ret222

script

`ret222.py`

- requirements:
  - `pwntools`

write-up

`ret222` 的漏洞有三點：

- 直接 `printf` format string。
- `gets` 可以用來 stack buffer overflow。
- `mrpotect(name)` 之後，就可以填入 shell code 來執行。

所以可以用 format string 來 leak address ，再用 gets 蓋掉 main 的 return address，來執行到 case 4 的 `mprotect` ，接下來就可以在 `name` 裡面填入開 shell 的 shell code 了。

而因為 `name` 長度只有 `16` ，不夠組成完整的 shell code，所以我先把 `'/bin/sh'` 的 address 利用 `ret` 前面的 `leave` `pop` 到 `rbp` ，就可以用 `mov rdi, rbp` 來放 `'/bin/sh'` 的 shell code 了。

> 我覺得這題可以只用 `printf` 和 " `argv` chain" 就做完了，不過那樣做有點麻煩，就先不試了。