start - pwnable.tw

b04902053 鄭淵仁

flag

```
FLAG{Pwn4bl3_tW_1s_y0ur_st4rt}
```

solution

我發現這支程式會 `read` `0x3c` 個 bytes 到大小只有 `0x14` 的 buffer。而且程式沒有開啟 `canary` 保護。

所以我就利用 stack overflow 把 return address 改成 `write(1, 0x14, $esp)` 的地方，這時候他就會給我一個在 stack 上的 address，再利用這個 address 就可以算到 buffer 在哪裡。

而接下來當程式要 `read` `0x3c` 個 bytes 的時候，就可以把 return address 蓋成指向 return address 後面 4 個 byte 的 stack 上，並且在那裡輸入 shell code。

這樣一來當程式 return 的時候就可以拿到 shell 了。

script

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