BÀI TẬP CÔNG NGHỆ WEB

Đề tài: cửa hàng thú cưng

Chung Tình B2306643

Nguyễn Văn Hiền B2306616

# Các đặc điểm đánh giá

A table with numbers and text

AI-generated content may be incorrect.

## Tiêu chí chung cho các thành phần đánh giá

* Mã lệnh sao chép y hệt từ nguồn khác có thể làm hạ mức đạt
* Mã lệnh hoạt động đúng, ít lỗi
* Trả lời chính xác các câu hỏi liên quan

## Xây dựng các trang web dùng Bootstrap

* Số lượng trang web >= 4 được xây dựng với Bootstrap 5, các trang có cấu trúc trang đầy đủ và có liên kết giữa các trang
* Sử dụng đa dạng các thành phần và tính năng của Bootstrap 5
* Khuyến khích thiết kế web hiển thị tốt trên thiết bị di động

## Dùng PHP và PDO tạo trang web động phía server có tương tác với CSDL (đọc/thêm/sửa/xóa)

* Thực hiện đúng quy trình xử lý yêu cầu HTTP (từ giai đoạn đọc tham số đến tạo nội dung trả lời)
* Số lượng trang web kết xuất phía server >= 4, có xử lý các yêu cầu HTTP chứa tập tin và/hoặc SSE
* Đọc dữ liệu từ CSDL ra trang web với số lượng bảng dữ liệu từ 2-5 bảng, có ít nhất một mối quan hệ giữa các bảng
* Sử dụng biểu mẫu (form) nhận nhập liệu từ người dùng và cập nhật dữ liệu (thêm/sửa/xóa) vào CSDL. Các tác vụ tương tác với CSDL cần liên quan đến các chức năng xử lý quy trình nghiệp vụ

## Sử dụng phù hợp các công cụ giúp tổ chức mã lệnh dự án PHP (PHP include, lập trình hướng đối tượng, tự động nạp lớp, Composer, MVC)

* Website có một thư mục riêng dùng làm Document Root (các tên thông thường của thư mục này là public, www, htdocs, ...).
* Khuyến khích tổ chức dự án theo MVC
* Nếu dùng include/require thì các script được include/require phải được bảo vệ ngăn truy cập trực tiếp từ người dùng\* (ví dụ như tổ chức các script này nằm ở ngoài thư mục Document Root)
* Nếu có tạo lớp thì PHẢI thực hiện tự động nạp lớp theo chuẩn PSR-4 (có thể dùng Composer để quản lý tự động nạp lớp)
* Nếu sử dụng mã lệnh/thư viện bên ngoài thì dùng Composer để quản lý (<https://stackoverflow.com/questions/409496/prevent-direct-access-to-a-php-include-file>)

## Đề phòng các lỗi bảo mật thường gặp (XSS, SQL Injection, CSRF, chứng thực) cho trang web

* Đề phòng XSS: dùng các hàm có sẵn của PHP như htmlspecialchars() hoặc một template engine
* Đề phòng SQL Injection: dùng Prepared Statement của PDO với tham số giữ chỗ (:varname hoặc ?) khi thực thi câu lệnh SQL
* Đề phòng CSRF: tạo session key đính kèm vào các form và kiểm tra session key khi form được gửi về
* Chứng thực người dùng với username/password hoặc OAuth2/OpenID Connect

## Cài đặt URL "sạch" cho website và thực hiện cấu hình web server phù hợp để vận hành website

* Sử dụng URL "sạch" trong website (có thể dùng thư viện định tuyến có sẵn hoặc tự cài đặt)
* Cấu hình web server cho website hoặc triển khai website với tên miền công khai (VPS, Cloudflare Tunnel, ...)

# Thành phần chang web:

## Thành phần chung:

### Header

Nav: chứa các đường dẫn đến các trang web còn lại ( Trang chủ, Trang sản phẩm, Trang đăng nhập, Trang đăng kí, Trang buôn bán, Trang Tài khoản); Logo, tên trang web

### Footer

Chứa địa chỉ liên hệ (email, sđt, địa chỉ,…); link nền tảng mxh (youtube, facebook, twister,…); trang riêng (Trang giới thiệu, Trang Điều khoản và dịch vụ, liên hệ, FAQ,..)

### Url

Sạch

### Bảo mật

* Đề phòng XSS: dùng các hàm có sẵn của PHP như htmlspecialchars() hoặc một template engine
* Đề phòng SQL Injection: dùng Prepared Statement của PDO với tham số giữ chỗ (:varname hoặc ?) khi thực thi câu lệnh SQL
* Đề phòng CSRF: tạo session key đính kèm vào các form và kiểm tra session key khi form được gửi về

## Trang chủ: index.html

Một số mặt hàng tiêu biểu, lời giới thiệu

## Trang sản phẩm

Gồm danh sách sản phẩm lấy từ database ProgessSQL (table: sản phẩm mua), sau khi đặt mua sẽ chuyển sang database ProgessSQL (table: sản phẩm duyệt mua)

## Trang buôn bán

Dùng để đăng bán sản phẩm được lưu vào database ProgessSQL (table: sản phẩm bán), sau khi được admin duyệt sẽ đưa vào database ProgessSQL (table: sản phẩm duyệt bán)

## Trang đăng nhập

Gồm ô nhập tài khoản, mật khẩu lấy từ database ProgessSQL (table: tài khoản). Nếu đúng với dữ liệu lấy được từ database sẽ cho phép đăng nhập

## Trang đăng kí:

Đăng kí tài khoản (check xem có tài khoản trong database ProgessSQL (table: tài khoản) không, nếu không thì tạo theo quy chuẩn.

## Trang Tài khoản:

Dùng để thay đổi thông tin cá nhân, thay đổi mật khẩu, xem các đơn hàng

## Trang giới thiệu:

Giới thiệu chung về nhóm

## Trang Điều khoản và dịch vụ:

Các điều khoản và dịch vụ

## Trang admin ( chỉ vào được khi đăng nhập bằng tài khoản tạo sẵn)

Đăng nhập khi dùng tài khoản trong database ProgessSQL (table: tài khoản admin dùng để:

* Quản lí phê duyệt, xem các tài khoản - table: tài khoản ( không xem mật khẩu được)
* Xem các bảng sản phẩm được mua - table: sản phẩm mua, table: sản phẩm duyệt mua
* Xem sản phẩm chờ duyệt để đăng bán, quyết định sản phẩm bán - table: sản phẩm bán, sản phẩm duyệt bán