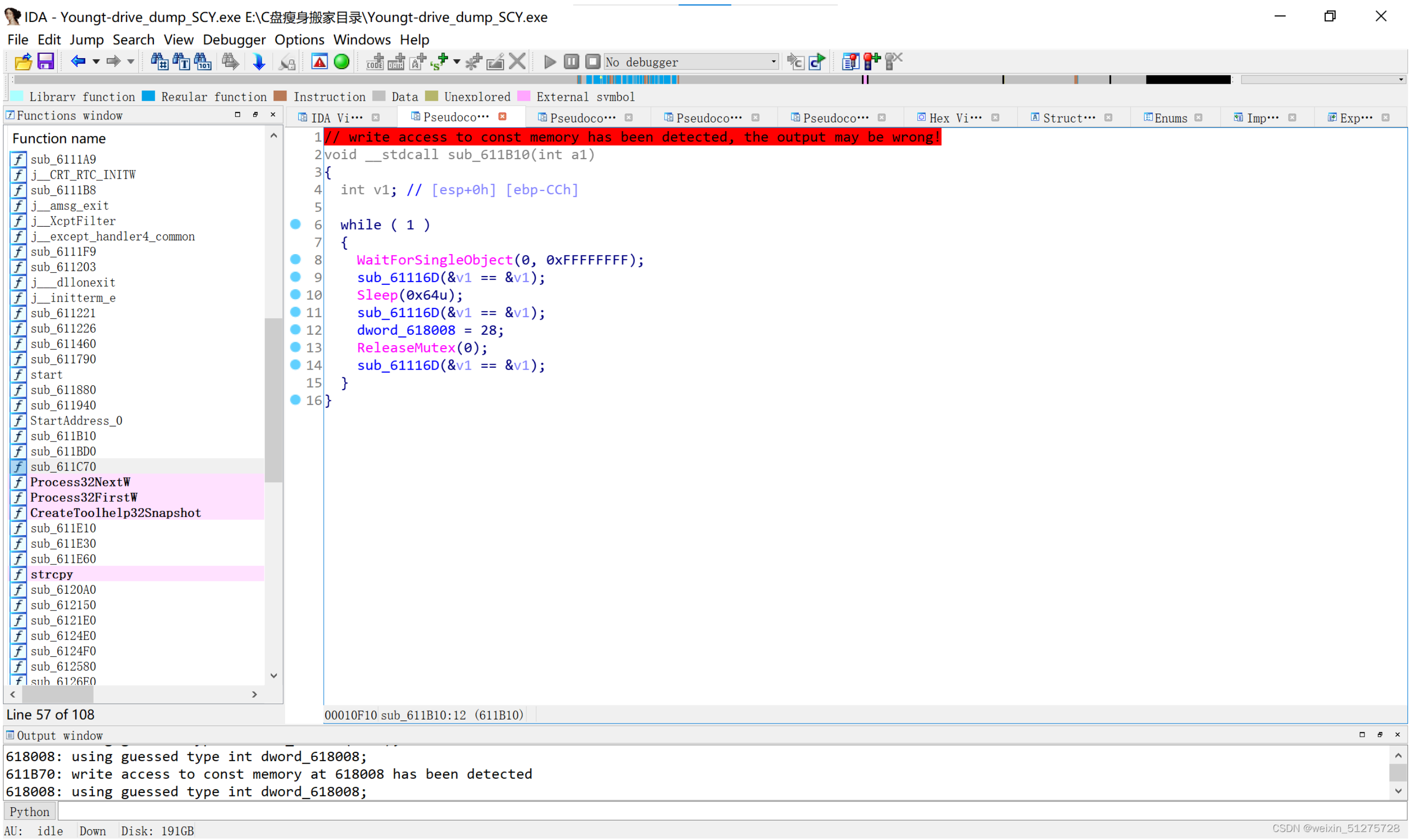
Line 57 of 108

```
// write access to const memory has been detected, the output may be wrong!
void __stdcall sub_611B10(int a1)
{
  int v1; // [esp+0h] [ebp-CCh]

  while ( 1 )
  {
    WaitForSingleObject(0, 0xFFFFFFFF);
    sub_61116D(&v1 == &v1);
    Sleep(0x64u);
    sub_61116D(&v1 == &v1);
    dword_618008 = 28;
    ReleaseMutex(0);
    sub_61116D(&v1 == &v1);
  }
}
```

00010F10 sub_611B10:12 (611B10)

```
618008: using guessed type int dword_618008;
611B70: write access to const memory at 618008 has been detected
618008: using guessed type int dword_618008;
```

AU: idle Down Disk: 191GB


IDA - Youngt-drive_dump_SCY.exe E:\C盘瘦身搬家目录\Youngt-drive_dump_SCY.exe

Function name
sub_6111A9
j__CRT_RTC_INITW
sub_6111B8
j__amsg_exit
j__XcptFilter
j__except_handler4_common
sub_6111F9
sub_611203
j__dllonexit
j__initterm_e
sub_611221
sub_611226
sub_611460
sub_611790
start
sub_611880
sub_611940
StartAddress_0
sub_611B10
sub_611BD0
sub_611C70
Process32NextW
Process32FirstW
CreateToolhelp32Snapshot
sub_611E10
sub_611E30
sub_611E60
strcpy
sub_6120A0
sub_612150
sub_6121E0
sub_6124E0
sub_6124F0
sub_612580
sub_6126F0

Line 57 of 108

// write access to const memory has been detected, the output may be wrong!
void __stdcall sub_611B10(int a1)
{
  int v1; // [esp+0h] [ebp-CCh]

  while ( 1 )
  {
    WaitForSingleObject(0, 0xFFFFFFFF);
    sub_61116D(&v1 == &v1);
    Sleep(0x64u);
    sub_61116D(&v1 == &v1);
    dword_618008 = 28;
    ReleaseMutex(0);
    sub_61116D(&v1 == &v1);
  }
}

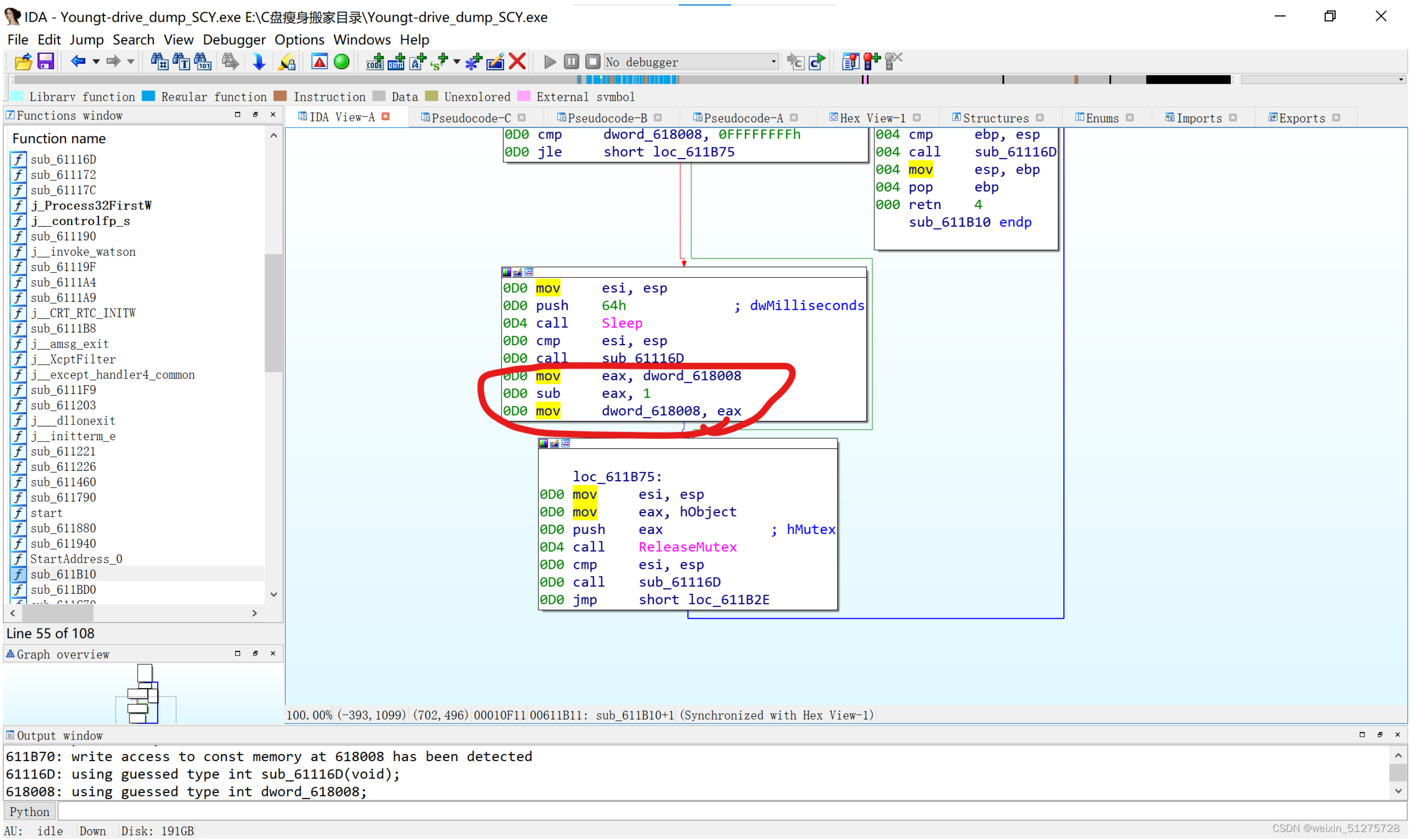
00010F10 sub_611B10:12 (611B10)

618008: using guessed type int dword_618008;
611B70: write access to const memory at 618008 has been detected
618008: using guessed type int dword_618008;

AU: idle Down Disk: 191GB

第二个感觉不对劲（1是上面的红字，2是这离谱的函数）

看汇编才知道dword_618008 -1不是数值减一，而是指针位置往前一格。



```
0D0 cmp     dword_618008, 0FFFFFFFFh
0D0 jle     short loc_611B75
```

```
004 cmp     ebp, esp
004 call    sub_61116D
004 mov     esp, ebp
004 pop     ebp
000 retn    4
    sub_611B10 endp
```

```
0D0 mov     esi, esp
0D0 push    64h             ; dwMilliseconds
0D4 call    Sleep
0D0 cmp     esi, esp
0D0 call    sub_61116D
0D0 mov     eax, dword_618008
0D0 sub     eax, 1
0D0 mov     dword_618008, eax
```

```
    loc_611B75:
0D0 mov     esi, esp
0D0 mov     eax, hObject
0D0 push    eax             ; hMutex
0D4 call    ReleaseMutex
0D0 cmp     esi, esp
0D0 call    sub_61116D
0D0 jmp     short loc_611B2E
```

```
100.00% (-393,1099) (702,496) 00010F11 00611B11: sub_611B10+1 (Synchronized with Hex View-1)
```

```
611B70: write access to const memory at 618008 has been detected
61116D: using guessed type int sub_61116D(void);
618008: using guessed type int dword_618008;
```

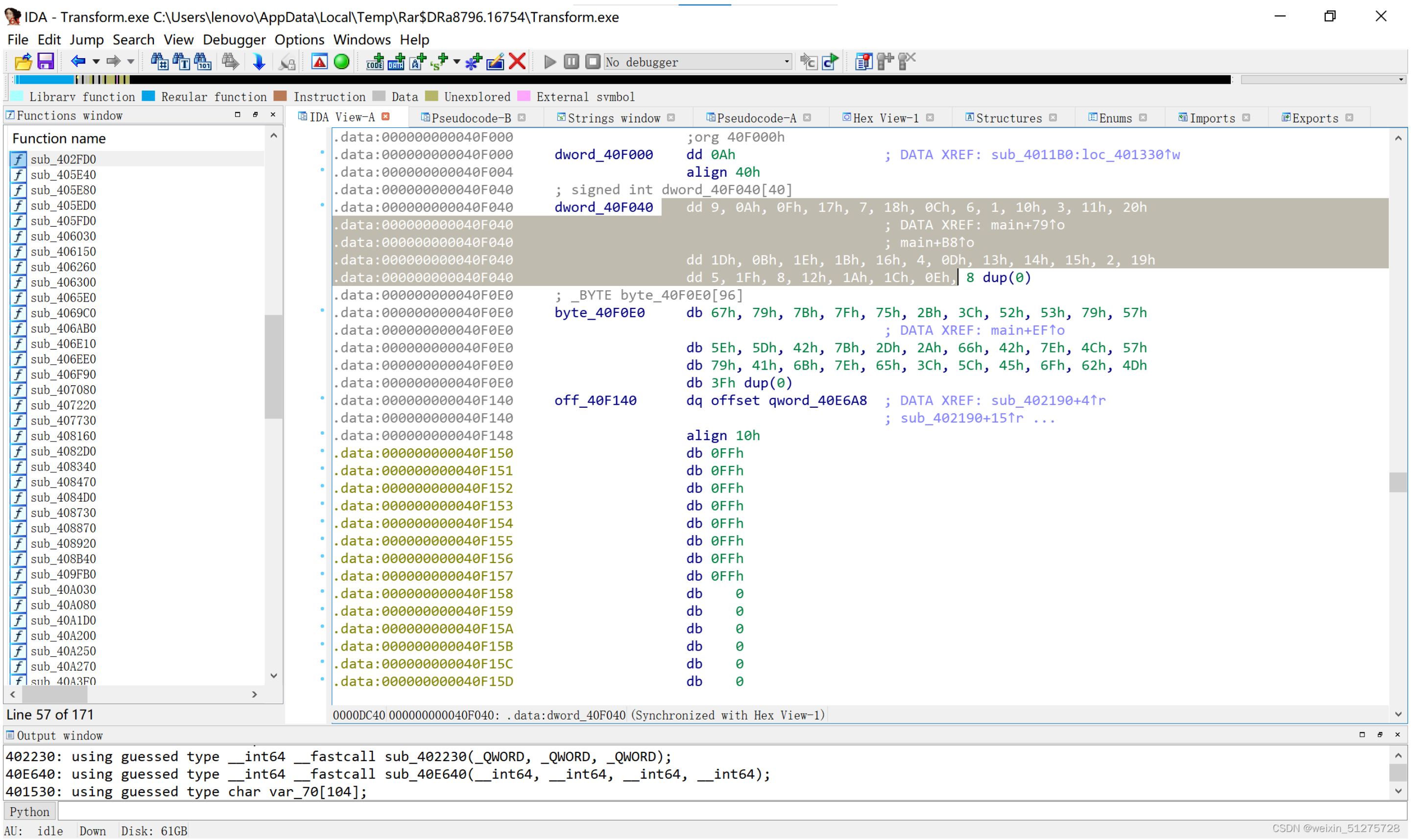
然后就不会了，双线程？？？看别人的writeup才知道是交替进行的意思

附代码(有点问题)

```
#include < iostream>
using namespace std;
int main(){
 string str="0abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ";//0来占个位
string k1="TOiZiZtOrYaToUwPnToBsOaOapsyS";
string k2="QWERTYUIOPASDFGHJKLZXCVBNMqwertyuiopasdfghjklzxcvbnm";
for(int i=0;i<k1.length();i++){
if(i%2==0)
 cout<<k1[i];
 else {
  for(int j=0;j<k1.length();j++){
   if(k2[j]==k1[i])
   cout<<str[j];
  }}}}
```

## 28 transform

## 28 transform 交换表后异或



```
sub_402FD0
sub_405E40
sub_405E80
sub_405ED0
sub_405FD0
sub_406030
sub_406150
sub_406260
sub_406300
sub_4065E0
sub_4069C0
sub_406AB0
sub_406E10
sub_406EE0
sub_406F90
sub_407080
sub_407220
sub_407730
sub_408160
sub_4082D0
sub_408340
sub_408470
sub_4084D0
sub_408730
sub_408870
sub_408920
sub_408B40
sub_409FB0
sub_40A030
sub_40A080
sub_40A1D0
sub_40A200
sub_40A250
sub_40A270
sub_40A3F0
Line 57 of 171
```

```
.data:000000000040F000                 ;org 40F000h
.data:000000000040F000 dword_40F000    dd 0Ah                  ; DATA XREF: sub_4011B0:loc_401330↑w
.data:000000000040F004                 align 40h
.data:000000000040F040 ; signed int dword_40F040[40]
.data:000000000040F040 dword_40F040    dd 9, 0Ah, 0Fh, 17h, 7, 18h, 0Ch, 6, 1, 10h, 3, 11h, 20h
.data:000000000040F040                                         ; DATA XREF: main+79↑o
.data:000000000040F040                                         ; main+B8↑o
.data:000000000040F040                 dd 1Dh, 0Bh, 1Eh, 1Bh, 16h, 4, 0Dh, 13h, 14h, 15h, 2, 19h
.data:000000000040F040                 dd 5, 1Fh, 8, 12h, 1Ah, 1Ch, 0Eh, 8 dup(0)
.data:000000000040F0E0 ; _BYTE byte_40F0E0[96]
.data:000000000040F0E0 byte_40F0E0     db 67h, 79h, 7Bh, 7Fh, 75h, 2Bh, 3Ch, 52h, 53h, 79h, 57h
.data:000000000040F0E0                                         ; DATA XREF: main+EF↑o
.data:000000000040F0E0                 db 5Eh, 5Dh, 42h, 7Bh, 2Dh, 2Ah, 66h, 42h, 7Eh, 4Ch, 57h
.data:000000000040F0E0                 db 79h, 41h, 6Bh, 7Eh, 65h, 3Ch, 5Ch, 45h, 6Fh, 62h, 4Dh
.data:000000000040F0E0                 db 3Fh dup(0)
.data:000000000040F140 off_40F140      dq offset qword_40E6A8  ; DATA XREF: sub_402190+4↑r
.data:000000000040F140                                         ; sub_402190+15↑r ...
.data:000000000040F148                 align 10h
.data:000000000040F150                 db 0FFh
.data:000000000040F151                 db 0FFh
.data:000000000040F152                 db 0FFh
.data:000000000040F153                 db 0FFh
.data:000000000040F154                 db 0FFh
.data:000000000040F155                 db 0FFh
.data:000000000040F156                 db 0FFh
.data:000000000040F157                 db 0FFh
.data:000000000040F158                 db    0
.data:000000000040F159                 db    0
.data:000000000040F15A                 db    0
.data:000000000040F15B                 db    0
.data:000000000040F15C                 db    0
.data:000000000040F15D                 db    0
0000DC40 000000000040F040: .data:dword_40F040 (Synchronized with Hex View-1)
```

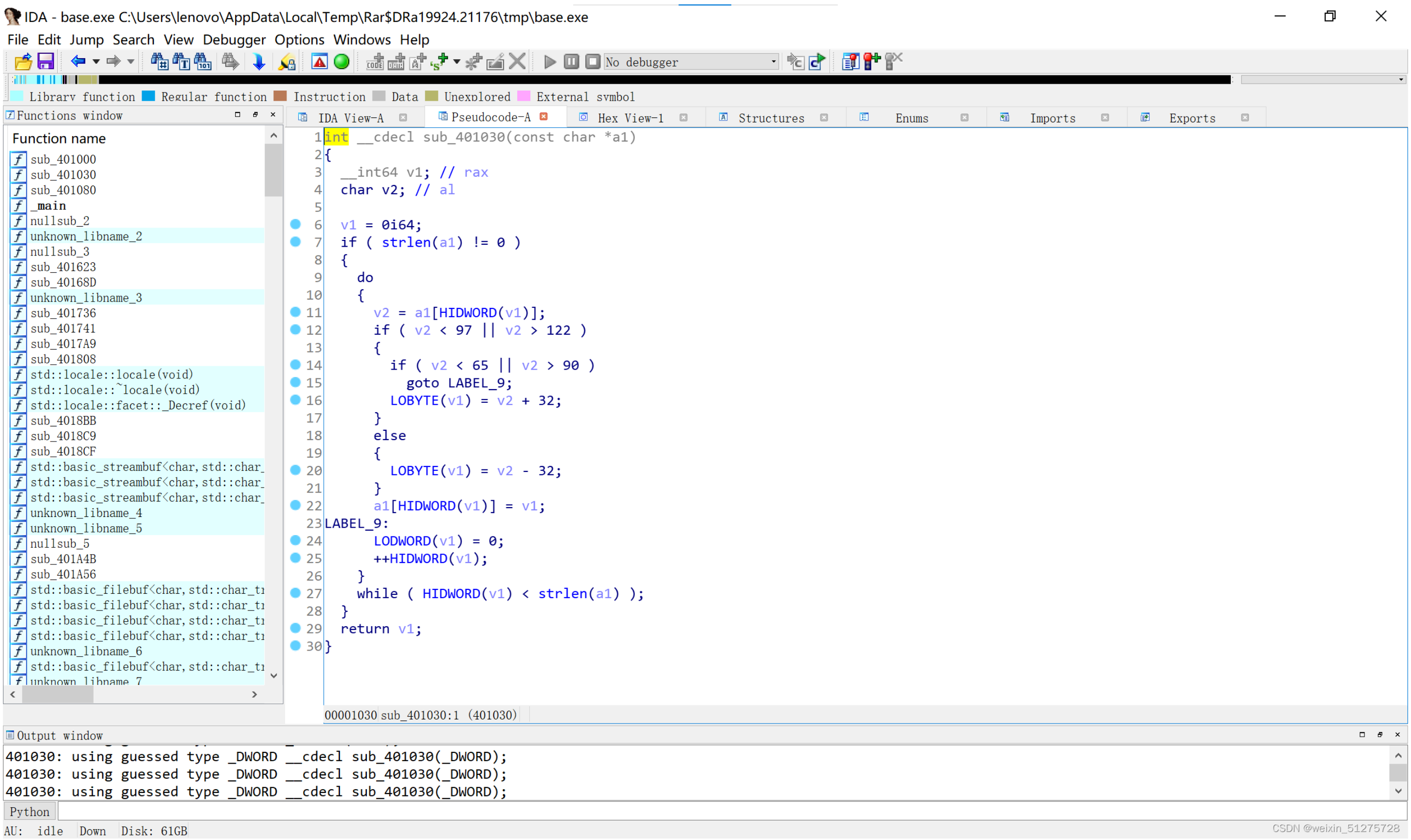
```
402230: using guessed type __int64 __fastcall sub_402230(_QWORD, _QWORD, _QWORD);
40E640: using guessed type __int64 __fastcall sub_40E640(__int64, __int64, __int64, __int64);
401530: using guessed type char var_70[104];
```

```
AU:  idle   Down   Disk: 61GB
```

```
#include < iostream>
using namespace std;
int main(){
 unsigned char ida_chars[]={0x09,0x0A,0x0F,0x17,0x07,0x18,0x0C,0x06,0x01,0x10,0x03,0x11,0x20,0x1D,0x0B,0x1E,0x1B
,0x16,0x04,0x0D,0x13,0x14,0x15,0x02,0x19,0x05,0x1F,0x08,0x12,0x1A,0x1C,0x0E};
unsigned char ida_char[] =
{0x67, 0x79, 0x7B, 0x7F, 0x75, 0x2B, 0x3C, 0x52, 0x53, 0x79,
  0x57, 0x5E, 0x5D, 0x42, 0x7B, 0x2D, 0x2A, 0x66, 0x42, 0x7E,
  0x4C, 0x57, 0x79, 0x41, 0x6B, 0x7E, 0x65, 0x3C, 0x5C, 0x45,
  0x6F, 0x62, 0x4D};
  for(int i=0;i<33;i++){
  ida_char[i]^=ida_chars[i];
  }
  for(int i=1;i<33;i++){
  for(int j=0;j<33;j++){
  if(ida_chars[j]==i)
  cout<<ida_char[j];
  }  }}
```

## 29 usualcrypt

29 usualcrypt base64 变表，先开始我没看到变表



```
sub_401000
sub_401030
sub_401080
_main
nullsub_2
unknown_libname_2
nullsub_3
sub_401623
sub_40168D
unknown_libname_3
sub_401736
sub_401741
sub_4017A9
sub_401808
std::locale::locale(void)
std::locale::~locale(void)
std::locale::facet::_Decref(void)
sub_4018BB
sub_4018C9
sub_4018CF
std::basic_streambuf<char,std::char_
std::basic_streambuf<char,std::char_
std::basic_streambuf<char,std::char_
unknown_libname_4
unknown_libname_5
nullsub_5
sub_401A4B
sub_401A56
std::basic_filebuf<char,std::char_tı
std::basic_filebuf<char,std::char_tı
std::basic_filebuf<char,std::char_tı
std::basic_filebuf<char,std::char_tı
unknown_libname_6
std::basic_filebuf<char,std::char_tı
unknown_libname_7
```

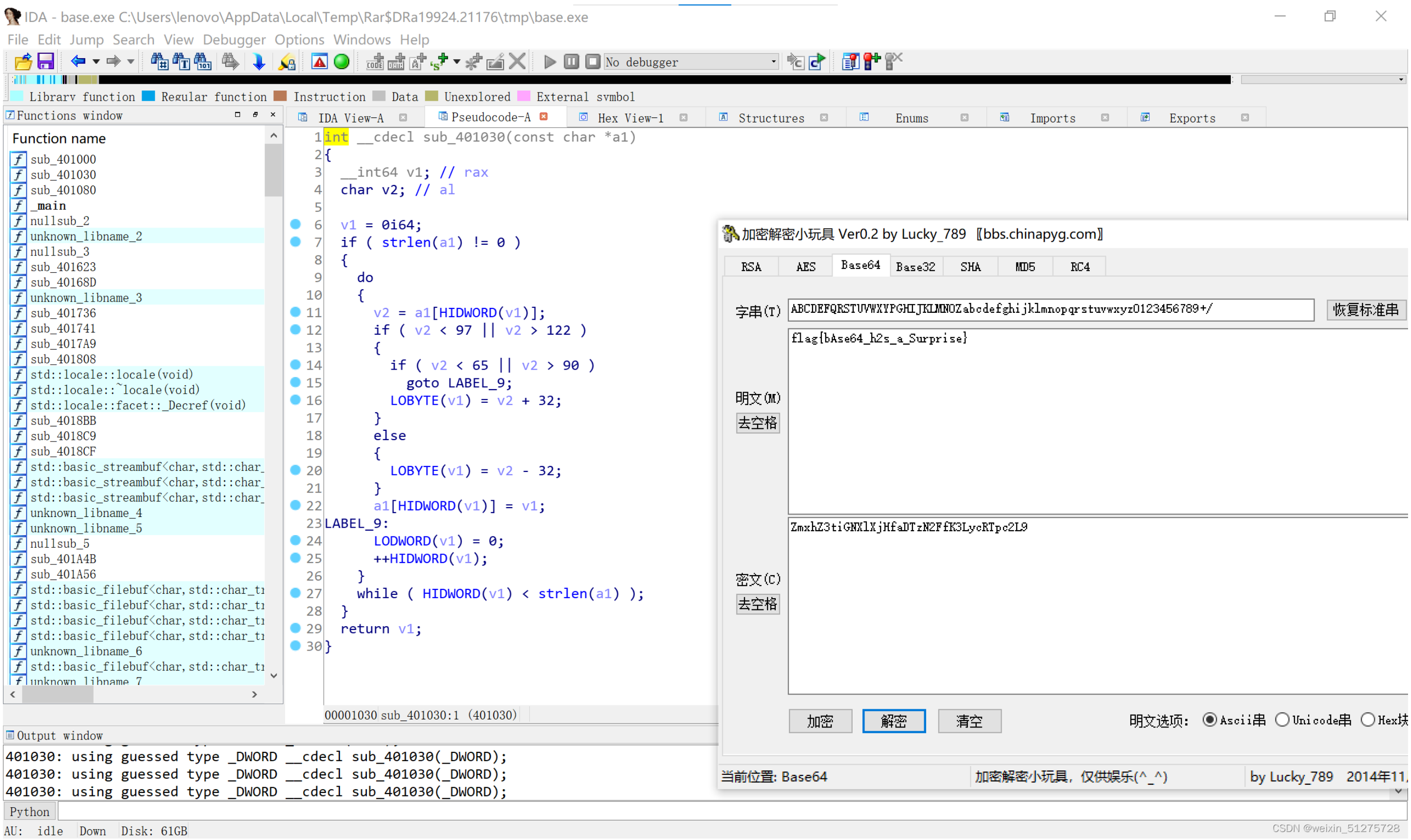
```
int __cdecl sub_401030(const char *a1)
{
  __int64 v1; // rax
  char v2; // al

  v1 = 0i64;
  if ( strlen(a1) != 0 )
  {
    do
    {
      v2 = a1[HIDWORD(v1)];
      if ( v2 < 97 || v2 > 122 )
      {
        if ( v2 < 65 || v2 > 90 )
          goto LABEL_9;
        LOBYTE(v1) = v2 + 32;
      }
      else
      {
        LOBYTE(v1) = v2 - 32;
      }
      a1[HIDWORD(v1)] = v1;
LABEL_9:
      LODWORD(v1) = 0;
      ++HIDWORD(v1);
    }
    while ( HIDWORD(v1) < strlen(a1) );
  }
  return v1;
}
```

00001030 sub_401030:1 (401030)

```
401030: using guessed type _DWORD __cdecl sub_401030(_DWORD);
401030: using guessed type _DWORD __cdecl sub_401030(_DWORD);
401030: using guessed type _DWORD __cdecl sub_401030(_DWORD);
```

```
#include < iostream>
using namespace std;
int main(){
 int i=6;
 char v1;
 string a="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
 do{v1=a[10+i];
 a[10+i]=a[i];
 a[i]=v1;
 i++;
 }while(i<15);
 cout<<a;
}
```

然后我发现不行，仔细看函数，发现还有大小写转换。



IDA - base.exe C:\Users\lenovo\AppData\Local\Temp\Rar$DRa19924.21176\tmp\base.exe
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol
Functions window
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
Imports
Exports
Function name
sub_401000
sub_401030
sub_401080
_main
nullsub_2
unknown_libname_2
nullsub_3
sub_401623
sub_40168D
unknown_libname_3
sub_401736
sub_401741
sub_4017A9
sub_401808
std::locale::locale(void)
std::locale::~locale(void)
std::locale::facet::_Decref(void)
sub_4018BB
sub_4018C9
sub_4018CF
std::basic_streambuf<char,std::char_
std::basic_streambuf<char,std::char_
std::basic_streambuf<char,std::char_
unknown_libname_4
unknown_libname_5
nullsub_5
sub_401A4B
sub_401A56
std::basic_filebuf<char,std::char_t
std::basic_filebuf<char,std::char_t
std::basic_filebuf<char,std::char_t
std::basic_filebuf<char,std::char_t
unknown_libname_6
std::basic_filebuf<char,std::char_t
unknown_libname_7
00001030 sub_401030:1 (401030)
Output window
Python
AU: idle Down Disk: 61GB
加密解密小玩具 Ver0.2 by Lucky_789 〖bbs.chinapyg.com〗
RSA
AES
Base64
Base32
SHA
MD5
RC4
恢复标准串
去空格
去空格
加密
解密
清空
当前位置: Base64
加密解密小玩具，仅供娱乐(^_^)
by Lucky_789 2014年11
CSDN @weixin_51275728

```
int __cdecl sub_401030(const char *a1)
{
  __int64 v1; // rax
  char v2; // al

  v1 = 0i64;
  if ( strlen(a1) != 0 )
  {
    do
    {
      v2 = a1[HIDWORD(v1)];
      if ( v2 < 97 || v2 > 122 )
      {
        if ( v2 < 65 || v2 > 90 )
          goto LABEL_9;
        LOBYTE(v1) = v2 + 32;
      }
      else
      {
        LOBYTE(v1) = v2 - 32;
      }
      a1[HIDWORD(v1)] = v1;
LABEL_9:
      LODWORD(v1) = 0;
      ++HIDWORD(v1);
    }
    while ( HIDWORD(v1) < strlen(a1) );
  }
  return v1;
}
```

```
401030: using guessed type _DWORD __cdecl sub_401030(_DWORD);
401030: using guessed type _DWORD __cdecl sub_401030(_DWORD);
401030: using guessed type _DWORD __cdecl sub_401030(_DWORD);
```

字串(T) ABCDEFQRSTUVWXYPGHIJKLMNOZabcdefghijklmnopqrstuvwxyz0123456789+/

明文(M) flag{bAse64_h2s_a_Surprise}

密文(C) ZmxhZ3tiGNXlXjHfaDTzN2FfK3LycRTpc2L9

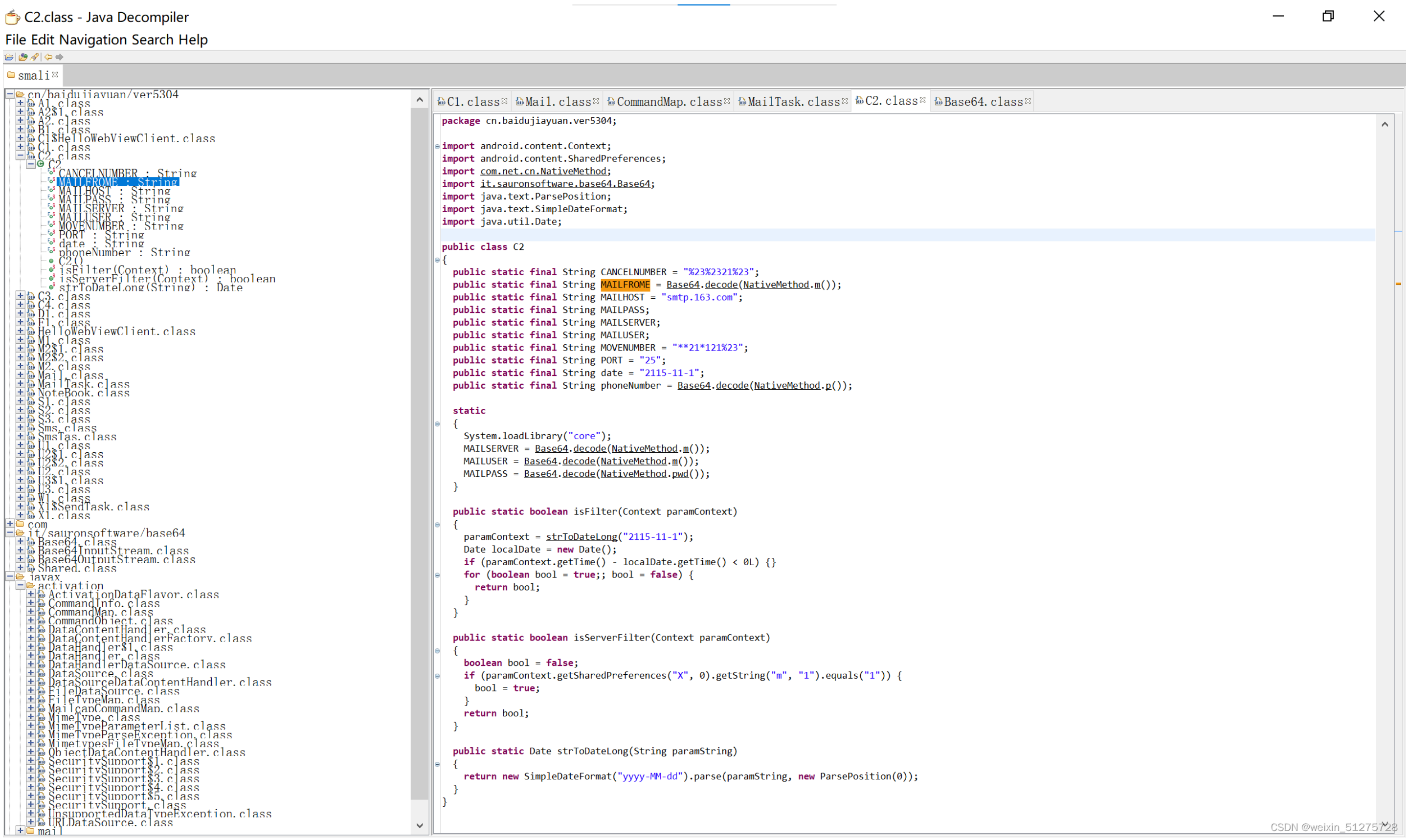
明文选项: ● Ascii串 ○ Unicode串 ○ Hex块

# 30 level2

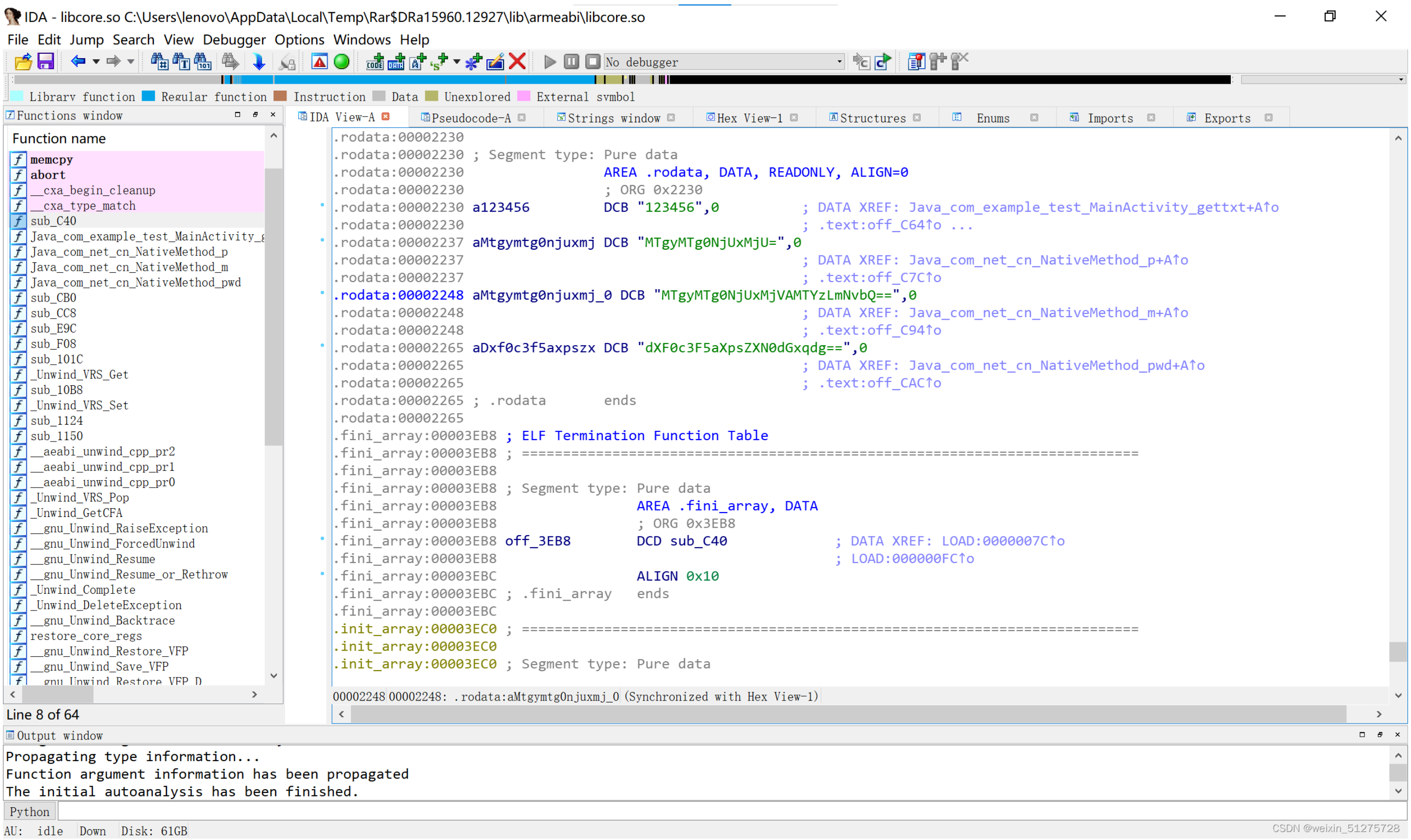
30level2 upx脱壳 明码

# 31 相册

31 相册 base64



```
package cn.baidujiayuan.ver5304;

import android.content.Context;
import android.content.SharedPreferences;
import com.net.cn.NativeMethod;
import it.sauronsoftware.base64.Base64;
import java.text.ParsePosition;
import java.text.SimpleDateFormat;
import java.util.Date;

public class C2
{
  public static final String CANCELNUMBER = "%23%2321%23";
  public static final String MAILFROME = Base64.decode(NativeMethod.m());
  public static final String MAILHOST = "smtp.163.com";
  public static final String MAILPASS;
  public static final String MAILSERVER;
  public static final String MAILUSER;
  public static final String MOVENUMBER = "**21*121%23";
  public static final String PORT = "25";
  public static final String date = "2115-11-1";
  public static final String phoneNumber = Base64.decode(NativeMethod.p());

  static
  {
    System.loadLibrary("core");
    MAILSERVER = Base64.decode(NativeMethod.m());
    MAILUSER = Base64.decode(NativeMethod.m());
    MAILPASS = Base64.decode(NativeMethod.pwd());
  }

  public static boolean isFilter(Context paramContext)
  {
    paramContext = strToDateLong("2115-11-1");
    Date localDate = new Date();
    if (paramContext.getTime() - localDate.getTime() < 0L) {}
    for (boolean bool = true;; bool = false) {
      return bool;
    }
  }

  public static boolean isServerFilter(Context paramContext)
  {
    boolean bool = false;
    if (paramContext.getSharedPreferences("X", 0).getString("m", "1").equals("1")) {
      bool = true;
    }
    return bool;
  }

  public static Date strToDateLong(String paramString)
  {
    return new SimpleDateFormat("yyyy-MM-dd").parse(paramString, new ParsePosition(0));
  }
}
```



```
memcpy
abort
__cxa_begin_cleanup
__cxa_type_match
sub_C40
Java_com_example_test_MainActivity_g
Java_com_net_cn_NativeMethod_p
Java_com_net_cn_NativeMethod_m
Java_com_net_cn_NativeMethod_pwd
sub_CB0
sub_CC8
sub_E9C
sub_F08
sub_101C
_Unwind_VRS_Get
sub_10B8
_Unwind_VRS_Set
sub_1124
sub_1150
__aeabi_unwind_cpp_pr2
__aeabi_unwind_cpp_pr1
__aeabi_unwind_cpp_pr0
_Unwind_VRS_Pop
_Unwind_GetCFA
__gnu_Unwind_RaiseException
__gnu_Unwind_ForcedUnwind
__gnu_Unwind_Resume
__gnu_Unwind_Resume_or_Rethrow
_Unwind_Complete
_Unwind_DeleteException
__gnu_Unwind_Backtrace
restore_core_regs
__gnu_Unwind_Restore_VFP
__gnu_Unwind_Save_VFP
__gnu_Unwind_Restore_VFP_D
```

```
.rodata:00002230
.rodata:00002230 ; Segment type: Pure data
.rodata:00002230                 AREA .rodata, DATA, READONLY, ALIGN=0
.rodata:00002230                 ; ORG 0x2230
.rodata:00002230 a123456         DCB "123456",0          ; DATA XREF: Java_com_example_test_MainActivity_gettxt+A↑o
.rodata:00002230                                         ; .text:off_C64↑o ...
.rodata:00002237 aMtgymtg0njuxmj DCB "MTgyMTg0NjUxMjU=",0
.rodata:00002237                                         ; DATA XREF: Java_com_net_cn_NativeMethod_p+A↑o
.rodata:00002237                                         ; .text:off_C7C↑o
.rodata:00002248 aMtgymtg0njuxmj_0 DCB "MTgyMTg0NjUxMjVAMTYzLmNvbQ==",0
.rodata:00002248                                         ; DATA XREF: Java_com_net_cn_NativeMethod_m+A↑o
.rodata:00002248                                         ; .text:off_C94↑o
.rodata:00002265 aDxf0c3f5axpszx DCB "dXF0c3F5aXpsZXN0dGxqdg==",0
.rodata:00002265                                         ; DATA XREF: Java_com_net_cn_NativeMethod_pwd+A↑o
.rodata:00002265                                         ; .text:off_CAC↑o
.rodata:00002265 ; .rodata       ends
.rodata:00002265
.fini_array:00003EB8 ; ELF Termination Function Table
.fini_array:00003EB8 ; ===========================================================================
.fini_array:00003EB8
.fini_array:00003EB8 ; Segment type: Pure data
.fini_array:00003EB8                 AREA .fini_array, DATA
.fini_array:00003EB8                 ; ORG 0x3EB8
.fini_array:00003EB8 off_3EB8        DCD sub_C40             ; DATA XREF: LOAD:0000007C↑o
.fini_array:00003EB8                                         ; LOAD:000000FC↑o
.fini_array:00003EBC                 ALIGN 0x10
.fini_array:00003EBC ; .fini_array   ends
.fini_array:00003EBC
.init_array:00003EC0 ; ===========================================================================
.init_array:00003EC0
.init_array:00003EC0 ; Segment type: Pure data
```

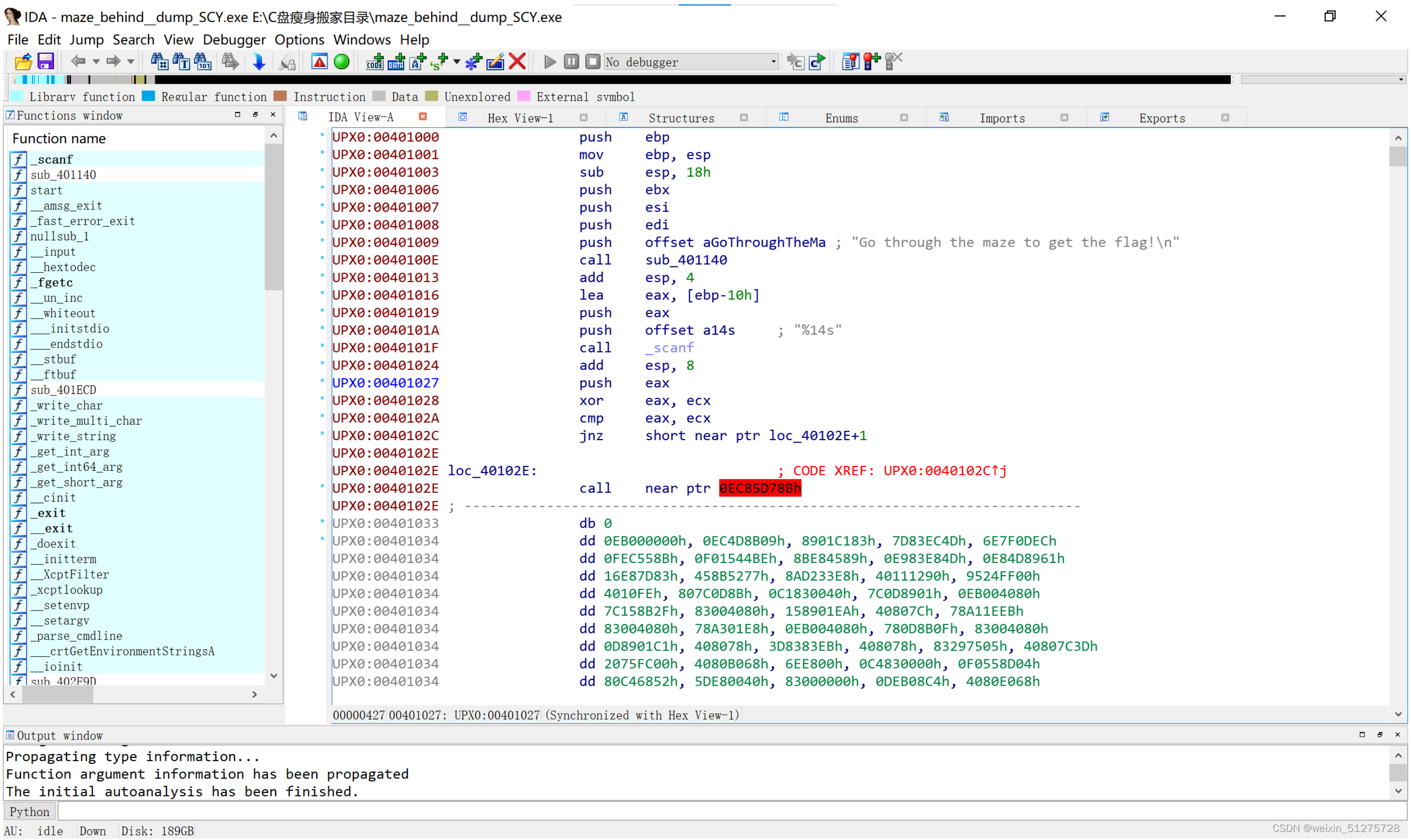
```
00002248 00002248: .rodata:aMtgymtg0njuxmj_0 (Synchronized with Hex View-1)
```

```
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle   Down   Disk: 61GB
```

# 32 maze

## 32 maze upx脱壳但我脱不好系列



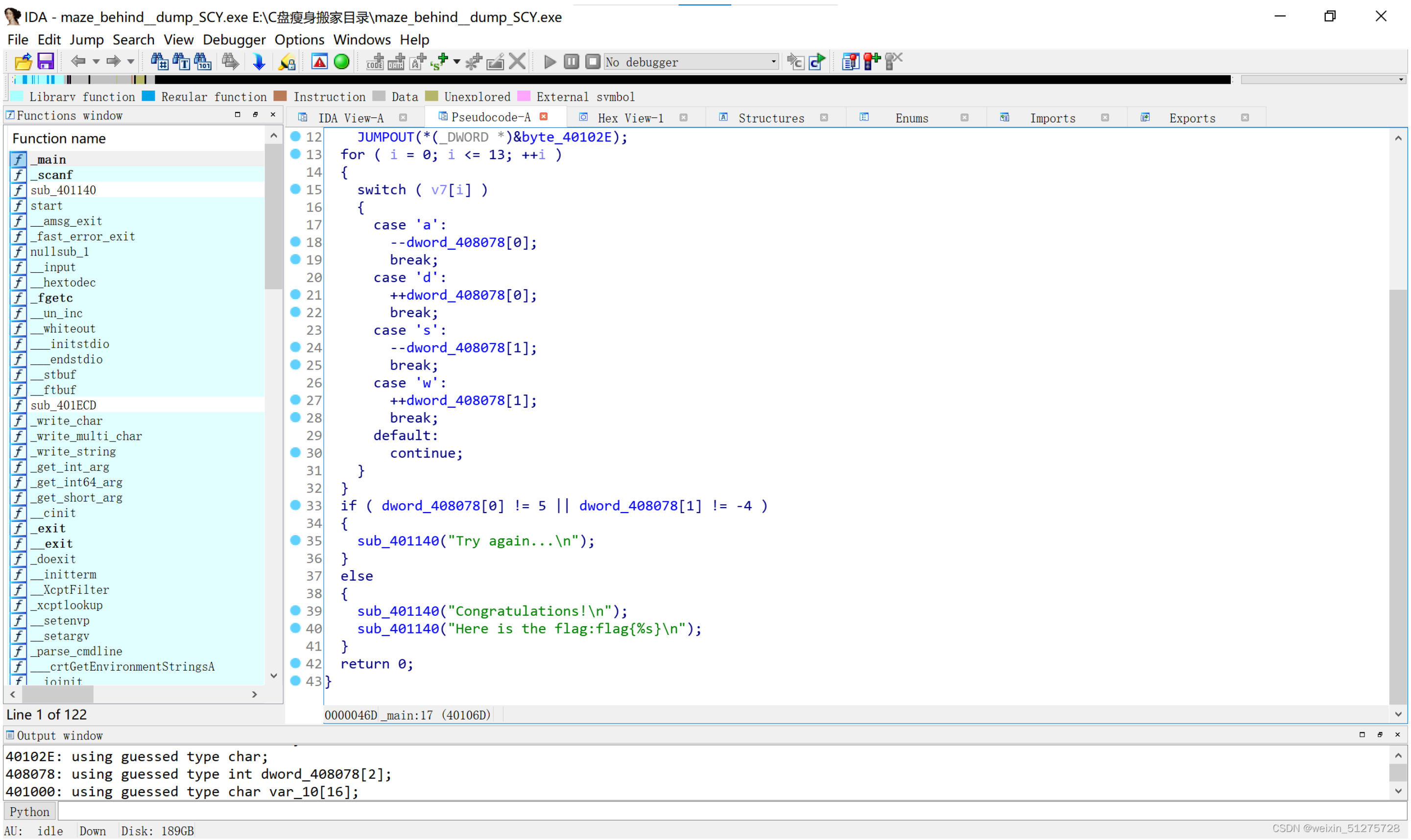
```
_scanf
sub_401140
start
__amsg_exit
__fast_error_exit
nullsub_1
__input
__hextodec
_fgetc
__un_inc
__whiteout
___initstdio
___endstdio
__stbuf
__ftbuf
sub_401ECD
_write_char
_write_multi_char
_write_string
_get_int_arg
_get_int64_arg
_get_short_arg
__cinit
_exit
__exit
_doexit
__initterm
__XcptFilter
__xcptlookup
__setenvp
__setargv
__parse_cmdline
___crtGetEnvironmentStringsA
__ioinit
sub_402F9D
```

```
UPX0:00401000                 push    ebp
UPX0:00401001                 mov     ebp, esp
UPX0:00401003                 sub     esp, 18h
UPX0:00401006                 push    ebx
UPX0:00401007                 push    esi
UPX0:00401008                 push    edi
UPX0:00401009                 push    offset aGoThroughTheMa ; "Go through the maze to get the flag!\n"
UPX0:0040100E                 call    sub_401140
UPX0:00401013                 add     esp, 4
UPX0:00401016                 lea     eax, [ebp-10h]
UPX0:00401019                 push    eax
UPX0:0040101A                 push    offset a14s     ; "%14s"
UPX0:0040101F                 call    _scanf
UPX0:00401024                 add     esp, 8
UPX0:00401027                 push    eax
UPX0:00401028                 xor     eax, ecx
UPX0:0040102A                 cmp     eax, ecx
UPX0:0040102C                 jnz     short near ptr loc_40102E+1
UPX0:0040102E
UPX0:0040102E loc_40102E:                             ; CODE XREF: UPX0:0040102C↑j
UPX0:0040102E                 call    near ptr 0EC85D78Bh
UPX0:0040102E ; ---------------------------------------------------------------------------
UPX0:00401033                 db 0
UPX0:00401034                 dd 0EB000000h, 0EC4D8B09h, 8901C183h, 7D83EC4Dh, 6E7F0DECh
UPX0:00401034                 dd 0FEC558Bh, 0F01544BEh, 8BE84589h, 0E983E84Dh, 0E84D8961h
UPX0:00401034                 dd 16E87D83h, 458B5277h, 8AD233E8h, 40111290h, 9524FF00h
UPX0:00401034                 dd 4010FEh, 807C0D8Bh, 0C1830040h, 7C0D8901h, 0EB004080h
UPX0:00401034                 dd 7C158B2Fh, 83004080h, 158901EAh, 40807Ch, 78A11EEBh
UPX0:00401034                 dd 83004080h, 78A301E8h, 0EB004080h, 780D8B0Fh, 83004080h
UPX0:00401034                 dd 0D8901C1h, 408078h, 3D8383EBh, 408078h, 83297505h, 40807C3Dh
UPX0:00401034                 dd 2075FC00h, 4080B068h, 6EE800h, 0C4830000h, 0F0558D04h
UPX0:00401034                 dd 80C46852h, 5DE80040h, 83000000h, 0DEB08C4h, 4080E068h
```

```
00000427 00401027: UPX0:00401027 (Synchronized with Hex View-1)
```

```
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle   Down   Disk: 189GB
```



```
  JUMPOUT(*(_DWORD *)&byte_40102E);
for ( i = 0; i <= 13; ++i )
{
  switch ( v7[i] )
  {
    case 'a':
      --dword_408078[0];
      break;
    case 'd':
      ++dword_408078[0];
      break;
    case 's':
      --dword_408078[1];
      break;
    case 'w':
      ++dword_408078[1];
      break;
    default:
      continue;
  }
}
if ( dword_408078[0] != 5 || dword_408078[1] != -4 )
{
  sub_401140("Try again...\n");
}
else
{
  sub_401140("Congratulations!\n");
  sub_401140("Here is the flag:flag{%s}\n");
}
return 0;
}
```

```
40102E: using guessed type char;
408078: using guessed type int dword_408078[2];
401000: using guessed type char var_10[16];
```

```
.......+..
....... ..
....    ..
..   .....
.. ..F....
..    ....
..........
```

70个字符7*10 不行，10*7可以

它还有花指令，对 call near ptr 0ecb5d7800h先按d 再把除dbe8h的部分按c 去除花指令。

按p，按f5即可