

Write-Up: Emojious (Rev)

Ομάδα: mousiko_gymsasio_agriniou_lt_1 (Μουσικό Γυμνάσιο

Αγρινίου - Λ.Τ.)

Μαθητές/Μαθήτριες Πέτρος Παπαθανασίου

Επισκόπηση Δοκιμασίας

Η συγκεκριμένη δοκιμασία μας δίνει έναν κώδικα σε python. Αυτός ασχολείται με τα emojies και ψάχνει ένα κρυμμένο κλειδί.

Επίλυση

Αρχική ανάλυση

Όταν τρέχω τον κώδικα μου βγάζει μήνυμα γία input.

Για αυτό, άνοιξα το <u>emojious.py</u> με ένα πρόγραμμα ανάγνωσης (π.χ. VSCode) και παρατήρησα τον κώδικα. Αμέσως είδα ότι το κλείδι είναι η λέξη flag σε μορφή FLAG{...}.

```
# Hint: The key is the flag and the flag format is FLAG{....}
```

Αφού έκανα κάποιες δοκιμές στην μορφή του μηνύματος όπως FLAG{....}, FLAG{}, FLAG{...., FLAG{, διαπίστωσα ότι πιθανόν έπρεπε να δω μόνο τους πρώτους χαρακτήρες του κωδικοποιημένου μηνύματος.

Κατάλαβα ότι το πλήθος χαρακτήρων στο key που πρέπει να δώσω σχετίζεται με τον πλήθος των emoji, με τα οποία πρέπει να λειτουργήσω.

Εκμετάλλευση ευπάθειας

Έχοντας ως γνωστούς τους 5 πρώτους χαρακτήρες έτρεξα το πρόγραμμα και έβαλα ως κλειδί την λέξη "FLAG{" έδωσε το αποτέλεσμα. Όμως η εκφραση που έδωσα αντιστοιχεί μόνο στα 5 πρώτα emoji.



```
This is interesting: [] $\infty , | \text{Proposition of the proposition of the proposit
```

Τρέχω ξανά το πρόγραμμα και δίνει ως κλειδί τα emoji που αντιστοιχούν στο "FLAG{". Έτσι το πρόγραμμα μου έδωσε το σωστό flag της δοκιμασίας.

```
This is interesting: $\begin{aligned}
\text{\text{M} \text{\text{M} \text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\tint{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\te\
```

Σημαία

Η σημαία που βρέθηκε:

FLAG{emojis_are_really_special_these_days}