### ****Chương 2: Các loại hình tấn công SQL Injection (10-12 trang)****

### ****Chương 3: Các kịch bản tấn công (15-20 trang)****

Mỗi phần dưới đây có thể trình bày theo format:

* Mục tiêu tấn công
* Mã nguồn ban đầu (vulnerable)
* Payload sử dụng
* Mã độc hoạt động như thế nào
* Kết quả
* Ghi chú/phân tích

#### 3.1. Vượt qua đăng nhập (Bypass Login)

* ' OR '1'='1 --
* ' OR 1=1 LIMIT 1--+

#### 3.2. Thêm dữ liệu trái phép

* INSERT INTO... thông qua lỗi xử lý form

#### 3.3. Sửa dữ liệu

* UPDATE users SET role='admin' WHERE id='1' AND '1'='1

#### 3.4. Xóa dữ liệu

* '; DELETE FROM users --

#### 3.5. Trích xuất dữ liệu nhạy cảm

* Dùng UNION SELECT
* Dùng information\_schema để dò bảng/cột

### ****Chương 4: Demo thực hành (10-15 trang)****

4.1. Môi trường demo (XAMPP/WAMP + MySQL + PHP)  
4.2. Thiết lập ứng dụng mẫu dễ bị tấn công  
4.3. Hướng dẫn chạy thử từng payload  
4.4. Screenshot kết quả  
4.5. Phân tích chi tiết mỗi case

### ****Chương 5: Biện pháp phòng chống SQL Injection (5-6 trang)****

5.1. Sử dụng Prepared Statement (PDO/MySQLi)  
5.2. Validation & Sanitization dữ liệu đầu vào  
5.3. Cấu hình đúng quyền truy cập DB  
5.4. Sử dụng Web Application Firewall (WAF)  
5.5. Các công cụ hỗ trợ scan & fix lỗ hổng (SQLmap, Acunetix…)