**BÀI THỰC HÀNH 04**

**LẬP TRÌNH PHP NÂNG CAO**

Họ và tên: Ngô Lê Trúc Quỳnh

MSSV: B2107119

**MỤC LỤC**

[1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả. 4](#_gjdgxs)

[2. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong https://www.w3schools.com/sql/sql\_injection.asp . Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả. 7](#_lnxbz9)

[3. Dựa vào https://www.w3schools.com/php/php\_cookies.asp , bạn hãy cho biết Cookie là gì, diễn giải ý nghĩa các tham số trong setcookie(). Cách lưu, lấy, xóa giá trị trong cookie. 8](#_35nkun2)

[4. Dựa vào https://www.w3schools.com/php/php\_sessions.asp , bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session. 9](#_1ksv4uv)

[5. Bạn hãy so sánh Cookie và Session 10](#_44sinio)

[6. Chỉnh sửa các đoạn gán, khởi tạo, lấy giá trị cookie trong log.php và homepage.php thay bằng cách dùng Session. Tạo tập tin thoat.php để xóa các giá trị trong session, cookie thực hiện chức năng log out khỏi hệ thống. 10](#_2jxsxqh)

[7. Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăng nhập. Yêu cầu gồm 3 input: ô để nhập mật khẩu cũ, 1 ô để nhập mật khẩu mới, 1 ô chophép nhập mật lại mật khẩu mới. Khi nhập xong cần đảm bảo: mật khẩu cũ là khớp với CSDL đang lưu, 2 ô nhập mật khẩu mới phải khớp với nhau và không giống với mật khẩu cũ, nếu đáp ứng điều kiện thì tiến hành băm mật khẩu với md5 và lưu mật khẩu mới vàoCSDL. 10](#_z337ya)

[8. Bạn đọc https://www.w3schools.com/php/php\_file\_upload.asp để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload. 10](#_3j2qqm3)

[9. Bạn hãy đọc https://www.w3schools.com/php/func\_filesystem\_file.asp mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php). 11](#_1y810tw)

[10. Bạn hãy tạo 1 tập tin csv ít nhất 10 dòng dữ liệu với các cột dữ liệu như bảng customer trong csdl qlbanhang. Tạo tập tin upload-csv.php với giao diện cho phép upload các tập tin csv, và tập tin upload-csv-processing để xử lý nút xử lý sự kiện upload file csv và đưa dữ liệu vào bảng customers trong CSDL. 11](#_4i7ojhp)

**PHỤ LỤC HÌNH**

[Hình 1 Chưa thiết lập 4](#_30j0zll)

[Hình 2 Được thiết lập 4](#_1fob9te)

[Hình 3 Tạo thành công bảng customers 4](#_3znysh7)

[Hình 4. formnhap.php 5](#_2et92p0)

[Hình 5 Formluu.php 5](#_tyjcwt)

[Hình 6 Người dùng ‘Ngo Le Truc Quynh’ với mật khẩu được mã hóa 5](#_3dy6vkm)

[Hình 7 Chọn ‘email’ là unique key 5](#_1t3h5sf)

[Hình 8 Login.php 6](#_4d34og8)

[Hình 9 Thông báo lỗi khi nhập sai mật khẩu 6](#_2s8eyo1)

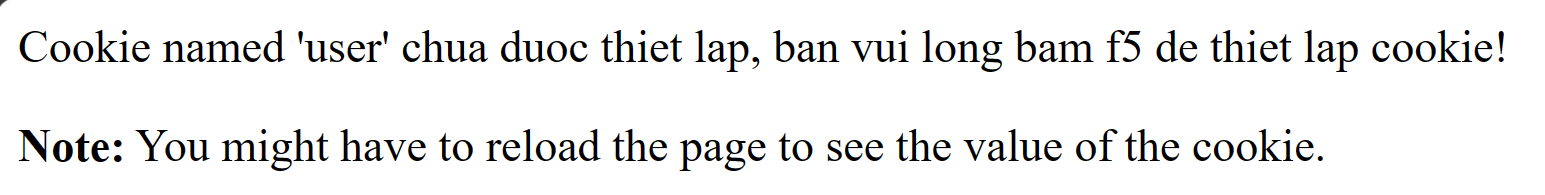
[Hình 10 Thông báo đăng nhập thành công 6](#_17dp8vu)

[Hình 11 Sau khi đăng nhập thành công và chuyển sang trang chủ khác 7](#_3rdcrjn)

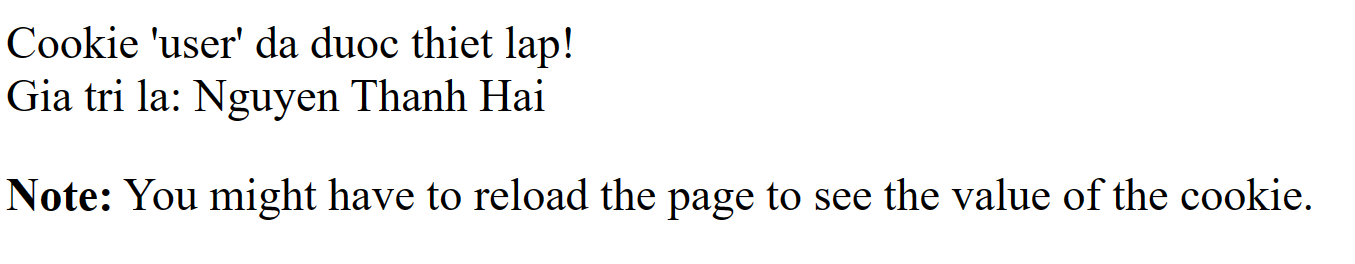
[Hình 12 Upload-img.php 7](#_26in1rg)

**BÀI LÀM**

# Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.



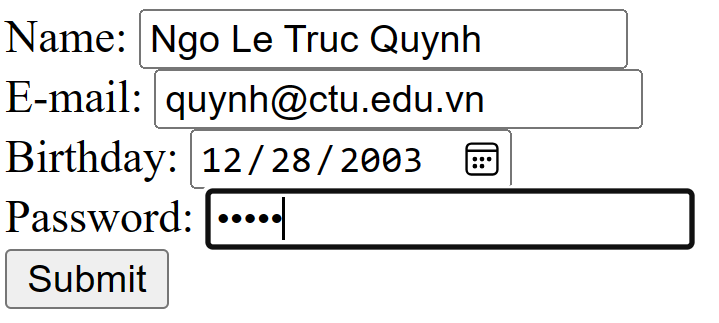
*Hình 1 Chưa thiết lập*



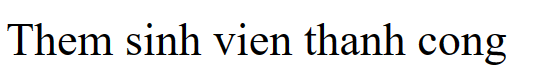
*Hình 2 Được thiết lập*



*Hình 3 Tạo thành công bảng customers*



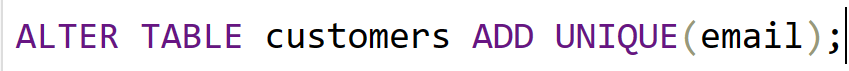
*Hình 4. formnhap.php*



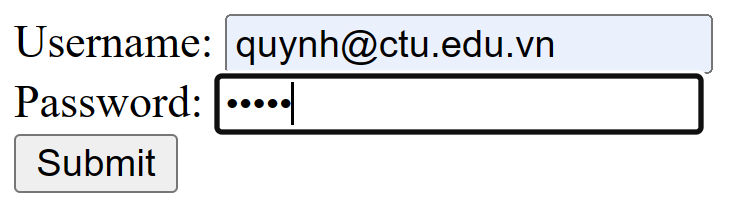
*Hình 5 Formluu.php*



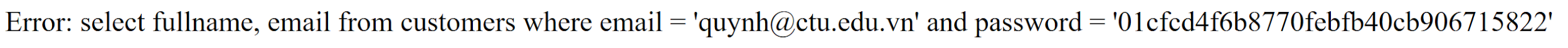
*Hình 6 Người dùng ‘Ngo Le Truc Quynh’ với mật khẩu được mã hóa*



*Hình 7 Chọn ‘email’ là unique key*



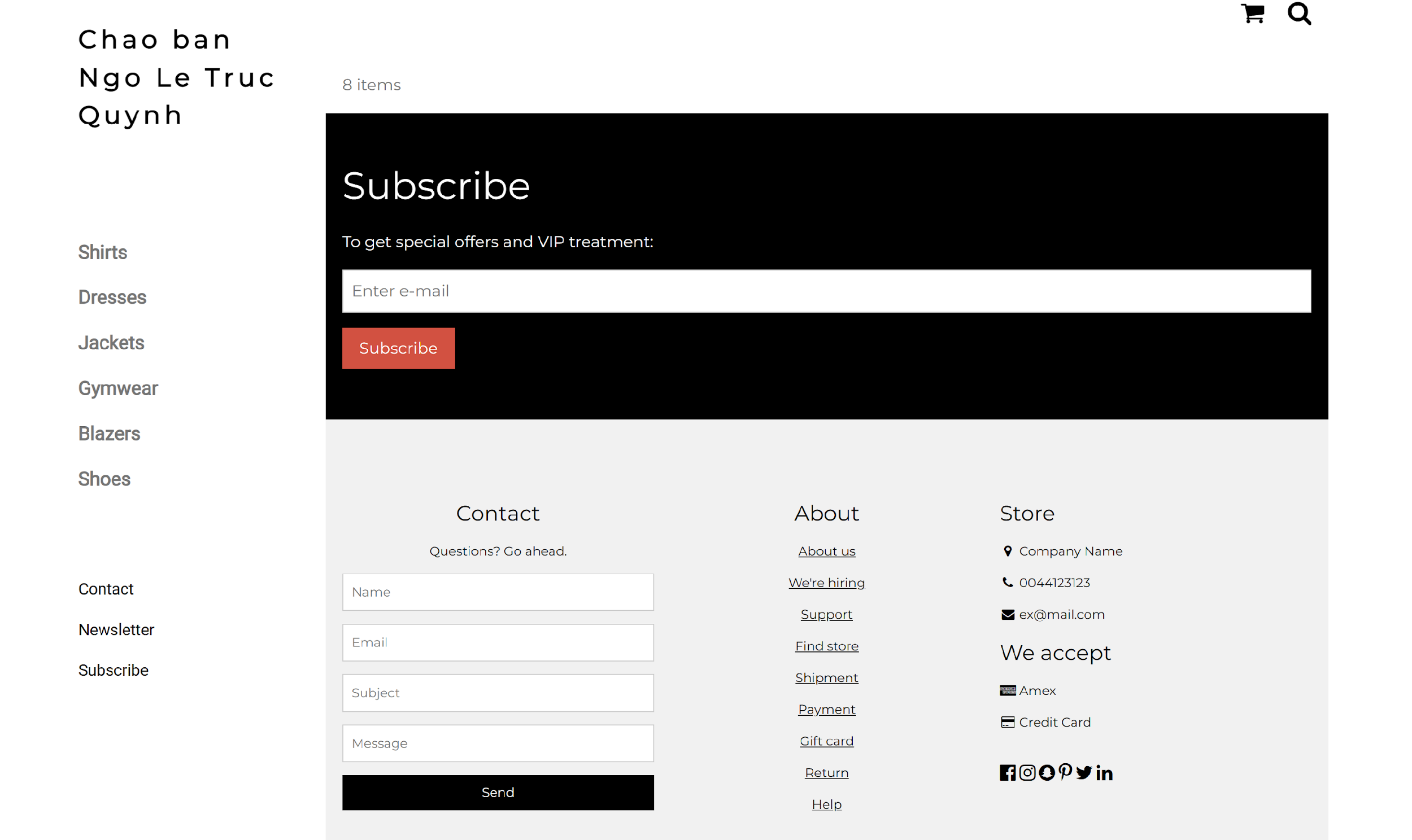
*Hình 8 Login.php*



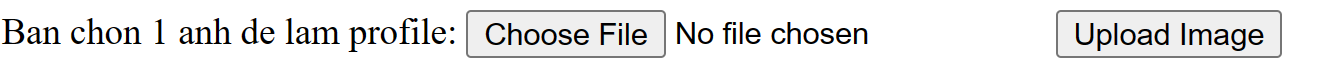
*Hình 9 Thông báo lỗi khi nhập sai mật khẩu*



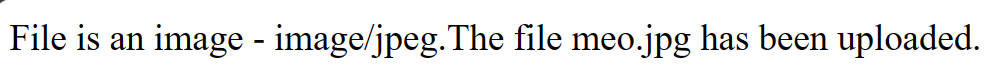
*Hình 10 Thông báo đăng nhập thành công*



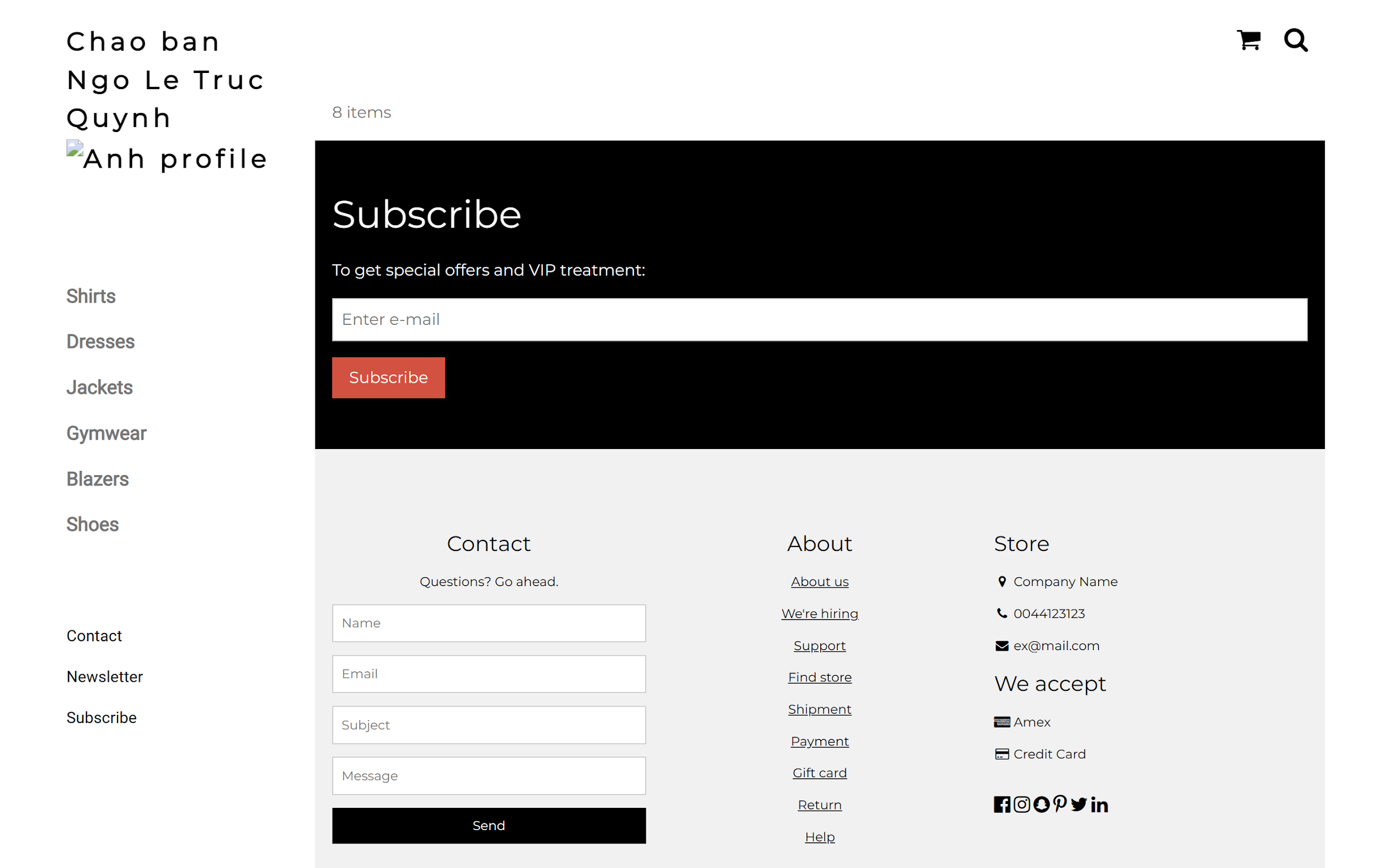
*Hình 11 Sau khi đăng nhập thành công và chuyển sang trang chủ khác*



*Hình 12 Upload-img.php*



*Hình 13 Thêm hình thành công*



*Hình 14 Tải hình lên page*

# Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong <https://www.w3schools.com/sql/sql_injection.asp> . Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

SQL Injection là gì?

SQL Injection là kỹ thuật tấn công mạng nhắm vào ứng dụng web sử dụng SQL. Kẻ tấn công lợi dụng lỗ hổng bảo mật để đưa mã SQL độc hại, cho phép:

• Truy cập trái phép dữ liệu nhạy cảm

• Sửa đổi hoặc xóa dữ liệu

• Kiểm soát hệ thống cơ sở dữ liệu

Ví dụ:

Ứng dụng đăng nhập:

• Thay đổi tên người dùng.

• Bỏ qua kiểm tra mật khẩu.

Cách bảo mật:

• Sử dụng tham số truy vấn

• Kiểm tra dữ liệu đầu vào

• Sử dụng prepared statements

• Cập nhật phần mềm

Tài liệu tham khảo:

• <https://www.w3schools.com/sql/sql_injection.asp>

# Dựa vào <https://www.w3schools.com/php/php_cookies.asp> , bạn hãy cho biết Cookie là gì, diễn giải ý nghĩa các tham số trong setcookie(). Cách lưu, lấy, xóa giá trị trong cookie.

Cookie là tập tin nhỏ lưu trữ thông tin về người dùng và cài đặt của họ trên máy tính để cải thiện trải nghiệm duyệt web.

setcookie():

name: Tên cookie.

value: Giá trị cookie.

expire: Thời gian hết hạn (tính bằng giây).

path: Đường dẫn cookie có hiệu lực.

domain: Tên miền cookie có hiệu lực.

secure: Cookie chỉ được gửi qua HTTPS.

httponly: Cookie chỉ truy cập được bởi JavaScript.

Lưu giá trị:

setcookie("name", "value", time() + 3600); // Lưu cookie trong 1 giờ

Lấy giá trị:

$name = $\_COOKIE["name"];

Xóa giá trị:

setcookie("name", "", time() - 3600); // Xóa cookie

Tài liệu tham khảo:

<https://www.w3schools.com/php/php_cookies.asp>

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>

# Dựa vào <https://www.w3schools.com/php/php_sessions.asp> , bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

Session là tập tin lưu trữ thông tin về người dùng trên máy chủ trong suốt phiên làm việc của họ.

Lưu giá trị:

$\_SESSION["name"] = "value";

Lấy giá trị:

$name = $\_SESSION["name"];

Xóa giá trị:

unset($\_SESSION["name"]);

# Bạn hãy so sánh Cookie và Session



Tài liệu tham khảo: <https://viblo.asia/p/cookie-va-session-07LKXEvEZV4>

# Chỉnh sửa các đoạn gán, khởi tạo, lấy giá trị cookie trong log.php và homepage.php thay bằng cách dùng Session. Tạo tập tin thoat.php để xóa các giá trị trong session, cookie thực hiện chức năng log out khỏi hệ thống.

# Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăng nhập. Yêu cầu gồm 3 input: ô để nhập mật khẩu cũ, 1 ô để nhập mật khẩu mới, 1 ô chophép nhập mật lại mật khẩu mới. Khi nhập xong cần đảm bảo: mật khẩu cũ là khớp với CSDL đang lưu, 2 ô nhập mật khẩu mới phải khớp với nhau và không giống với mật khẩu cũ, nếu đáp ứng điều kiện thì tiến hành băm mật khẩu với md5 và lưu mật khẩu mới vàoCSDL.

# Bạn đọc <https://www.w3schools.com/php/php_file_upload.asp> để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.

Cơ chế upload file:

* Upload file là quá trình truyền tải file từ máy tính của người dùng lên máy chủ.
* PHP sử dụng $\_FILES biến toàn cục để lưu trữ thông tin về file được upload.

Có hai phương thức upload:

* POST: Phương thức phổ biến nhất, sử dụng form HTML với enctype="multipart/form-data".
* PUT: Ít phổ biến hơn, sử dụng HTTP PUT method.

Hàm/thủ tục upload file:

* move\_uploaded\_file(): Hàm di chuyển file đã upload đến vị trí mong muốn trên máy chủ.
* is\_uploaded\_file(): Kiểm tra xem file đã được upload hay chưa.
* getimagesize(): Lấy thông tin về kích thước và loại hình ảnh.
* file\_exists(): Kiểm tra xem file có tồn tại hay không.
* unlink(): Xóa file khỏi máy chủ.

# Bạn hãy đọc <https://www.w3schools.com/php/func_filesystem_file.asp> mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php).

Tham số:

* + filename: Đường dẫn đến file cần đọc.
  + mode: Chế độ mở file (tùy chọn).

r: Mở file để đọc (chế độ mặc định).

w: Mở file để ghi (tạo file mới nếu không tồn tại).

a: Mở file để ghi (thêm nội dung vào cuối file).

Giá trị trả về: Hàm file() trả về một mảng, mỗi phần tử trong mảng là một dòng trong file. Nếu file không tồn tại hoặc không thể mở được, hàm sẽ trả về FALSE.

# Bạn hãy tạo 1 tập tin csv ít nhất 10 dòng dữ liệu với các cột dữ liệu như bảng customer trong csdl qlbanhang. Tạo tập tin upload-csv.php với giao diện cho phép upload các tập tin csv, và tập tin upload-csv-processing để xử lý nút xử lý sự kiện upload file csv và đưa dữ liệu vào bảng customers trong CSDL.

Gợi ý:

○ Xem cấu trúc của bảng customer, mở excel và nhập liệu lưu lại với định dạngCSV.

○ Tham khảo upload-img.php để thiết kế giao diện upload file

○ Tham khảo upload-csdl.php để thiết kế action xử lý việc upload file, chú ý chỉnh sửa loại tập tin chấp nhận các file csv. Tham khảo:

<https://www.php.net/manual/en/features.file-upload.post-method.php>

<https://stackoverflow.com/questions/6654351/check-file-uploaded-is-in-csv-format>

Ở đoạn sau khi uploadthành công, bạn lấy tên file vừa upload đưa vào hàm đọc tập tin. Bạn tham khảo read-csv.php chỉnh sửa đọc dữ liệu từ csv đưa vào mảng để lần lượt thực hiện insert từng dòng dữ liệu trong csv vào CSDL.