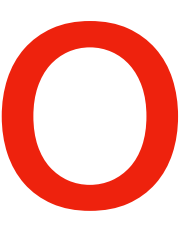
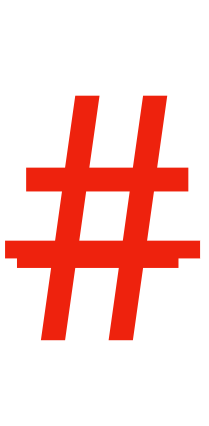
<user input> <user input>

‘ or 1 = 1 #





Injection
SQL injection

SELECT name, email FROM ph.users WHERE name=‘‘ or 1 = 1 #’ and password=‘<user input>’ ;

User input: ‘ or 1 = 1 #

SQL 當中 # 之後會被當成註解，並不會被執行
而上述的指令就會變成：

SELECT name, email FROM ph.users WHERE name=‘’ or 1=1 #~~’ and password=‘<user input>’;~~

Injection
OS Command Injection

$ dig <user input>