

Write-Up: It is all about da strings (Rev)

Ομάδα: mousiko_gymsasio_agrinou_lt_1 (Μουσικό Γυμνάσιο
Αγρινίου - Λ.Τ.)
Μαθητές/Μαθήτριες Πέτρος Παπαθανασίου

Επισκόπηση Δοκιμασίας

Η δοκιμασία μας δίνει ένα αρχείο binary. Από την εκφώνηση καταλαβαίνουμε ότι πρέπει να βρούμε κάποιον συγκεκριμένο κωδικό

Επίλυση

Αρχική ανάλυση

Άνοιξα το αρχείο με έναν hex editor (πχ. VSCode) και είδα ότι θέλει να το τρέξω με παράμετρο.

```
00002000 01 00 02 00 00 00 00 55 73 61 67 65 3A 20 25  . . . . Usage: % float32 0
00002010 73 20 3C 73 65 63 72 65 74 3E 0A 00 00 00 00  s <secret> . . . . float64 9.718864971055825e+189
00002020 43 6F 72 72 65 63 74 20 73 65 63 72 65 74 21 20  C o r r e c t   s e c r e t ! . . . . GUID End of File
00002030 41 63 63 65 73 73 20 67 72 61 6E 74 65 64 21 00  A c c e s s   g r a n t e d ! . . . . ASCII []
00002040 49 6E 63 6F 72 72 65 63 74 20 73 65 63 72 65 74  I n c o r r e c t   s e c r e t . . . . UTF-8 []
00002050 21 20 54 72 79 20 61 67 61 69 6E 2E 00 00 00 00  !   T r y   a g a i n . . . . UTF-16 []
00002060 01 1B 03 3B 44 00 00 00 07 00 00 00 C0 EF FF FF  . . . ; D . . . . GB18030 []
```

Σε ένα terminal έδωσα την εντολή `./binary` και μου έδωσε ως απάντηση `Usage: ./binary <secret>`.

```
$ ./binary
Usage: ./binary <secret>
```

Εκμετάλλευση ευπάθειας

Για να δω όλα τα σύμβολα που περιέχει το binary έτρεξα την εντολή `strings ./binary`

```
└─$ strings ./binary
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
__stack_chk_fail
printf
__cxa_finalize
strcmp
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
FLAG{w3l1
1_th1s_wH
4S_n0T_th
h4T_hArDh
[]A\A]A^A_
Usage: %s <secret>
Correct secret! Access granted!
Incorrect secret! Try again.
:*3$"
```

Έτσι μπόρεσα να πάρω ένα κείμενο στην μορφή σημαίας. Άφου έτρεξα το αρχείο με διάφορους συνδιασμούς της μορφής του flag, κατάφερα να βρω το σωστό.

```
└─$ ./binary FLAG{w3l1_1_th1s_w4S_n0T_th4T_hArD}
Correct secret! Access granted!
```

Σημαία

Η σημαία που βρέθηκε:

FLAG{w3l1_1_th1s_w4S_n0T_th4T_hArD}