攻防世界simple-unpack，文件脱壳

原创

starmultiple 于 2022-01-21 22:13:23 发布 192 收藏

分类专栏： 做题 文章标签： 开发语言

本文链接：https://blog.csdn.net/starmultiple/article/details/122630340

版权

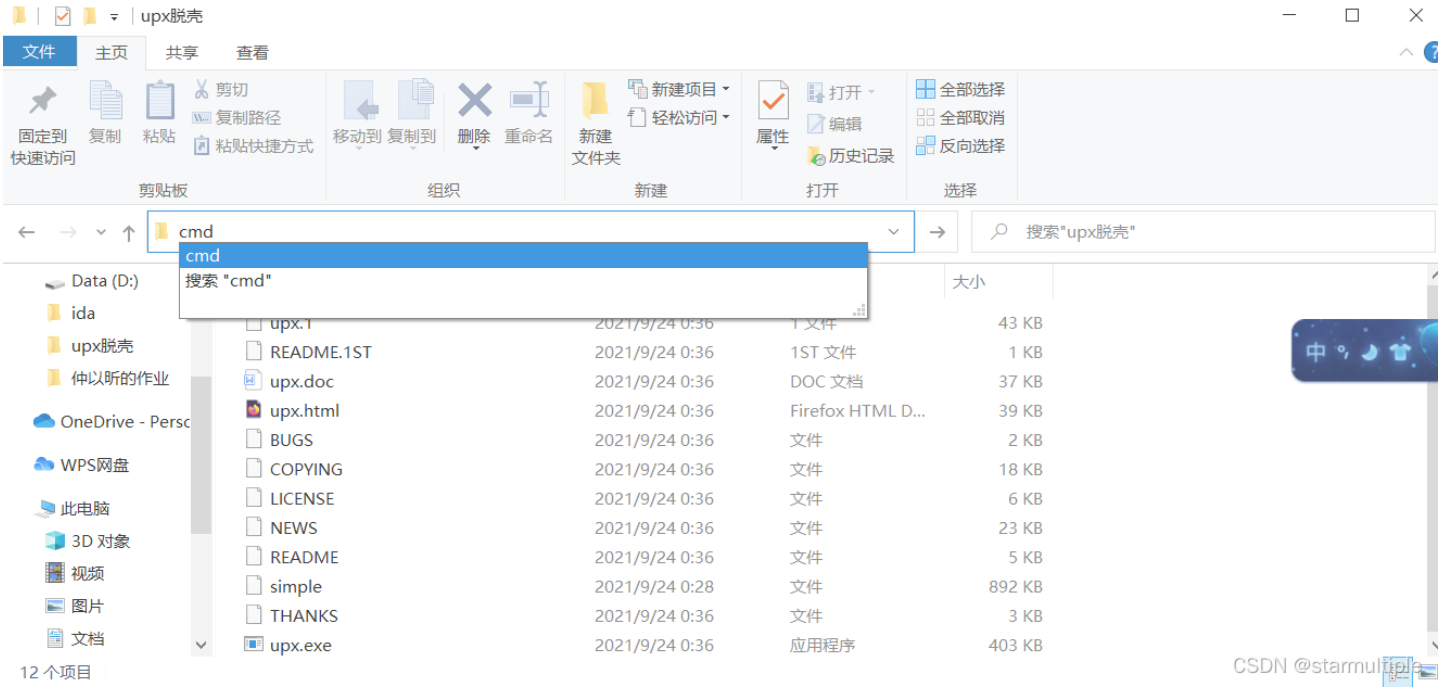
做题 专栏收录该内容

11 篇文章 0 订阅

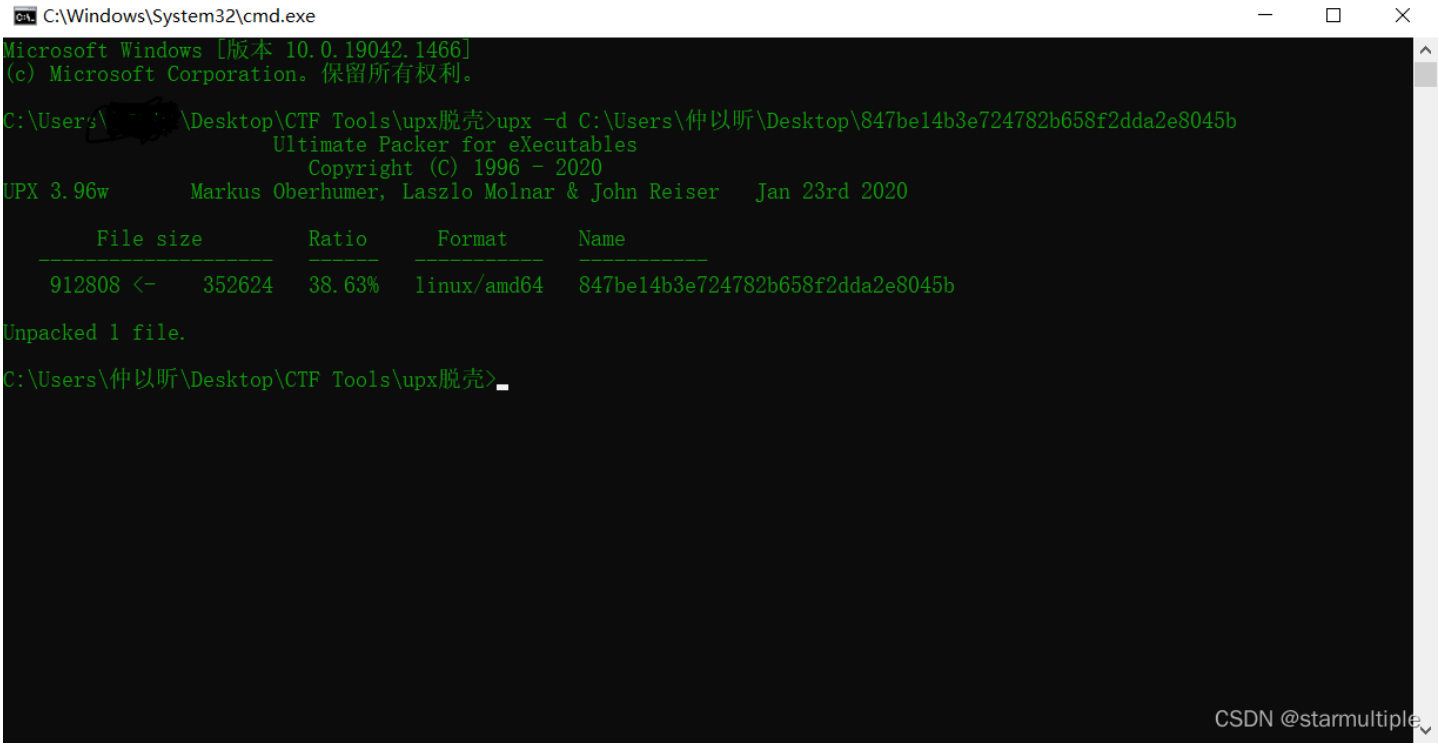
订阅专栏

upx脱壳

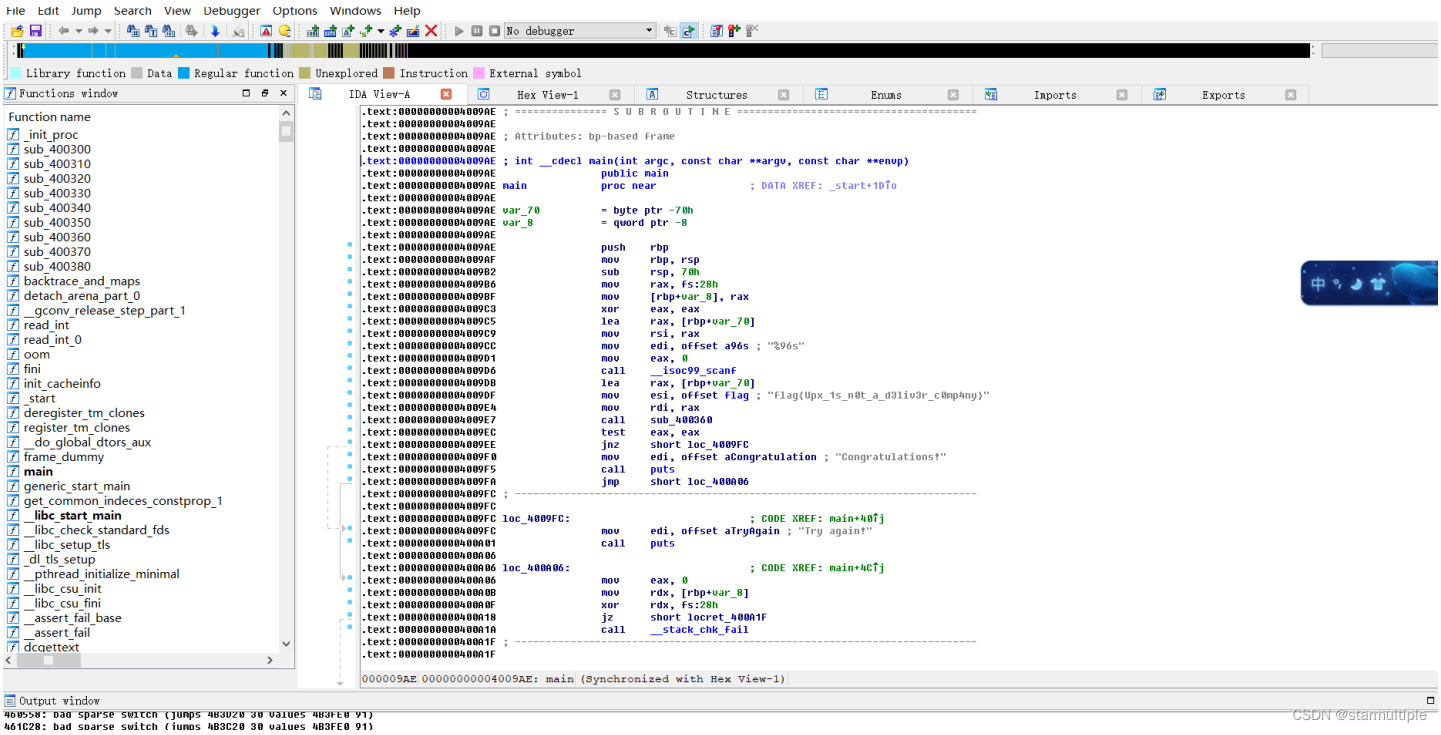
第一步：打开脱壳软件upx的cmd窗口

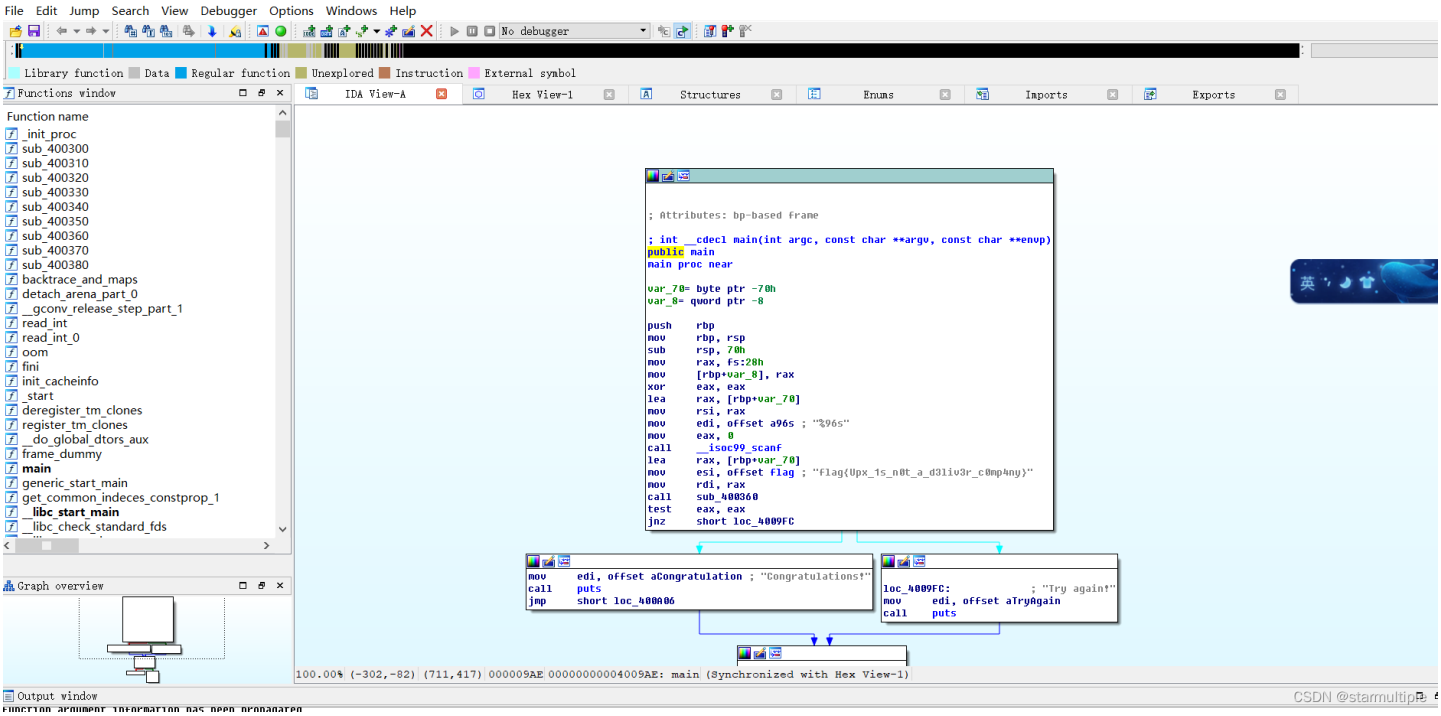


输入 -d 后拖入待脱壳软件



下面两幅图都能发现flag


File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
_init_proc
sub_400300
sub_400310
sub_400320
sub_400330
sub_400340
sub_400350
sub_400360
sub_400370
sub_400380
backtrace_and_maps
detach_arena_part_0
__gconv_release_step_part_1
read_int
read_int_0
oom
fini
init_cacheinfo
_start
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
frame_dummy
main
generic_start_main
get_common_indeces_constprop_1
__libc_start_main
__libc_check_standard_fds
__libc_setup_tls
_dl_tls_setup
__pthread_initialize_minimal
__libc_csu_init
__libc_csu_fini
__assert_fail_base
__assert_fail
dcgettext
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
.text:00000000004009AE ; =============== S U B R O U T I N E =======================================
.text:00000000004009AE ; Attributes: bp-based frame
.text:00000000004009AE ; int __cdecl main(int argc, const char **argv, const char **envp)
.text:00000000004009AE public main
.text:00000000004009AE main proc near ; DATA XREF: _start+1D↑o
.text:00000000004009AE var_70 = byte ptr -70h
.text:00000000004009AE var_8 = qword ptr -8
.text:00000000004009AE push rbp
.text:00000000004009AF mov rbp, rsp
.text:00000000004009B2 sub rsp, 70h
.text:00000000004009B6 mov rax, fs:28h
.text:00000000004009BF mov [rbp+var_8], rax
.text:00000000004009C3 xor eax, eax
.text:00000000004009C5 lea rax, [rbp+var_70]
.text:00000000004009C9 mov rsi, rax
.text:00000000004009CC mov edi, offset a96s ; "%96s"
.text:00000000004009D1 mov eax, 0
.text:00000000004009D6 call __isoc99_scanf
.text:00000000004009DB lea rax, [rbp+var_70]
.text:00000000004009DF mov esi, offset flag ; "flag{Upx_1s_n0t_a_d3liv3r_c0mp4ny}"
.text:00000000004009E4 mov rdi, rax
.text:00000000004009E7 call sub_400360
.text:00000000004009EC test eax, eax
.text:00000000004009EE jnz short loc_4009FC
.text:00000000004009F0 mov edi, offset aCongratulation ; "Congratulations!"
.text:00000000004009F5 call puts
.text:00000000004009FA jmp short loc_400A06
.text:00000000004009FC ; ---
.text:00000000004009FC
.text:00000000004009FC loc_4009FC: ; CODE XREF: main+40↑j
.text:00000000004009FC mov edi, offset aTryAgain ; "Try again!"
.text:0000000000400A01 call puts
.text:0000000000400A06
.text:0000000000400A06 loc_400A06: ; CODE XREF: main+4C↑j
.text:0000000000400A06 mov eax, 0
.text:0000000000400A0B mov rdx, [rbp+var_8]
.text:0000000000400A0F xor rdx, fs:28h
.text:0000000000400A18 jz short locret_400A1F
.text:0000000000400A1A call __stack_chk_fail
.text:0000000000400A1F ; ---
.text:0000000000400A1F
000009AE 00000000004009AE: main (Synchronized with Hex View-1)
Output window
CSDN @starmultiple


File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
_init_proc
sub_400300
sub_400310
sub_400320
sub_400330
sub_400340
sub_400350
sub_400360
sub_400370
sub_400380
backtrace_and_maps
detach_arena_part_0
__gconv_release_step_part_1
read_int
read_int_0
oom
fini
init_cacheinfo
_start
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
frame_dummy
main
generic_start_main
get_common_indeces_constprop_1
__libc_start_main
__libc_check_standard_fds
Graph overview
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
; Attributes: bp-based frame
; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near
var_70= byte ptr -70h
var_8= qword ptr -8
push rbp
mov rbp, rsp
sub rsp, 70h
mov rax, fs:28h
mov [rbp+var_8], rax
xor eax, eax
lea rax, [rbp+var_70]
mov rsi, rax
mov edi, offset a96s ; "%96s"
mov eax, 0
call __isoc99_scanf
lea rax, [rbp+var_70]
mov esi, offset flag ; "flag{Upx_1s_n0t_a_d3liv3r_c0mp4ny}"
mov rdi, rax
call sub_400360
test eax, eax
jnz short loc_4009FC
mov edi, offset aCongratulation ; "Congratulations!"
call puts
jmp short loc_400A06
loc_4009FC: ; "Try again!"
mov edi, offset aTryAgain
call puts
100.00% (-302,-82) (711,417) 000009AE 00000000004009AE: main (Synchronized with Hex View-1)
Output window
CSDN @starmultiple