

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN
THÔNG**



BÁO CÁO TUẦN 5

**ĐỀ TÀI
XÂY DỰNG WEBSITE BÃI ĐỖ XE THÔNG
MINH**

Giảng viên hướng dẫn :	Kim Ngọc Bách
Sinh viên thực hiện:	Trần Xuân Kiên
Mã sinh viên :	B22DCVT269
Lớp :	E22CQCN02-B

Giai đoạn 1 (tiếp tục): Phân quyền

1. Vai trò và quyền hạn

a. Admin (Quản trị viên)

- Mô tả: Có toàn quyền trên hệ thống
- Quyền hạn:
 - Quản lý người dùng (xem, thêm, sửa, xóa, thay đổi vai trò, khóa/mở tài khoản)
 - Quản lý khu vực đỗ xe (xem, thêm, sửa, xóa, thay đổi trạng thái)
 - Quản lý vị trí đỗ xe (xem, thêm, sửa, xóa, thay đổi trạng thái)
 - Quản lý biểu giá (xem, thêm, sửa, xóa, cập nhật)
 - Quản lý thành viên và ưu đãi (xem, thêm, sửa, xóa)
 - Xem và xuất báo cáo thống kê
 - Xem nhật ký hệ thống
 - Quản lý cấu hình hệ thống
 - Phân quyền cho người dùng khác

b. Operator (Nhân viên vận hành)

- Mô tả: Vận hành bãi đỗ xe hàng ngày
- Quyền hạn:
 - Xem thông tin khu vực và vị trí đỗ xe
 - Cập nhật trạng thái vị trí đỗ xe (available, occupied, disabled)
 - Quản lý vé đỗ xe (tạo, cập nhật, hủy)
 - Quản lý đăng ký đỗ xe (xem, xác nhận, hủy)
 - Xử lý thanh toán (thu tiền, xác nhận)
 - Xem báo cáo hàng ngày
 - Hỗ trợ khách hàng

c. Customer (Khách hàng)

- Mô tả: Người sử dụng dịch vụ đỗ xe

- Quyền hạn:
 - Quản lý thông tin cá nhân
 - Quản lý phương tiện của mình (thêm, sửa, xóa)
 - Đặt chỗ đỗ xe (tạo, hủy đơn đặt)
 - Xem lịch sử đỗ xe và thanh toán
 - Xem thông tin thẻ thành viên và ưu đãi
 - Thanh toán phí đỗ xe
 - Xem tình trạng bãi đỗ (khu vực còn trống)

2. Ma trận quyền truy cập theo bảng dữ liệu

Bảng dữ liệu	Admin	Operator	Customer
parking_areas	CRUD	R	R
parking_slots	CRUD	RU	R
users	CRUD	R	RU*
vehicles	CRUD	R	CRUD*
parking_reservation	CRUD	CRUD	CRUD*
parking_tickets	CRUD	CRUD	R*
payments	CRUD	CRU	R*
pricing	CRUD	R	R
system_logs	R	-	-
memberships	CRUD	R	R*
reports	CRUD	R	-

*Chú thích:

R: Read (Đọc)

C: Create (Tạo)

U: Update (Cập nhật)

D: Delete (Xóa)

*: Chỉ áp dụng cho dữ liệu của chính người dùng

3. Triển khai phân quyền trong cơ sở dữ liệu

```
-- Bảng quyền hạn
CREATE TABLE permissions (
    permission_id INT AUTO_INCREMENT PRIMARY KEY,
    permission_name VARCHAR(100) NOT NULL UNIQUE,
    description TEXT,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

-- Bảng liên kết vai trò và quyền
CREATE TABLE role_permissions (
    id INT AUTO_INCREMENT PRIMARY KEY,
    role ENUM('admin', 'operator', 'customer') NOT NULL,
    permission_id INT NOT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    FOREIGN KEY (permission_id) REFERENCES permissions(permission_id) ON DELETE CASCADE,
    UNIQUE KEY (role, permission_id)
);

INSERT INTO permissions (permission_name, description) VALUES
-- Quản lý khu vực đỗ xe
('view_parking_areas', 'Xem thông tin khu vực đỗ xe'),
('create_parking_areas', 'Tạo khu vực đỗ xe mới'),
('update_parking_areas', 'Cập nhật thông tin khu vực đỗ xe'),
('delete_parking_areas', 'Xóa khu vực đỗ xe'),

-- Quản lý vị trí đỗ xe
('view_parking_slots', 'Xem thông tin vị trí đỗ xe'),
('create_parking_slots', 'Tạo vị trí đỗ xe mới'),
('update_parking_slots', 'Cập nhật thông tin vị trí đỗ xe'),
('delete_parking_slots', 'Xóa vị trí đỗ xe'),

-- Quản lý người dùng
('view_all_users', 'Xem thông tin tất cả người dùng'),
('create_users', 'Tạo người dùng mới'),
('update_users', 'Cập nhật thông tin người dùng'),
('delete_users', 'Xóa người dùng'),
('update_own_profile', 'Cập nhật thông tin cá nhân'),
```

```
-- Quản lý phương tiện
('view_all_vehicles', 'Xem thông tin tất cả phương tiện'),
('view_own_vehicles', 'Xem thông tin phương tiện của chính mình'),
('create_own_vehicles', 'Đăng ký phương tiện mới'),
('update_own_vehicles', 'Cập nhật thông tin phương tiện'),
('delete_own_vehicles', 'Xóa phương tiện'),

-- Quản lý đăng ký đỗ xe
('view_all_reservations', 'Xem tất cả các đơn đăng ký'),
('view_own_reservations', 'Xem đơn đăng ký của chính mình'),
('create_reservations', 'Tạo đơn đăng ký mới'),
('update_reservations', 'Cập nhật đơn đăng ký'),
('cancel_reservations', 'Hủy đơn đăng ký'),

-- Quản lý vé đỗ xe
('view_all_tickets', 'Xem tất cả vé đỗ xe'),
('view_own_tickets', 'Xem vé đỗ xe của chính mình'),
('create_tickets', 'Tạo vé đỗ xe mới'),
('update_tickets', 'Cập nhật vé đỗ xe'),
('cancel_tickets', 'Hủy vé đỗ xe'),
```

```

-- Quản lý thanh toán
('view_all_payments', 'Xem tất cả thanh toán'),
('view_own_payments', 'Xem thanh toán của chính mình'),
('create_payments', 'Tạo thanh toán mới'),
('update_payment_status', 'Cập nhật trạng thái thanh toán'),

-- Quản lý định giá
('view_pricing', 'Xem biểu giá'),
('create_pricing', 'Tạo biểu giá mới'),
('update_pricing', 'Cập nhật biểu giá'),
('delete_pricing', 'Xóa biểu giá'),

-- Quản lý báo cáo
('view_reports', 'Xem báo cáo'),
('create_reports', 'Tạo báo cáo mới'),
('export_reports', 'Xuất báo cáo'),

-- Quản lý nhật ký hệ thống
('view_system_logs', 'Xem nhật ký hệ thống'),

-- Quản lý thành viên
('view_all_memberships', 'Xem tất cả thành viên'),
('view_own_membership', 'Xem thông tin thành viên của mình'),
('create_memberships', 'Tạo thẻ thành viên mới'),
('update_memberships', 'Cập nhật thẻ thành viên'),
('delete_memberships', 'Xóa thẻ thành viên');

```

- Phân quyền:

```

-- Phân quyền cho Admin
▶ INSERT INTO role_permissions (role, permission_id)
  SELECT 'admin', permission_id FROM permissions;

-- Phân quyền cho Operator
▶ INSERT INTO role_permissions (role, permission_id)
  SELECT 'operator', permission_id FROM permissions WHERE permission_name IN (
    'view_parking_areas', 'view_parking_slots', 'update_parking_slots',
    'view_all_users', 'view_all_vehicles',
    'view_all_reservations', 'create_reservations', 'update_reservations', 'cancel_reservations',
    'view_all_tickets', 'create_tickets', 'update_tickets', 'cancel_tickets',
    'view_all_payments', 'create_payments', 'update_payment_status',
    'view_pricing', 'view_reports', 'view_all_memberships',
    'update_own_profile'
  );

-- Phân quyền cho Customer
▶ INSERT INTO role_permissions (role, permission_id)
  SELECT 'customer', permission_id FROM permissions WHERE permission_name IN (
    'view_parking_areas', 'view_parking_slots',
    'update_own_profile',
    'view_own_vehicles', 'create_own_vehicles', 'update_own_vehicles', 'delete_own_vehicles',
    'view_own_reservations', 'create_reservations', 'cancel_reservations',
    'view_own_tickets',
    'view_own_payments', 'create_payments',
    'view_pricing', 'view_own_membership'
  );

```

4. Hàm kiểm tra quyền hạn

```
-- Hàm kiểm tra quyền hạn
DELIMITER //
CREATE FUNCTION check_permission(p_user_id INT, p_permission_name VARCHAR(100))
RETURNS BOOLEAN
DETERMINISTIC
BEGIN
    DECLARE v_has_permission BOOLEAN;

    SELECT EXISTS (
        SELECT 1 FROM users u
        JOIN role_permissions rp ON u.role = rp.role
        JOIN permissions p ON rp.permission_id = p.permission_id
        WHERE u.user_id = p_user_id AND p.permission_name = p_permission_name
    ) INTO v_has_permission;

    RETURN v_has_permission;
END//
DELIMITER ;
```

5. Stored Procedure để cấp/thu hồi quyền

- Cấp quyền


```

-- Procedure cấp quyền cho vai trò
DELIMITER //

CREATE PROCEDURE grant_permission_to_role(
    IN p_role ENUM('admin', 'operator', 'customer'),
    IN p_permission_name VARCHAR(100)
)
BEGIN
    DECLARE v_permission_id INT;

    -- Lấy ID của quyền
    SELECT permission_id INTO v_permission_id
    FROM permissions
    WHERE permission_name = p_permission_name;

    -- Nếu quyền tồn tại và chưa được cấp cho vai trò
    IF v_permission_id IS NOT NULL AND NOT EXISTS (
        SELECT 1 FROM role_permissions
        WHERE role = p_role AND permission_id = v_permission_id
    ) THEN
        -- Cấp quyền
        INSERT INTO role_permissions (role, permission_id)
        VALUES (p_role, v_permission_id);

        SELECT CONCAT('Đã cấp quyền ', p_permission_name, ' cho vai trò ', p_role) AS result;
    ELSE
        SELECT 'Quyền không tồn tại hoặc đã được cấp' AS result;
    END IF;
END//
DELIMITER ;

```

- Thu hồi quyền:

```

51
52 -- Procedure thu hồi quyền từ vai trò
53 DELIMITER //
54 ● ○ CREATE PROCEDURE revoke_permission_from_role(
55     IN p_role ENUM('admin', 'operator', 'customer'),
56     IN p_permission_name VARCHAR(100)
57 )
58 ○ BEGIN
59     DECLARE v_permission_id INT;
60
61     -- Lấy ID của quyền
62     SELECT permission_id INTO v_permission_id
63     FROM permissions
64     WHERE permission_name = p_permission_name;
65
66     -- Nếu quyền tồn tại và đã được cấp cho vai trò
67     ○ IF v_permission_id IS NOT NULL AND EXISTS (
68         SELECT 1 FROM role_permissions
69         WHERE role = p_role AND permission_id = v_permission_id
70     ) THEN
71         -- Thu hồi quyền
72         DELETE FROM role_permissions
73         WHERE role = p_role AND permission_id = v_permission_id;
74
75         SELECT CONCAT('Đã thu hồi quyền ', p_permission_name, ' từ vai trò ', p_role) AS result;
76     ELSE
77         SELECT 'Quyền không tồn tại hoặc chưa được cấp' AS result;
78     END IF;
79 END//
80 DELIMITER ;

```

6. Trigger để ghi log hoạt động phân quyền

- Trigger ghi log khi cấp quyền:

```

-- Trigger ghi log khi cấp quyền
DELIMITER //
CREATE TRIGGER log_permission_grant
AFTER INSERT ON role_permissions
FOR EACH ROW
BEGIN
    DECLARE v_permission_name VARCHAR(100);

    -- Lấy tên quyền
    SELECT permission_name INTO v_permission_name
    FROM permissions
    WHERE permission_id = NEW.permission_id;

    -- Ghi log
    INSERT INTO system_logs (user_id, action_type, description)
    VALUES (NULL, 'PERMISSION_GRANT', CONCAT('Cấp quyền ', v_permission_name, ' cho vai trò ', NEW.role));
END//
DELIMITER ;

```

- Trigger ghi log khi thu hồi quyền:

```

-- Trigger ghi log khi thu hồi quyền
DELIMITER //
CREATE TRIGGER log_permission_revoke
BEFORE DELETE ON role_permissions
FOR EACH ROW
BEGIN
    DECLARE v_permission_name VARCHAR(100);

    -- Lấy tên quyền
    SELECT permission_name INTO v_permission_name
    FROM permissions
    WHERE permission_id = OLD.permission_id;

    -- Ghi log
    INSERT INTO system_logs (user_id, action_type, description)
    VALUES (NULL, 'PERMISSION_REVOKE', CONCAT('Thu hồi quyền ', v_permission_name, ' từ vai trò ', OLD.role));
END//
DELIMITER ;

```