



flag

flag - 7 pt [writeup]

Papa brought me a packed present! let's open it.

Download : <http://pwnable.kr/bin/flag>

This is reversing task. all you need is binary

pwned (12365) times. early 30 pwners are : cd80 ▼

Flag?: auth

wget으로 다운받아서 gdb로 살펴보았으나 나오는데 없다..

packed present!.. unpack하면 될거 같은데.. 그게 뭐징?ㅋㅋㅋㅋ

This is reversing task. 리버싱.. 하하 처음들어보는 거 리버싱이 뭔지 살펴보자

리버싱(reversing)

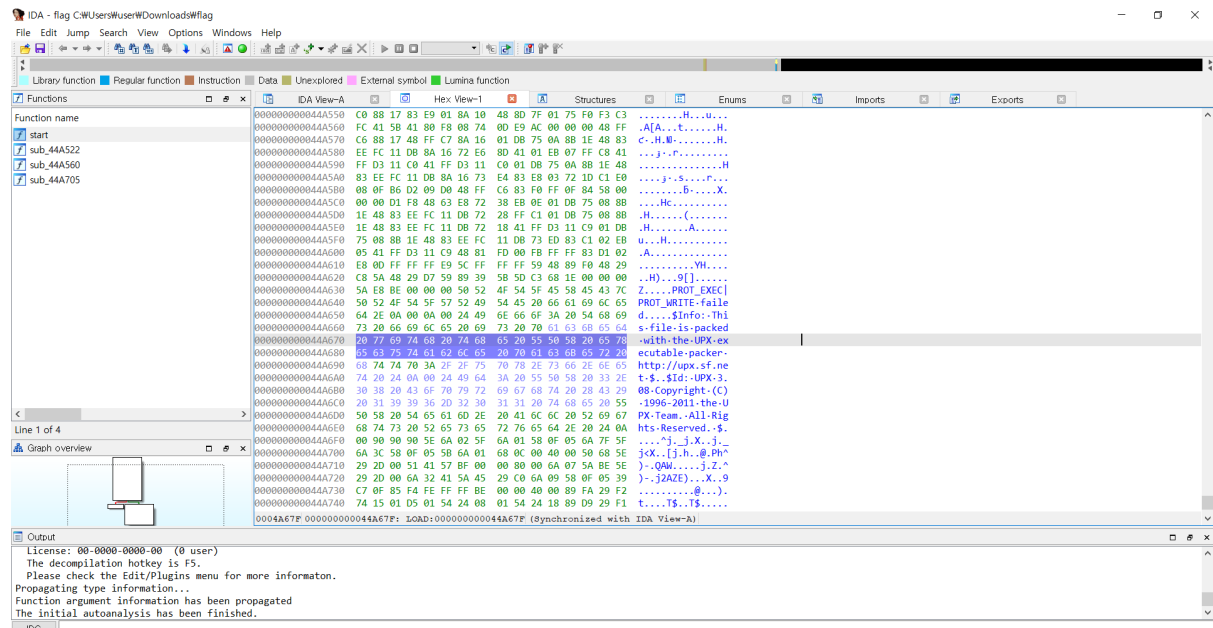
리버스(reverse)와 엔지니어링(engineering)을 합친 엔지니어링을 줄인 말로써 역공학의 한 분야이다

리버스 엔지니어링

- 소스를 역추적하는 것을 말함
- 소스코드를 빌드해서 만들어진 exe, dll의 바이너리르 분석해 원래의 소스코드가 어떤 식으로 만들어져 있는지 파악한다.

리버싱은 해야할 것 같으니 리버싱 도구중 IDA를 설치해봤다...

ida로 파일을 열어서 보니까

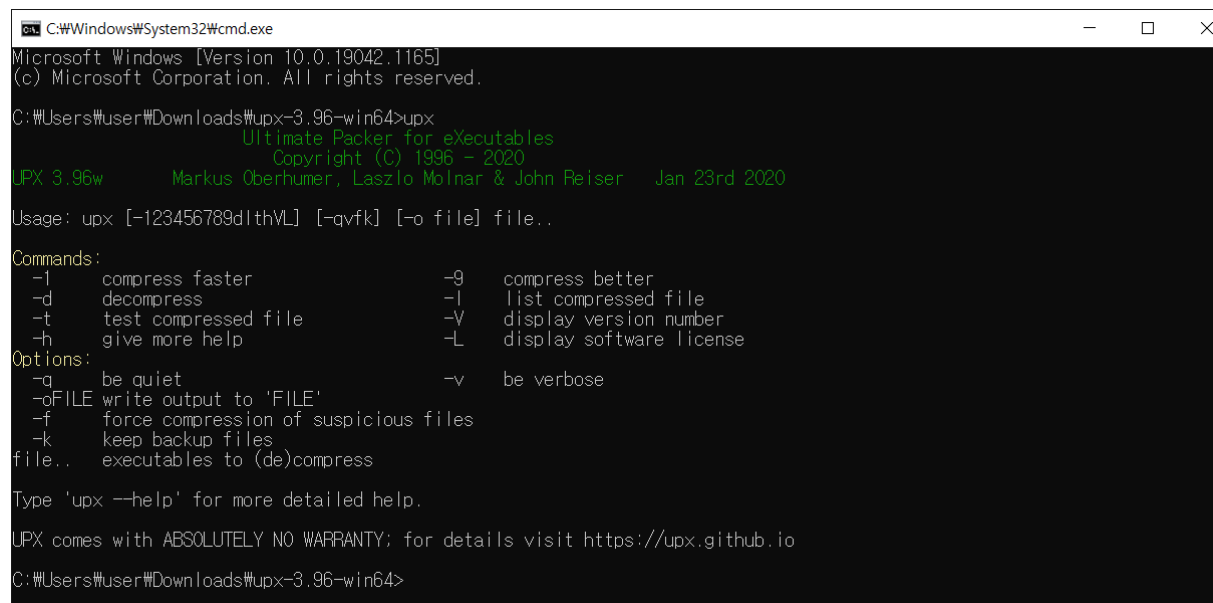


Info This file is packed with the UPX executable packer 이라는 말이 보인다. 그럼이제 UPX executable packer를 구글링해보자ㅋㅋㅋ아놔!!!!!!

UPX를 언패킹하기 위해선 이 [사이트](#)에서 upx를 다운받아야한다고 한다.

그 다음 upx.exe와 언패킹할 flag파일을 같은 폴더에 두고 해당 폴더에서 cmd를 실행시킨다.

cmd에 upx라고 치면 upx사용법을 보여준다



IDA - flag C:\Users\User\Downloads\upx-396-win64\flag

File Edit Jump Search View Options Windows Help

Library function Regular function Instruction Data Unexplored External symbol Lumina function

Functions

Function name

- __init_proc
- strcpy
- strcpy
- strlen
- memmove
- memcpy
- strcmp
- __strncasecmp
- memset
- strcmp
- __strncasecmp
- __strchr
- check_one_fd_part_0
- mummap_chunk_part_4
- group_number
- j18n_number_rewrite
- j18n_number_rewrite_0
- trusted_path_normalize
- print_search_path
- strip
- group_number_0
- j18n_number_rewrite_1
- fini
- init_cachefn

IDA View-A Hex View-1 Structures Enums Imports Exports

```

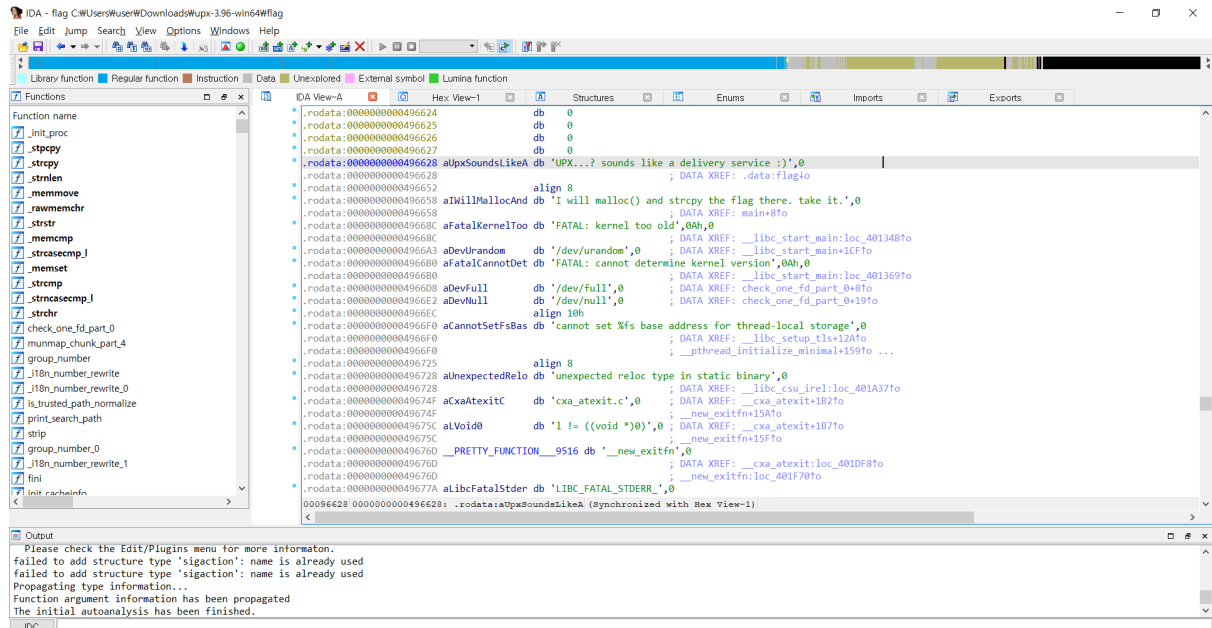
.data:000000000000C2068      dso_handle dq 0 ; DATA XREF: ptmalloc_init_part_8+440
.data:000000000000C2068      public flag ; ptmalloc_init_part_8+52ftr ...
.data:000000000000C2070      flag dq offset alpxSoundsLikeA ; DATA XREF: main+20ftr
; DATA XREF: ? sounds like a delivery service ...
.data:000000000000C2078      align 20h public _dl_tls_static_size
; DATA XREF: _libc_setup_tls:loc_401520ftr
; _libc_setup_tls+1C8ftr ...
.data:000000000000C2080      _dl_tls_static_size dq 800h
; DATA XREF: _libc_setup_tls:loc_401520ftr
; _libc_setup_tls+1C8ftr ...
.data:000000000000C2088      align 10h public __exit_funcs
; DATA XREF: exit+0ftr
; _cxa_atexit:loc_401C8Bftr ...
.data:000000000000C2090      __exit_funcs dq offset initial
; DATA XREF: _IO_2_1_stderr_
; _IO_2_1_stderr_+21Bftr ...
.data:000000000000C2098      align 20h public _IO_list_all
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20A0      _IO_list_all dq offset _IO_2_1_stderr_
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20A8      align 20h public _IO_2_1_stderr_
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20B0      _IO_2_1_stderr_ db 80h
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20C0      db 20h
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20C2      db 0ADh
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20C3      db 0FBh
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20C4      db 0
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20C5      db 0
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20C6      db 0
; DATA XREF: _data:_IO_list_allto
; _data:stderr
.data:000000000000C20C7      db 0
; DATA XREF: _data:_IO_list_allto
; _data:stderr
000C2070 000000000000C2070: .data:flag (Synchronized with Hex View-1)

```

Output

Please check the Edit/Plugins menu for more information.
 failed to add structure type 'sigaction': name is already used
 failed to add structure type 'sigaction': name is already used
 Propagating type information...
 Function argument information has been propagated
 The initial autoanalysis has been finished.

flag



다음과 같이 뜯다. 그래서 초록색 줄을 입력해보니 정답이더라!! 근데 아직 뭐가 뭔지 모르겠는 기분..... 아 그리고 peid를 이용하면 따로 안 찾아봐도 upx packing인지 아닌지 알려주는 듯 하다.

간지나게 적고싶다.....