



Học phần:

Các hệ quản trị CSDL



Giảng viên: ThS. Lê Văn Hòa

Khoa QLSK&CNTT – Trường Du lịch



BÀI 8

BẢO MẬT CƠ SỞ DỮ LIỆU



NỘI DUNG CHÍNH

- 1. Tổng quan về bảo mật cơ sở dữ liệu
- 2. Cấp phát quyền
- 3. Thu hồi quyền



1. Tổng quan về bảo mật CSDL

- Bảo mật là một trong những yếu tố đóng vai trò quan trọng đối với sự sống còn của CSDL.
- Hầu hết các hệ quản trị CSDL thương mại hiện nay đều cung cấp khả năng bảo mật CSDL với những chức năng như:
 - Cấp phát quyền truy cập CSDL cho người dùng, phát hiện và ngăn chặn những thao tác trái phép của người sử dụng trên CSDL.
 - Cấp phát quyền sử dụng các câu lệnh, các đối tượng CSDL đối với người dùng.
 - Thu hồi (huỷ bỏ) quyền của người dùng.



1. Tổng quan về bảo mật CSDL

- Bảo mật dữ liệu trong SQL Server được thực hiện dựa trên ba khái niệm chính sau đây:
 - Người dùng CSDL (Database user)
 - Các đối tượng CSDL (Database objects)
 - Đặc quyền (Privileges)



1. Tổng quan về bảo mật CSDL

Người dùng CSDL (Database user)

- Là đối tượng sử dụng CSDL, thực thi các thao tác trên CSDL như tạo bảng, truy xuất dữ liệu,...
- Mỗi một người dùng trong CSDL được xác định thông qua tên người dùng (User ID).
- Chính sách bảo mật CSDL được áp dụng cho mỗi người dùng.



1. Tổng quan về bảo mật CSDL

Các đối tượng CSDL (Database objects)

- Tập hợp các đối tượng, các cấu trúc lưu trữ được sử dụng trong CSDL như bảng, khung nhìn, thủ tục, hàm được gọi là các đối tượng CSDL.
- Đây là những đối tượng cần được bảo vệ trong chính sách bảo mật của CSDL.



1. Tổng quan về bảo mật CSDL

Đặc quyền (Privileges)

- Là tập những thao tác được cấp phát cho người dùng trên các đối tượng CSDL.
- **Ví dụ:** Một người dùng có thể truy xuất dữ liệu trên một bảng bằng câu lệnh SELECT nhưng có thể không thể thực hiện các câu lệnh INSERT, UPDATE hay DELETE trên bảng đó.



1. Tổng quan về bảo mật CSDL

- SQL cung cấp hai câu lệnh cho phép chúng ta thiết lập các chính sách bảo mật trong CSDL:
 - Lệnh **GRANT**: Sử dụng để **cấp phát quyền** cho người sử dụng trên các đối tượng CSDL hoặc quyền sử dụng các câu lệnh SQL trong CSDL.
 - Lệnh **REVOKE**: Được sử dụng để **thu hồi quyền** đối với người sử dụng.



1. Tổng quan về bảo mật CSDL

Tạo tài khoản đăng nhập (login)

- *Cú pháp*

CREATE LOGIN Tên_Login

WITH PASSWORD = Mật_khẩu

- *Ví dụ:*

CREATE LOGIN thuchanh

WITH PASSWORD = '12345'

- *Lưu ý:* Những tài khoản đăng nhập này chỉ có quyền truy cập vào Server chứ chưa thể vào được database (cơ sở dữ liệu) ở bên trong.



1. Tổng quan về bảo mật CSDL

Tạo người dùng (user)

- Cú pháp:

CREATE USER Tên_User FOR LOGIN Tên_Login

- Ví dụ:

CREATE USER thuchanh FOR LOGIN thuchanh

- **Lưu ý:** Chúng ta thực hiện câu lệnh CREATE USER trên CSDL nào thì người dùng được tạo ra được phép truy cập vào CSDL đó.



2. Cấp phát quyền

- Câu lệnh **GRANT** được sử dụng để cấp phát quyền cho người dùng trên các đối tượng CSDL.
- Câu lệnh GRANT thường được sử dụng trong các trường hợp sau:
 - Người sở hữu đối tượng CSDL muốn cho phép người dùng khác quyền sử dụng những đối tượng mà anh ta đang sở hữu.
 - Người sở hữu CSDL cấp phát quyền thực thi các câu lệnh (như CREATE TABLE, CREATE VIEW,...) cho những người dùng khác.



2.1 Cấp phát quyền trên đối tượng

- Chỉ có người sở hữu CSDL hoặc người sở hữu đối tượng CSDL mới có thể cấp phát quyền cho người dùng trên các đối tượng CSDL.
- Cú pháp câu lệnh GRANT:

**GRANT ALL [PRIVILEGES] | Các_quyền_cấp_phát
[(Danh_sách_cột)] ON Tên_bảng | Tên_khung_nhìn
|ON Tên_bảng | Tên_khung_nhìn [(Danh_sách_cột)]
|ON Tên_thủ_tục
|ON Tên_hàm
TO Danh_sách_người_dùng
[WITH GRANT OPTION]**



2.1 Cấp phát quyền trên đối tượng

- **ALL [PRIVILEGES]**: Cấp phát tất cả các quyền cho người dùng trên đối tượng CSDL được chỉ định. Các quyền có thể cấp phát cho người dùng bao gồm:
 - Đối với bảng, khung nhìn, và hàm trả về dữ liệu kiểu bảng: SELECT, INSERT, DELETE, UPDATE và REFERENCES.
 - Đối với cột trong bảng, khung nhìn: SELECT và UPDATE.
 - Đối với thủ tục lưu trữ và hàm vô hướng: EXECUTE.



2.1 Cấp phát quyền trên đối tượng

- Các_quyền_cấp_phát: Danh sách các quyền cần cấp phát cho người dùng trên đối tượng CSDL được chỉ định. Các quyền được phân cách nhau bởi dấu phẩy.
- Tên_bảng | Tên_khung_nhìn: Tên của bảng hoặc khung nhìn cần cấp phát quyền.
- Danh_sách_cột: Danh sách các cột của bảng hoặc khung nhìn cần cấp phát quyền.
- Danh_sách_người_dùng: Danh sách tên người dùng nhận quyền được cấp phát. Tên của các người dùng được phân cách nhau bởi dấu phẩy.
- **WITH GRANT OPTION**: Cho phép người dùng chuyển tiếp quyền cho người dùng khác.



2.1 Cấp phát quyền trên đối tượng

- Ví dụ:** Cấp phát cho người dùng có tên Thuchanh quyền thực thi các câu lệnh SELECT, INSERT và UPDATE trên bảng lop.

```
GRANT SELECT, INSERT, UPDATE  
ON lop  
TO Thuchanh
```



2.1 Cấp phát quyền trên đối tượng

- Ví dụ:** Cho phép người dùng Thuchanh quyền xem họ tên và ngày sinh của các sinh viên (cột hodem, ten và ngaysinh của bảng SINHVIEN)

GRANT SELECT

(hodem,ten,ngaysinh) ON sinhvien

TO Thuchanh

hoặc:

GRANT SELECT

ON sinhvien(hodem,ten,ngaysinh)

TO Thuchanh



2.1 Cấp phát quyền trên đối tượng

- Với quyền được cấp phát như trên, người dùng Thuchanh có thể thực hiện câu lệnh sau trên bảng SINHVIEN

```
SELECT hoden, ten, ngaysinh
FROM sinhvien
```
- **Lưu ý:** Câu lệnh dưới đây lại không thể thực hiện được

```
SELECT * FROM sinhvien
```



2.1 Cấp phát quyền trên đối tượng

- Trong trường hợp cần cấp phát tất cả các quyền có thể thực hiện được trên đối tượng CSDL cho người dùng, thay vì liệt kê các câu lệnh, chúng ta chỉ cần sử dụng từ khoá **ALL PRIVILEGES** (từ khóa **PRIVILEGES** có thể không cần chỉ định).
- Ví dụ:** Cấp phát cho người dùng Thuchanh các quyền SELECT, INSERT, UPDATE, DELETE VÀ REFERENCES trên bảng DIEMTHI
GRANT ALL
ON diemthi
TO Thuchanh



2.1 Cấp phát quyền trên đối tượng

- Khi cấp phát quyền nào đó cho một người dùng trên một đối tượng CSDL, người dùng đó có thể thực thi câu lệnh được cho phép trên đối tượng đã cấp phát.
- Tuy nhiên, người dùng đó không có quyền cấp phát những quyền mà mình được phép cho những người sử dụng khác.
- Trong một số trường hợp, khi cấp phát quyền cho một người dùng nào đó, chúng ta có thể cho phép người đó chuyển tiếp quyền cho người dùng khác bằng cách chỉ định tùy chọn **WITH GRANT OPTION** trong câu lệnh GRANT.



2.1 Cấp phát quyền trên đối tượng

- Ví dụ:** Cho phép người dùng Thuchanh quyền xem dữ liệu trên bảng SINHVIEN đồng thời có thể chuyển tiếp quyền này cho người dùng khác.

```
GRANT SELECT  
ON sinhvien  
TO Thuchanh  
WITH GRANT OPTION
```



2.2. Cấp phát quyền thực thi câu lệnh

- Ngoài chức năng cấp phát quyền cho người sử dụng trên các đối tượng CSDL, câu lệnh GRANT còn có thể sử dụng để cấp phát cho người sử dụng một số quyền trên hệ quản trị CSDL hoặc CSDL.
- Những quyền có thể cấp phát bao gồm:
 - Tạo cơ sở dữ liệu: CREATE DATABASE.
 - Tạo bảng: CREATE TABLE
 - Tạo khung nhìn: CREATE VIEW
 - Tạo thủ tục lưu trữ: CREATE PROCEDURE
 - Tạo hàm: CREATE FUNCTION
 - Sao lưu cơ sở dữ liệu: BACKUP DATABASE



2.2. Cấp phát quyền thực thi câu lệnh

- Cú pháp câu lệnh **GRANT** cấp phát quyền thực thi các câu lệnh:

GRANT ALL | Danh_sách_câu_lệnh

TO Danh_sách_người_dùng

- Ví dụ:** Để cấp phát quyền tạo bảng và khung nhìn cho người dùng có tên là Thuchanh, ta sử dụng câu lệnh như sau:

GRANT CREATE TABLE, CREATE VIEW

TO Thuchanh



2.2. Cấp phát quyền thực thi câu lệnh

- Với câu lệnh **GRANT**, chúng ta có thể cho phép người sử dụng tạo các đối tượng CSDL trong CSDL.
- Đối tượng CSDL do người dùng nào tạo ra sẽ do người đó sở hữu và do đó người này có quyền cho người dùng khác sử dụng đối tượng và cũng có thể xóa bỏ (DROP) đối tượng do mình tạo ra.
- Khác với trường hợp sử dụng câu lệnh **GRANT** để cấp phát quyền trên đối tượng CSDL, câu lệnh **GRANT** trong trường hợp này không thể sử dụng tùy chọn **WITH GRANT OPTION**, tức là người dùng không thể chuyển tiếp được các quyền thực thi các câu lệnh đã được cấp phát.



3. Thu hồi quyền

- Câu lệnh **REVOKE** được sử dụng để thu hồi quyền đã được cấp phát cho người dùng.
- Tương ứng với câu lệnh GRANT, câu lệnh REVOKE được sử dụng trong hai trường hợp:
 - Thu hồi quyền đã cấp phát cho người dùng trên các đối tượng cơ sở dữ liệu.
 - Thu hồi quyền thực thi các câu lệnh trên cơ sở dữ liệu đã cấp phát cho người dùng.



3.1 Thu hồi quyền trên đối tượng CSDL

- Cú pháp câu lệnh **REVOKE** sử dụng để thu hồi quyền đã cấp phát trên đối tượng CSDL:

REVOKE [GRANT OPTION FOR]

**ALL [PRIVILEGES] | Các_quyền_cần_thu_hồi
[(Danh_sách_cột)] ON Tên_bảng | Tên_khung_nhìn
| ON Tên_bảng | Tên_khung_nhìn [(Danh_sách_cột)]
| ON Tên_thủ_tục
| ON Tên_hàm
FROM Danh_sách_người_dùng
[CASCADE]**



3.1 Thu hồi quyền trên đối tượng CSDL

- Câu lệnh **REVOKE** có thể sử dụng để thu hồi một số quyền đã cấp phát cho người dùng hoặc là thu hồi tất cả các quyền (**ALL PRIVILEGES**).
- Ví dụ:** Thu hồi quyền thực thi lệnh INSERT trên bảng LOP đối với người dùng Thuchanh.

```
REVOKE INSERT  
ON lop  
FROM Thuchanh
```



3.1 Thu hồi quyền trên đối tượng CSDL

- Giả sử người dùng Thuchanh đã được cấp phát quyền xem dữ liệu trên các cột hodem, ten và ngaysinh của bảng SINHVIEN, câu lệnh dưới đây sẽ thu hồi quyền đã cấp phát trên cột ngaysinh (chỉ cho phép xem dữ liệu trên cột hodem và ten)

```
REVOKE SELECT  
ON SINHVIEN(NgaySinh)  
FROM Thuchanh
```

3.1 Thu hồi quyền trên đối tượng CSDL

- **Lưu ý:** Khi ta sử dụng câu lệnh **REVOKE** để thu hồi quyền trên một đối tượng CSDL từ một người dùng nào đó, chỉ những quyền mà ta đã cấp phát trước đó mới được thu hồi, những quyền mà người dùng này được cho phép bởi những người dùng khác vẫn còn có hiệu lực. Nói cách khác, nếu hai người dùng khác nhau cấp phát cùng các quyền trên cùng một đối tượng CSDL cho một người dùng khác, sau đó người thu nhất thu hồi lại quyền đã cấp phát thì những quyền mà người dùng thứ hai cấp phát vẫn có hiệu lực.



3.1 Thu hồi quyền trên đối tượng CSDL

- **Ví dụ:** Giả sử trong CSDL chúng ta có 3 người dùng là User_A, User_B và User_C. User_A và User_B đều có quyền sử dụng và cấp phát quyền trên bảng Table_1. User_A thực hiện lệnh sau để cấp phát quyền xem dữ liệu trên bảng Table_1 cho User_C:

```
GRANT SELECT  
ON Table_1 TO User_C
```

- User_B cấp phát quyền xem và bổ sung dữ liệu trên bảng Table_1 cho User_C bằng câu lệnh:

```
GRANT SELECT, INSERT  
ON Table_1 TO User_C
```

3.1 Thu hồi quyền trên đối tượng CSDL

- Như vậy, User_C có quyền xem và bổ sung dữ liệu trên bảng Table_1. Nay giờ, nếu User_B thực hiện lệnh:

```
REVOKE SELECT, INSERT  
ON Table_1 FROM User_C
```
- Người dùng User_C sẽ không còn quyền bổ sung dữ liệu trên bảng Table_1 nhưng vẫn có thể xem được dữ liệu của bảng này (quyền này do User_A cấp cho User_C và vẫn còn hiệu lực).



3.1 Thu hồi quyền trên đối tượng CSDL

- **Lưu ý:** Nếu chúng ta đã cấp phát quyền cho người dùng nào đó bằng câu lệnh **GRANT** với tùy chọn **WITH GRANT OPTION** thì khi thu hồi quyền bằng câu lệnh **REVOKE** phải chỉ định tùy chọn **CASCADE**. Trong trường hợp này, các quyền được chuyển tiếp cho những người dùng khác cũng đồng thời được thu hồi.



3.1 Thu hồi quyền trên đối tượng CSDL

- **Ví dụ:** Ta cấp phát cho người dùng User_A trên bảng Table_1 với câu lệnh GRANT như sau:

```
GRANT SELECT  
ON Table_1 TO User_A  
WITH GRANT OPTION
```

- Người dùng User_A lại cấp phát cho người dùng User_B quyền xem dữ liệu trên Table_1 với câu lệnh:

```
GRANT SELECT  
ON Table_1 TO User_B
```



3.1 Thu hồi quyền trên đối tượng CSDL

- Nếu muốn thu hồi quyền đã cấp phát cho người dùng User_A, ta sử dụng câu lệnh **REVOKE** như sau:

```
REVOKE SELECT  
ON Table_1 FROM User_A  
CASCADE
```
- Câu lệnh trên sẽ đồng thời thu hồi quyền mà User_A đã cấp cho User_B và như vậy cả User_A và User_B đều không thể xem được dữ liệu trên bảng Table_1.



3.1 Thu hồi quyền trên đối tượng CSDL

- Trong trường hợp cần thu hồi các quyền đã được chuyển tiếp và khả năng chuyển tiếp các quyền đối với những người đã được cấp phát quyền với tùy chọn **WITH GRANT OPTION**, trong câu lệnh **REVOKE** ta chỉ định mệnh đề **GRANT OPTION FOR**.



3.1 Thu hồi quyền trên đối tượng CSDL

- **Ví dụ:** Trong ví dụ trên, nếu ta thay câu lệnh:

```
REVOKE SELECT ON Table_1  
FROM User_A CASCADE
```

- bởi câu lệnh:

```
REVOKE GRANT OPTION FOR SELECT  
ON Table_1  
FROM User_A CASCADE
```

- Thì User_B sẽ không còn quyền xem dữ liệu trên bảng Table_1 đồng thời User_A không thể chuyển tiếp quyền mà ta đã cấp phát cho những người dùng khác (tuy nhiên User_A vẫn còn quyền xem dữ liệu trên bảng Table_1).



3.2. Thu hồi quyền thực thi các câu lệnh trên CSDL

- Cú pháp câu lệnh REVOKE sử dụng để thu hồi quyền thực thi các câu lệnh trên cơ sở dữ liệu (CREATE DATABASE, CREATE TABLE, CREATE VIEW,...):

**REVOKE ALL | các_câu_lệnh_cần_thu_hồi
FROM danh_sách_người_dùng**



3.2. Thu hồi quyền thực thi các câu lệnh trên CSDL

- Ví dụ:** Để không cho phép người dùng Thuchanh thực hiện lệnh CREATE TABLE trên cơ sở dữ liệu, ta sử dụng câu lệnh:

```
REVOKE CREATE TABLE  
FROM Thuchanh
```