

1. Lý thuyết Cốt lõi (Khái niệm)

Chương này tập trung vào việc "nhận" và "nhớ" dữ liệu từ người dùng.

- **Nhận dữ liệu (3.2):** Chúng ta dùng các biến "siêu toàn cục" (Superglobals) mà PHP tự động cung cấp:
 - `$_GET`: Lấy dữ liệu được gửi **trên thanh địa chỉ (URL)**. Ví dụ: `search.php?keyword=tlu`. Dữ liệu keyword sẽ nằm trong `$_GET['keyword']`. Dùng cho dữ liệu không nhạy cảm (tìm kiếm, lọc sản phẩm).
 - `$_POST`: Lấy dữ liệu được gửi "**ngầm**" trong thân (body) của yêu cầu HTTP, thường là từ một biểu mẫu `<form>`. Dùng cho dữ liệu nhạy cảm (đăng nhập, đăng ký).
- **Nhớ dữ liệu (3.5):** HTTP là giao thức "phi trạng thái" (stateless) - nó quên bạn ngay sau khi tải xong trang. Để "nhớ" người dùng (như trạng thái đăng nhập), chúng ta dùng:
 - `$_COOKIE`: Lưu một file text nhỏ **phía trình duyệt (Client)**. Trình duyệt tự động gửi nó lên server mỗi khi truy cập.
 - `$_SESSION`: Lưu dữ liệu **phía máy chủ (Server)**. PHP chỉ gửi một ID (Session ID) duy nhất cho trình duyệt (lưu ID đó bằng cookie). Khi trình duyệt gửi ID đó lên, server sẽ tìm và nạp đúng dữ liệu của người dùng. **Đây là cách chuẩn để làm chức năng đăng nhập.**
- **Điều hướng:** Để chuyển hướng người dùng từ trang này sang trang khác (ví dụ: sau khi đăng nhập thành công), ta dùng hàm: `header('Location: ten_trang_moi.php');`.

2. Nhiệm vụ Thực hành (BẮT BUỘC)

Kịch bản: Bạn sẽ xây dựng luồng đăng nhập đơn giản nhất, sử dụng `$_POST` để nhận và

`$_SESSION` để lưu trạng thái đăng nhập.

Code Khởi đầu (Starter Code):

Tạo 3 tệp sau trong cùng một thư mục (ví dụ: `htdocs/cse485/chapter3/`):

Tệp 1: login.html (Bạn chỉ cần copy & paste file này)

HTML

```
<!DOCTYPE html>
<html lang="vi">
<head>
<meta charset="UTF-8">
<title>PHT Chffong 3 - Đăng nhập</title>
</head>
<body>
<h2>Form Đăng Nhập</h2>
```

```
<form action="handle_login.php" method="POST">
<div>
<label>Tên đăng nhập:</label>
<input type="text" name="username">
</div>
<div>
<label>Mật khẩu:</label>
<input type="password" name="password">
</div>
<button type="submit">Đăng nhập</button>
</form>
</body>
</html>
```

Tệp 2: handle_login.php (Bạn phải hoàn thiện các TODO)

PHP

```
<?php

// TODO 1: (Cực kỳ quan trọng) Khởi động session
// Phải gọi hàm này TRƯỚC BẤT KỲ output HTML nào
// Gợi ý: Dùng hàm session_...()

// TODO 2: Kiểm tra xem người dùng đã nhấn nút "Đăng nhập" (gửi form) chưa
// Gợi ý: Dùng hàm isset() để kiểm tra sự tồn tại của $_POST['username']

// TODO 3: Nếu đã gửi form, lấy dữ liệu 'username' và 'password' từ $_POST
$user = ...; // Gợi ý: $_POST['...']
$pass = ...;

// TODO 4: (Giả lập) Kiểm tra logic đăng nhập
// Nếu $user == 'admin' VÀ $pass == '123' thì là đăng nhập thành công if
    ($user == 'admin' && $pass == '123') {

// TODO 5: Nếu thành công, lưu tên username vào SESSION
// Gợi ý: $_SESSION['ten_ban_dat'] = $user;
```

```
// TODO 6: Chuyển hướng người dùng sang trang "chào mừng"
// Gợi ý: Dùng hàm header('Location: ...');
// Và luôn gọi exit() ngay sau khi dùng header() exit;

} else {
// Nếu thất bại, chuyển hướng về login.html
header('Location: login.html?error=1'); // Kèm theo thông báo lỗi trên URL
exit;
}

// TODO 7: Nếu người dùng truy cập trực tiếp file này (không qua POST),
// "đá" họ về trang login.html
// Gợi ý: Dùng else cho TODO 2 và cũng header() về login.html

?>
```

Tập 3: welcome.php (Bạn phải hoàn thiện các TODO)

PHP

```
<?php
// TODO 1: Khởi động session (BẮT BUỘC ở mọi trang cần dùng SESSION)
// Gợi ý: Dùng hàm session_...()

// TODO 2: Kiểm tra xem SESSION (lưu tên đăng nhập) có tồn tại không?
// Gợi ý: Dùng isset($_SESSION['...']) (dùng đúng tên bạn đặt ở Tập 2, TODO 5) if
( ... ) {

// TODO 3: Nếu tồn tại, lấy username từ SESSION ra
$loggedInUser = ...;

// TODO 4: In ra lời chào mừng
echo "<h1>Chào mừng trở lại, $loggedInUser!</h1>";
```

```

echo "<p>Bạn đã đăng nhập thành công.</p>";

// TODO 5: (Tạm thời) Tạo 1 link để "Đăng xuất" (chỉ là quay về login.html) echo
    '<a href="login.html">Đăng xuất (Tạm thời)</a>';

} else {

// TODO 6: Nếu không tồn tại SESSION (chưa đăng nhập)
// Chuyển hướng người dùng về trang login.html
// Gợi ý: Dùng header('Location: ...'); exit;
}
?>

```

3. Yêu cầu Bằng chứng (Proof of Work)

Bạn phải nộp lại 2 bằng chứng sau:

A. Code đã hoàn thiện: Dán (paste) toàn bộ code của 2 tệp bạn đã sửa:

- handle_login.php

```

<?php

// TODO 1: Khởi động session

session_start();

// TODO 2: Kiểm tra xem người dùng đã gửi form chưa
if (isset($_POST['username']) && isset($_POST['password'])) {

    // TODO 3: Lấy dữ liệu từ POST

    $user = $_POST['username'];

    $pass = $_POST['password'];

    // TODO 4: Kiểm tra đăng nhập (giả lập)

    if ($user === 'admin' && $pass === '123') {

```

```

        // TODO 5: Lưu username vào SESSION

        $_SESSION['username'] = $user;

        // TODO 6: Chuyển hướng sang welcome.php

        header("Location: welcome.php");

        exit;

    } else {

        // Sai thông tin → quay về login

        header("Location: login.html?error=1");

        exit;

    }

} else {

    // TODO 7: Truy cập trực tiếp file → quay về login.html

    header("Location: login.html");

    exit;

}

?>

```

- welcome.php

```

<?php

// TODO 1: Khởi động session (BẮT BUỘC ở mọi trang cần dùng
SESSION)

// Gợi ý: Dùng hàm session_...()

session_start();

```

```
// TODO 2: Kiểm tra xem SESSION (lưu tên đăng nhập) có tồn tại
không?

// Gợi ý: Dùng isset($_SESSION['...']) (dùng đúng tên bạn đặt ở Tập
2, TODO 5)

if (isset($_SESSION['username'])) {

    // TODO 3: Nếu tồn tại, lấy username từ SESSION ra

    $loggedInUser = $_SESSION['username'];

    // TODO 4: In ra lời chào mừng

    echo "<h1>Chào mừng trở lại, $loggedInUser!</h1>";

    echo "<p>Bạn đã đăng nhập thành công.</p>";

    // TODO 5: (Tạm thời) Tạo 1 link để "Đăng xuất" (chỉ là quay về
login.html)

    echo '<a href="login.html">Đăng xuất (Tạm thời)</a>';

} else {

    // TODO 6: Nếu không tồn tại SESSION (chưa đăng nhập)

    // Chuyển hướng người dùng về trang login.html

    // Gợi ý: Dùng header('Location: ...'); exit;

    header('Location: login.html');

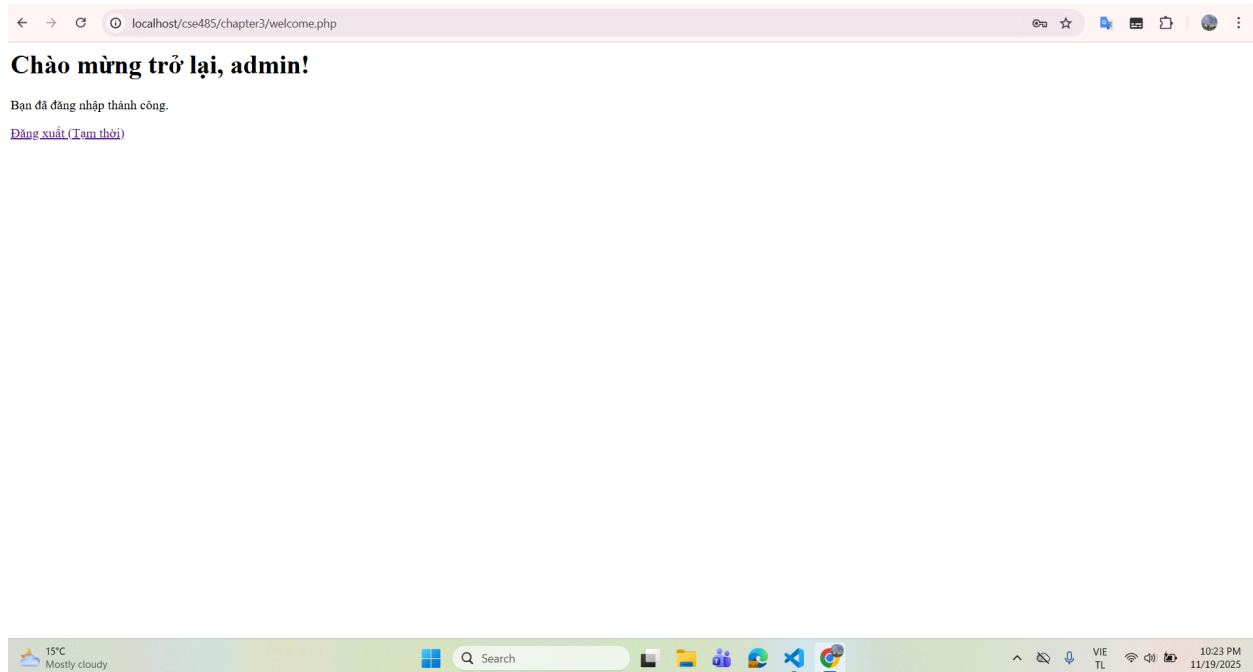
    exit;

}

?>
```


B. Ảnh chụp màn hình Kết quả (Trình duyệt Web): Chụp 01 ảnh màn hình trình duyệt hiển thị trang welcome.php sau khi bạn đăng nhập thành công (phải thấy rõ dòng chữ "Chào mừng trở lại, admin!").

(Dán Code A và Ảnh B của bạn vào đây)



4. Câu hỏi Phản biện (Bắt buộc)

Sau khi hoàn thành Phần 2 & 3, hãy đặt 01 câu hỏi tư duy.

(Gợi ý: "Tại sao `$_SESSION` (lưu ở Server) lại an toàn hơn `$_COOKIE` (lưu ở Client) để lưu trạng thái đăng nhập?" hoặc "Tại sao hàm `session_start()` phải được gọi ở cả file `handle_login.php` VÀ file `welcome.php`?").

Câu hỏi của em là: Tại sao không lưu toàn bộ thông tin đăng nhập (như username, role) trực tiếp trong cookie, mà thay vào đó chỉ lưu session ID rồi truy xuất thông tin từ server? Các hacker có tận dụng vào đó để đánh cắp được thông tin hay không ?

5. 9 Kết nối Đánh giá (Rất quan trọng)

Các kỹ thuật bạn vừa thực hành (`$_POST`, `$_SESSION`, `header()`) là nền tảng cốt lõi của **mọi**

ứng dụng web có đăng nhập.

Bạn sẽ vận dụng chúng trực tiếp để hoàn thành **Bài tập trên lớp (Phần PHP)**, chiếm **20%** tổng điểm, dự kiến vào **Tuần 5**. Nếu bạn không thể tự làm PHT này, bạn chắc chắn sẽ không thể làm được bài kiểm tra đó.