

orw - pwnable.tw

b04902053 鄭淵仁

flag

```
FLAG{sh3llc0ding_w1th_op3n_r34d_writ3}
```

solution

這支程式會 read 200 個 bytes，然後執行他們。但是只能使用 `open` `read` `write` 。

所以我就寫 shell code 先把 `"/home/orw/flag"` push 進去，再 `open` 那個 flag、`read`、最後把結果 `write` 出來，就可以拿到 flag 了。

script

- `orw.py`：自動傳 shellcode 後取得 flag 的 python3 script。