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

Ομάδα: mousiko_gymsasio_agriniou_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

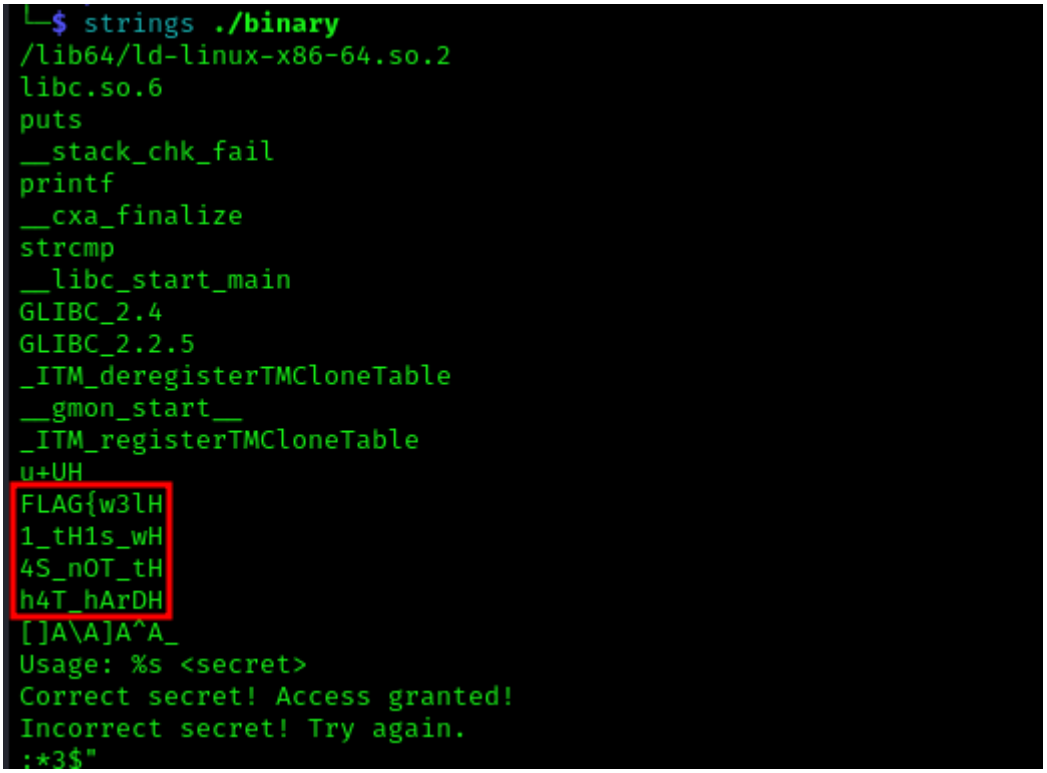
Αρχική ανάλυση

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

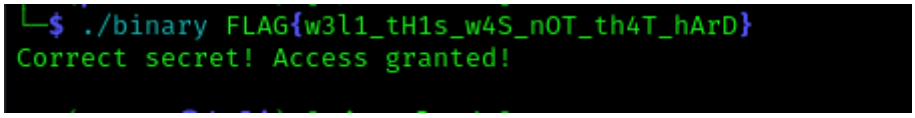
Σε ένα terminal έδωσα την εντόλη ./binary και μου έδωσε ως απάντηση “Usage: ./binary <secret>”.

Εκμετάλλευση ευπάθειας

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



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.



Σημαία

Η σημαία που βρέθηκε:

```
FLAG{w3l1_tH1s_w4S_nOT_th4T_hArD}
```