

THỰC HÀNH CÔNG NGHỆ WEB

YÊU CẦU CHUNG:

- **Sinh viên tạo một báo cáo duy nhất cho TẤT CẢ các buổi thực hành (4 buổi).** Sau mỗi buổi thực hành sinh viên nộp báo cáo (chứa bài làm của buổi hiện thời và các buổi trước đó) dưới dạng tập tin PDF xem như báo cáo tiến độ, không tính điểm. **Điểm thực hành sẽ là điểm của bài báo cáo PDF sinh viên nộp trong buổi thực hành cuối cùng (chứa tất cả bài làm của tất cả các buổi).** Không nộp bài báo cáo tiến độ đúng hạn buổi nào sẽ không tính điểm buổi đó.
- Trong báo cáo ghi thông tin MSSV, Họ tên, Nhóm học phần.
- Các sinh viên bị phát hiện sao chép bài làm của nhau *sẽ bị điểm 0 toàn bộ phần thực hành.*
- Điểm tối đa cho mỗi buổi thực hành là 10 điểm (tương đương 1 điểm của học phần).

BUỔI 3: LẬP TRÌNH WEB ĐỘNG VỚI PHP VÀ MYSQL

Nội dung thực hành

- Xây dựng web động đơn giản với ngôn ngữ lập trình PHP.
- Sử dụng PDO để truy xuất (đọc, thêm, sửa, xóa) dữ liệu trong cơ sở dữ liệu (CSDL) MySQL.

Báo cáo của buổi 3 là các hình ảnh minh họa kết quả thực thi các script PHP hoặc các chức năng được yêu cầu cài đặt. Mỗi chức năng cần phải có đầy đủ các hình minh họa, ví dụ:

- Giao diện trang khi đang sử dụng chức năng
- Các giao diện các trang thông báo thành công, thông báo lỗi (nếu có)
- Giao diện cho thấy kết quả sau thực hiện chức năng thành công, ...

Cấu hình MySQL và Apache

Chú ý: Hướng dẫn dưới đây giả định rằng XAMPP được cài đặt tại thư mục *C:/xampp*, sinh viên tự thực hiện những điều chỉnh thích hợp nếu XAMPP được cài đặt ở vị trí khác.

1. Dùng một MySQL client (phpMyadmin, HeidiSQL, ...) tạo CSDL *ct275_lab3* và tạo một bảng dữ liệu tên *quotes* trong *ct275_lab3* với các trường thông tin sau: *id*, *quote*, *source*, *favorite*, *date_entered*.

```
CREATE TABLE `quotes` (  
  `id` INT(10) NOT NULL AUTO_INCREMENT,  
  `quote` TEXT NOT NULL,  
  `source` VARCHAR(100) NOT NULL,  
  `favorite` TINYINT(1) NOT NULL,  
  `date_entered` TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,  
  PRIMARY KEY (`id`)  
) ENGINE = InnoDB;
```

Chèn dữ liệu ví dụ vào bảng vừa tạo:

```
INSERT INTO `quotes` (`quote`, `source`, `favorite`, `date_entered`) VALUES
('Anh yêu em!', 'Ai đó', 0, '2022-01-18 08:59:21'),
('Học lập trình web thật thú vị!', 'Albert Einstein', 1, '2022-01-18
10:21:27'),
('Yêu là chết trong lòng một ít!', 'Xuân Diệu', 0, '2022-03-02 05:53:13');
```

2. Tạo thư mục `C:/xampp/apps/lab3` và sao chép **nội dung** thư mục `quotes-app-start` đã cho vào thư mục này. (Sinh viên có thể sử dụng thư mục khác. Trong trường hợp đó, khi thực hiện theo các chỉ dẫn bên dưới thì cần chú ý điều chỉnh vị trí thư mục cho thích hợp).
3. Cấu hình host ảo cho thư mục `C:/xampp/apps/lab3/public`:
 - 3.1. Hiệu chỉnh tập tin `C:/xampp/apache/conf/extra/httpd-vhosts.conf` (có thể lấy nội dung từ file `vhost.txt` đính kèm):

```
<VirtualHost *:80>
    DocumentRoot "C:/xampp/htdocs"
    ServerName localhost
    # Set access permission
    <Directory "C:/xampp/htdocs">
        AllowOverride None
        Require all granted
    </Directory>
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot "C:/xampp/apps/lab3/public"
    ServerName ct275-lab3.localhost
    # Set access permission
    <Directory "C:/xampp/apps/lab3/public">
        AllowOverride None
        Require all granted
    </Directory>
</VirtualHost>
```

- 3.2. Restart lại server Apache.

[VirtualHost](#) là một tính năng của máy chủ web Apache HTTP Server cho phép chạy nhiều website đồng thời trên cùng một server, mỗi website có Document Root riêng. Các virtual host được phân biệt dựa trên địa chỉ IP (trường hợp server có nhiều địa chỉ IP) hoặc dựa theo tên. Cấu hình ở trên khai báo 2 virtual host dựa theo tên `localhost` và `ct275-lab3.localhost` với Document Root lần lượt là `C:/xampp/htdocs` và `C:/xampp/apps/lab3/public`.

4. Mở script `partials/db_connect.php`, **hiệu chỉnh các thông số kết nối đến MySQL** cho phù hợp với môi trường của bạn. **Trong các phòng thực hành của khoa, tài khoản kết nối đến MySQL là người dùng root, mật khẩu trống.**
5. Mở trình duyệt bất kì, kiểm tra đường dẫn <http://ct275-lab3.localhost/> hoạt động. **TỪ ĐÂY, KHI CHỤP HÌNH MINH HỌA CẦN THỂ HIỆN ĐƯỜNG DẪN URL TRÊN THANH ĐỊA CHỈ.**

Tìm hiểu mã nguồn dự án

Cấu trúc mã nguồn đã cho:

```
lab3/
+---partials
  +---check_admin.php      // Hiển thị thông báo lỗi nếu không là admin
  +---footer.php           // Định nghĩa footer chung cho các trang web
  +---header.php           // Định nghĩa header chung cho các trang web
  +---db_connect.php       // Script tạo kết nối đến CSDL
  +---show_error.php       // Hiển thị thông báo lỗi
+---public
  +---css                  // Thư mục chứa css cho các trang web
  +---add_quote.php        // Thêm trích dẫn
  +---delete_quote.php     // Xóa trích dẫn
  +---edit_quote.php       // Hiệu chỉnh trích dẫn
  +---index.php            // Trang chủ, hiển thị một trích dẫn
  +---login.php            // Đăng nhập
  +---logout.php           // Đăng xuất
  +---view_quotes.php      // Xem tất cả các trích dẫn
  +---functions.php        // Các hàm trợ giúp
```

Nội dung script **show_error.php** được cho như sau:

```
<?php

$error_message ??= 'Đã có lỗi xảy ra';
$error = "<p class=\"error\">$error_message";
$error .= isset($reason) ? " vì:<br>$reason</p>" : "</p>";
$error .= isset($query) ? "<p>Câu truy vấn là: {$query}</p>" : '';
echo $error;
```

Script **show_error.php** có thể cần các biến sau: `$error_message` lưu thông báo lỗi, `$reason` lưu nguyên nhân lỗi và `$query` câu truy vấn SQL bị lỗi. Lệnh `$error_message ??= 'Đã có lỗi xảy ra';` gán giá trị cho `$error_message` chỉ khi `$error_message` chưa được định nghĩa hoặc có giá trị NULL.

Yêu cầu cài đặt

Với mã nguồn đã cho, ba script trong thư mục public đã được hoàn chỉnh (cho bài tập này) là `index.php` (trang chủ, mặc định sẽ hiển thị trích dẫn mới nhất), `login.php` (thực hiện đăng nhập) và `logout.php` (thực hiện đăng xuất). Ứng dụng web có hỗ trợ đăng nhập với tài khoản đăng nhập được gán cứng là email: me@example.com, mật khẩu: testpass.

Sau khi tìm hiểu mã nguồn đã cho, hãy hoàn thành các script sau đây:

- **view_quotes.php**: hiển thị tất cả các trích dẫn trong CSDL, với mỗi trích dẫn hiển thị hai đường link quản trị: sửa và xóa trích dẫn đó.
- **add_quote.php**: thêm một trích dẫn vào CSDL.
- **edit_quote.php**: hiệu chỉnh một trích dẫn trong CSDL với id của trích dẫn do người dùng gửi về qua chuỗi truy vấn (ví dụ: `edit_quote.php?id=1`).
- **delete_quote.php**: xóa một trích dẫn trong CSDL dựa trên id. Khi người dùng chọn xóa cần hiển thị một trang xác nhận trước khi thực hiện xóa.
- Hiển thị các thông báo thành công hoặc thất bại khi thực hiện các tác vụ.

Hướng dẫn cài đặt

Chú ý:

- (1) Sinh viên có thể có các cài đặt khác với hướng dẫn bên dưới, chỉ cần đảm bảo đúng yêu cầu.
- (2) Để chạy một script PHP nào đó nằm trong thư mục public (thư mục Document Root), dùng đường dẫn URL tính từ thư mục Document Root đến script. Ví dụ, để chạy script `view_quotes.php` nằm ngay trong thư mục public thì nhập URL:

http://ct275-lab3.localhost/view_quotes.php

- **view_quotes.php:** thay vào chỗ câu lệnh `echo "<p>Trang đang được xây dựng...</p>"` bằng đoạn mã lệnh sau đây và chạy kiểm tra kết quả:

```
include '../partials/db_connect.php';

$query = 'SELECT id, quote, source, favorite FROM quotes ORDER BY date_entered DESC';

try {
    $sth = $pdo->query($query);
    while ($row = $sth->fetch()) {
        $htmlspecialchars = 'htmlspecialchars';
        echo "<div><blockquote>{$htmlspecialchars($row['quote'])}</blockquote>-
            {$htmlspecialchars($row['source'])}<br>";

        if ($row['favorite'] = 1) {
            echo ' <strong>Yêu thích!</strong>';
        }

        echo "<p><b>Quản trị Trích dẫn:</b> <a href=\"edit_quote.php?id={$row['id']}\">Sửa</a> ↔
            <a href=\"delete_quote.php?id={$row['id']}\">Xóa</a></p></div><br>";
    }
} catch (PDOException $e) {
    $error_message = 'Không thể lấy dữ liệu';
    $reason = $pdo_error;
    include '../partials/show_error.php';
}

include '../partials/footer.php';
```

Muốn gọi hàm `htmlspecialchars()` trong chuỗi nhưng PHP lại không thể nhận biết tên hàm trong một chuỗi. Một giải pháp là tạo biến có giá trị là tên hàm cần gọi ('htmlspecialchars' trong trường hợp trên) và thực hiện gọi hàm trong chuỗi thông qua biến như đã trình bày trong đoạn code ở trên. Giải pháp khác là thực hiện nối chuỗi, ví dụ:

```
echo "<div><blockquote>" . htmlspecialchars($row['quote']) . "</blockquote>-" .
    htmlspecialchars($row['source']) . "<br>";
```

- **add_quote.php:** thay vào chỗ câu lệnh `echo "<p>Trang đang được xây dựng...</p>"` bằng đoạn mã lệnh sau đây và chạy kiểm tra kết quả:

```

if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    if (!empty($_POST['quote']) && !empty($_POST['source'])) {
        include '../partials/db_connect.php';

        $query = "INSERT INTO quotes (quote, source, favorite) VALUES (?, ?, ?)";

        try {
            $sth = $pdo->prepare($query);
            $sth->execute([
                $_POST['quote'],
                $_POST['source'],
                + (isset($_POST['favorite']))
            ]);
        } catch (PDOException $e) {
            $pdo_error = $e->getMessage();
        }

        if ($sth && $sth->rowCount() == 1) {
            echo '<p>Trích dẫn của bạn đã được lưu trữ.</p>';
        } else {
            $error_message = 'Không thể lưu trữ trích dẫn';
            $reason = $pdo_error ?? 'Không rõ nguyên nhân';
            include '../partials/show_error.php';
        }
    } else {
        $error_message = 'Hãy gõ vào cả Trích dẫn và Nguồn của nó!';
        include '../partials/show_error.php';
    }
}

```

Biến **\$_SERVER** là biến được tạo sẵn chứa các thông tin về môi trường thực thi phía server. Chúng ta có thể dùng giá trị của **\$_SERVER['REQUEST_METHOD']** để xác định yêu cầu đang được xử lý là yêu cầu dạng GET hay POST.

+ (isset(\$_POST['favorite'])) chuyển đổi giá trị boolean sang số nguyên (TRUE = 1, FALSE = 0).

- **edit_quote.php**: thay vào chỗ câu lệnh echo "<p>Trang đang được xây dựng...</p>" bằng đoạn mã lệnh sau đây và chạy kiểm tra kết quả:

```

include '../partials/db_connect.php';

if (isset($_GET['id']) && is_numeric($_GET['id']) && ($_GET['id'] > 0)) {
    $query = "SELECT quote, source, favorite FROM quotes WHERE id={$_GET['id']}";

    try {
        $sth = $pdo->query($query);
        $row = $sth->fetch();
    } catch (PDOException $e) {
        $pdo_error = $e->getMessage();
    }

    if (!empty($row)) {
        echo '<form action="edit_quote.php" method="post">
            <p><label>Trích dẫn <textarea name="quote" rows="5" cols="30">' .
                htmlspecialchars($row['quote']) . '</textarea></label></p>
            <p><label>Nguồn <input type="text" name="source" value="' .
                htmlspecialchars($row['source']) . '"></label></p>
            <p><label>Đây là trích dẫn được yêu thích?
            <input type="checkbox" name="favorite" value="yes"' .
                ($row['favorite'] == 1 ? 'checked' : '') . '</p>

            <input type="hidden" name="id" value="' . $_GET['id'] . '">
            <p><input type="submit" name="submit" value="Cập nhật Trích dẫn này!"></p>
        </form>';

    } else {
        $error_message = 'Không thể lấy được trích dẫn này';
        $reason = $pdo_error ?? 'Không rõ nguyên nhân';
        include '../partials/show_error.php';
    }
}

```

```

} elseif (isset($_POST['id']) && is_numeric($_POST['id']) && ($_POST['id'] > 0)) {
    if (!empty($_POST['quote']) && !empty($_POST['source'])) {
        $query = "UPDATE quotes SET quote=?, source=?, favorite=? WHERE id=?";

        try {
            $sth = $pdo->prepare($query);
            $sth->execute([
                $_POST['quote'],
                $_POST['source'],
                (isset($_POST['favorite'])) ? 1 : 0,
                $_POST['id']
            ]);
            echo '<p>Trích dẫn này đã được cập nhật.</p>';
        } catch (PDOException $e) {
            $error_message = 'Không thể cập nhật Trích dẫn này';
            $reason = $e->getMessage();
            include '../partials/show_error.php';
        }
    } else {
        $error_message = 'Hãy gõ vào cả Trích dẫn và Nguồn của nó!';
        include '../partials/show_error.php';
    }
} else {
    include '../partials/show_error.php';
}

include '../partials/footer.php';

```

- **delete_quote.php:** thay vào chỗ câu lệnh echo "<p>Trang đang được xây dựng...</p>" bằng đoạn mã lệnh sau đây và chạy kiểm tra kết quả:

```
include '../partials/db_connect.php';

if (isset($_GET['id']) && is_numeric($_GET['id']) && ($_GET['id'] > 0)) {
    $query = "SELECT quote, source, favorite FROM quotes WHERE id={$_GET['id']}";

    try {
        $sth = $pdo->query($query);
        $row = $sth->fetch();
    } catch (PDOException $e) {
        $pdo_error = $e->getMessage();
    }

    if (!empty($row)) {
        echo '<form action="delete_quote.php" method="post">
        <p>Bạn có chắc là muốn xóa trích dẫn này?</p>
        <div><blockquote>' . htmlspecialchars($row['quote']) .
        '</blockquote>- ' . htmlspecialchars($row['source']);

        if ($row['favorite'] = 1) {
            echo ' <strong>Yêu thích!</strong>';
        }

        echo '</div><br><input type="hidden" name="id" value="' . $_GET['id'] . '">
        <p><input type="submit" name="submit" value="Xóa Trích dẫn này!"></p>
        </form>';
    } else {
        $error_message = 'Không thể lấy được trích dẫn này';
        $reason = $pdo_error ??= 'Không rõ nguyên nhân';
        include '../partials/show_error.php';
    }
}

} elseif (isset($_POST['id']) && is_numeric($_POST['id']) && ($_POST['id'] > 0)) {
    $query = "DELETE FROM quotes WHERE id={$_POST['id']} LIMIT 1";

    try {
        $sth = $pdo->query($query);
    } catch (PDOException $e) {
        $pdo_error = $e->getMessage();
    }

    if ($sth && $sth->rowCount() == 1) {
        echo '<p>Trích dẫn đã bị xóa.</p>';
    } else {
        $error_message = 'Không thể xóa trích dẫn này';
        $reason = $pdo_error ??= 'Không rõ nguyên nhân';
        include '../partials/show_error.php';
    }
} else {
    include '../partials/show_error.php';
}

include '../partials/footer.php';
```