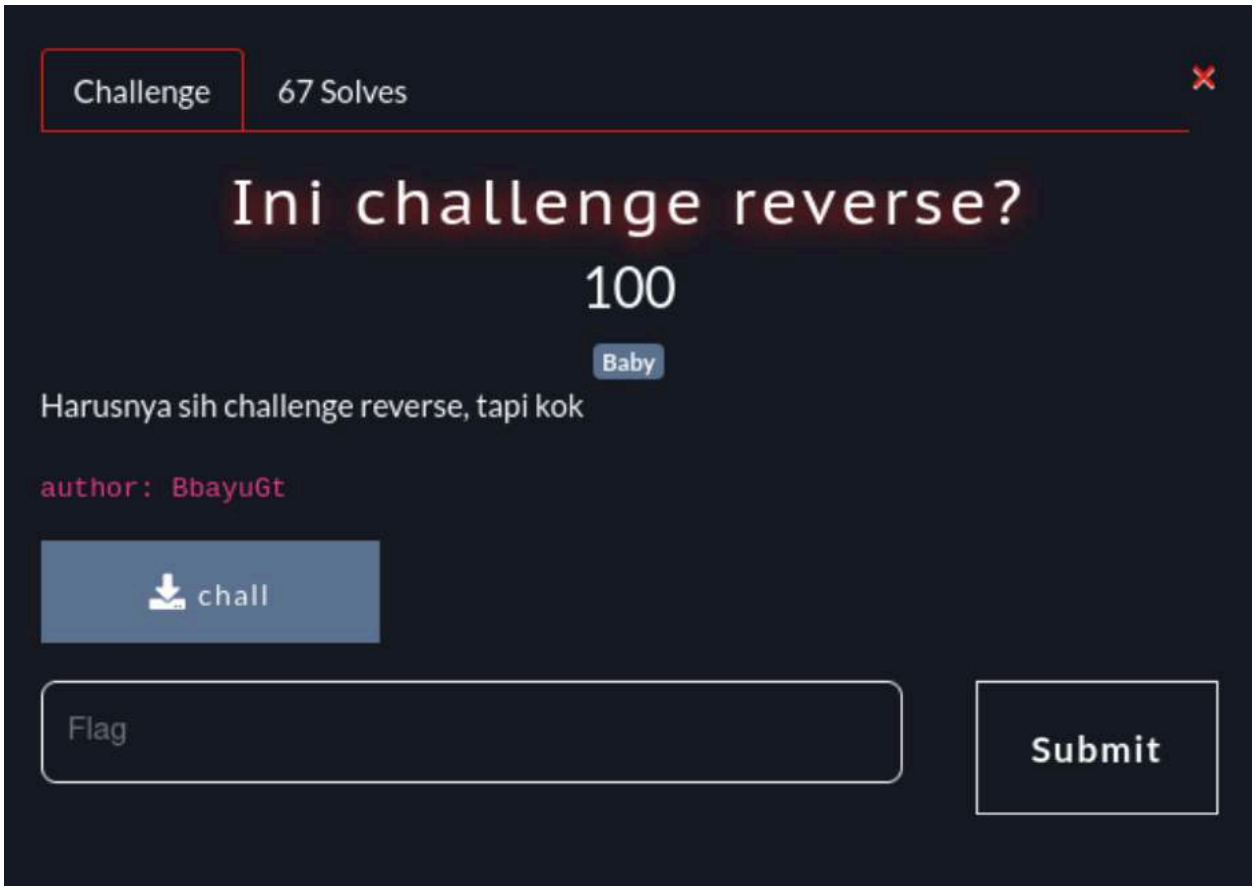
Ini Challenge Reverse?

Player: constantine
Kategori: Reverse Engineer



Phase 1: Initial Inspection

Pada challenge ini diberikan sebuah file executable tanpa konteks tambahan. Untuk reverse engineering paling dasar, langkah pertama adalah melakukan **static reconnaissance**, yaitu menganalisis file tanpa menjalankannya.

1. Identifikasi File

Gunakan tool *file* untuk mengetahui tipe file:

```
CTF & Cybersecurity/OprecForesty/ini challenge reverse? (solved)
❯ file chall
chall: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-
64.so.2, for GNU/Linux 4.4.0, BuildID[sha1]=5b884c6505153be68f9c6855c103e6d0784de4c1, with debug_info, not stripped
```

Ini menentukan apakah file tersebut adalah:

- ELF (Linux binary)
- PE (Windows executable)
- Script yang dibungkus
- Atau file biner custom

2. Cek Proteksi Binary

```
CTF & Cybersecurity/OprecForesty/ini challenge reverse? (solved)
❯ checksec --file=chall
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      Symbols         FORTIFY Fortified      Fortifiable     FILE
Full RELRO      No canary found   NX enabled    PIE enabled     No RPATH   No RUNPATH   1075 Symbols      No    0              8               chall
```

checksec membantu kita memahami apakah binary memiliki proteksi seperti NX, PIE, Canaries, atau RelRO, berguna untuk exploit dev meskipun challenge ini bukan exploitation.

Phase 2: Strings

Sebagian besar CTF reverse engineering challenge di level beginner memakai teknik sederhana seperti **stack strings, static embedded flag**, atau **plaintext artifacts**.

Tool yang bisa kita pakai adalah strings, kenapa strings?

Penjelasan:

- strings membaca *semua byte printable* dalam file.
- Binary sederhana tanpa obfuscation sering menyimpan flag sebagai literal.
- less digunakan untuk scroll dan mencari manual.

Untuk mempercepat:

```
CTF & Cybersecurity/OprecForesty/ini challenge reverse? (solved)
❯ strings chall | grep 'FORESTY'
This indicates a bug in the program. This Undefined Behavior check is optional, and cannot be relied on for safety.FORESTY{4l@h_c0k_b1
s4_di_str1n9s!!!!>:[}Hello, world!
```

Dengan command ini, kita mencari substring yang mengandung nama format flag, dan benar flag ditemukan langsung dalam hasil strings.

Final Flag

FORESTY{4l@h_c0k_b1s4_di_str1n9s!!!!>:[}