# Bài thực hành số 2

# QUYỀN và ROLE

## ❖ *Tóm tắt nội dung:*

- Quyền (privilege)
- Role
- Data Dictionary

# I. Quyền và Role

## A. Lý thuyết

### 1. Quyền (privilege)

- Một quyền là 1 sự cho phép thực hiện 1 câu lệnh SQL nào đó hoặc được phép truy xuất đến một đối tượng nào đó (vd: quyền tạo bảng CREATE TABLE, quyền connect đến cơ sở dữ liệu CREATE SESSION, quyền SELECT trên một bảng cụ thể nào đó,…).
- Chỉ cấp cho user chính xác những quyền mà user cần đến. Việc cấp dư thừa những quyền không cần thiết có thể gây nguy hại cho việc bảo mật hệ thống.
- Có 2 loại quyền:
  - ✓ Quyền hệ thống (System Privilege):
    - Là quyền thực hiện một tác vụ CSDL cụ thể hoặc quyền thực hiện một loại hành động trên tất cả những đối tượng schema của hệ thống. Vd: quyền ALTER SYSTEM, quyền CREATE TABLE, quyền DELETE ANY TABLE (xóa các hàng của bất kỳ bảng nào trong CSDL),…
    - User có thể cấp 1 quyền hệ thống nếu có một trong các điều kiện sau:
      - User đã được cấp quyền hệ thống đó với tùy chọn WITH ADMIN OPTION.
      - User có quyền GRANT ANY PRIVILEGE.
  - ✓ Quyền đối tượng (Schema Object Privilege hoặc Object Privilege):
    - Là quyền thực hiện một hành động cụ thể trên một đối tượng schema cụ thể.

Vd: quyền xóa các hàng dữ liệu khỏi bảng Department.

- Có nhiều quyền đối tượng khác nhau dành cho các loại đối tượng schema khác nhau.
- Dùng để quản lý việc truy xuất đến các đối tượng schema cụ thể nào đó.
- User có thể cấp 1 quyền đối tượng nếu có một trong các điều kiện sau:
  - User có tất cả mọi quyền đối tượng trên tất cả các đối tượng thuộc schema của mình. Vì vậy user có quyền cấp bất kỳ quyền đối tượng trên bất kỳ đối tượng nào thuộc sở hữu của mình cho bất cứ user nào khác.
  - User có quyền GRANT ANY OBJECT PRIVILEGE.
  - User được cấp quyền đối tượng đó với tùy chọn WITH GRANT OPTION.

### 2. Role

- Role là một tập hợp bao gồm các quyền và các role khác.
- Role được gán cho các user hoặc các role khác.
- Role giúp cho việc quản trị người dùng dễ dàng và tiết kiệm công sức hơn.
- Có một số role có sẵn do hệ thống định nghĩa (vd: DBA, RESOURCE, CONNECT,…) nhưng đa phần các role là do người quản trị CSDL tạo ra.
- Role không phải là một đối tượng schema (schema object) nên không được lưu trữ trong schema của user tạo ra nó. Do vậy, user tạo ra một role có thể bị xóa mà không ảnh hưởng đến role đó.
- User có thể cấp 1 role nếu có một trong các điều kiện sau:
  - ✓ User đã tạo ra role đó.
  - ✓ User đã được cấp role đó với tùy chọn WITH ADMIN OPTION.
  - ✓ Có quyền GRANT ANY ROLE.

## B. Thực hành

### 1. Tạo ROLE

- Tạo một role mới với câu lệnh:

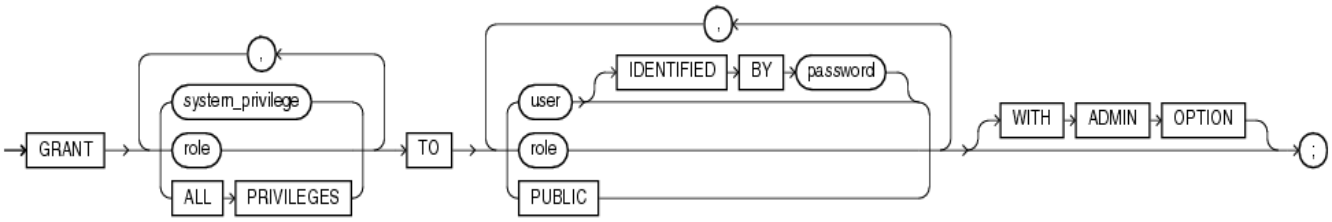
```
CREATE ROLE myrole;
Role created.
```

- Lưu ý, để tạo được role, phải có quyền hệ thống CREATE ROLE.

## 2. Lệnh GRANT

a. Gán quyền hệ thống/role:

- Ta dùng cú pháp dưới đây để gán các quyền hệ thống/role cho các user/role khác:




Ví dụ:

```
GRANT DELETE ANY TABLE TO salapati;
Grant succeeded.
GRANT CREATE USER TO myrole;
Grant succeeded.
GRANT myrole TO salapati;
Grant succeeded.
GRANT myrole TO lavender;
Grant succeeded.
```

- Xem lệnh sau:

```
GRANT CREATE SESSION TO lavender IDENTIFIED BY purple;
Grant succeeded.
```

Với câu lệnh vừa rồi, nếu user `lavender` đã tồn tại, password của `lavender` sẽ được thay đổi thành `purple`. Ngược lại, hệ thống sẽ tạo ra 1 người dùng mới có username là `lavender` và password là `purple`. Sinh viên tự tìm hiểu xem để câu lệnh trên có thể thực hiện được, user cần phải có quyền gì?

- Dùng từ khóa PUBLIC nếu muốn cấp quyền/role cho mọi user:

```
GRANT CREATE SESSION TO PUBLIC;
```

- Dùng từ khóa ALL PRIVILEGES nếu muốn cấp tất cả các quyền hệ thống (trừ quyền SELECT ANY DICTIONARY):

```
GRANT ALL PRIVILEGES TO salapati;
```

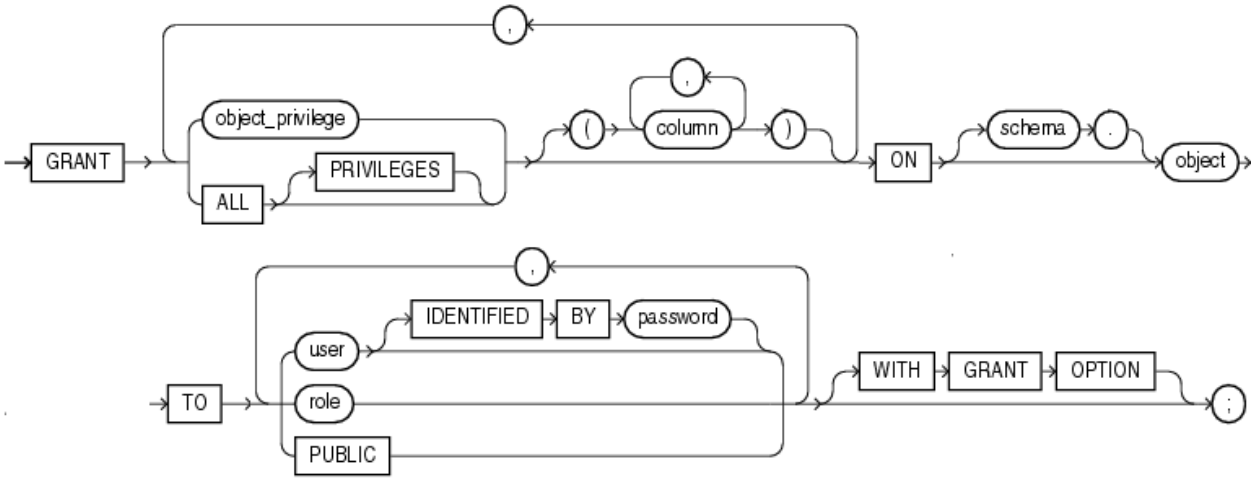
Để thực hiện câu lệnh trên thành công thì user cần phải có quyền gì?

- Tùy chọn WITH ADMIN OPTION sẽ cho phép người được cấp role/quyền:
  - ✓ Cấp lại role/quyền đó cho một user hoặc role khác (có hoặc không có tùy chọn WITH ADMIN OPTION).
  - ✓ Thu hồi lại role/quyền đó từ một user hoặc role bất kỳ.
  - ✓ Thay đổi role đó bằng lệnh ALTER ROLE.
  - ✓ Xóa role đó.

  Ví dụ:

```
GRANT CREATE SESSION TO salapati WITH ADMIN OPTION;
Grant succeeded.
```

b. Gán quyền đối tượng:




Ví dụ:

```
GRANT DELETE ON mytable TO salapati;
GRANT SELECT ON mytable TO public;
GRANT SELECT,INSERT,UPDATE,DELETE ON mytable TO lavender;
GRANT SELECT ON salapati.xyz TO myrole;
```

- Dùng từ khóa ALL [PRIVILEGES] khi muốn cấp tất cả các quyền đối tượng mà user có trên 1 đối tượng nào đó (với điều kiện user phải có quyền cấp những quyền đó):

```
GRANT ALL ON salapati.xyz TO paris;
GRANT ALL PRIVILEGES ON salapati.xyz TO paris;
```

- Nếu chỉ muốn cấp quyền trên vài cột nào đó của table hoặc view, ta chỉ ra cụ thể tên các cột đó:

```
GRANT UPDATE (name) ON salapati.xyz TO myrole;
Grant succeeded.
```

Lưu ý là ta chỉ có thể chỉ ra các cột cụ thể khi cấp quyền INSERT và UPDATE.

- Dùng tùy chọn WITH GRANT OPTION khi muốn user được cấp quyền có thể cấp quyền đó cho user/role khác. Tuy nhiên chỉ được dùng tùy chọn này khi cấp quyền cho một user hay PUBLIC:

```
GRANT ALL ON salapati.xyz TO paris WITH GRANT OPTION;
```

c. Xem thông tin các quyền hệ thống đã được gán cho user hiện tại:

```
SELECT * FROM user_sys_privs;
```

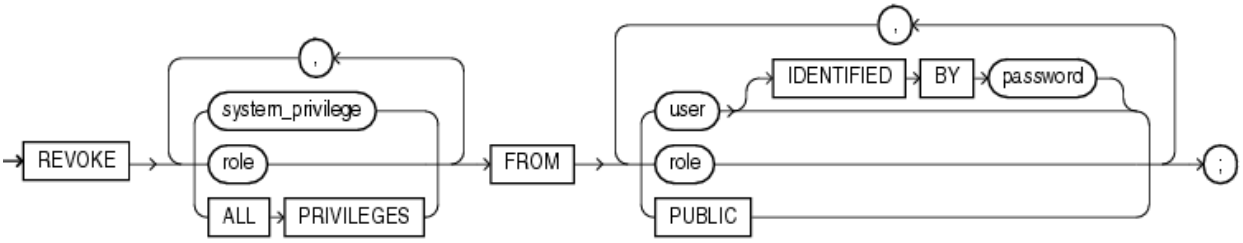
Xem thông tin các quyền đối tượng đã được gán cho user hiện tại:

```
SELECT * FROM user_tab_privs_recd;
```

d. Sinh viên tham khảo danh sách các quyền hệ thống, quyền đối tượng trong phần mô tả lệnh GRANT của cuốn SQL Reference thuộc Oracle Document Library.

## 3. Lệnh REVOKE

a. Thu hồi quyền hệ thống/role:




- Để thu hồi quyền hệ thống, user phải được cấp quyền đó với WITH ADMIN OPTION hoặc có quyền GRANT ANY PRIVILEGES.
- Để thu hồi role, user phải được cấp role đó với WITH ADMIN OPTION hoặc có quyền GRANT ANY ROLE.
- Không thể dùng lệnh REVOKE để thu hồi những role/quyền hệ thống được cấp thông qua những role khác.

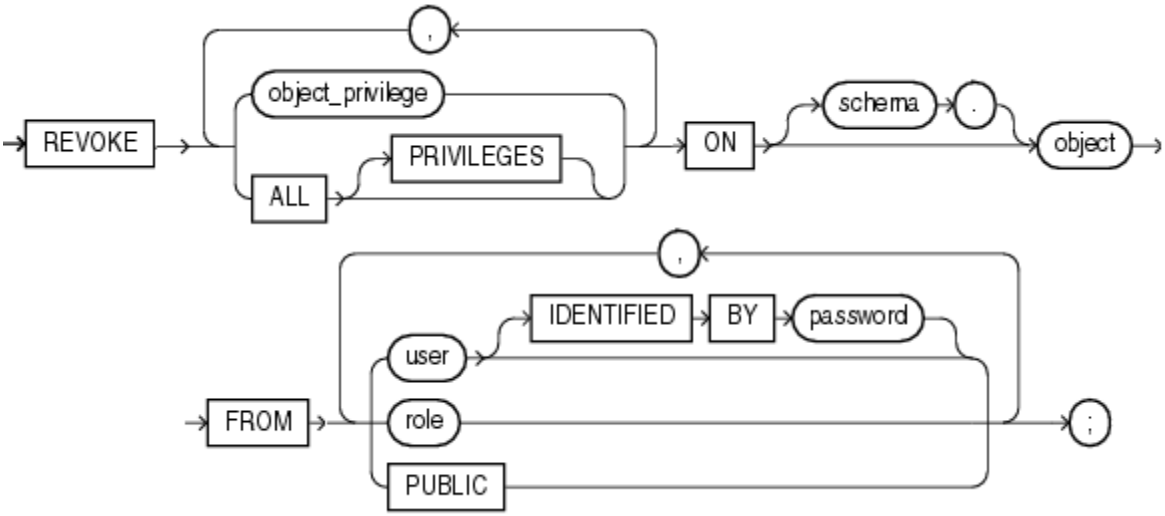
```
REVOKE DELETE ANY TABLE FROM salapati;
Revoke succeeded.
REVOKE myrole FROM lavender;
Revoke succeeded.
```

- Dùng từ khóa PUBLIC để thu hồi 1 quyền hệ thống/role đã được cấp cho tất cả các user thông qua PUBLIC. Tuy nhiên không thể dùng PUBLIC để thu hồi những quyền được gán trực tiếp hoặc thông qua 1 role khác.

```
REVOKE CREATE SESSION FROM PUBLIC;
```

- Các từ khóa khác có ý nghĩa như trong lệnh GRANT.

b. Thu hồi quyền đối tượng:




- Để thu hồi 1 quyền đối tượng từ 1 user/role, bạn phải là người đã cấp quyền đó cho user/role đó hoặc bạn có quyền GRANT ANY OBJECT PRIVILEGE. Tuy nhiên, đối với trường hợp bạn có quyền GRANT ANY OBJECT PRIVILEGE, bạn chỉ có thể thu hồi những quyền đối tượng được cấp cho user/role, nếu quyền đối tượng đó đã được cấp cho user/role bởi chủ nhân của chính đối tượng hoặc bởi những user có quyền GRANT ANY OBJECT PRIVILEGE.
- Không thể dùng lệnh REVOKE để thu hồi quyền/role đã được cấp thông qua các role khác.

```
REVOKE SELECT ON mytable FROM salapati;
```

- Dùng từ khóa ALL [PRIVILEGES] để thu hồi tất cả những quyền đối tượng mà bạn đã cấp cho user/role đó.

```
REVOKE ALL ON salapati.xyz FROM paris;
```

- Dùng từ khóa PUBLIC để thu hồi 1 quyền đối tượng khỏi những user đã được cấp quyền đó thông qua việc gán cho PUBLIC. Không thể dùng PUBLIC để thu hồi những quyền được gán trực tiếp hoặc thông qua 1 role khác.

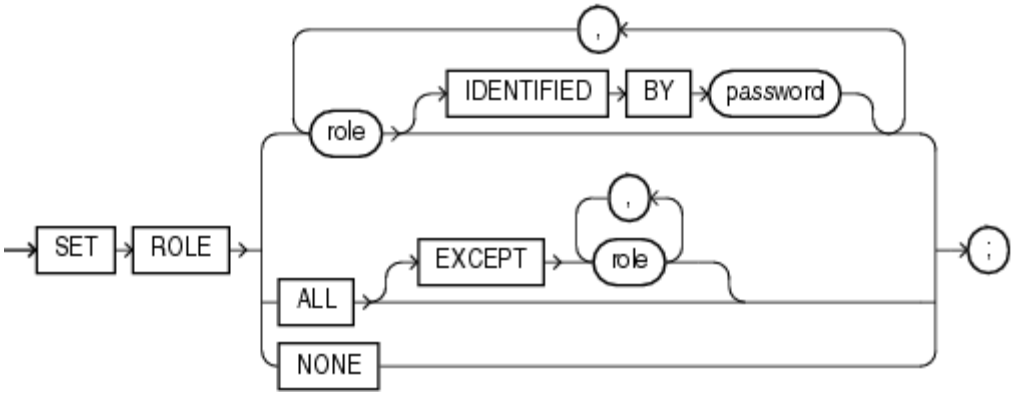
```
REVOKE INSERT ON salapati.xyz FROM paris;
```

- Lưu ý:
  - ✓ Nếu user bị thu hồi quyền đối tượng mà quyền này đã được cấp cho user/role khác, hệ thống cũng thu hồi quyền đối tượng đó của những user/role kia.
  - ✓ Nếu schema của user bị thu hồi quyền đối tượng có chứa các procedure, function, package có sử dụng lệnh SQL liên quan đến quyền bị thu hồi thì những procedure, function, package đó không còn có thể thực thi được.

## 4. Enable và disable một ROLE

a. Một user có thể có nhiều role. Tuy nhiên không phải session nào cũng cần sử dụng tất cả các role đó. Oracle cho phép bản thân user enable/disable các role mà mình được cấp để quản lý sự cần thiết của các role trong session hiện tại.

- Mặc định khi bắt đầu 1 session mới, user sẽ được hệ thống enable tất cả các role mặc định (default role). Sau đó user có thể dùng lệnh SET ROLE để enable/disable các role theo ý mình theo cú pháp sau:




Ví dụ:

```
SET ROLE myrole, sysrole;
```

Lệnh trên sẽ enable 2 role được chỉ định và disable tất cả các role còn lại của user.

- Để enable tất cả các role dùng lệnh:

```
SET ROLE ALL;
```

- Để disable tất cả các role dùng lệnh:

```
SET ROLE NONE;
```

- Để enable tất cả các role ngoại trừ role lavender ta dùng lệnh:

```
SET ROLE ALL EXCEPT sysrole;
```

b. Để bảo vệ một role với mục đích không cho phép các user tùy ý enable/disable một role, người tạo role có thể thiết lập password cho role đó ngay khi tạo role:

```
CREATE ROLE newrole IDENTIFIED BY protected;
```

- Ta cũng có thể thay đổi việc thiết lập password cho role:

```
ALTER ROLE newrole IDENTIFIED BY changed;
ALTER ROLE newrole NOT IDENTIFIED;
```

c. Để biết hiện tại role nào đang được enable ta truy xuất view SESSION_ROLES:

```
SELECT * FROM SESSION_ROLES;
```

d. Để quy định những role nào là role mặc định ta dùng lệnh ALTER USER:

```
ALTER USER salapati DEFAULT ROLE myrole, sysrole;
ALTER USER salapati DEFAULT ROLE ALL;
ALTER USER salapati DEFAULT ROLE ALL EXCEPT myrole;
ALTER USER salapati DEFAULT ROLE NONE;
```

### 5. Xóa ROLE

```
DROP ROLE myrole;
```

# II. Từ điển dữ liệu (Data Dictionary)

## A. Lý thuyết

### 1. Tổng quan

- Mọi CSDL Oracle đều có một Từ điển dữ liệu. Từ điển dữ liệu được tạo ra khi

CSDL được tạo.

- Từ điển dữ liệu trong Oracle là một tập các bảng và view được sử dụng như một tham khảo dạng *chỉ đọc* (read-only) về bản thân CSDL đó.
- Từ điển dữ liệu nằm trên tablespace SYSTEM, thuộc schema của user SYS, bao gồm 2 loại:
  - ✓ Các bảng cơ bản (Base table):
    Là các bảng lưu trữ thông tin của từ điển dữ liệu. Dữ liệu được lưu trong các bảng này dưới dạng mã hóa.
  - ✓ Các view dành cho người dùng truy xuất (User-accessible View):
    Tổng hợp và hiển thị thông tin được lưu trong các bảng cơ bản ở dạng người bình thường có thể đọc hiểu. Tùy vào quyền của mỗi user mà user đó có thể truy xuất view nào và truy xuất những dữ liệu nào của view đó.
- Một Từ điển dữ liệu sẽ lưu trữ tất cả các thông tin về cấu trúc luận lý và cấu trúc vật lý của CSDL:
  - ✓ Định nghĩa của tất cả các đối tượng schema trong CSDL.
  - ✓ Các quy định, giới hạn về sử dụng tài nguyên của các user,v.v
  - ✓ Danh sách các user. Các quyền, role được cấp cho các user.
  - ✓ Các ràng buộc toàn vẹn của dữ liệu
  - ✓ Thông tin audit
  - ✓ Các thông tin CSDL tổng quát khác.
- Oracle tự động cập nhật từ điển dữ liệu để phản ánh chính xác trạng thái thực tế của CSDL.

**2. Các tiếp đầu ngữ trong tên view**

- Trong nhiều trường hợp, một tập gồm 3 view chứa những thông tin tương tự như nhau và tên của chúng chỉ khác nhau ở các tiếp đầu ngữ: user, all, dba.
  - ✓ USER: hiển thị những gì thuộc schema của user đó.
  - ✓ ALL: hiển thị những gì mà user đó có thể truy xuất.
  - ✓ DBA: hiển thị tất cả thông tin thuộc schema của mọi user (view dành cho những người quản trị).
- Các column trong các view thuộc 1 bộ ba view hầu như là giống nhau, ngoại trừ một số ngoại lệ.

### 3. Các view thường sử dụng

- DBA_USERS: cung cấp thông tin của các user trong CSDL.
- DBA_TS_QUOTAS: cung cấp thông tin tablespace quota của các user.
- DBA_PROFILES: cung cấp thông tin về các profile.
- DBA_ROLES: cung cấp thông tin về các role.
- DBA_SYS_PRIVS: hiển thị thông tin về việc cấp quyền hệ thống cho các user.
- DBA_TAB_PRIVS: hiển thị thông tin về việc cấp quyền đối tượng cho các user.
- DBA_COL_PRIVS: hiển thị thông tin về việc cấp quyền đối tượng mức cột cho các user.
- DBA_ROLE_PRIVS: hiển thị tất cả các user và role của họ.
- ROLE_ROLE_PRIVS: hiển thị thông tin về việc cấp role cho các role.
- ROLE_SYS_PRIVS: hiển thị thông tin về việc cấp quyền hệ thống cho các role.
- ROLE_TAB_PRIVS: hiển thị thông tin về việc cấp quyền đối tượng cho các role.
- SESSION_ROLES: hiển thị các role hiện tại đang được enable cho user.
- SESSION_PRIVS: hiển thị các quyền hiện tại mà user có thể sử dụng.

## B. Thực hành

- Sinh viên dùng cuốn Reference trên Oracle Documentation Library để tra cứu danh sách các view của Từ điển dữ liệu.
- Truy xuất các view trên để xem các dữ liệu được hiển thị.

# III. Bài Tập

1. Tạo các users John, Joe, Fred, Lynn, Amy, and Beth:
   a. Password là tên username.
   b. Đảm bảo các user này có thể tạo bất kỳ bảng nào trong tablespace với quota 10M.

2. Cho bảng Attendance

```
(
    ID INT PRIMARY KEY,
    Name NVARCHAR2
)
```

Làm các bước sau:

a. Tạo các role sau: DataEntry, Supervisor, và Management.
b. Gán John, Joe, và Lynn vào role DataEntry, gán Fred vào role Supervisor, và gán Amy và Beth vào role Management.
c. Cho role DataEntry các quyền SELECT, INSERT, và UPDATE trên bảng Attendance.
d. Cho role Supervisor các quyền SELECT và DELETE trên bảng Attendance.
e. Cho role Management quyền SELECT trên bảng Attendance.
f. Lần lượt kiểm tra kết quả phân quyền đã cấp cho các role

3. Tạo một user mới tên NameManager với password là pc123. Gán quyền update cho user này trên cột Name của bảng Attendance.

4. Thực hiện các yêu cầu sau đối với các view được liệt kê ở phần II (Từ điển dữ liệu):
   a. Tìm quyền mà trong tên của quyền có chữ CONTEXT
   b. Liệt kê tất cả user có quyền SELECT ANY TABLE

5. Thực hiện các bước sau:
   a. Gán password cho role DataEntry ở bài 1 là "mgt"
   b. Cho phép user John quyền cấp quyền cho các user khác
   c. Gán tất cả các quyền mà John có cho Beth. Beth có quyền INSERT và UPDATE trên bảng Attendance không?
6. Cho đoạn code sau:

```
CONN giaovien/p123;
CREATE ROLE sinhvien;
GRANT select ON Attendance TO sinhvien WITH GRANT OPTION;
```

Đoạn code trên sẽ báo lỗi ở đâu và trong trường hợp nào?