# SƠ LƯỢC CHUNG VỀ BÀI TẬP [**Zixem SQLi**](https://www.bing.com/ck/a?!&&p=be4e819c20a2bb6cJmltdHM9MTcxMjAxNjAwMCZpZ3VpZD0yYWU4MjFmOS02YzlmLTY2OGQtMTQ4Ny0zMjExNmQ0NjY3MjAmaW5zaWQ9NTE4OA&ptn=3&ver=2&hsh=3&fclid=2ae821f9-6c9f-668d-1487-32116d466720&psq=write+up+https%3a%2f%2fzixem.altervista.org%2fSQLi%2f&u=a1aHR0cDovL3ppeGVtLmFsdGVydmlzdGEub3JnL1NRTGkv&ntb=1)

1. **Tìm tên người dùng (username) và phiên bản (version) của trang web hoặc hệ thống cơ sở dữ liệu**: Chúng ta cần phải thực hiện các truy vấn SQL để trích xuất thông tin về tên người dùng đăng nhập (username) và phiên bản của trang web hoặc hệ thống cơ sở dữ liệu. Điều này có thể thực hiện thông qua việc sử dụng các truy vấn SELECT để truy vấn các bảng hoặc thông tin cụ thể.
2. **Sử dụng câu lệnh UNION cho tất cả các truy vấn**: Câu lệnh UNION cho phép ta kết hợp các kết quả từ các truy vấn khác nhau vào một kết quả duy nhất. Bằng cách sử dụng UNION, chúng ta có thể kết hợp các kết quả từ các truy vấn riêng lẻ để thu thập thông tin cần thiết.
3. **Không sử dụng information\_schema để lấy thông tin**: Thông thường, chúng ta có thể sử dụng bảng information\_schema trong cơ sở dữ liệu để truy vấn thông tin về cơ sở dữ liệu, bảng, cột, v.v. Tuy nhiên, trong trường hợp này, chúng ta không được phép sử dụng information\_schema và phải sử dụng các truy vấn tùy chỉnh khác để trích xuất thông tin.
4. **Không sử dụng công cụ (ví dụ: Sqlmap, Sqlninja, v.v.)**: Chúng ta không được phép sử dụng bất kỳ công cụ tự động nào như Sqlmap hoặc Sqlninja để thực hiện các tác vụ truy vấn SQL. Thay vào đó, chúng ta cần tự viết và thực thi các truy vấn SQL bằng tay để thu thập thông tin yêu cầu.

# GIẢI LẦN LƯỢT 10 LEVEL

## LEVEL 1: [Zixem-lvl 1](https://zixem.altervista.org/SQLi/level1.php?id=1)

A screenshot of a computer

Description automatically generated

* + Challenge này là một cuộc tấn công Injection dựa trên Union đơn giản.
  + Đoạn mã SQL **SELECT \* FROM exploits WHERE ID=1** được sử dụng để truy vấn dữ liệu từ bảng "exploits" trong cơ sở dữ liệu, với điều kiện là chỉ lấy ra dòng có ID bằng 1.
  + Bằng cách sử dụng câu lệnh UNION trong SQL, chúng ta có thể kết hợp kết quả của truy vấn này với dữ liệu khác mà chúng ta muốn. Điều này giúp chúng ta khai thác lỗ hổng bảo mật để truy xuất dữ liệu không được phép từ cơ sở dữ liệu thông qua các truy vấn SQL độc hại.
  + Đầu tiên, chúng ta cần xác định số cột trong bảng: SELECT \* FROM exploits WHERE ID=**1 UNION SELECT 1,2—**

A screenshot of a computer

Description automatically generated

* + Thông báo trên cho ta biết, số cột chưa đúng, vì vậy ta thử nhập số lượng cột khác như sau

A screenshot of a computer

Description automatically generated

* + Bây giờ, ta có thể thấy thông báo lỗi đã biến mất 🡺 có 3 cột.
  + Tuy nhiên, dữ liệu không hiển thị trên trang. Điều này là do dữ liệu từ tuyên bố ban đầu được đưa ra trước dữ liệu của chúng ta. Để giải quyết vấn đề này, chúng ta chỉ cần vô hiệu hóa id đầu tiên: SELECT \* FROM exploits WHERE ID=**1 AND 1=2 UNION SELECT 1,2,3—**

A screenshot of a computer

Description automatically generated

* + Rõ ràng, ID và Price được trả về lần lượt là 2 và 1, điều đó có nghĩa là dữ liệu đầu vào của chúng ta đang được trả về.
  + Bây giờ hãy thay đổi thành version() và user(), câu lệnh cuối cùng của chúng ta trông như sau: SELECT \* FROM exploits WHERE ID=**1 AND 1=2 UNION SELECT version(),user(),3—**

A white background with black text and a black and white image

Description automatically generated

* + Username and version đã được trả về!

## LEVEL 2: [Zixem-lvl 2](https://zixem.altervista.org/SQLi/level2.php?showprofile=4)

A person with a puzzle piece in their head

Description automatically generated

* + Việc thử payload tương tự như lần trước sẽ không trả lại bất kỳ kết quả nào:

A person's head with a puzzle piece in the middle

Description automatically generated

* + Ta thử thay đổi số cột nhưng vẫn không có tiết lộ gì.
  + Xem lại concept statement ban đầu: SELECT \* FROM exploits WHERE ID=**1**
  + Có thể trang web này đang lấy ID dưới dạng string, thay vì integer.
  + Sửa statement 1 chút: SELECT \* FROM exploits WHERE ID=**1'**
  + Và câu lệnh cuối cùng là: SELECT \* FROM exploits WHERE ID=**1 AND 1=2' UNION SELECT version(),user(),3--**

A silhouette of a person's head with a puzzle piece in the middle

Description automatically generated

* + Lỗi cho chúng ta biết rằng có lỗi liên quan đến dấu nháy đơn. Chúng ta có thể giải quyết vấn đề này bằng cách thêm dấu nháy đơn vào cuối câu lệnh: SELECT \* FROM exploits WHERE ID=**1 AND 1=2' UNION SELECT version(),user(),3--'**

A person's head with a puzzle piece in the middle

Description automatically generated

* + Bây giờ chúng ta được thông báo rằng số lượng cột bị sai. Bằng cách thêm cột thứ 4 vào vùng chọn, chúng ta sẽ được trả về username và version.

A person's head with a puzzle piece in the middle

Description automatically generated

## LEVEL 3: [Zixem-lvl 3](https://zixem.altervista.org/SQLi/level3.php?item=3)

A screenshot of a computer

Description automatically generated

* + Hãy bắt đầu bằng cách thử thực hiện union injection tương tự như trước: SELECT \* FROM exploits WHERE ID=**3' UNION SELECT user(),version(),3,4--'**

A screenshot of a computer

Description automatically generated

* + Thông báo lỗi cho chúng ta biết rằng câu lệnh đang được hiểu là "uni select user(),version(),3,4 — '", có nghĩa là **on của union** đang được lọc ra. Để giải quyết điều này, chúng ta có thể thêm một cái khác vào, để ngay cả sau khi nó bị xóa, câu lệnh vẫn đọc được là union: SELECT \* FROM exploits WHERE ID=**3 AND 1=2' UNIONON SELECT user(),version(),3,4--'**

A screenshot of a computer

Description automatically generated

* + Username và version đã xuất hiện.

## LEVEL 4: [Zixem-lvl 4](https://zixem.altervista.org/SQLi/level4.php?ebookid=7)

A screenshot of a computer

Description automatically generated

* + Cũng như các level trên, việc đầu tiên là chúng ta hãy thử thêm: **7 AND 1=2' UNION SELECT user(),version(),3 --'**

A screenshot of a computer

Description automatically generated

* + Ta thấy, số cột chưa đúng, tiếp tục tăng cột để thử.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* + Vậy là chúng ta đã thực hiện thành công.

## LEVEL 5: [Zixem - lvl5](https://zixem.altervista.org/SQLi/login_lvl5.php)

A screenshot of a computer

Description automatically generated

* + Câu này thì chúng ta có thể thử brute force password và có nguồn tham khảo như sau:

A screenshot of a computer program

Description automatically generatedA screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* + Vậy khi brute force chúng ta tìm ra mật khẩu chính xác và thành công giải được challenge này.

## LEVEL 6: [Zixem -lvl\_6](https://zixem.altervista.org/SQLi/blind_lvl6.php?serial=10)

## LEVEL 7: [Zixem-lvl 7](https://zixem.altervista.org/SQLi/level7.php?id=1)

## LEVEL 8: [Zixem-lvl 8](https://zixem.altervista.org/SQLi/lvl8.php?id=1)

## LEVEL 9: [Zixem-lvl 9](https://zixem.altervista.org/SQLi/lvl9.php?id=1)

## LEVEL 10: [Zixem-lvl 10](https://zixem.altervista.org/SQLi/lvl10.php?x=ISwwYGAKYAo%3D)