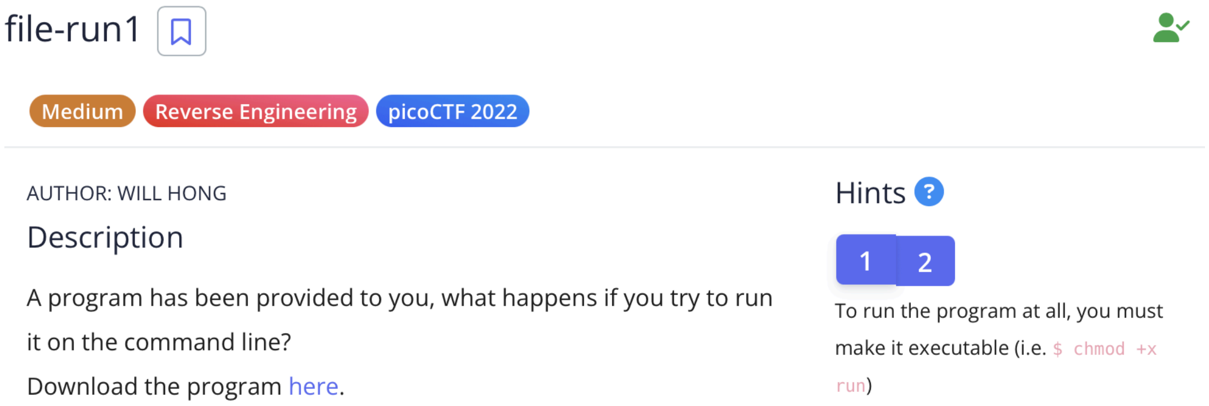


file-run1

Medium Reverse Engineering picoCTF 2022

AUTHOR: WILL HONG

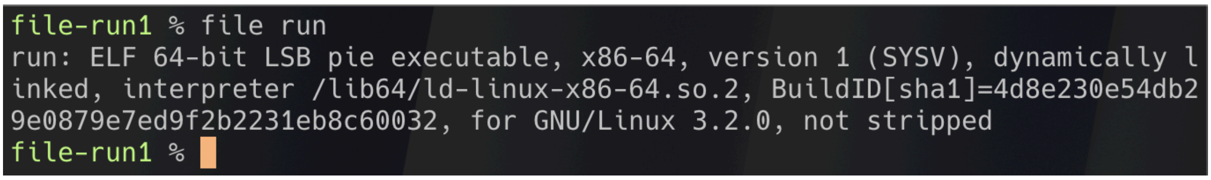
Description

A program has been provided to you, what happens if you try to run it on the command line?

Download the program here.

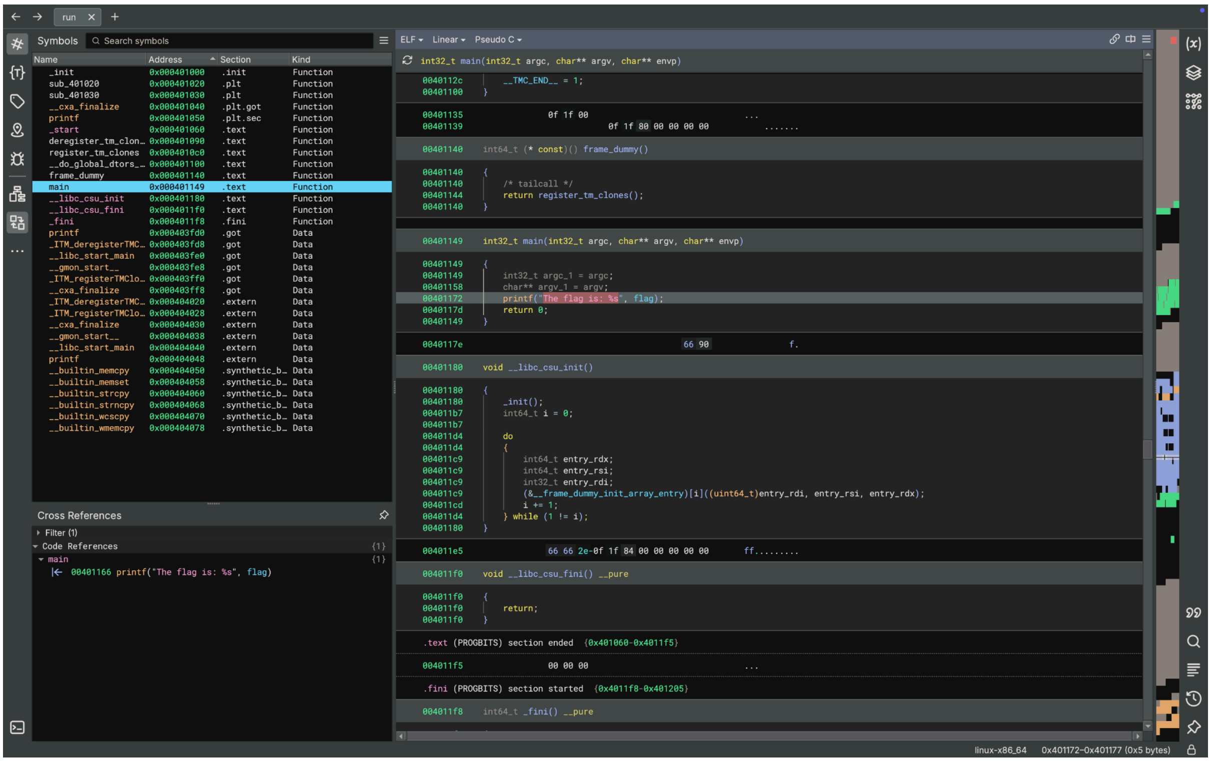
Hints

To run the program at all, you must make it executable (i.e. `$ chmod +x run`)



```
file-run1 % file run
run: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically l
inked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=4d8e230e54db2
9e0879e7ed9f2b2231eb8c60032, for GNU/Linux 3.2.0, not stripped
file-run1 %
```

Solusi :

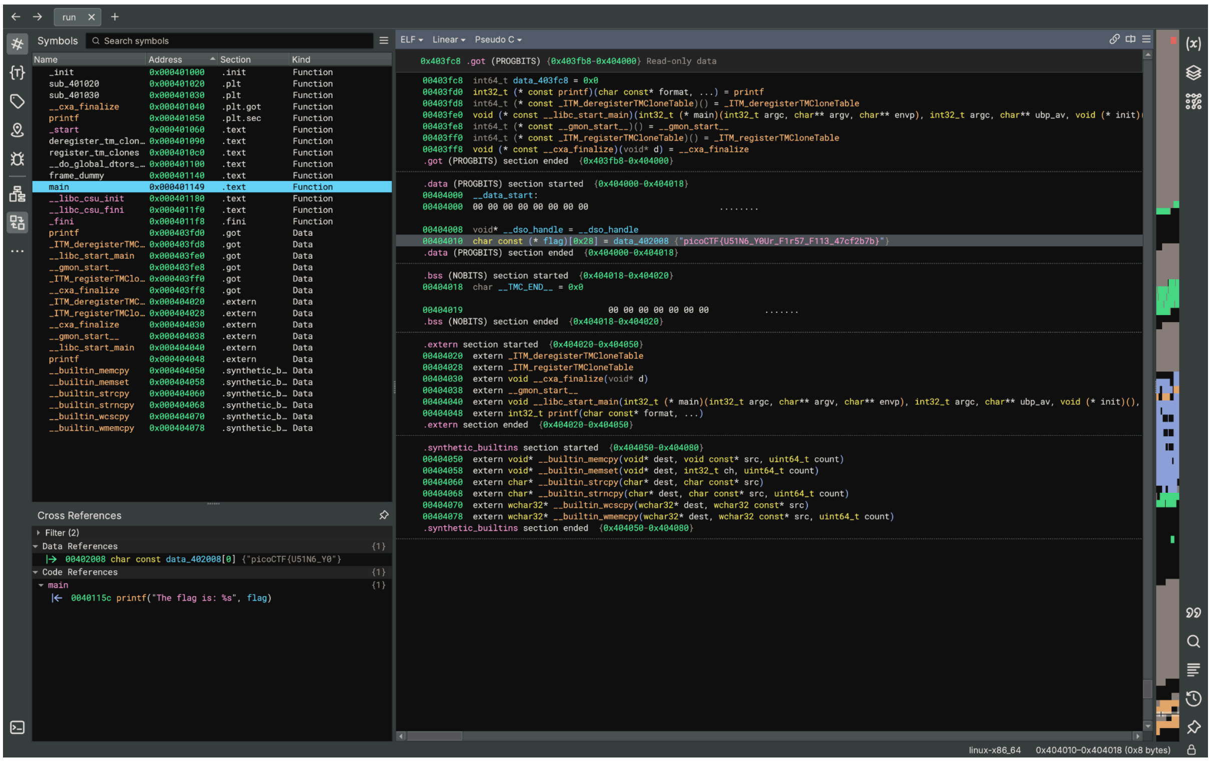


Name	Address	Section	Kind
_init	0x000401000	.init	Function
sub_401020	0x000401020	.plt	Function
sub_401030	0x000401030	.plt	Function
__cxa_finalize	0x000401040	.plt.got	Function
printf	0x000401050	.plt.sec	Function
_start	0x000401060	.text	Function
deregister_tm_clon…	0x000401090	.text	Function
register_tm_clones	0x0004010c0	.text	Function
__do_global_dtors_…	0x000401100	.text	Function
frame_dummy	0x000401140	.text	Function
main	0x000401149	.text	Function
__libc_csu_init	0x000401180	.text	Function
__libc_csu_fini	0x0004011f0	.text	Function
_fini	0x0004011f8	.fini	Function
printf	0x000403fd0	.got	Data
_ITM_deregisterTMC…	0x000403fd8	.got	Data
__libc_start_main	0x000403fe0	.got	Data
__gmon_start__	0x000403fe8	.got	Data
_ITM_registerTMClo…	0x000403ff0	.got	Data
__cxa_finalize	0x000403ff8	.got	Data
_ITM_deregisterTMC…	0x000404020	.extern	Data
_ITM_registerTMClo…	0x000404028	.extern	Data
__cxa_finalize	0x000404030	.extern	Data
__gmon_start__	0x000404038	.extern	Data
__libc_start_main	0x000404040	.extern	Data
printf	0x000404048	.extern	Data
__builtin_memcpy	0x000404050	.synthetic_b…	Data
__builtin_memset	0x000404058	.synthetic_b…	Data
__builtin_strcpy	0x000404060	.synthetic_b…	Data
__builtin_strncpy	0x000404068	.synthetic_b…	Data
__builtin_wcscpy	0x000404070	.synthetic_b…	Data
__builtin_wmemcpy	0x000404078	.synthetic_b…	Data

```
Cross References
Filter (1)
Code References                                  {1}
  main                                           {1}
    |← 00401166 printf("The flag is: %s", flag)
```

```
int32_t main(int32_t argc, char** argv, char** envp)
0040112c        __TMC_END__ = 1;
00401100    }

00401135                0f 1f 00                          ...
00401139                        0f 1f 80 00 00 00 00        .......

00401140    int64_t (* const)() frame_dummy()

00401140    {
00401140        /* tailcall */
00401144        return register_tm_clones();
00401140    }

00401149    int32_t main(int32_t argc, char** argv, char** envp)

00401149    {
00401149        int32_t argc_1 = argc;
00401158        char** argv_1 = argv;
00401172        printf("The flag is: %s", flag);
0040117d        return 0;
00401149    }

0040117e                                66 90                 f.

00401180    void __libc_csu_init()

00401180    {
00401180        _init();
004011b7        int64_t i = 0;
004011b7
004011d4        do
004011d4        {
004011c9            int64_t entry_rdx;
004011c9            int64_t entry_rsi;
004011c9            int32_t entry_rdi;
004011c9            (&__frame_dummy_init_array_entry)[i]((uint64_t)entry_rdi, entry_rsi, entry_rdx);
004011cd            i += 1;
004011d4        } while (1 != i);
00401180    }

004011e5            66 66 2e-0f 1f 84 00 00 00 00 00      ff.........

004011f0    void __libc_csu_fini() __pure

004011f0    {
004011f0        return;
004011f0    }

.text (PROGBITS) section ended  {0x401060-0x4011f5}

004011f5            00 00 00                              ...

.fini (PROGBITS) section started  {0x4011f8-0x401205}

004011f8    int64_t _fini() __pure
```

Di dalam fungsi main, terdapat tulisan flag, bisa kita pencet 2 kali untuk mengetahui dimana letak flag tersebut disimpan.



Name	Address	Section	Kind
_init	0x000401000	.init	Function
sub_401020	0x000401020	.plt	Function
sub_401030	0x000401030	.plt	Function
__cxa_finalize	0x000401040	.plt.got	Function
printf	0x000401050	.plt.sec	Function
_start	0x000401060	.text	Function
deregister_tm_clon…	0x000401090	.text	Function
register_tm_clones	0x0004010c0	.text	Function
__do_global_dtors_…	0x000401100	.text	Function
frame_dummy	0x000401140	.text	Function
main	0x000401149	.text	Function
__libc_csu_init	0x000401180	.text	Function
__libc_csu_fini	0x0004011f0	.text	Function
_fini	0x0004011f8	.fini	Function
printf	0x000403fd0	.got	Data
_ITM_deregisterTMC…	0x000403fd8	.got	Data
__libc_start_main	0x000403fe0	.got	Data
__gmon_start__	0x000403fe8	.got	Data
_ITM_registerTMClo…	0x000403ff0	.got	Data
__cxa_finalize	0x000403ff8	.got	Data
_ITM_deregisterTMC…	0x000404020	.extern	Data
_ITM_registerTMClo…	0x000404028	.extern	Data
__cxa_finalize	0x000404030	.extern	Data
__gmon_start__	0x000404038	.extern	Data
__libc_start_main	0x000404040	.extern	Data
printf	0x000404048	.extern	Data
__builtin_memcpy	0x000404050	.synthetic_b…	Data
__builtin_memset	0x000404058	.synthetic_b…	Data
__builtin_strcpy	0x000404060	.synthetic_b…	Data
__builtin_strncpy	0x000404068	.synthetic_b…	Data
__builtin_wcscpy	0x000404070	.synthetic_b…	Data
__builtin_wmemcpy	0x000404078	.synthetic_b…	Data

```
Filter (2)
Data References                                                      {1}
  |→ 00402008 char const data_402008[0] {"picoCTF{U51N6_Y0"}
Code References                                                      {1}
  main                                                               {1}
    |← 0040115c printf("The flag is: %s", flag)
```

```
0x403fc8 .got (PROGBITS) {0x403fb8-0x404000} Read-only data

00403fc8  int64_t data_403fc8 = 0x0
00403fd0  int32_t (* const printf)(char const* format, ...) = printf
00403fd8  int64_t (* const _ITM_deregisterTMCloneTable)() = _ITM_deregisterTMCloneTable
00403fe0  void (* const __libc_start_main)(int32_t (* main)(int32_t argc, char** argv, char** envp), int32_t argc, char** ubp_av, void (* init)(
00403fe8  int64_t (* const __gmon_start__)() = __gmon_start__
00403ff0  int64_t (* const _ITM_registerTMCloneTable)() = _ITM_registerTMCloneTable
00403ff8  void (* const __cxa_finalize)(void* d) = __cxa_finalize
.got (PROGBITS) section ended  {0x403fb8-0x404000}

.data (PROGBITS) section started  {0x404000-0x404018}
00404000  __data_start:
00404000  00 00 00 00 00 00 00 00                          ........

00404008  void* __dso_handle = __dso_handle
00404010  char const (* flag)[0x28] = data_402008 {"picoCTF{U51N6_Y0Ur_F1r57_F113_47cf2b7b}"}
.data (PROGBITS) section ended  {0x404000-0x404018}

.bss (NOBITS) section started  {0x404018-0x404020}
00404018  char __TMC_END__ = 0x0

00404019                       00 00 00 00 00 00 00          .......
.bss (NOBITS) section ended  {0x404018-0x404020}

.extern section started  {0x404020-0x404050}
00404020  extern _ITM_deregisterTMCloneTable
00404028  extern _ITM_registerTMCloneTable
00404030  extern void __cxa_finalize(void* d)
00404038  extern __gmon_start__
00404040  extern void __libc_start_main(int32_t (* main)(int32_t argc, char** argv, char** envp), int32_t argc, char** ubp_av, void (* init)(),
00404048  extern int32_t printf(char const* format, ...)
.extern section ended  {0x404020-0x404050}

.synthetic_builtins section started  {0x404050-0x404080}
00404050  extern void* __builtin_memcpy(void* dest, void const* src, uint64_t count)
00404058  extern void* __builtin_memset(void* dest, int32_t ch, uint64_t count)
00404060  extern char* __builtin_strcpy(char* dest, char const* src)
00404068  extern char* __builtin_strncpy(char* dest, char const* src, uint64_t count)
00404070  extern wchar32* __builtin_wcscpy(wchar32* dest, wchar32 const* src)
00404078  extern wchar32* __builtin_wmemcpy(wchar32* dest, wchar32 const* src, uint64_t count)
.synthetic_builtins section ended  {0x404050-0x404080}
```

Flag : picoCTF{U51N6_Y0Ur_F1r57_F113_47cf2b7b}