HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

MÔN HỌC: AN TOÀN ỨNG DỤNG WEB & CSDL

BÁO CÁO BÀI TẬP LỚN

Đề tài : Tìm hiểu về hệ quản trị CSDL MySQL

Giảng viên hướng dẫn : Vũ Minh Mạnh

Nhóm thực hiện : Nhóm 05

Thành viên nhóm :

Nguyễn Hoài Ngọc	B20DCAT133
Lường Thế Vinh	B20DCAT201
Trịnh Thị Huyền Trang	B20DCAT189

HÀ NỘI – 2023

MỤC LỤC

LỜI CẢM ƠN

Lời đầu tiên, xin trân trọng cảm ơn thầy đã tạo điều kiện thuận lợi và tận tình hướng dẫn chúng em trong quá trình học tập cũng như trong việc hoàn thành bài tập lớn.

Trong quá trình tìm hiểu, cũng như là trong quá trình làm bài báo cáo, khó tránh khỏi sai sót, rất mong thầy bỏ qua. Đồng thời do trình độ lý luận cũng như kinh nghiệm thực tiễn còn hạn chế nên bài báo cáo không thể tránh khỏi những thiếu sót, chúng em rất mong nhận được ý kiến đóng góp của thầy để học thêm được nhiều kinh nghiệm và có thêm kiến thức.

I. GIỚI THIỆU CHUNG

MySQL là một hệ quản trị cơ sở dữ liệu mã nguồn mở (open-source) phổ biến, được sử dụng rộng rãi trên toàn cầu. Nó là một hệ thống quản lý cơ sở dữ liệu (Database Management System - DBMS) cho phép người dùng lưu trữ, truy xuất và quản lý dữ liệu trong một môi trường ứng dụng. MySQL được phát triển bởi một nhóm nhà phát triển độc lập và hiện tại được Oracle Corporation sở hữu và duy trì.

1. Ưu – Nhược điểm của MySQL

MySQL Được sử dụng rộng rãi bởi các website lớn với lượt truy cập 'khủng', MySQL có được những ưu điểm và tiện ích nổi bật vượt xa các phần mềm khác như:

- Dễ sử dụng: MySQL đơn giản, dễ sử dụng. Ngoài ra, phần mềm này có thể hoạt động trên khá nhiều hệ điều hành nhằm cung cấp nhiều hàm tiện ích mạnh mẽ.
- Bảo mật cao: MySQL sở hữu khá nhiều tính năng bảo mật, bao gồm các loại hình bảo mật cấp cao.
- Đa tính năng: MySQL cung cấp nhiều tính năng mà bất cứ hệ quản trị CSDL quan hệ nào cũng phải mong đợi.
- Vận hành mạnh mẽ và mở rộng dễ dàng: MySQL có khả năng xử lý một lượng lớn dữ liệu. Bên cạnh đó, người dùng có thể mở rộng nó nếu có nhu cầu.
- Nhanh chóng: Tốc độ hoạt động của MySQL nhanh hơn các phần mềm khác nhờ các tiêu chuẩn được tích hợp sẵn.
- Có thể khôi phục dữ liệu: MySQL cho phép người dùng khôi phục dữ liệu, tránh khỏi ảnh hưởng của các sự cố.

Tuy nhiên, nó cũng tồn tại một số nhược điểm cần cân nhắc sau:

- Bị giới hạn: MySQL bị hạn chế về một vài tính năng mà các ứng dụng có thể sẽ cần đến
- Độ tin cậy không quá cao: So với các hệ quản trị CSDL quan hệ khác, độ tin cậy của MySQL không quá cao.
- Bị hạn chế về dung lượng: Số bản ghi trong MySQL càng tăng thì truy xuất dữ liệu càng trở nên khó khăn do hạn chế về dung lượng.

2. Cách thức hoạt động của MySQL

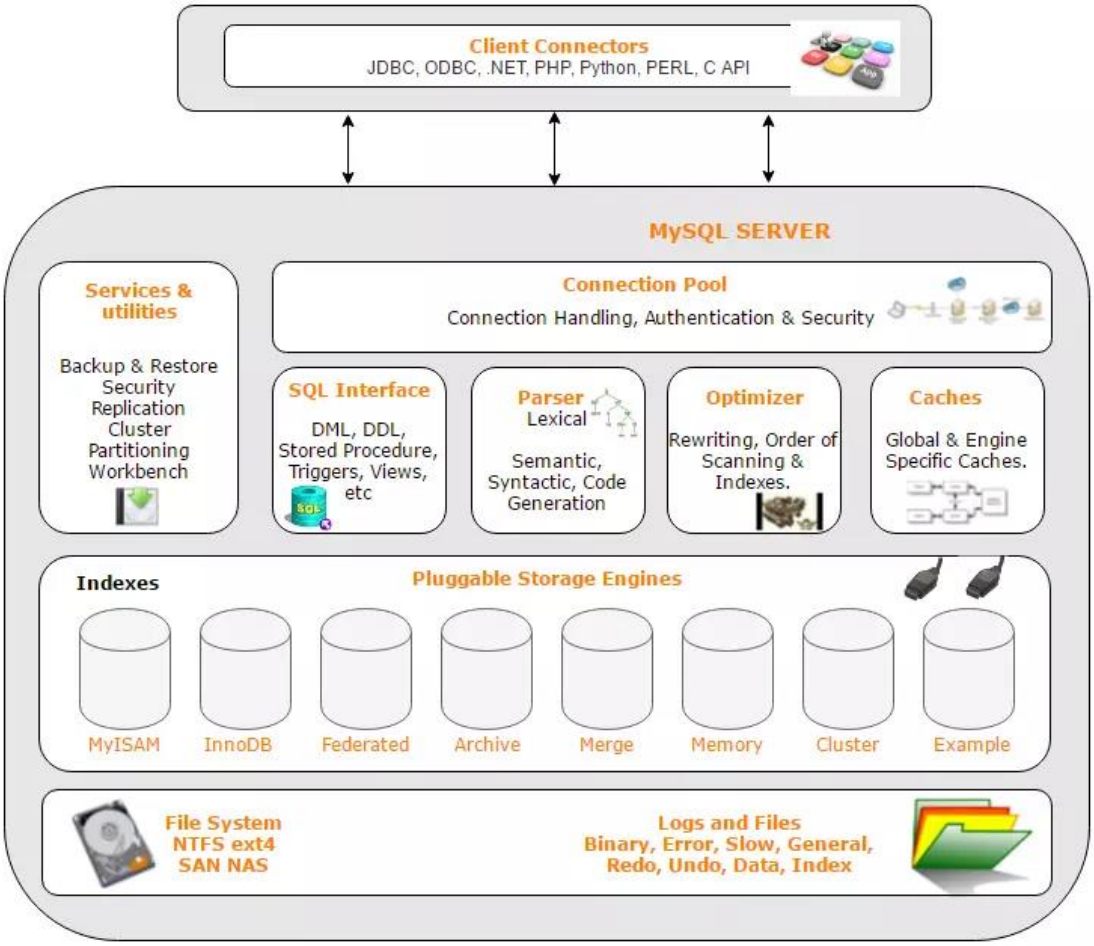
Trong môi trường MySQL, máy khách (client) và máy chủ (server) tương tác qua lại với nhau theo nguyên lý:

- MySQL tạo ra các bảng nhằm lưu trữ dữ liệu, đồng thời định nghĩa mối quan hệ giữa các bảng đó.
- Client gửi các yêu cầu SQL bằng lệnh đặc biệt lên trên MySQL.
- Ứng dụng trên server nhận được và phản hồi thông tin, trả kết quả về máy khách.

II. TÌM HIỂU VỀ MYSQL

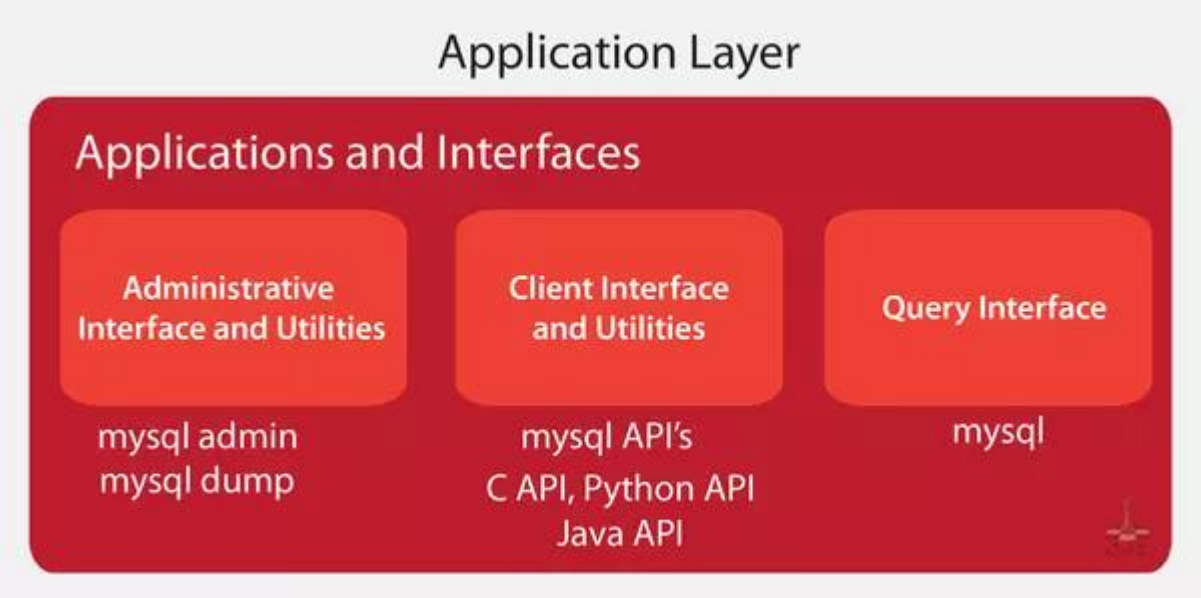
1. Kiến trúc của MySQL

Kiến trúc logic của MySQL gồm 3 layers chính.



1.1. Application Layer (layer 1)

Application Layer chính là lớp trên cùng nhất trong kiến trúc MySQL. Đây là nơi client và user dùng tương tác với MySQL RDBMS. Một số dịch vụ được cung cấp bên dưới: connection handling, authentication, security đều có ở đây. Có ba thành phần chính trong lớp này là Administrators, Clients, Query Users như thể hiện trong hình bên dưới.



- Administrators sử dụng các tiện ích và giao diện quản trị khác nhau như mysqladmin thực hiện các tác vụ như tắt máy chủ và tạo hoặc hủy cơ sở dữ liệu, mysqldump để sao lưu cơ sở dữ liệu hoặc sao chép cơ sở dữ liệu sang một máy chủ khác.
- Clients giao tiếp với MySQL thông qua các giao diện và tiện ích khác nhau như MySQL API. MySQL API gửi truy vấn đến máy chủ dưới dạng một chuỗi các mã thông báo.
- Query Users truy vấn tương tác với MySQL RDBMS thông qua giao diện truy vấn là mysql .

a) Connection handling

Khi một client kết nối với server, Client sẽ nhận được thread riêng cho kết nối của nó. Tất cả các truy vấn từ client đó được thực thi trong thread được chỉ định đó. Thread được lưu trong bộ nhớ cache của máy chủ, vì vậy chúng không cần phải tạo và hủy mỗi khi có kết nối mới.

Để quản lý số kết nối thì mysql có cung cấp cho ta biến `max_connection`. Có một tip nhỏ đấy chính là mysqld cho phép `max_connections + 1` kết nối Client. Với điều kiện kết nối bổ sung là các tài khoản có `CONNECTION_ADMIN`. Bằng cách cấp đặc quyền cho administrators , Nó có thể kết nối với máy chủ và sử dụng `SHOW PROCESSLIST` để chẩn đoán sự cố ngay cả khi số lượng kết nối từ Client đã đạt mức tối đa.

Khi đặt giá trị của `max_connections` chúng ta nên cân nhắc đến một số yếu tố sau:

- Chất lượng của thread library trên một platform nhất định.
- Dung lượng RAM có sẵn.

- Dung lượng RAM được sử dụng cho mỗi kết nối.
- Khối lượng công việc từ mỗi kết nối.
- Thời gian phản hồi mong muốn.
- Số lượng file mô tả có sẵn.

b) Authentication

Bất cứ khi nào client kết nối với MySQL server, máy chủ sẽ thực hiện xác thực ở phía máy chủ. Việc xác thực dựa trên username, password và host của client.

c) Security

Sau khi Client được kết nối thành công với MySQL Server, server sẽ kiểm tra xem client đó có đặc quyền đưa ra các truy vấn nhất định đối với máy chủ MySQL.

1.2. MySQL Server layer (layer 2)

Lớp này đảm nhất tất cả các chức năng logic của hệ thống mysql RDBMS, Nó còn được ví như bộ não của mysql. Lớp logic của MySQL được chia thành các thành phần phụ khác nhau, được đưa ra dưới đây:

a) MySQL services and utilities

Mysql cung cấp nhiều loại dịch vụ và tiện ích. Đây là một trong những lý do chính cho sự phổ biến của MySQL. Lớp này cung cấp các dịch vụ và tiện ích để quản trị và bảo trì hệ thống MySQL, một số trong số chúng được đề cập dưới đây:

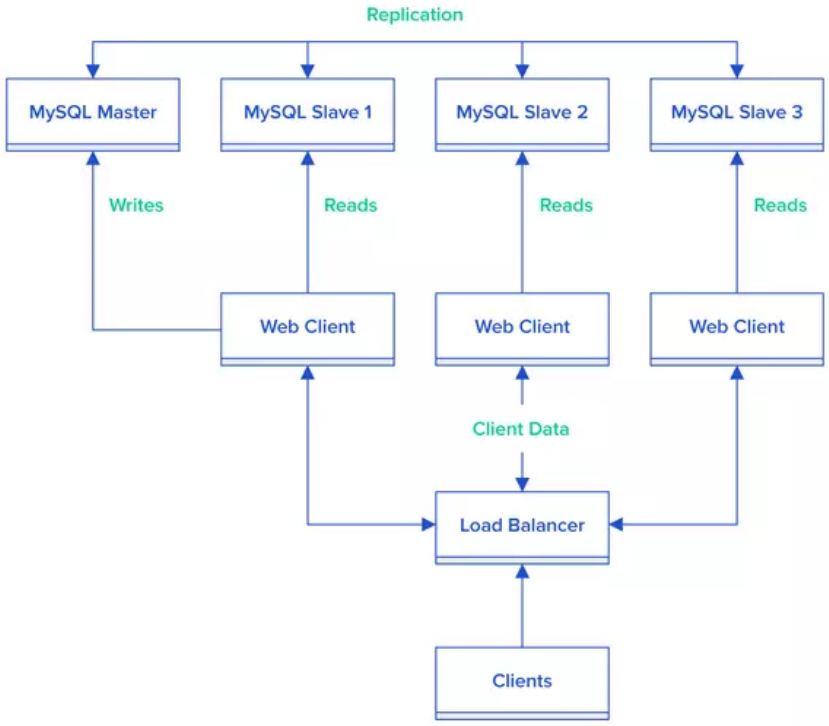
Backup & recovery : Có một điều quan trọng là phải sao lưu cơ sở dữ liệu để bạn có thể khôi phục dữ liệu của mình và chạy lại trong trường hợp xảy ra sự cố.

Security : MySQL sử dụng bảo mật dựa trên Danh sách kiểm soát truy cập (ACL) cho tất cả các kết nối, truy vấn và các hoạt động khác mà người dùng có thể cố gắng thực hiện. Ngoài ra còn có hỗ trợ cho các kết nối được mã hóa SSL giữa máy khách và máy chủ MySQL. Khi chạy mysql hãy làm theo 1 số nguyên tắc sau:

- Một điều quan trong là đừng bao giờ cấp cho bất kỳ ai (ngoại trừ tài khoản root của MySQL) quyền truy cập vào bảng user trong mysql cơ sở dữ liệu hệ thống!
- Không cấp nhiều đặc quyền hơn mức cần thiết. Và không bao giờ cấp đặc quyền cho tất cả các máy chủ.

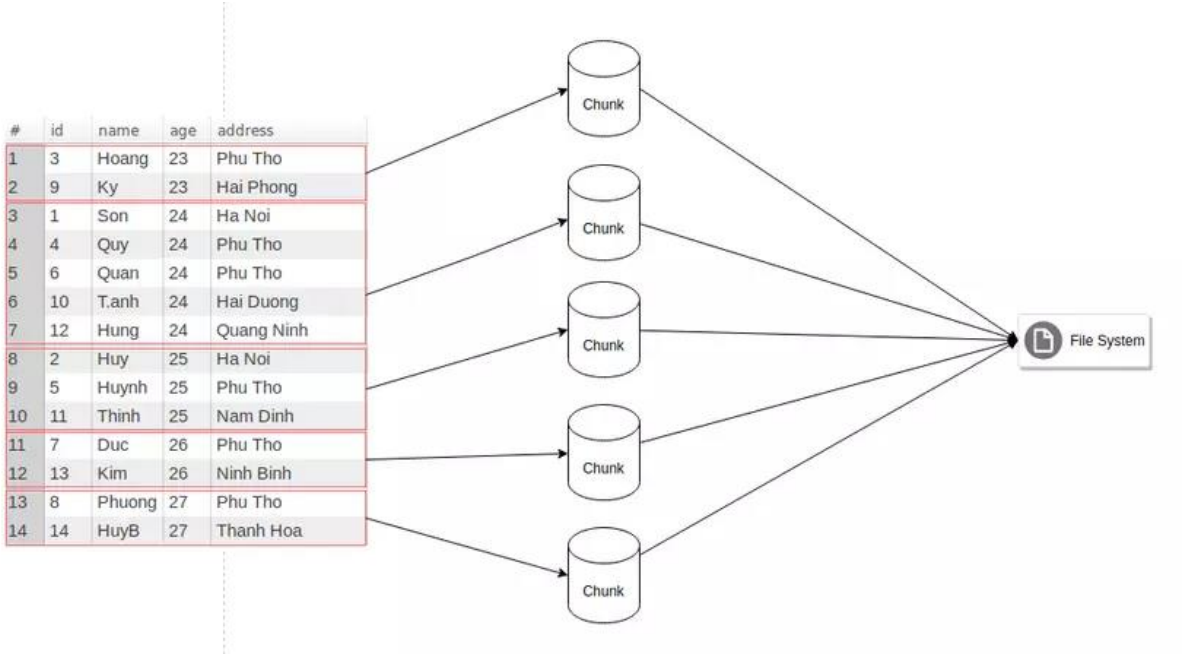
- Không lưu trữ mật khẩu một các rõ ràng. Thay vào đó hay sử dụng , hãy sử dụng SHA2() hoặc một số hàm hash một chiều khác và lưu trữ giá trị hash.
- Thiết lập firewall, Điều này bảo vệ bạn khỏi ít nhất 50% tất cả các loại khai thác trong bất kỳ phần mềm nào. Đặt MySQL sau firewall hoặc trong demilitarized zone (DMZ).
- Các ứng dụng của MYSQL không được tin tưởng bất kì dữ liệu gì mà được người dùng nhập vào. Mọi câu lệnh phải được mã hoá thích hợp.
- Không truyền dữ liệu thuần túy (không được mã hóa) qua Internet.
- Tìm hiểu cách sử dụng các tiện ích tcpdump và strings .

Replication : Replication MySQL là một quá trình cho phép dữ liệu từ một máy chủ cơ sở dữ liệu MySQL (máy chủ) được sao chép tự động sang một hoặc nhiều máy chủ cơ sở dữ liệu MySQL (máy chủ). Replication thường được sử dụng để lan truyền quyền truy cập đọc trên nhiều máy chủ, để có khả năng mở rộng.



Cluster : MySQL Cluster là cơ sở dữ liệu phân tán kết hợp khả năng mở rộng liên tục và tính sẵn sàng cao. Nó cung cấp truy cập thời gian thực trong bộ nhớ với sự nhất quán về tiến trình xử lý trên các bộ dữ liệu phân tán và phân vùng.

Partitioning : Mysql Partitioning theo đúng như tên của nó là việc phân chia một table thành những phần nhỏ theo một logic nhất định, được phân biệt bằng key, key này thường là tên column trong table.



Workbench : MySQL Workbench là một công cụ trực quan hợp nhất dành cho database architects, developer và DBA. MySQL Workbench cung cấp data modeling, SQL development và các công cụ quản trị toàn diện để cấu hình máy chủ, quản trị người dùng, sao lưu và hơn thế nữa. MySQL Workbench có sẵn trên Windows, Linux và Mac OS.

b) SQL Interface

Structured Query Language (SQL) là một ngôn ngữ truy vấn, được sử dụng để truy vấn máy chủ MySQL. Nó là một công cụ để tương tác giữa người dùng máy khách MySQL và máy chủ. Một số thành phần SQL Interface :

- Data Manipulation Language (DML).
- Data Definition Language (DDL).
- Stored Procedures.
- Views.
- Triggers.

c) Parser

Máy chủ MySQL nhận các truy vấn ở định dạng SQL. Sau khi nhận được một truy vấn, trước tiên nó cần được phân tích cú pháp. Quá trình này được gọi tắt là Parser. MySQL phân tích cú pháp các truy vấn để tạo cấu trúc bên trong (Parser tree). MySQL parser hoạt động như một trình biên dịch truyền đơn.

d) Optimizer

Sau khi tạo Parser tree nội bộ, MySQL áp dụng nhiều kỹ thuật tối ưu hóa khác nhau. Các kỹ thuật này có thể bao gồm, viết lại truy vấn, thứ tự quét các bảng và chọn các index phù hợp để sử dụng.

e) Caches

MySQL cache (bộ đệm truy vấn) lưu trữ các bộ kết quả hoàn chỉnh cho các câu lệnh SELECT . Trước khi Parser truy vấn, máy chủ MySQL tham khảo bộ đệm truy vấn. Nếu bất kỳ client nào đưa ra một truy vấn giống hệt với một truy vấn đã có trong bộ nhớ cache, máy chủ chỉ cần hiển thị đầu ra từ bộ nhớ cache.

MySQL cache có thể hữu ích trong môi trường mà bạn có các bảng không thường xuyên thay đổi và máy chủ nhận được nhiều truy vấn giống nhau.

1.3. Storage Engine Layer (layer 3)

Tính năng Storage Engine có thể cắm được làm cho MySQL trở thành lựa chọn độc nhất và ưa thích của hầu hết các developer. MySQL cho phép chúng ta lựa chọn các công cụ lưu trữ khác nhau cho các tình huống và yêu cầu khác nhau. Danh sách các công cụ lưu trữ được hỗ trợ được đề cập bên dưới.

- MyISAM.
- InnoDB.
- Federated.
- Mrg_MyISAM.
- Blackhole.
- CSV.
- Memory.
- Archive.
- Performance_schema.

2. Tính năng của MySQL

Khả năng mở rộng và tính linh hoạt cao : chỉ 1MB để chạy các data warehouse khổng lồ chứa hàng terabyte thông tin. MySQL có thể được mở rộng theo nhiều cách khác nhau (như replication, clustering, sharding hoặc kết hợp nhiều cách). Tính linh hoạt là một ưu điểm nổi bật của MySQL, tất cả các phiên bản Linux, UNIX và Windows đều được hỗ trợ.

Hiệu suất cao : Với các tiện ích tải tốc độ cao, distinctive memory cache hay full text index và các cơ chế nâng cao hiệu suất khác, MySQL cung cấp tất cả các phương pháp phù hợp cho các hệ thống kinh doanh quan trọng hiện nay.

Tính sẵn sàng cao : MySQL sử dụng nhiều chiến lược sao lưu và phục hồi để đảm bảo dữ liệu không bị mất trong trường hợp hệ thống gặp sự cố hoặc xóa không chủ ý.

Bảo mật dữ liệu mạnh mẽ : MySQL cung cấp các cơ chế mạnh mẽ để đảm bảo chỉ những người dùng được ủy quyền mới có quyền truy cập vào máy chủ cơ sở dữ liệu. MySQL hỗ trợ SSH và SSL và các lớp bảo mật khác để bảo vệ tính toàn vẹn của dữ liệu.

Phát triển ứng dụng toàn diện : Một trong những lý do khiến MySQL là cơ sở dữ liệu mã nguồn mở phổ biến nhất thế giới là nó cung cấp hỗ trợ toàn diện cho mọi nhu cầu phát triển ứng dụng. MySQL hỗ trợ cho các stored procedures, triggers, views, ANSI-standard SQL, v.v.

Quản lý dễ dàng : MySQL có khả năng khởi động nhanh. Sau khi được cài đặt, các tính năng tự quản lý như tự động mở rộng không gian, tự động khởi động lại và thay đổi cấu hình động sẽ giảm bớt gánh nặng cho các quản trị viên cơ sở dữ liệu.

Là mã nguồn mở và hỗ trợ 24/7 : MySQL có sẵn dưới dạng công cụ mã nguồn mở, các nhà phát triển phần mềm có tùy chọn để tùy chỉnh mã nguồn theo ứng dụng của riêng họ một cách linh hoạt.

Chi phí tối ưu : Với việc sử dụng MySQL, có thể đạt được mức độ mở rộng và hiệu suất đáng kinh ngạc với chi phí thấp hơn nhiều. Ngoài ra, độ tin cậy và khả năng bảo trì dễ dàng của MySQL cũng giúp quản trị viên cơ sở dữ liệu không mất quá nhiều thời gian để khắc phục sự cố về hiệu suất hoặc downtime, mà thay vào đó có thể tập trung vào công việc khác quan trọng hơn.

3. Cơ chế bảo mật của MySQL

Khi quan tâm đến vấn đề bảo mật trong cài đặt MySQL, cần xem xét một loạt các vấn đề và cách chúng ảnh hưởng đến bảo mật máy chủ MySQL của bạn và các ứng dụng liên quan:

- Các yếu tố chung ảnh hưởng đến bảo mật. Chúng bao gồm:
  - Lựa chọn mật khẩu tốt
  - Không cấp các đặc quyền không cần thiết cho người dùng
  - Đảm bảo an ninh ứng dụng bằng cách ngăn chặn chèn mã SQL, đánh cắp dữ liệu và những vấn đề gây mất an toàn ứng dụng khác.
- Bảo mật của chính cài đặt. Các tệp dữ liệu, tệp nhật ký và tất cả các tệp ứng dụng cài đặt của bạn phải được bảo vệ để đảm bảo rằng chúng không thể đọc được hoặc ghi được bởi các bên trái phép.
- Kiểm soát truy cập và bảo mật trong chính hệ thống cơ sở dữ liệu, bao gồm người dùng và cơ sở dữ liệu được cấp quyền truy cập vào cơ sở dữ liệu,

chế độ xem và các chương trình được lưu trữ đang được sử dụng trong cơ sở dữ liệu.

- Các tính năng được cung cấp bởi các plugin liên quan đến bảo mật.
- An ninh mạng của MySQL và hệ thống của bạn. Bảo mật có liên quan đến cấp quyền cho từng người dùng cụ thể, nhưng bạn cũng có thể muốn hạn chế MySQL chỉ sẵn sàng truy cập cục bộ trên máy chủ MySQL hoặc trên một tập hợp hạn chế các máy chủ khác (nói cách khác là hạn chế việc truy cập MySQL từ xa). Điều này giúp ngăn chặn các tấn công từ xa và bảo vệ cơ sở dữ liệu khỏi các mối đe dọa không mong muốn từ internet.
- Đảm bảo bạn có sao lưu đầy đủ và phù hợp cho các tệp dữ liệu cơ sở dữ liệu, tệp cấu hình và tệp nhật ký. Ngoài ra, đảm bảo bạn có một giải pháp khôi phục sẵn sàng và kiểm tra xem bạn có thể khôi phục thông tin từ các bản sao lưu một cách thành công hay không.

3.1. Kiểm soát truy cập và quản lý tài khoản

MySQL cho phép tạo các tài khoản cho phép người dùng từ phía máy khách kết nối với máy chủ MySQL và truy cập vào dữ liệu được quản lý bởi máy chủ đó. Hệ thống quyền ưu tiên của MySQL có chức năng chính là xác thực người dùng kết nối từ một máy chủ cụ thể và liên kết người dùng đó với các quyền truy cập vào cơ sở dữ liệu, Ví dụ như:

- SELECT (truy vấn dữ liệu)
- INSERT (thêm dữ liệu)
- UPDATE (cập nhật dữ liệu)
- DELETE (xóa dữ liệu)

Chức năng bổ sung bao gồm khả năng cấp quyền cho các hoạt động quản trị hệ thống. Điều này có nghĩa là bạn có thể chỉ định các người dùng hoặc vai trò cụ thể để thực hiện các tác vụ quản trị, chẳng hạn như tạo bảng, sao lưu dữ liệu hoặc quản lý người dùng.

Để kiểm soát được người dùng nào có thể kết nối vào cơ sở dữ liệu, mỗi tài khoản có thể được gán các thông tin xác thực như mật khẩu. Giao diện người dùng của MySQL cho phép quản lý các tài khoản bằng cách sử dụng các câu lệnh SQL như CREATE USER (tạo người dùng), GRANT (cấp quyền), và REVOKE (hủy quyền).

Để xem các quyền của một tài khoản cụ thể, bạn có thể sử dụng câu lệnh SHOW GRANTS.

Ví dụ: `SHOW GRANTS FOR 'joe@office.example.com';` sẽ hiển thị các quyền của tài khoản "joe" khi kết nối từ máy chủ "office.example.com", trong khi `SHOW GRANTS FOR 'joe@home.example.com';` sẽ hiển thị các quyền của tài

khoản "joe" khi kết nối từ máy chủ "home.example.com". Điều này cho phép bạn quản lý quyền của từng tài khoản trên các máy chủ khác nhau một cách tùy ý.

Kiểm soát truy cập MySQL liên quan đến hai giai đoạn khi bạn chạy một chương trình máy khách kết nối vào máy chủ:

Giai đoạn 1: Máy chủ chấp nhận hoặc từ chối kết nối dựa trên danh tính của bạn và xem bạn có thể xác minh danh tính của mình bằng cách cung cấp mật khẩu chính xác hay không. Máy chủ MySQL thực hiện kiểm tra danh tính và thông tin xác thực bằng cách sử dụng các cột trong bảng, và chỉ chấp nhận kết nối nếu các điều kiện sau được thỏa mãn:

- Tên host và tên người dùng của máy khách phải khớp với các giá trị trong các cột "Host" và "User" của một hàng trong một bảng nào đó. Điều này có nghĩa rằng máy chủ MySQL chỉ cho phép kết nối nếu thông tin tên host và tên người dùng của máy khách khớp với thông tin trong bảng.
- Máy khách cung cấp thông tin xác thực được chỉ định trong hàng đó (ví dụ, mật khẩu), như đã chỉ định trong cột tương ứng. Thông tin xác thực này được hiểu bằng cách sử dụng plugin xác thực đã chỉ định trong cột "authentication_stringplugin".
- Hàng trong bảng phải chỉ định rằng tài khoản không bị khóa. Trạng thái khóa tài khoản được ghi lại trong cột "account_locked", và giá trị của nó phải là 'N'. Trạng thái khóa tài khoản có thể được đặt hoặc thay đổi bằng cách sử dụng lệnh CREATE USER hoặc ALTER USER.

Nói chung, danh tính của bạn trong quá trình kết nối với máy chủ MySQL dựa trên hai thông tin:

- Tên người dùng MySQL của bạn.
- Tên host của máy khách từ đó bạn thực hiện kết nối.

Giai đoạn 2: Giả sử rằng bạn có thể kết nối, máy chủ sẽ kiểm tra mỗi lệnh mà bạn gửi để xác định xem bạn có đủ quyền để thực hiện nó hay không. Ví dụ, nếu bạn cố gắng lấy dữ liệu từ một bảng trong cơ sở dữ liệu hoặc xóa một bảng khỏi cơ sở dữ liệu, máy chủ sẽ kiểm tra xem bạn có quyền SELECT cho bảng đó hay quyền DROP cho cơ sở dữ liệu hay không.

Việc kiểm tra quyền dựa vào các bảng trong cơ sở dữ liệu MySQL liên quan đến việc cấp quyền và quản lý quyền truy cập. Dưới đây là mô tả chi tiết về mỗi bảng:

- `user`: Bảng này chứa thông tin về tài khoản người dùng, các quyền toàn cầu (global privileges) tĩnh, và các cột không liên quan đến quyền truy cập.
- `global_grants`: Bảng này chứa thông tin về các quyền toàn cầu (global privileges) động, có thể thay đổi trong thời gian chạy của hệ thống.

- `db`: Bảng này chứa thông tin về quyền truy cập cấp cho cơ sở dữ liệu ở mức cơ sở dữ liệu (database-level privileges).
- `tables_priv`: Bảng này lưu trữ thông tin về quyền truy cập cấp cho bảng (table-level privileges).
- `columns_priv`: Bảng này chứa thông tin về quyền truy cập cấp cho các cột của bảng (column-level privileges).
- `procs_priv`: Bảng này lưu thông tin về quyền truy cập cấp cho các stored procedure và function.
- `proxies_priv`: Bảng này chứa thông tin về quyền truy cập của các proxy-user.
- `default_roles`: Bảng này chứa thông tin về các vai trò người dùng mặc định.
- `role_edges`: Bảng này chứa thông tin về các mối quan hệ (edges) giữa các vai trò (role) trong hệ thống.
- `password_history`: Bảng này ghi lại lịch sử thay đổi mật khẩu của người dùng.

Nếu quyền ưu tiên của bạn được thay đổi (bất kỳ là bạn tự thay đổi hoặc có người khác thay đổi) trong khi bạn đang kết nối vào cơ sở dữ liệu, những thay đổi đó không nhất thiết phải có hiệu lực ngay lập tức cho lệnh tiếp theo mà bạn gửi đi.

Có một số điều bạn không thể làm được bằng hệ thống quyền ưu tiên của MySQL:

- Bạn không thể xác định một cách rõ ràng rằng một người dùng cụ thể sẽ bị từ chối truy cập. Điều này có nghĩa là bạn không thể đặt ra một quy tắc để từ chối một người dùng cụ thể kết nối vào cơ sở dữ liệu. Hệ thống quyền ưu tiên của MySQL được xây dựng trên cơ sở cấp quyền, chứ không phải từ chối quyền.
- Bạn không thể chỉ định rằng một người dùng có quyền tạo hoặc xóa bảng trong một cơ sở dữ liệu nhưng không có quyền tạo hoặc xóa chính cơ sở dữ liệu đó. Hệ thống quyền của MySQL không cho phép bạn quản lý quyền truy cập vào các đối tượng dữ liệu cụ thể như cơ sở dữ liệu, bảng một cách độc lập với nhau.
- Mật khẩu được áp dụng toàn cầu cho một tài khoản. Bạn không thể liên kết mật khẩu với một đối tượng cụ thể như cơ sở dữ liệu, bảng, hoặc thủ tục. Mật khẩu chỉ liên quan đến việc xác thực người dùng khi họ kết nối và không thể được sử dụng để kiểm soát quyền truy cập vào các đối tượng dữ liệu cụ thể.

3.2. Sử dụng kết nối được mã hóa

Với một kết nối chưa được mã hóa giữa máy khách MySQL và máy chủ, ai đó có quyền truy cập vào mạng có thể theo dõi toàn bộ lưu lượng giao tiếp và kiểm tra dữ liệu được gửi hoặc nhận giữa máy khách và máy chủ. Điều này có nghĩa là thông tin nhạy cảm hoặc dữ liệu quan trọng, chẳng hạn như tên người dùng, mật khẩu, hoặc dữ liệu cơ sở dữ liệu, có thể bị người khác theo dõi và đánh cắp khi truyền qua mạng.

Khi bạn cần truyền thông tin qua mạng một cách an toàn, một kết nối chưa được mã hóa là không chấp nhận được. Để làm cho bất kỳ loại dữ liệu nào trở thành không thể đọc, bạn cần sử dụng mã hóa. Các thuật toán mã hóa phải bao gồm các yếu tố bảo mật để đối phó với nhiều loại tấn công đã biết, chẳng hạn như thay đổi thứ tự của các thông điệp đã được mã hóa hoặc lặp lại dữ liệu hai lần.

MySQL hỗ trợ kết nối được mã hóa giữa máy khách và máy chủ bằng cách sử dụng giao thức TLS (Transport Layer Security). Đôi khi TLS còn được gọi là SSL (Secure Sockets Layer), nhưng MySQL thực tế không sử dụng giao thức SSL cho các kết nối được mã hóa vì mã hóa của SSL không đủ mạnh.

TLS (Transport Layer Security) sử dụng các thuật toán mã hóa để đảm bảo rằng dữ liệu nhận được qua mạng công cộng có thể được tin cậy. Nó có cơ chế để phát hiện sự thay đổi, mất mát hoặc việc gửi lại dữ liệu. TLS cũng tích hợp các thuật toán cung cấp xác minh danh tính bằng cách sử dụng tiêu chuẩn X.509.

Tiêu chuẩn X.509 cho phép xác định một cá nhân hoặc thực thể trên Internet. Một cách đơn giản, có một thực thể gọi là "Certificate Authority" (hoặc CA) gán chứng chỉ điện tử cho bất kỳ ai cần chúng. Chứng chỉ dựa vào các thuật toán mã hóa bất đối xứng có hai khóa mã hóa (một khóa công khai và một khóa bí mật). Chủ sở hữu của chứng chỉ có thể trình chứng chỉ cho một bên khác làm bằng chứng về danh tính của họ. Một chứng chỉ bao gồm khóa công khai của chủ sở hữu. Mọi dữ liệu được mã hóa bằng khóa công khai này chỉ có thể được giải mã bằng khóa bí mật tương ứng, mà chủ sở hữu của chứng chỉ giữ.

Hỗ trợ cho các kết nối được mã hóa trong MySQL được cung cấp bằng cách sử dụng OpenSSL. Để biết thêm thông tin về các giao thức và thuật toán mã hóa mà OpenSSL hỗ trợ, bạn có thể tham khảo tài liệu và tài liệu tham khảo chính thức của OpenSSL. Điều này sẽ giúp bạn hiểu rõ về cách OpenSSL hỗ trợ mã hóa và các tùy chọn cụ thể.

Mặc định, các phiên bản của MySQL liên kết với một thư viện OpenSSL đã được cài đặt và có sẵn khi chạy để hỗ trợ các kết nối được mã hóa và các hoạt động liên quan đến mã hóa khác. Tuy nhiên, bạn cũng có khả năng biên dịch MySQL từ mã nguồn và sử dụng tùy chọn CMake WITH_SSL để chỉ định đường dẫn đến một phiên bản OpenSSL cụ thể đã cài đặt hoặc một gói hệ thống

OpenSSL thay thế. Trong trường hợp này, MySQL sẽ sử dụng phiên bản OpenSSL bạn đã chỉ định.

Từ phiên bản MySQL 8.0.11 đến 8.0.17, bạn có thể biên dịch MySQL bằng cách sử dụng thư viện wolfSSL thay vì OpenSSL. Tuy nhiên, từ phiên bản MySQL 8.0.18 trở đi, hỗ trợ cho wolfSSL đã bị loại bỏ và tất cả phiên bản MySQL sử dụng OpenSSL. Điều này có nghĩa rằng từ phiên bản MySQL 8.0.18 trở đi, bạn không thể sử dụng wolfSSL như một tùy chọn mã hóa thay thế nữa và tất cả các phiên bản MySQL sẽ liên kết và sử dụng thư viện OpenSSL cho các kết nối được mã hóa và hoạt động mã hóa khác.

Nếu bạn đã biên dịch MySQL bằng một phiên bản của OpenSSL và muốn chuyển sang một phiên bản khác mà không cần biên dịch lại MySQL, bạn có thể thực hiện điều này bằng cách chỉnh sửa đường dẫn của trình tải thư viện động (dynamic library loader path). Trên hệ thống Unix, bạn có thể chỉnh sửa biến môi trường LD_LIBRARY_PATH, còn trên hệ thống Windows, bạn có thể chỉnh sửa biến môi trường PATH.

Mặc định, các chương trình MySQL sẽ thử kết nối sử dụng mã hóa nếu máy chủ hỗ trợ các kết nối được mã hóa, và nếu không thể thiết lập được kết nối mã hóa, chúng sẽ dự phòng bằng kết nối không được mã hóa. Điều này đảm bảo tính linh hoạt và tương thích khi kết nối với các máy chủ có hỗ trợ mã hóa và máy chủ không hỗ trợ mã hóa.

MySQL thực hiện mã hóa theo từng kết nối, và việc sử dụng mã hóa cho một người dùng cụ thể có thể là tùy chọn hoặc bắt buộc. Điều này cho phép bạn lựa chọn kết nối được mã hóa hoặc không được mã hóa tùy theo yêu cầu của từng ứng dụng cụ thể. Bạn có thể quy định xem kết nối mã hóa có bắt buộc hay không bằng cách sử dụng câu lệnh REQUIRE trong tài liệu SQL khi tạo người dùng.

Kết nối được mã hóa có thể được sử dụng giữa các máy chủ nguồn và máy chủ sao chép trong quá trình sao chép dữ liệu.

Ngoài ra, bạn cũng có thể kết nối sử dụng mã hóa thông qua một kết nối SSH tới máy chủ MySQL. Điều này cho phép bạn bảo mật kết nối từ xa tới máy chủ MySQL sử dụng kết nối SSH.

3.3. Các thành phần bảo mật và plugin

Plugins cho việc xác thực kết nối: MySQL cung cấp các plugin cho việc xác thực các yêu cầu kết nối từ các client đến MySQL Server. Có sẵn các plugin cho nhiều giao thức xác thực. Điều này giúp bảo vệ sự an toàn khi có ai đó cố gắng kết nối vào máy chủ MySQL.

Thông tin chi tiết về quá trình xác thực diễn ra như sau:

- Khi một client kết nối vào máy chủ MySQL, máy chủ sử dụng tên người dùng mà client cung cấp và địa chỉ host của client để chọn hàng tài khoản thích hợp từ bảng hệ thống. Máy chủ sau đó thực hiện việc xác thực client, xác định từ hàng tài khoản rằng plugin xác thực nào áp dụng cho client trong bảng `mysql.user`.
- Nếu máy chủ không thể tìm thấy plugin, một lỗi xảy ra và cuộc kết nối sẽ bị từ chối.
- Nếu tìm thấy plugin, máy chủ gọi plugin đó để xác thực người dùng, và plugin trả về một trạng thái cho máy chủ chỉ ra xem người dùng đã cung cấp mật khẩu đúng và được phép kết nối hay không.

Tính năng Pluggable Authentication trong MySQL cung cấp các khả năng quan trọng sau đây:

- **Lựa chọn phương thức xác thực**: Giúp người quản trị cơ sở dữ liệu (DBAs) dễ dàng lựa chọn và thay đổi phương thức xác thực được sử dụng cho từng tài khoản MySQL cụ thể. Điều này cho phép bạn tùy chỉnh cách mà người dùng cụ thể sẽ được xác thực, phù hợp với yêu cầu cụ thể của ứng dụng hoặc môi trường.
- **Xác thực bên ngoài (External Authentication)**: Cho phép các client kết nối vào máy chủ MySQL bằng thông tin xác thực phù hợp với các phương thức xác thực lưu trữ thông tin xác thực ở nơi khác, không phải trong bảng hệ thống (như bảng `mysql.user`). Ví dụ, bạn có thể tạo các plugin để sử dụng các phương thức xác thực bên ngoài như PAM, Windows login IDs, LDAP hoặc Kerberos. Điều này mở rộng khả năng kết nối vào MySQL bằng các tài khoản xác thực từ nguồn bên ngoài hệ thống MySQL.
- **Người dùng ẩn danh (Proxy Users)**: Khi một người dùng được phép kết nối, một plugin xác thực có thể trả về máy chủ một tên người dùng khác với tên của người dùng đang kết nối, để chỉ ra rằng người dùng đang kết nối là một người dùng ẩn danh cho một người dùng khác (người được ẩn danh). Trong thời gian kết nối, người dùng ẩn danh sẽ được xem xét, về mục đích kiểm soát quyền truy cập, như có đặc quyền của người được ẩn danh. Hiệu quả, một người dùng thay mặt cho một người dùng khác. Điều này có thể hữu ích trong trường hợp quản lý quyền truy cập và quản lý ứng dụng phức tạp.

Chi tiết về từng plugin xác thực cụ thể có thể được tìm hiểu trong Section 6.4.1, “Authentication Plugins”.

Thành phần kiểm tra mật khẩu: MySQL cung cấp một thành phần kiểm tra mật khẩu để thực hiện các chính sách về độ mạnh của mật khẩu và đánh giá độ mạnh của mật khẩu tiềm năng. Điều này giúp đảm bảo mật khẩu của người dùng đủ mạnh để ngăn chặn các cuộc tấn công dự đoán mật khẩu yếu. Thông tin

chi tiết có thể được tìm hiểu trong Section 6.4.3, “The Password Validation Component”.

Các plugin Keyring cho lưu trữ an toàn thông tin nhạy cảm: MySQL cung cấp các plugin Keyring cho lưu trữ an toàn thông tin nhạy cảm. Điều này giúp bảo vệ thông tin quan trọng và mật khẩu khỏi các nguy cơ bị truy cập trái phép. Thông tin chi tiết có thể được tìm hiểu trong Section 6.4.4, “The MySQL Keyring”.

MySQL Enterprise Audit (Chỉ dành cho phiên bản MySQL Enterprise): Đây là một plugin của MySQL Enterprise Edition, sử dụng MySQL Audit API để theo dõi và ghi lại các hoạt động kết nối và truy vấn được thực hiện trên máy chủ MySQL. Điều này giúp quản trị viên dễ dàng theo dõi và tuân thủ các quy định và chuẩn mực về bảo mật. Thông tin chi tiết có thể được tìm hiểu trong Section 6.4.5, “MySQL Enterprise Audit”.

Chức năng cho phép ứng dụng thêm các sự kiện thông điệp riêng vào nhật ký kiểm tra: Điều này cho phép ứng dụng thêm thông điệp tùy chỉnh vào nhật ký kiểm tra. Thông tin chi tiết có thể được tìm hiểu trong Section 6.4.6, “The Audit Message Component”.

MySQL Enterprise Firewall (Chỉ dành cho phiên bản MySQL Enterprise): Đây là một tường lửa cấp ứng dụng cho MySQL, cho phép quản trị viên cấp phép hoặc từ chối thực thi các câu lệnh SQL dựa trên việc so sánh với danh sách các mẫu câu lệnh được chấp nhận. Điều này giúp bảo vệ MySQL Server khỏi các cuộc tấn công như SQL injection hoặc việc lợi dụng ứng dụng ngoài phạm vi truy vấn hợp pháp của chúng. Thông tin chi tiết có thể được tìm hiểu trong Section 6.4.7, “MySQL Enterprise Firewall”.

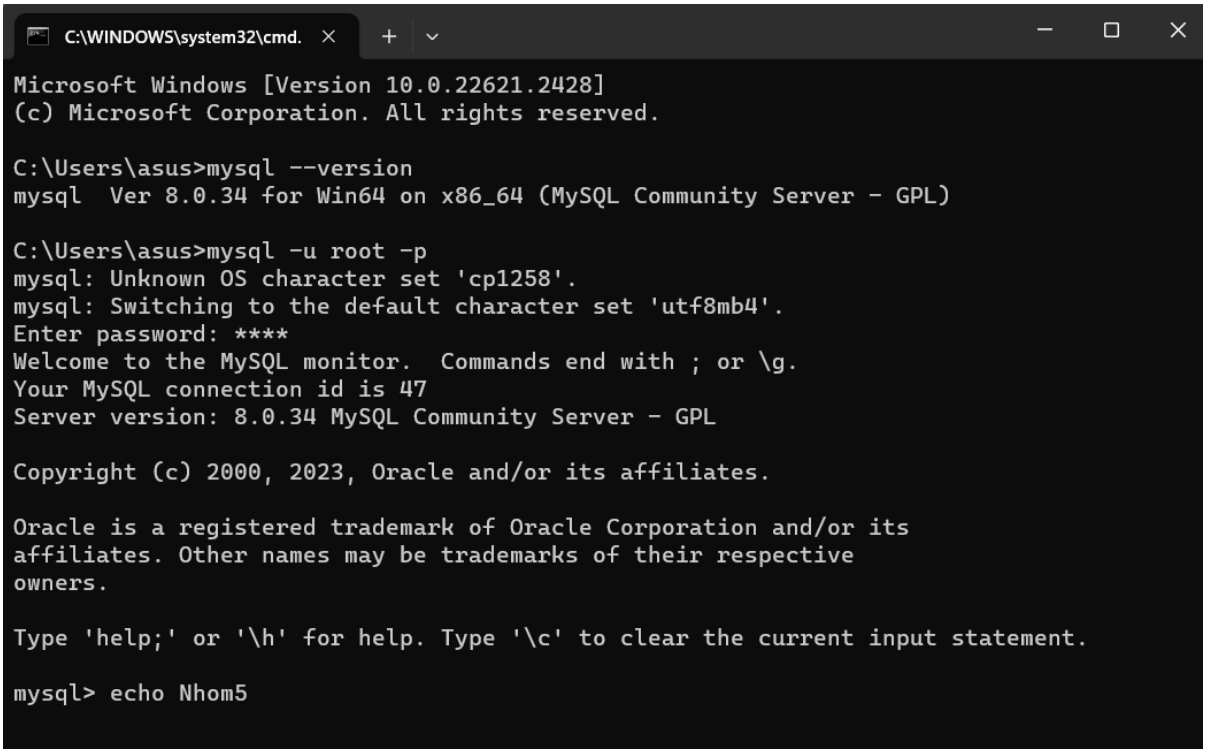
MySQL Enterprise Data Masking and De-Identification (Chỉ dành cho phiên bản MySQL Enterprise): Được thực hiện dưới dạng một thư viện plugin chứa các chức năng, cho phép ẩn thông tin nhạy cảm bằng cách thay thế các giá trị thực bằng giá trị thay thế. Các chức năng này giúp che giấu dữ liệu hiện có bằng nhiều phương pháp như làm mờ (loại bỏ các đặc điểm nhận dạng), tạo dữ liệu ngẫu nhiên theo định dạng và thay thế hoặc ghi đè dữ liệu. Thông tin chi tiết có thể được tìm hiểu trong Section 6.5, “MySQL Enterprise Data Masking and De-Identification”.

III. CÀI ĐẶT VÀ QUẢN TRỊ MYSQL

1. Cài đặt

Có thể download tại trang chủ : MySQL

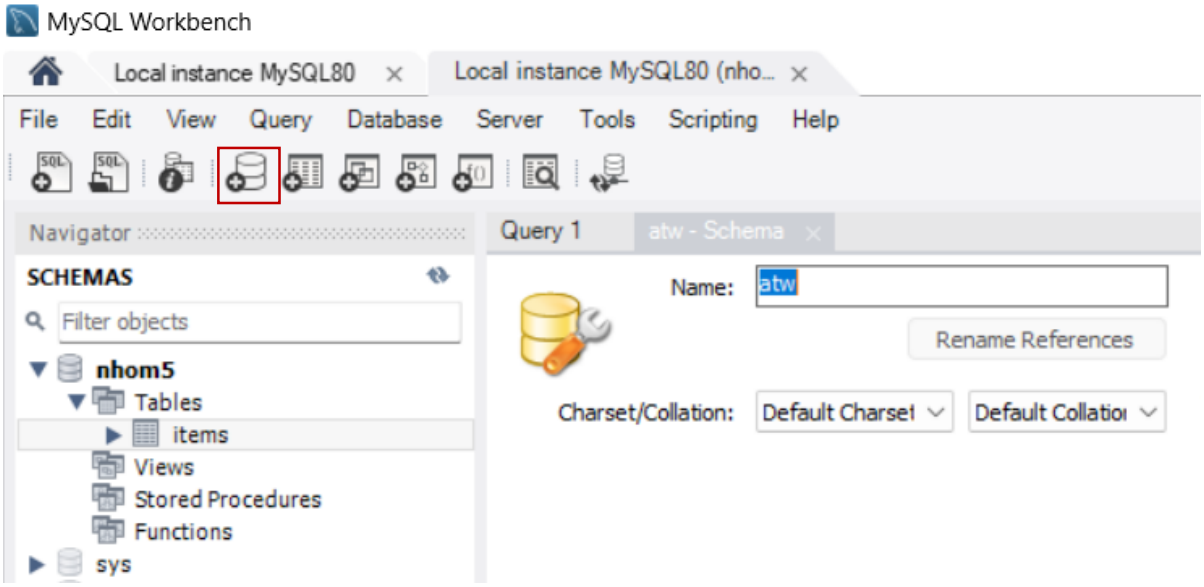
Thực hiện cài đặt (Server, Workbench, Shell, Document,…). Set mật khẩu và kiểm tra cài đặt thành công tại cmd



2. Quản trị MySQL

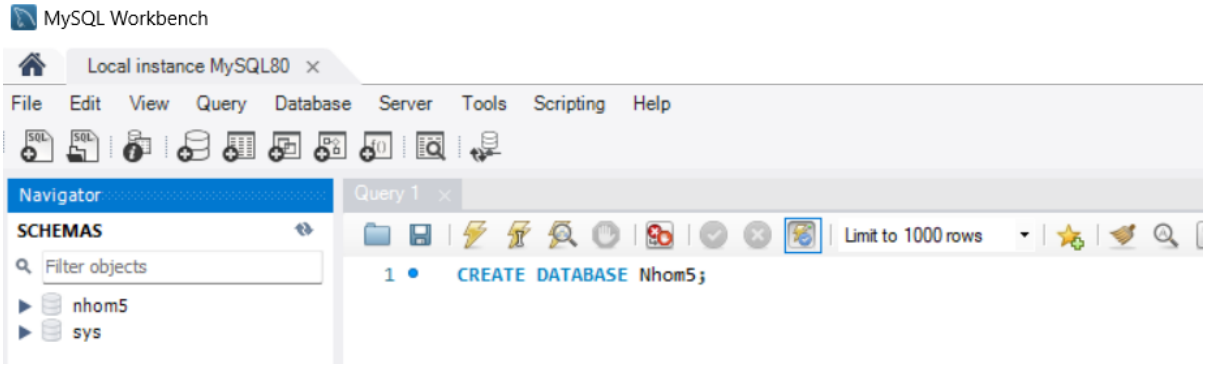
2.1. Tạo CSDL

Chúng ta có thể tạo mới CSDL bằng cách Nhấp vào biểu tượng cơ sở dữ liệu với dấu cộng (hiển thị trong hình bên dưới). Nhập tên và nhấp Apply.



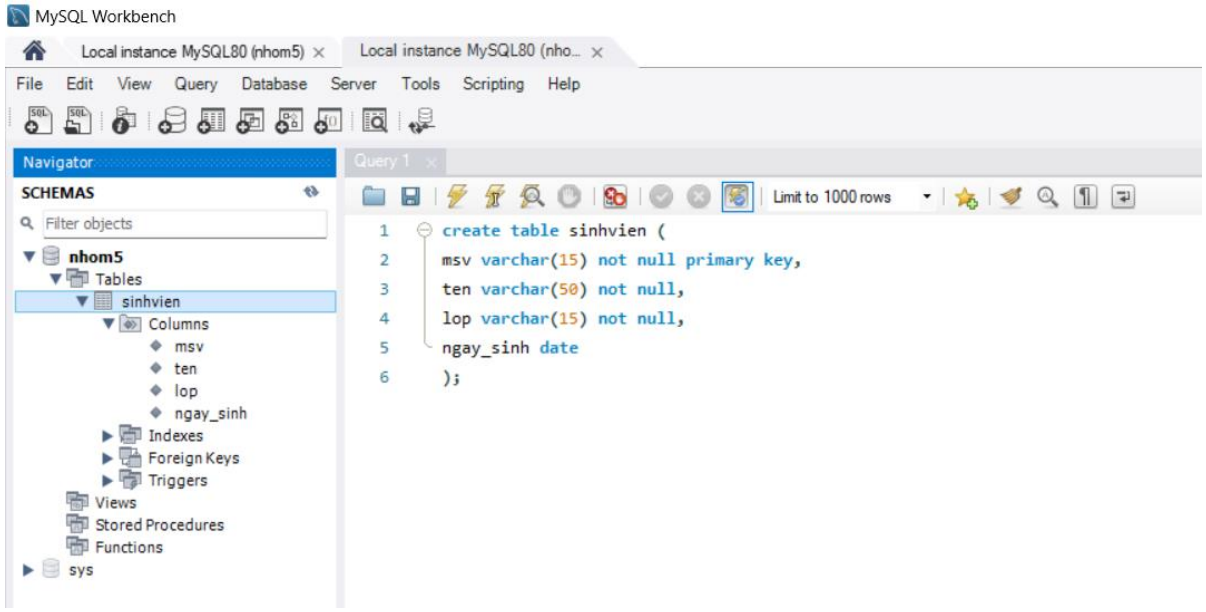
Hoặc ta có thể tạo CSDL bằng câu lệnh

```
CREATE DATABASE <database_name>;
```



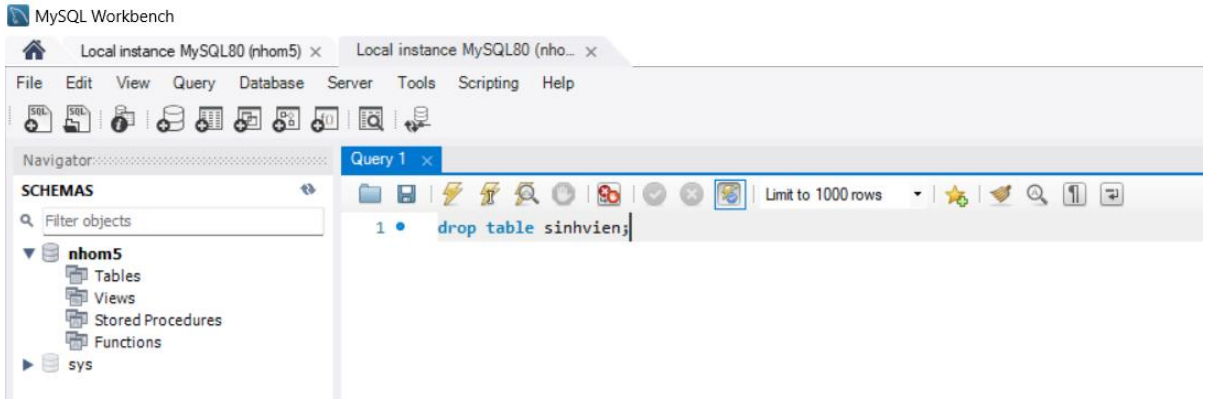
2.2. Thêm bảng

Ta có thể thêm bảng bằng cách nhấp chuột phải vào Table -> Create Table hoặc làm như hình dưới đây



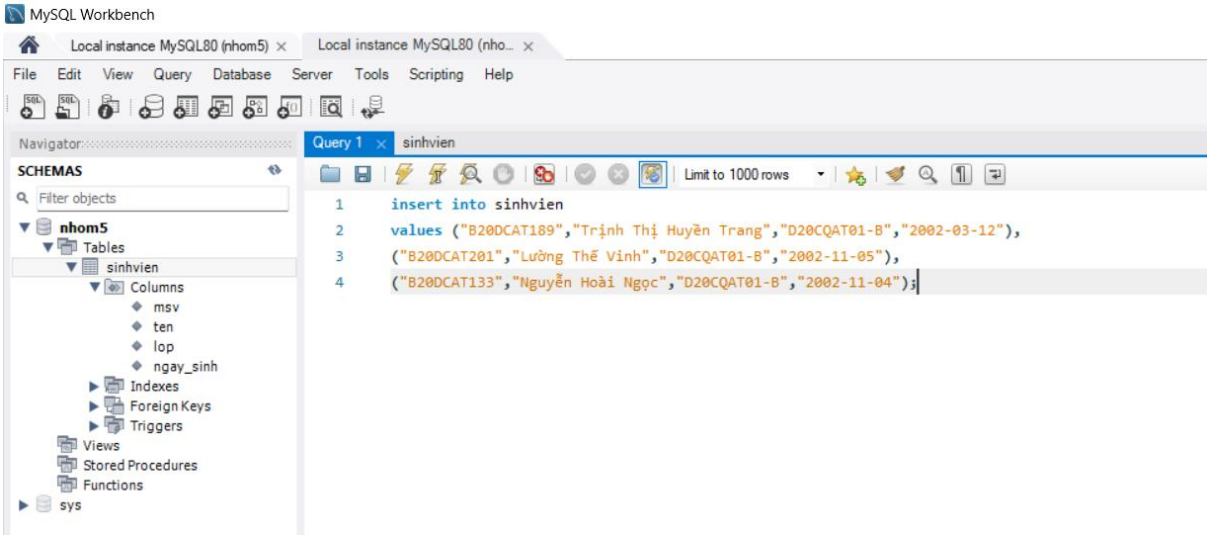
2.3. Xóa bảng

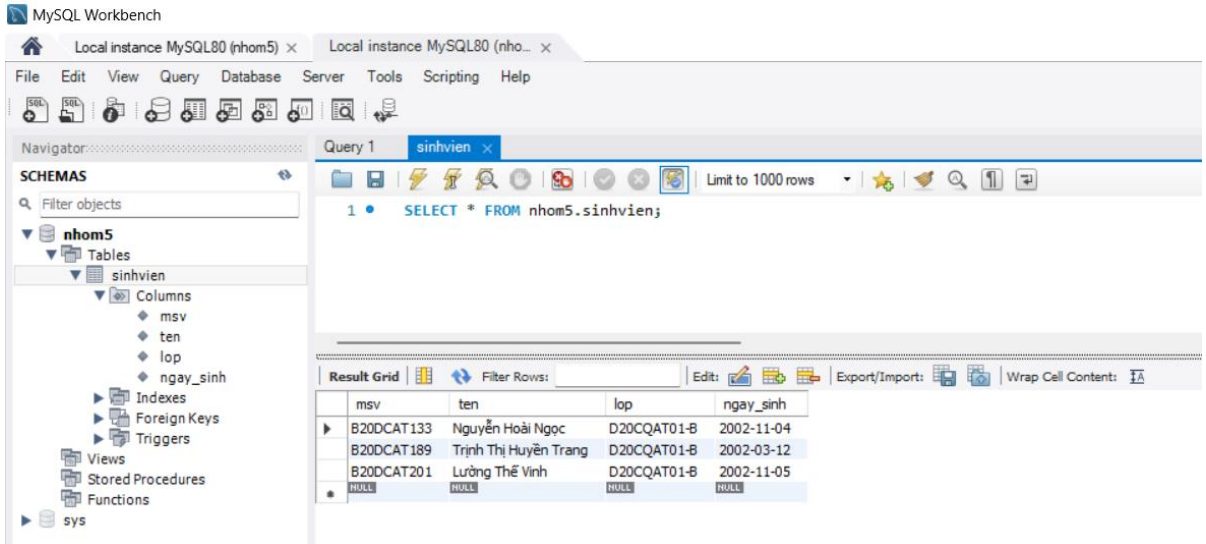
Chúng ta có thể xóa bảng bằng cách nhấp chuột phải vào bảng -> Drop Table hoặc dùng câu lệnh dưới đây.



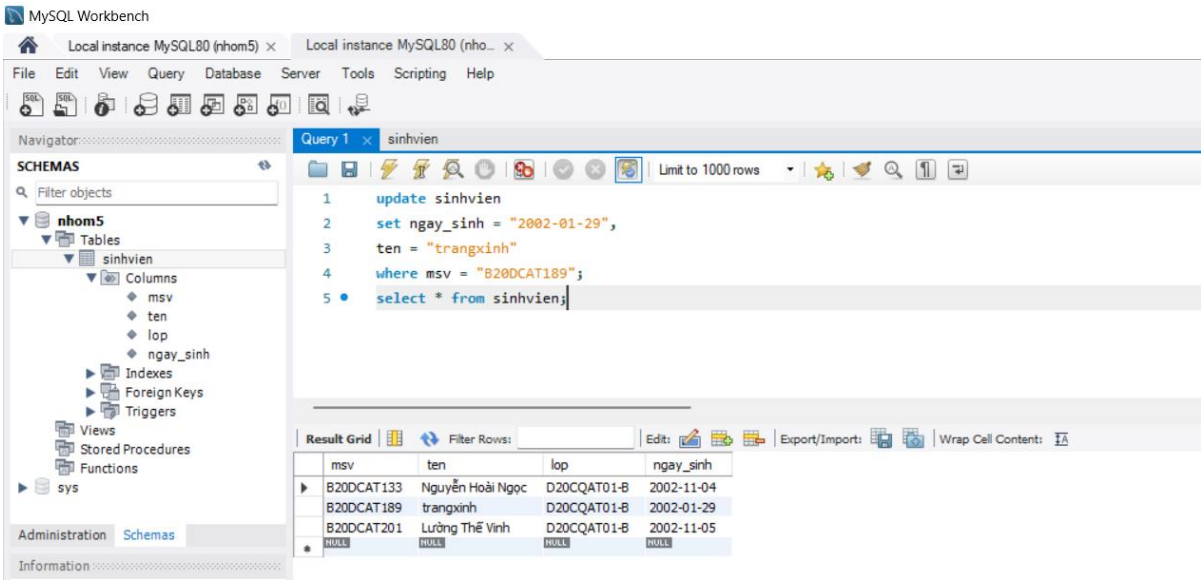
2.4. Thêm/ Sửa dữ liệu

Thêm thông tin một số sinh viên

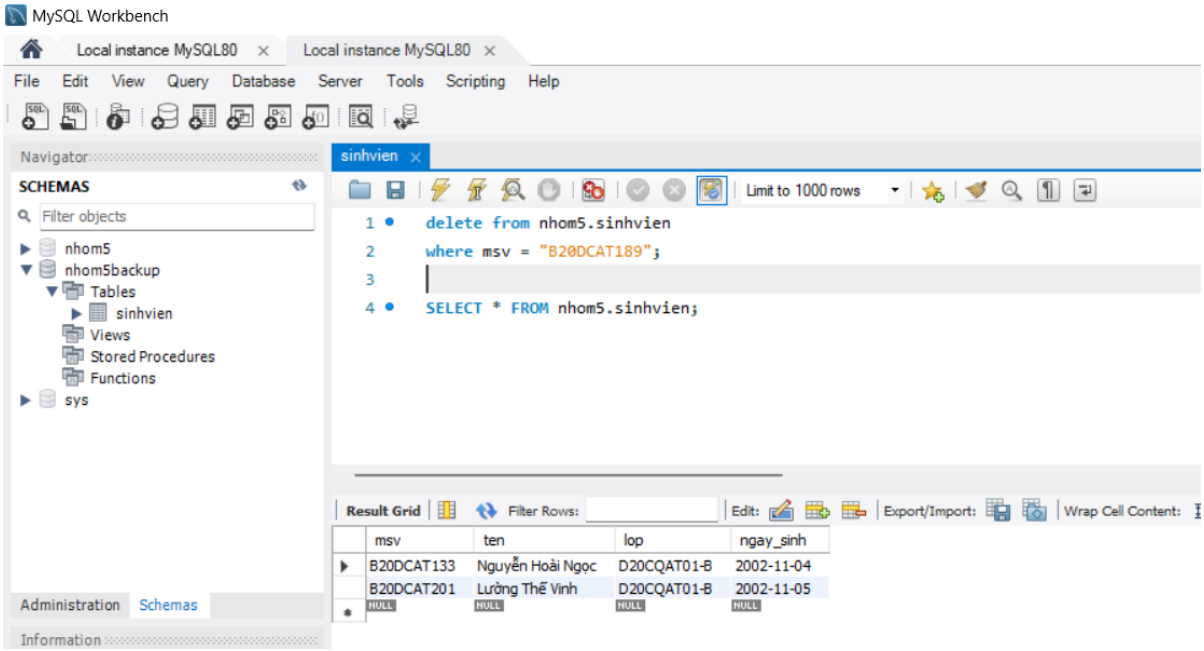




Sửa dữ liệu

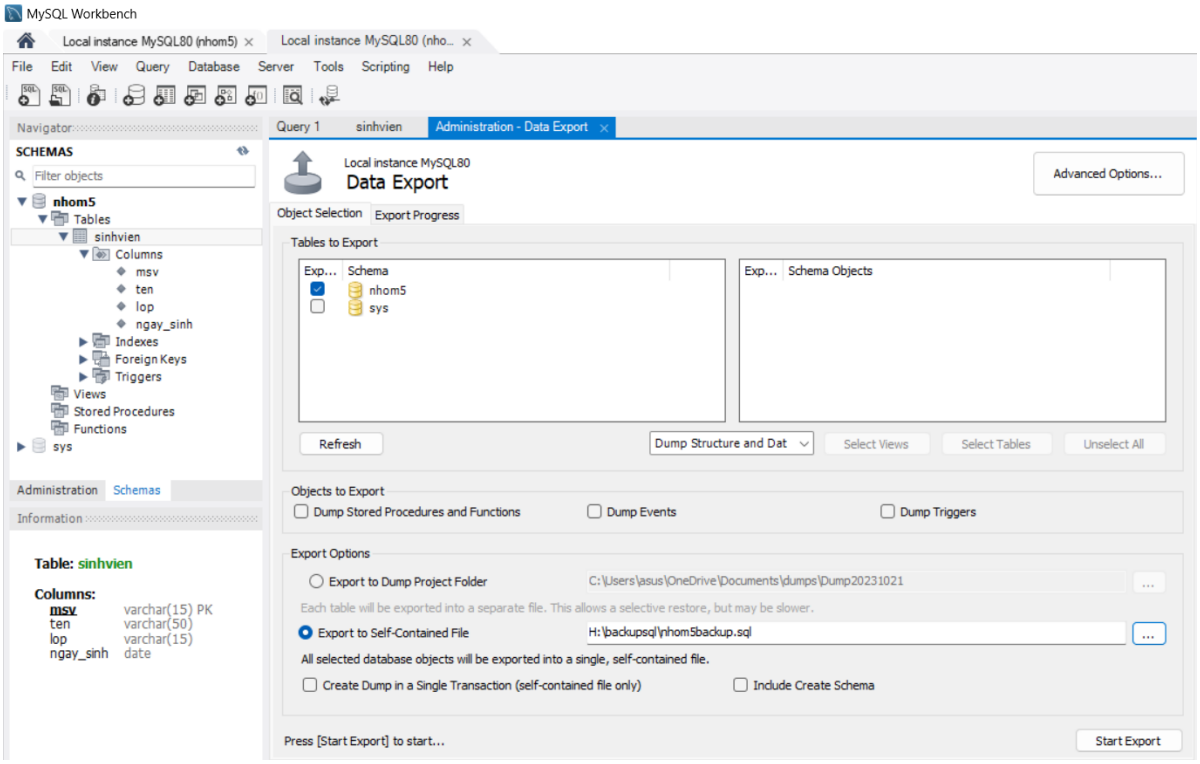


Xóa dữ liệu

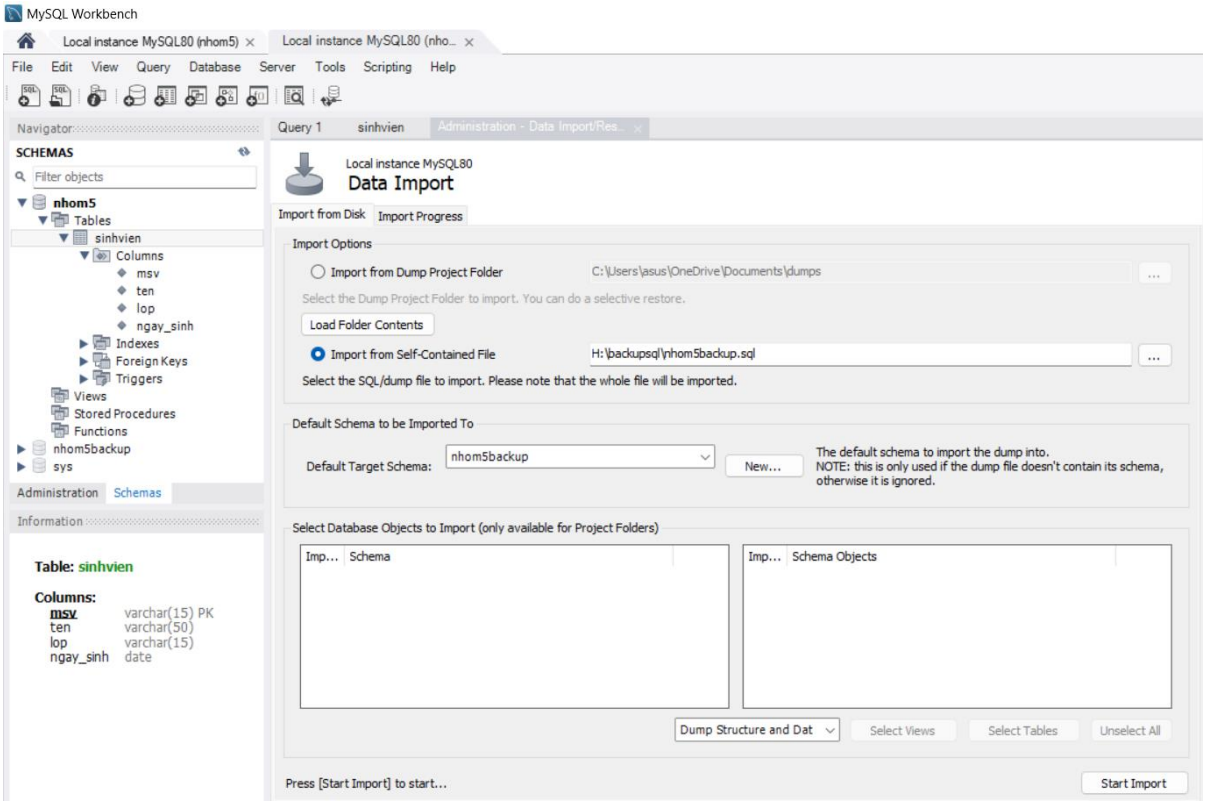


2.5. Tạo backup CSDL

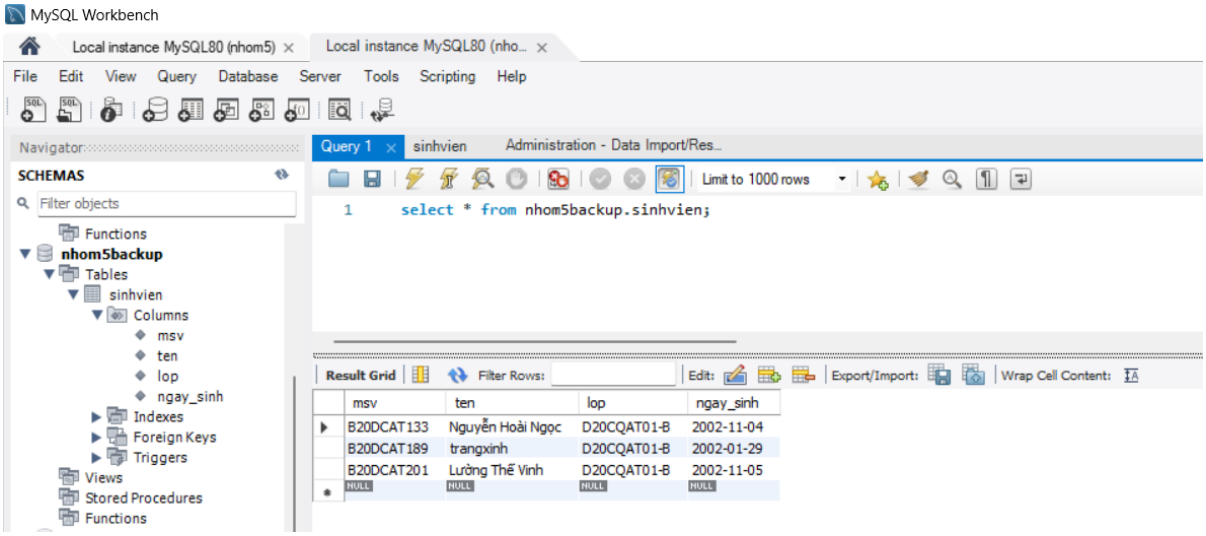
Tại MySQL Workbench -> Server -> Data Export -> Chọn csdl muốn backup, chọn Dump Structure and Data, chọn Export ra file sql -> chọn nơi muốn lưu -> Start Export.



Khi muốn khôi phục lại dữ liệu, Đầu tiên ta tạo một csdl mới. Tại Server -> Data Import -> Chọn import file sql và chọn file backup mà ta đã lưu trữ, chọn csdl -> Start Import.



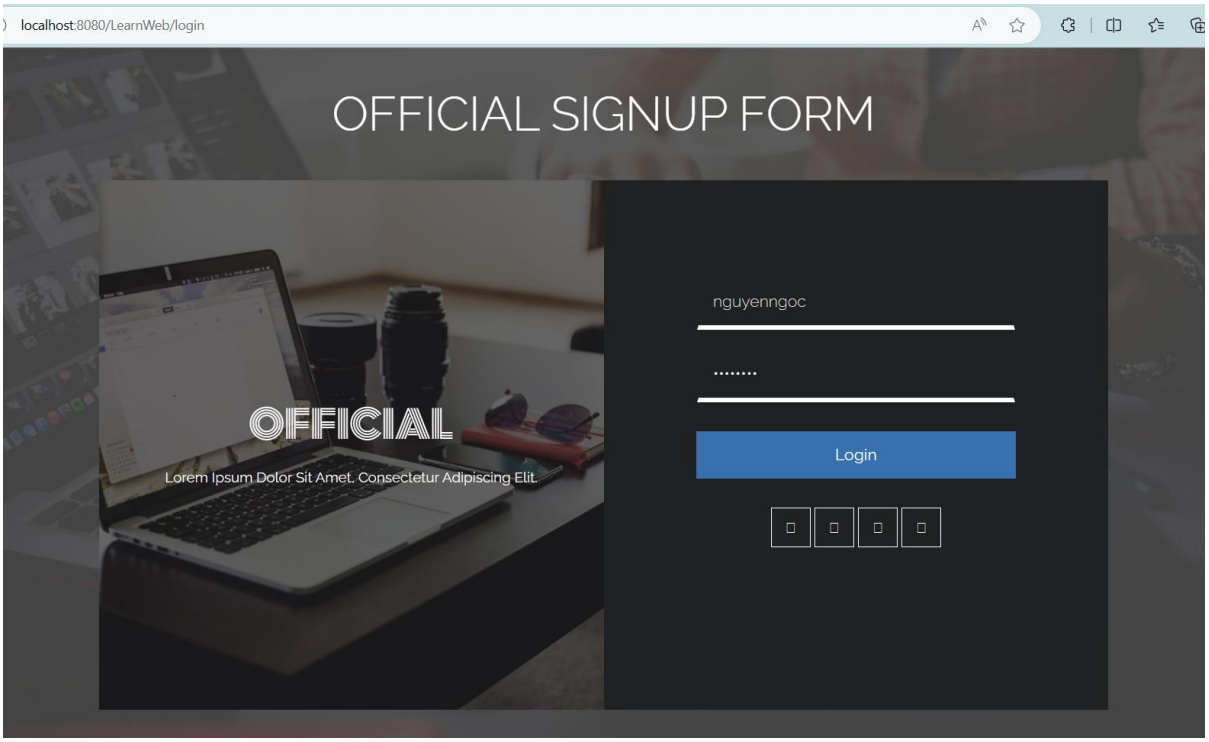
Refresh và kiểm tra lại



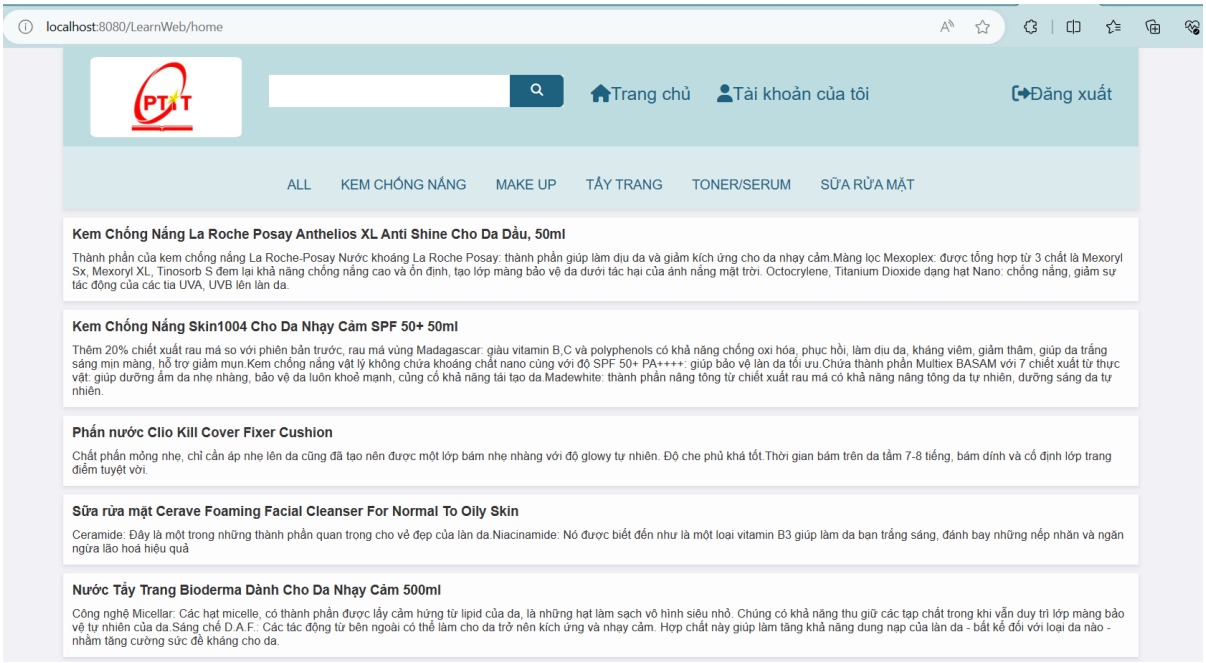
IV. DEMO TẤN CÔNG LỖ HỔNG QUẢN TRỊ MYSQL

Chuẩn bị một trang Web, sử dụng cuộc tấn công UNION để khai thác lỗ hổng SQL Injection nhằm lấy được tài khoản và mật khẩu người dùng trong CSDL.

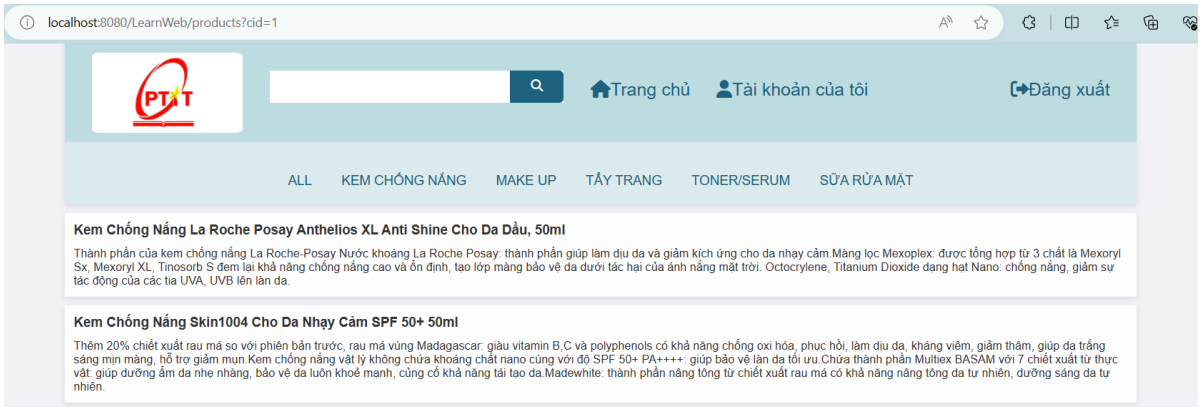
Bước 1: Đăng nhập với username=nguyenngoc, password=ngoc0411



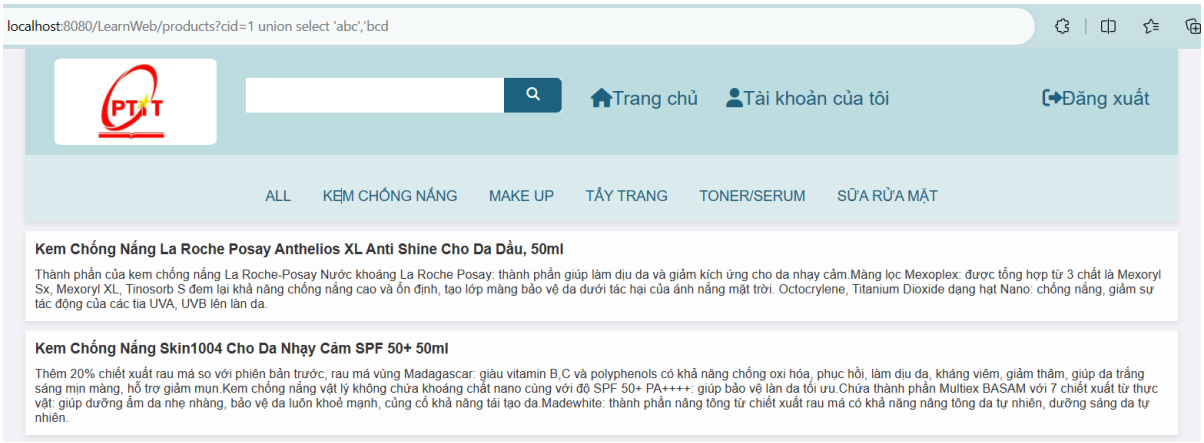
Giao diện trang chủ hiện ra



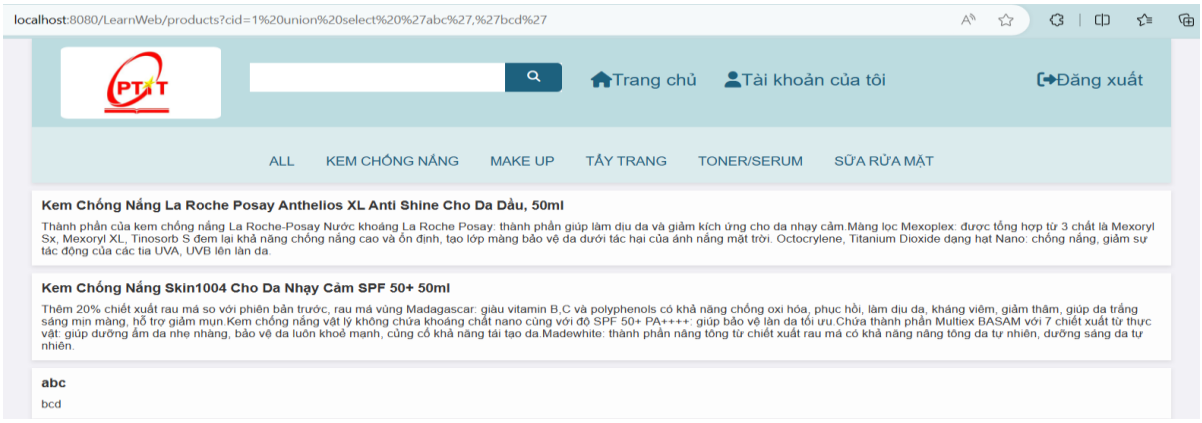
Click mục kem chống nắng hiển thị sản phẩm



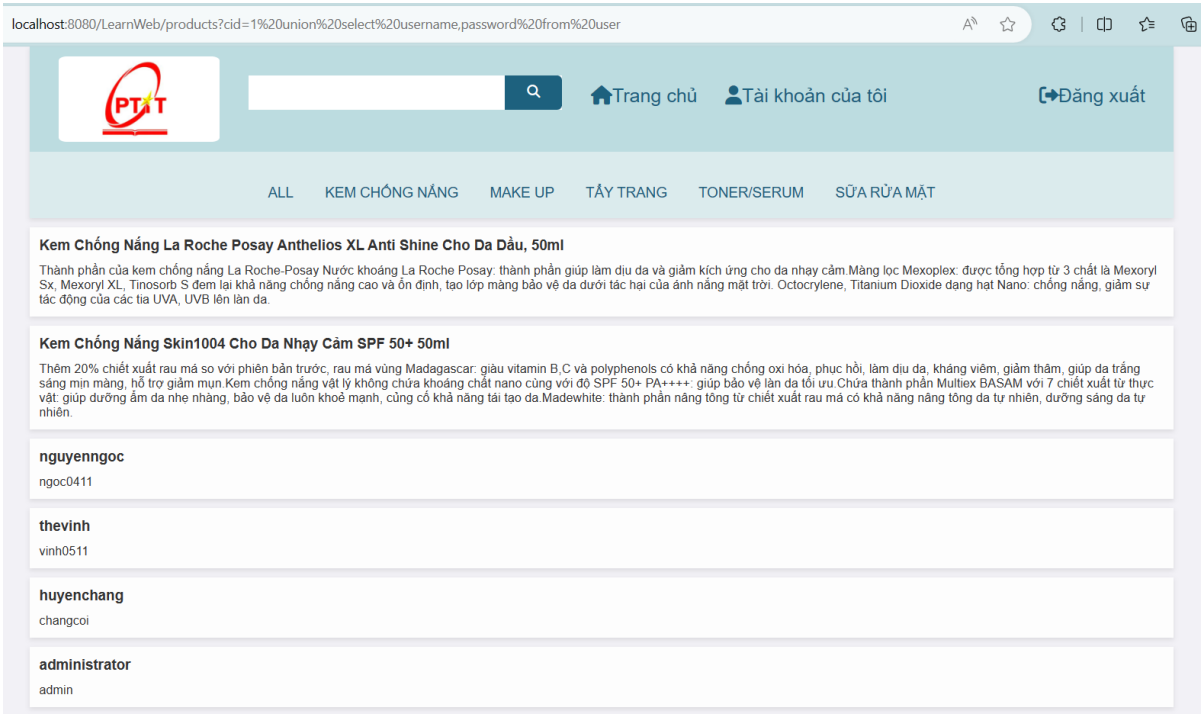
Thực hiện chèn union select ‘abc’,’bcd’ vào trong url để kiểm tra số cột trả về

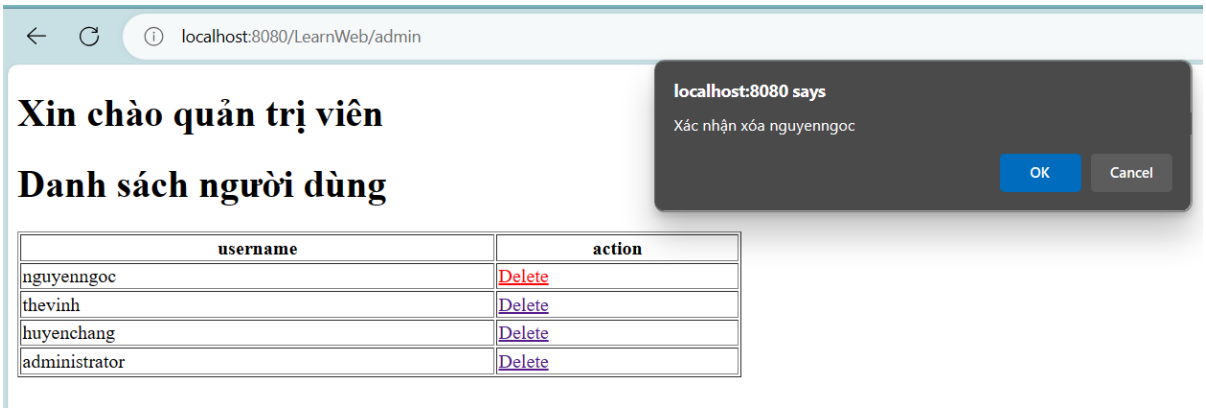


Thu được kết quả như sau

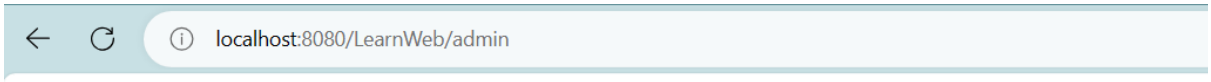


Tiến hành truy xuất nội dung bảng user với việc chèn thêm tải trọng union select username,password from user thu được kết quả hiển thị tên người dùng kèm mật khẩu lên màn hình





Xóa thành công người dùng



Xin chào quản trị viên

Danh sách người dùng

username	action
thevinh	Delete
huyenchang	Delete
administrator	Delete

TÀI LIỆU THAM KHẢO

Huyền. (2020, 9 17). *Mysql là gì? Tổng hợp thông tin chi tiết nhất về Mysql*. Được truy lục từ Bizflycloud: https://bizflycloud.vn/tin-tuc/mysql-la-gi-tai-sao-nen-su-dung-mysql-20200917180705499.htm

Linh, C. P. (2022, 8 10). *Cơ chế bảo mật trong my SQL*. Được truy lục từ Studocu: https://www.studocu.com/vn/document/hoc-vien-cong-nghe-buu-chinh-vien-thong/tieng-anh/co-che-bao-mat-trong-my-sql/37069883

Minh, T. C. (2021, 5 2). *Tìm hiểu MYSQL Architecture*. Được truy lục từ VIBLO: https://viblo.asia/p/tim-hieu-mysql-architecture-RnB5pj9JZPG