

CHƯƠNG 4: BẢO MẬT TRONG SQL.....	2
4.1 Các khái niệm .....	2
4.2 Cấp phát quyền .....	3
4.2.1 Cấp phát quyền cho người dùng trên các đối tượng cơ sở dữ liệu .....	3
4.2.2 Cấp phát quyền thực thi các câu lệnh .....	5
4.3 Thu hồi quyền .....	6
4.3.1 Thu hồi quyền trên đối tượng cơ sở dữ liệu:.....	6
4.3.2 Thu hồi quyền thực thi các câu lệnh: .....	9

## Chương 4

---

# BẢO MẬT TRONG SQL

---

### 4.1 Các khái niệm

Bảo mật là một trong những yếu tố đóng vai trò quan trọng đối với sự sống còn của cơ sở dữ liệu. Hầu hết các hệ quản trị cơ sở dữ liệu thương mại hiện nay đều cung cấp khả năng bảo mật cơ sở dữ liệu với những chức năng như:

- Cấp phát quyền truy cập cơ sở dữ liệu cho người dùng và các nhóm người dùng, phát hiện và ngăn chặn những thao tác trái phép của người sử dụng trên cơ sở dữ liệu.
- Cấp phát quyền sử dụng các câu lệnh, các đối tượng cơ sở dữ liệu đối với người dùng.
- Thu hồi (huỷ bỏ) quyền của người dùng.

Bảo mật dữ liệu trong SQL được thực hiện dựa trên ba khái niệm chính sau đây:

- **Người dùng cơ sở dữ liệu (Database user):** Là đối tượng sử dụng cơ sở dữ liệu, thực thi các thao tác trên cơ sở dữ liệu như tạo bảng, truy xuất dữ liệu,... Mỗi một người dùng trong cơ sở dữ liệu được xác định thông qua tên người dùng (User ID). Một tập nhiều người dùng có thể được tổ chức trong một nhóm và được gọi là nhóm người dùng (User Group). Chính sách bảo mật cơ sở dữ liệu có thể được áp dụng cho mỗi người dùng hoặc cho các nhóm người dùng.
- **Các đối tượng cơ sở dữ liệu (Database objects):** Tập hợp các đối tượng, các cấu trúc lưu trữ được sử dụng trong cơ sở dữ liệu như bảng, khung nhìn, thủ tục, hàm được gọi là các đối tượng cơ sở dữ liệu. Đây là những đối tượng cần được bảo vệ trong chính sách bảo mật của cơ sở dữ liệu.
- **Đặc quyền (Privileges):** Là tập những thao tác được cấp phát cho người dùng trên các đối tượng cơ sở dữ liệu. Chẳng hạn 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.

SQL cung cấp hai câu lệnh cho phép chúng ta thiết lập các chính sách bảo mật trong cơ sở dữ liệu:

- **Lệnh GRANT:** Sử dụng để cấp phát quyền cho người sử dụng trên các đối tượng cơ sở dữ liệu hoặc quyền sử dụng các câu lệnh SQL trong cơ sở dữ liệu.
- **Lệnh REVOKE:** Được sử dụng để thu hồi quyền đối với người sử dụng.

## 4.2 Cấp phát quyền

Câu lệnh GRANT được sử dụng để cấp phát quyền cho người dùng hay nhóm người dùng trên các đối tượng cơ sở dữ liệu. Câu lệnh này thường được sử dụng trong các trường hợp sau:

- Người sở hữu đối tượng cơ sở dữ liệu muốn cho phép người dùng khác quyền sử dụng những đối tượng mà anh ta đang sở hữu.
- Người sở hữu cơ sở dữ liệu cấp phát quyền thực thi các câu lệnh (như CREATE TABLE, CREATE VIEW,...) cho những người dùng khác.

### 4.2.1 Cấp phát quyền cho người dùng trên các đối tượng cơ sở dữ liệu

Chỉ có người sở hữu cơ sở dữ liệu hoặc người sở hữu đối tượng cơ sở dữ liệu mới có thể cấp phát quyền cho người dùng trên các đối tượng cơ sở dữ liệu. Câu lệnh GRANT trong trường hợp này có cú pháp như sau:

```
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 | nhóm_người_dùng
[WITH GRANT OPTION ]
```

Trong đó:

ALL [PRIVILEGES]

Cấp phát tất cả các quyền cho người dùng trên đối tượng cơ sở dữ liệu 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

	Trong các quyền được đề cập đến ở trên, quyền REFERENCES được sử dụng nhằm cho phép tạo khóa ngoài tham chiếu đến bảng cấp phát.
<i>các_quyền_cấp_phát</i>	Danh sách các quyền cần cấp phát cho người dùng trên đối tượng cơ sở dữ liệu được chỉ định. Các quyền được phân cách nhau bởi dấu phẩy
<i>tên_bảng tên_khung_nhìn</i>	Tên của bảng hoặc khung nhìn cần cấp phát quyền.
<i>danh_sách_cột</i>	Danh sách các cột của bảng hoặc khung nhìn cần cấp phát quyền.
<i>tên_thủ_tục</i>	Tên của thủ tục được cấp phát cho người dùng.
<i>tên_hàm</i>	Tên hàm (do người dùng định nghĩa) được cấp phát quyền.
<i>danh_sách_người_dùng</i>	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.

Các ví dụ dưới đây sẽ minh họa cho ta cách sử dụng câu lệnh GRANT để cấp phát quyền cho người dùng trên các đối tượng cơ sở dữ liệu.

**Ví dụ 4.1:** 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
```

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
```

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
```

Nhưng câu lệnh dưới đây lại không thể thực hiện được

```
SELECT * FROM sinhvien
```

Trong trường hợp cần cấp phát tất cả các quyền có thể thực hiện được trên đối tượng cơ sở dữ liệu cho người dùng, thay vì liệt kê các câu lệnh, ta chỉ cần sử dụng từ khóa ALL PRIVILEGES (từ khóa PRIVILEGES có thể không cần chỉ định). Câu lệnh dưới đây cấp phát cho người dùng *thuchanh* các quyền SELECT, INSERT, UPDATE, DELETE VÀ REFERENCES trên bảng DIEMTHI

```
GRANT ALL
ON DIEMTHI
TO thuchanh
```

Khi ta cấp phát quyền nào đó cho một người dùng trên một đối tượng cơ sở dữ liệu, 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 ta cấp phát quyền cho một người dùng nào đó, 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.

**Ví dụ 4.2:** 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
```

#### 4.2.2 Cấp phát quyền thực thi các câu lệnh

Ngoài chức năng cấp phát quyền cho người sử dụng trên các đối tượng cơ sở dữ liệu, câu lệnh GRANT còn có thể sử dụng để cấp phát cho người sử dụng một số quyền trên hệ quản trị cơ sở dữ liệu hoặc cơ sở dữ liệu. Những quyền có thể cấp phát trong trường hợp này 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

Câu lệnh GRANT sử dụng trong trường hợp này có cú pháp như sau:

```
GRANT ALL | danh_sách_câu_lệnh
TO danh_sách_người_dùng
```

**Ví dụ 4.3:** 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
```

Với câu lệnh GRANT, ta có thể cho phép người sử dụng tạo các đối tượng cơ sở dữ liệu trong cơ sở dữ liệu. Đối tượng cơ sở dữ liệu 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 cơ sở dữ liệu, 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.

## 4.3 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.

### 4.3.1 Thu hồi quyền trên đối tượng cơ sở dữ liệu:

Cú pháp câu lệnh REVOKE sử dụng để thu hồi quyền đã cấp phát trên đối tượng cơ sở dữ liệu có cú pháp như sau:

```
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]
```

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 4.4:** Thu hồi quyền thực thi lệnh INSERT trên bảng LOP đối với người dùng *thuchanh*.

```
REVOKE INSERT  
ON lop  
FROM thuchanh
```

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
```

Khi ta sử dụng câu lệnh REVOKE để thu hồi quyền trên một đối tượng cơ sở dữ liệu 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 cơ sở dữ liệu cho một người dùng khác, sau đó người thứ nhất thu hồi lại quyền đã cấp phát thì những quyền mà người dùng thứ hai cấp phát vẫn có hiệu lực.

**Ví dụ 4.5:** Giả sử trong cơ sở dữ liệu ta có 3 người dùng là *A*, *B* và *C*. *A* và *B* đều có quyền sử dụng và cấp phát quyền trên bảng *R*. *A* thực hiện lệnh sau để cấp phát quyền xem dữ liệu trên bảng *R* cho *C*:

```
GRANT SELECT  
ON R TO C
```

và *B* cấp phát quyền xem và bổ sung dữ liệu trên bảng *R* cho *C* bằng câu lệnh:

```
GRANT SELECT, INSERT  
ON R TO C
```

Như vậy, *C* có quyền xem và bổ sung dữ liệu trên bảng *R*. Bây giờ, nếu *B* thực hiện lệnh:

```
REVOKE SELECT, INSERT
ON R FROM C
```

Người dùng C sẽ không còn quyền bổ sung dữ liệu trên bảng R nhưng vẫn có thể xem được dữ liệu của bảng này (quyền này do A cấp cho C và vẫn còn hiệu lực).

Nếu 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.

**Ví dụ 4.6:** Ta cấp phát cho người dùng A trên bảng R với câu lệnh GRANT như sau:

```
GRANT SELECT
ON R TO A
WITH GRANT OPTION
```

sau đó người dùng A lại cấp phát cho người dùng B quyền xem dữ liệu trên R với câu lệnh:

```
GRANT SELECT
ON R TO B
```

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

```
REVOKE SELECT
ON NHANVIEN
FROM A CASCADE
```

Câu lệnh trên sẽ đồng thời thu hồi quyền mà A đã cấp cho B và như vậy cả A và B đều không thể xem được dữ liệu trên bảng R.

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.

**Ví dụ 4.7:** Trong ví dụ trên, nếu ta thay câu lệnh:

```
REVOKE SELECT
ON NHANVIEN
FROM A CASCADE
```

bởi câu lệnh:

```
REVOKE GRANT OPTION FOR SELECT
ON NHANVIEN
FROM A CASCADE
```



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

#### 4.3.2 Thu hồi quyền thực thi các câu lệnh:

Việc thu hồi quyền thực thi các câu lệnh trên cơ sở dữ liệu (CREATE DATABASE, CREATE TABLE, CREATE VIEW,...) được thực hiện đơn giản với câu lệnh REVOKE có cú pháp:

```
REVOKE ALL | các_câu_lệnh_cần_thu_hồi  
FROM danh_sách_người_dùng
```

**Ví dụ 4.8:** 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
```