

## Objective

By the end of this lab, students will be able to:

- Create roles (users)
- Assign permissions
- Use **GRANT** and **REVOKE**
- Understand role-based access control

---

## Scenario

You are managing a **University Database System** with:

- Admin
- Teacher
- Students

---

### ◇ Step 1: Create Database

```
CREATE DATABASE university_lab;
```

Connect to it:

```
\c university_lab
```

---

### ◇ Step 2: Create Sample Table

```
CREATE TABLE students (  
    id SERIAL PRIMARY KEY,  
    name VARCHAR(50),  
    course VARCHAR(50)  
);
```

Insert sample data:

```
INSERT INTO students (name, course)  
VALUES
```

```
('Ali', 'CS'),  
( 'Sara', 'IT'),  
( 'Ahmed', 'SE');
```

---

## ◇ Step 3: Create Roles

---

### Admin Role

```
CREATE ROLE admin_user WITH LOGIN PASSWORD 'admin123' SUPERUSER;
```

### Teacher Role

```
CREATE ROLE teacher WITH LOGIN PASSWORD 'teacher123';
```

### Student Role

```
CREATE ROLE student WITH LOGIN PASSWORD 'student123';
```

---

## ◇ Step 4: Grant Permissions

---

### Teacher Permissions (Read + Insert)

```
GRANT SELECT, INSERT ON students TO teacher;
```

### Student Permissions (Read Only)

```
GRANT SELECT ON students TO student;
```

---

## ◇ Step 5: Test Roles

---

Switch role:

```
SET ROLE teacher;
```

Try:

```
SELECT * FROM students;  
INSERT INTO students (name, course) VALUES ('Zain', 'AI');
```

Now test student:

```
SET ROLE student;
```

Try:

```
SELECT * FROM students;  
INSERT INTO students (name, course) VALUES ('Test', 'CS'); -- Should FAIL
```

---

## ◇ Step 6: Revoke Permission

---

```
REVOKE INSERT ON students FROM teacher;
```

---

## Lab Tasks

---

Task 1:

Create a new role:

```
librarian
```

- Can only **SELECT** data

---

Task 2:

Create a new table:

```
books (id, title, author)
```

Give:

- Teacher → SELECT, INSERT
- Student → SELECT only

---

Task 3:

Test access using **SET ROLE**

---

Task 4:

Revoke SELECT from student and test again

---

## Challenge

- Create a **group role**:

```
staff_group
```

- Assign teacher to it
- Grant permissions to group instead of individual users