Write-Up: Nwbin (Rev)

|  |  |
| --- | --- |
| Ομάδα: | mousiko\_gymsasio\_agriniou\_lt\_1 (Μουσικό Γυμνάσιο Αγρινίου - Λ.Τ.) |
| Μαθητές/Μαθήτριες | Πέτρος Παπαθανασίου |

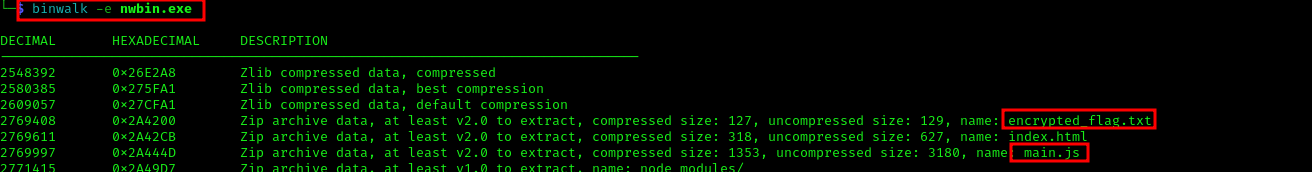
# Επισκόπηση Δοκιμασίας

Η δοκιμασία μας δίνει ένα zip αρχείο που περιέχει ένα exe binary. Αναζητεί την λύση ενός γρίφου ωστέ να μας δώσει την σημαία.

# Επίλυση

## Αρχική ανάλυση

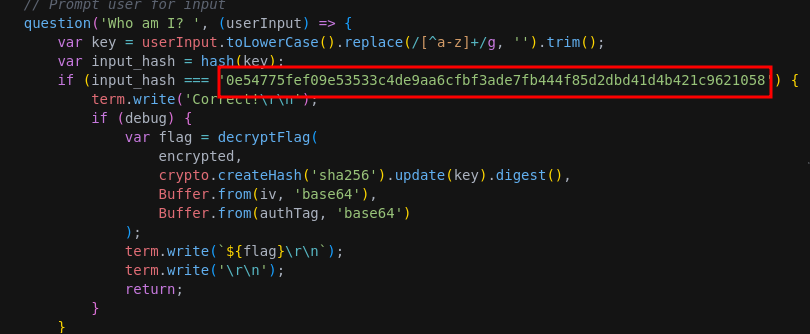
Το ανοίγω με έναν hex editor και βλέπω ότι έχει μέσα κρυμμένο ένα αρχείο με όνομα encrypted\_flag.txt. Με το εργαλείο binwalk μπορώ να εξάγω όλα τα αρχεία που βρίσκονται πίσω από το exe. Ανάμεσα σε αυτά βρίσκεται και το encrypted\_flag.txt, όπως και το main.js.

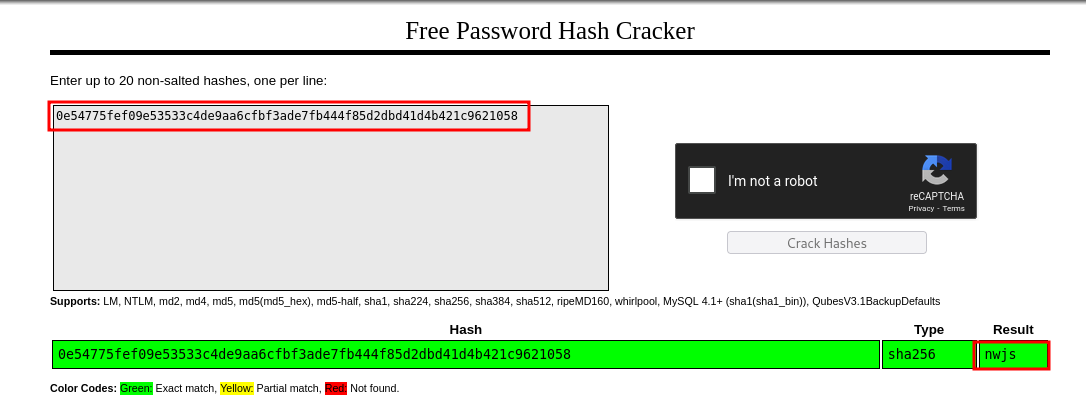


Ψάχνοντας όλα τα διαθέσιμα αρχεία, το μόνο που ήταν αναγνώσιμο ήταν το main.js, το οποίο περιείχε τον κώδικα της εφαρμογής.

## Εκμετάλλευση ευπάθειας

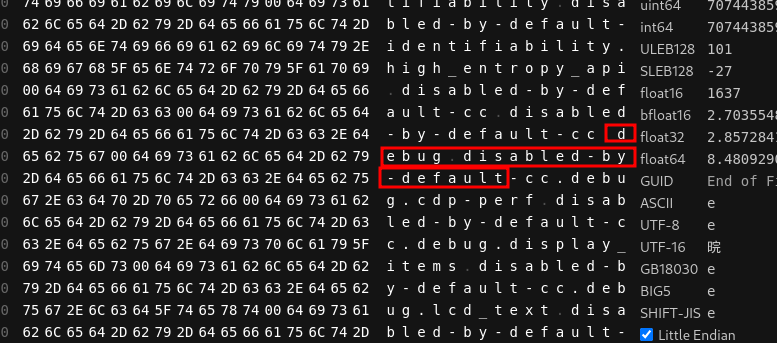
Από αυτόν πήρα το σωστό hash και με ένα εργαλείο όπως το CrackStation μπόρεσα να δω το σωστό κλειδί.



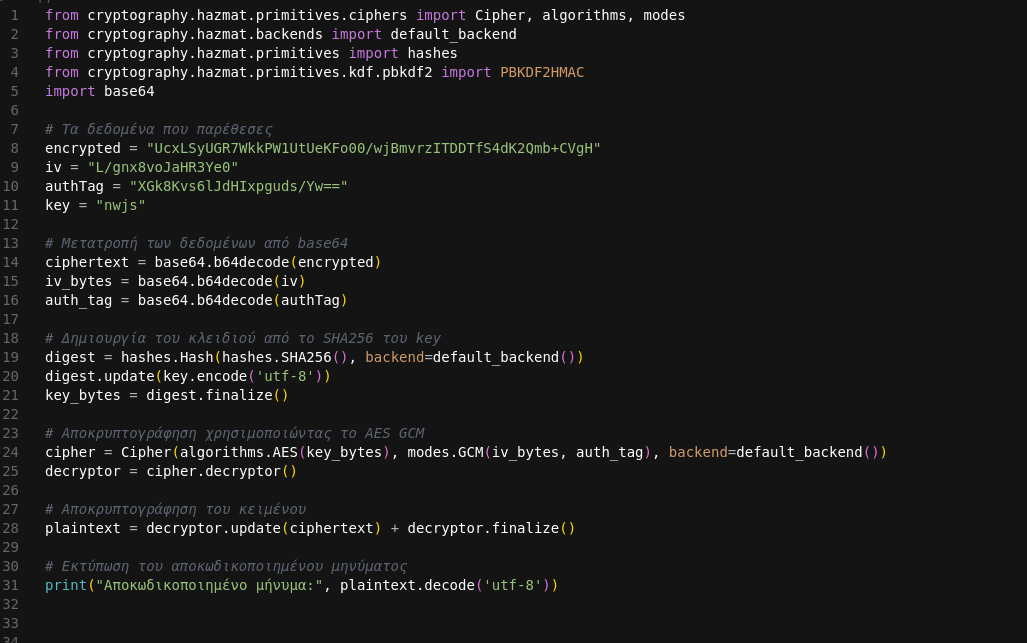


Στην συνέχεια γνωρίζοντας τον σωστό κωδικό μπόρεσα να τρέξω την εφαρμογή για να δείξει την σημαία.

Παρατήρησα ότι εμφανίζει την λέξη “Correct”, αλλά όχι την σημαία. Αυτό συμβαίνει γιατι στην εντολή “if (debug)”, που φαίνεται πιο πάνω το debug είναι απενεργοποιημένο. Αυτό μπορούμε να το δούμε από το binary αρχείο.



Το προφανές είναι να ενεργοποιήσουμε το debug. Όμως αφού δεν μπόρεσα να το τρέξω έτσι, δημιούργησα έναν κώδικα σε python, ο οποίος παίρνει την κωδικοποιημένη σημαία, την λέξη κλειδί και την μέθοδο κωδικοποίησης και δίνει ως αποτέλεσμα την αποκωδικοποιημένη σημαία.





# Σημαία

Η σημαία που βρέθηκε:

|  |
| --- |
| FLAG{i\_tH1nK\_I\_4m\_uNp4cK1nG\_l1KE\_a\_Pr0} |