# Write-Up: Luck out loud (Misc)

Ομάδα: mousiko_gymsasio_agriniou_lt_1 (Μουσικό Γυμνάσιο Αγρινίου - Λ.Τ.)
Μαθητές/Μαθήτριες Πέτρος Παπαθανασίου

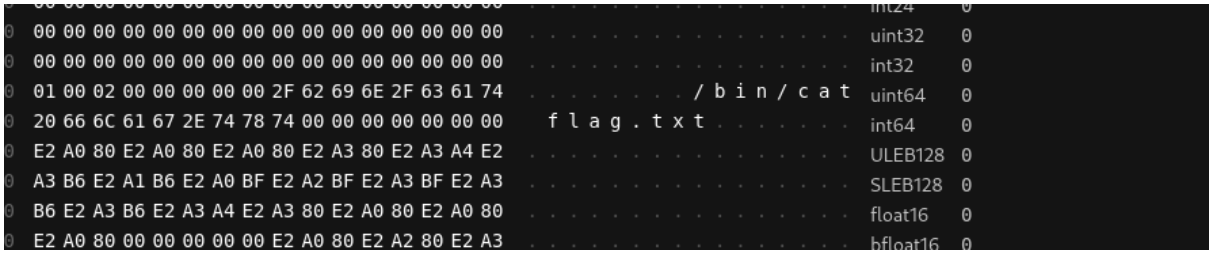
## Επισκόπηση Δοκιμασίας

Η δοκιμασία μας δίνει ένα εκτέλισιμο αρχείο linux. Μας ζητάει να μαντέψουμε 100 αριθμούς, σύμφωνα με την σειρά που τους έχει το πρόγραμμα. Αν δώσουμε λάθος αριθμό, το πρόγραμμα σταματάει.

## Επίλυση

### Αρχική ανάλυση

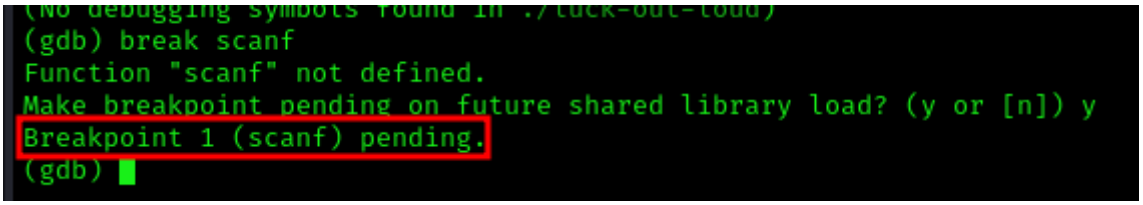
Έτρεξα το VSCode και άνοιξα το εκτελέσιμο αρχείο με hex editor. Παρατήρησα ότι όταν τελειώσει το πρόγραμμα τυπώνει ένα αρχείο, που πιθανόν βρίσκεται η σημαία.



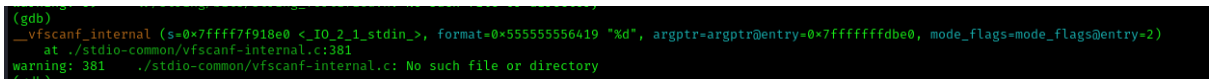

Στην αρχή προσπάθησα να δώσω εντολές με σκοπό την τεχνική command injection. Για παράδειγμα, έδωσα είσοδο “11 && ls” με διάφορους συνδυασμούς. Μετά από αρκετές προσπάθειες κατάλαβα ότι μάλλον λύνεται με διαφορετικό τρόπο.

### Εκμετάλλευση ευπάθειας

Άνοιξα με την εφαρμογή gdb το εκτελέσιμο αρχείο της δοκιμασίας και έβαλα breakpoint στην συνάρτηση scanf, για να δω στην συνέχεια που γίνεται ο έλεγχος του αριθμού μήπως και τον παρακάμψω. Όμως δεν μου επέτρεπε το πρόγραμμα να βάλω εκεί breakpoint.

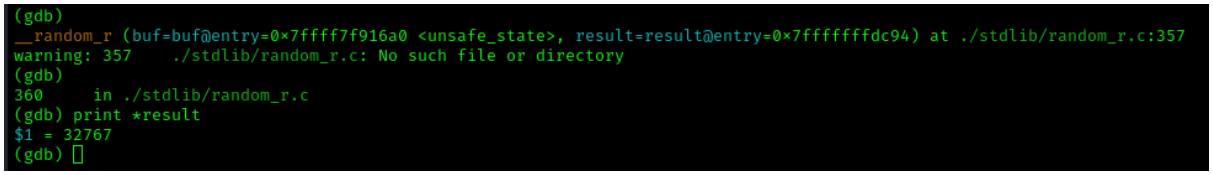


Σκέφτηκα να πάω στην προηγούμενη printf και να προχωρήσω με βήματα. Όταν βρήκα την scanf, συνέχησα με βήμα μέχρι να βρω την εντολή που ελέγχει.




Δεν μπόρεσα να την βρω και το πρόγραμμα πέρασε πάλι στην συνάρτηση main. Για αυτό έκανα breakpoint στην main, που είναι μετά την scanf. Και πάλι όμως μετά την εισαγωγή αριθμού δεν έχω αποτέλεσμα.

Αφού δεν μπόρεσα να εντοπίσω την if που ελέγχει το input με την σωστή απάντηση, αποφάσισα να κινηθώ προς την συνάρτηση που δημιουργεί τον τυχαίο αριθμό (rand). Προχωρώντας με βήματα είδα ότι η σωστή απάντηση αποθηκεύεται σε μια μεταβλητή result με μία συγκεκριμένη διεύθυνση (0x7fffffffdc94). Δίνοντας την εντολή “print *result” μου επέστρεψε “32767”.

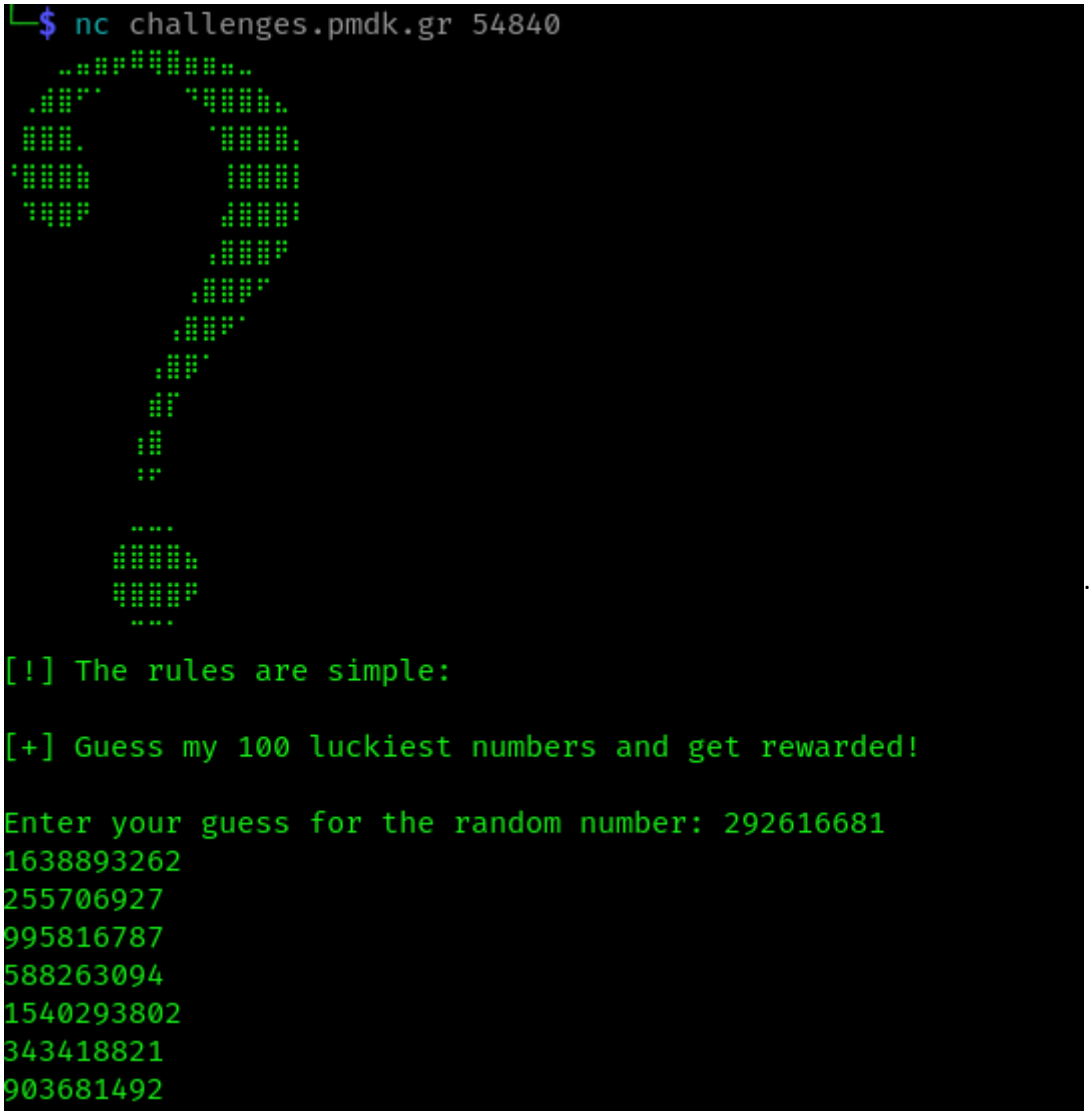


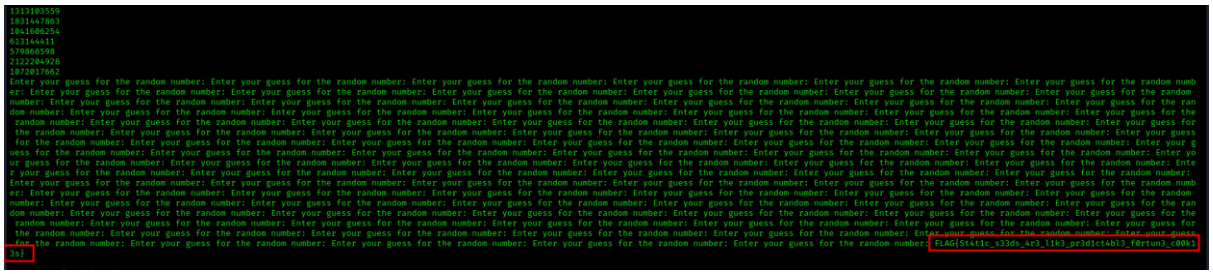

Θεώρησα ότι αυτός είναι ο πρώτος αριθμός. Με την εντολή continue έτρεξα το πρόγραμμα και τον έδωσα ως input. Παρ’ όλ’ αυτά δεν δούλεψε. Οπότε σκέφτηκα μήπως γίνεται κάποιος μετασχηματισμός σε αυτόν τον αριθμό.

Έτρεξα ξανά το πρόγραμμα και προχώρησα λίγο περισσότερο ώσπου έφτασα στην printf. Έδειχνε να είναι αδιέξοδο, γιατί ακολουθούσα προηγούμενα βήματα.

Ξεκίνησα από την αρχή με την εντολή “break rand” και σε κάθε βήμα έκανα “print *result”. Διαπίστωσα ότι το “32767” άλλαξε. Πήρα τον αριθμό αυτόν και τον έβαλα στο input. Ήταν σωστός. Επανέλαβα την διαδικασία για τον επόμενο και ήταν και αυτός σωστός. Δοκιμάζοντας να ξανατρέξω το πρόγραμμα με τον debugger είδα ότι εμφανίζονταν οι αριθμοί με την ίδια σειρά, γεγονός που οφείλεται στον ίδιο σπόρο (32767). Οπότε το ξαναέκανα για 100 φορές κρατώντας κάθε φορά σε ένα αρχείο τους αριθμούς.

Συνδέθηκα στον server με το εργαλείο netcat και για δοκιμή έδωσα αμέσως όλους τους αριθμούς. Το πρόγραμμα δούλεψε και μου έδωσε την σημαία.




## Σημαία

Η σημαία που βρέθηκε:

```
FLAG{St4t1c_s33ds_4r3_l1k3_pr3d1ct4bl3_f0rtun3_c00k1s}
```