Phiếu học tập chủ động

Môn học: CSE485- Công nghệ web

Họ và tên: Nguyễn Anh Tuấn

Mã sinh viên: 2251162199

Lớp: 64HTTT4

Lớp học phần: 65HTTT

CHƯƠNG 3: TRANG WEB ĐỘNG

Code:

- File handle_login.php:

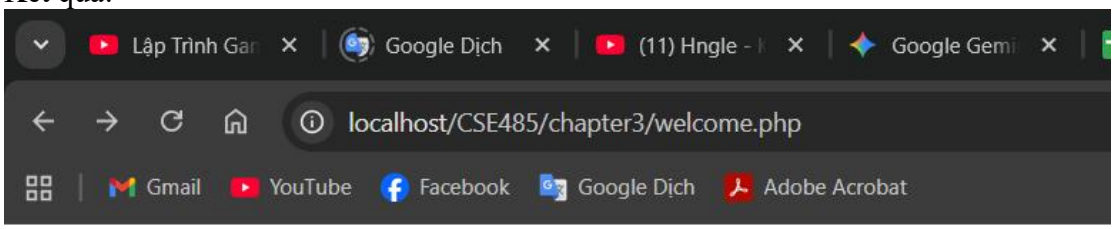
```php
<?php
// TODO 1: (Cực kỳ quan trọng) Khởi động session
// Phải gọi hàm này TRƯỚC BẤT KỲ output HTML nào
// Gợi ý: Dùng hàm session_...()
session_start();
// TODO 2: Kiểm tra xem người dùng đã nhấn nút "Đăng nhập" (gửi form) chưa
// Gợi ý: Dùng hàm isset() để kiểm tra sự tồn tại của $_POST['username']
if (isset($_POST['username'])) {
 // TODO 3: Nếu đã gửi form, lấy dữ liệu 'username' và 'password' từ $_POST
$user = $_POST['username'];
$pass = $_POST['password'];
 // 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;
 $_SESSION['username'] = $user; // Tôi đặt tên key là 'username'
 // 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()
header('Location: welcome.php');
        exit;
    } else {
        // Nếu thất bại, chuyển hướng về login.html kèm lỗi
        header('Location: login.html?error=1');
        exit;
    }

} else {
// 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
header('Location: login.html');
    exit;
}
?>
```

File Welcome.php.

```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($_SESSION['...']) (dùng đúng tên bạn đặt ở Tệp 2, TODO 5)
if (isset($_SESSION['username'])) {

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

```php
$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: ...');
header('Location: login.html');
    exit;
}
?>
```

Kết quả:



Chào mừng trở lại, admin!

Bạn đã đăng nhập thành công.

Đăng xuất (Tạm thời)

Câu hỏi của tôi là: Tại sao $_SESSION (lưu ở Server) lại an toàn hơn $_COOKIE (lưu ở Client) để lưu trạng thái đăng nhập của người dùng?

Câu trả lời: Sự khác biệt nằm ở quyền kiểm soát dữ liệu:

$_COOKIE (Client-side): Dữ liệu được lưu trực tiếp trên trình duyệt của người dùng dưới dạng văn bản.

Rủi ro: Người dùng (hoặc hacker) có thể dễ dàng mở công cụ Developer Tools (F12) để xem và chỉnh sửa giá trị này. Ví dụ: Nếu ta lưu user_role=student trong cookie, hacker có thể sửa thành user_role=admin để chiếm quyền.

$_SESSION (Server-side): Dữ liệu thực tế được lưu trong bộ nhớ hoặc file trên Máy chủ (Server). Người dùng chỉ giữ một mã định danh duy nhất là Session ID (vô nghĩa nếu không có dữ liệu khớp trên server).

An toàn: Người dùng không thể chạm vào hay chỉnh sửa dữ liệu gốc nằm trên server.

Kết luận: Vì lý do bảo mật, ta luôn dùng $_SESSION cho các thông tin nhạy cảm (đăng nhập, thanh toán) và chỉ dùng $_COOKIE cho các thông tin ít quan trọng (như ghi nhớ màu nền, ngôn ngữ ưu thích).