writeme

flag

```
FLAG{y33SuTd5GsmOPwonYWqePbS3y3R9Tz33}
```

參與解題的人

b04902053 鄭淵仁

write-up

這支程式讓人選擇一個 address，接下來會告知使用者那個 address 的 value，再讓使用者決定要寫什麼 value 到那個 address。而且這支程式沒有開 RELOR 的保護，所以可以對 got 直接寫值。

所以我的作法就是給他 `printf@GOT` ，而因為 `printf` 已經執行過了，所以可以從 `printf@GOT` 的值 leak 出 libc 的位置，接下來就可以算出 `one_gadget` 的 address ，就把 `one_gadget` 的值給他，這樣一來程式最後 call `printf` 的時候就執行了 `execve('/bin/sh', 0, 0)` 了。

script

- `writeme.py` ：可以拿到 `shell` 的 `python3` script。