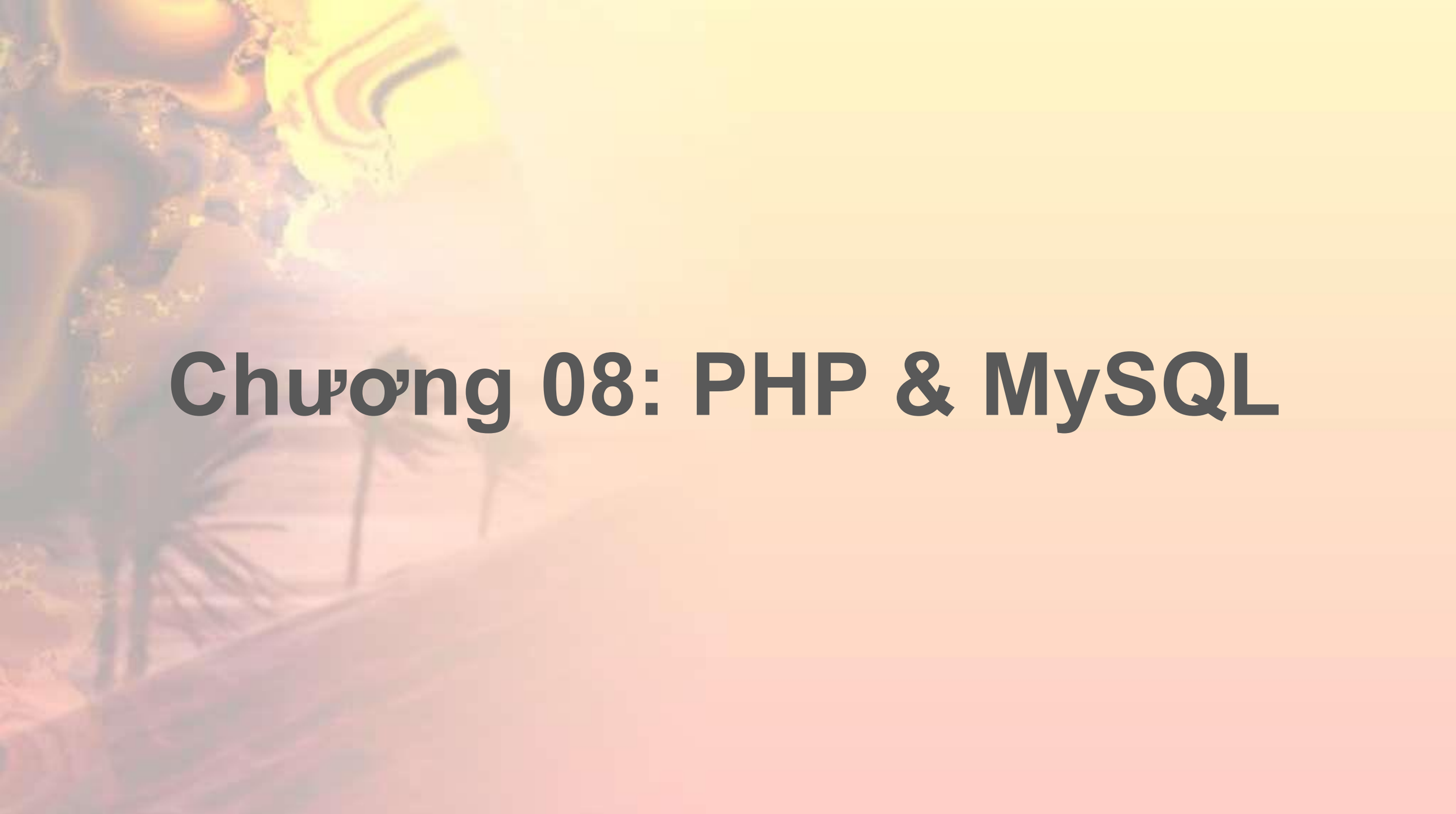

Chương 08: PHP & MySQL

Kết nối – Hủy kết nối

- mysql_connect() kết nối đến hệ quản trị cơ sở dữ liệu MySQL
- mysql_error() ghi nhận lỗi trong quá trình kết nối
- mysql_select_db() lựa chọn cơ sở dữ liệu muốn thao tác
- mysql_close() đóng kết nối

Insert – Update – Delete

- mysql_query() thực thi câu SQL
- mysql_affected_rows() trả về số dòng đã được insert, update, delete

Truy xuất dữ liệu

SQL Injection

KHÁI NIỆM

- SQL injection - kỹ thuật cho phép thực hiện những câu SQL bất hợp pháp dựa vào lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu

- Thường xãy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase.

SQL Injection

CÁCH TẤN CÔNG CƠ BẢN

SELECT * FROM user WHERE name = **[userName]** ;

→ điều gì xảy ra nếu **[userName]** mang giá trị:

- johnsmith OR “a” = “a”
- johnsmith; DROP TABLE user; SELECT * FROM data WHERE “a” = “a”

XÂY DỰNG CLASS THAO TÁC VỚI DATABASE

Exercise 01 – Login website

Exercise 02 – User online

Exercise 02 – User online

MIÊU TẢ

- Page: index.php Info: userA – 19h00 Online: 1 (userA)
- Page: index.php Info: userB – 19h10 Online: 2 (userA, userB)
- Page: index.php Info: userB – 19h20 Online: 1 (userB)

(quy định trong 15 phút nếu người dùng không có thao tác gì đối với trang hiện tại xem như không online ở trang đó)

Exercise 02 – User online

HƯỚNG GIẢI QUYẾT

- Cơ sở dữ liệu: online (id, ip, url, time)
- Khi người dùng truy cập một trang nào đó, xử lý
  - Tìm kiếm thông tin người dùng trong bảng online
    - ❑ Nếu có: Cập nhật lại cột time
    - ❑ Nếu không có: thêm mới
  - Xóa các dòng dữ liệu có time không phù hợp với thời gian quy định
  - Hiển thị danh sách các người dùng online tại trang đó

Exercise 03 – Manage User

Pagination