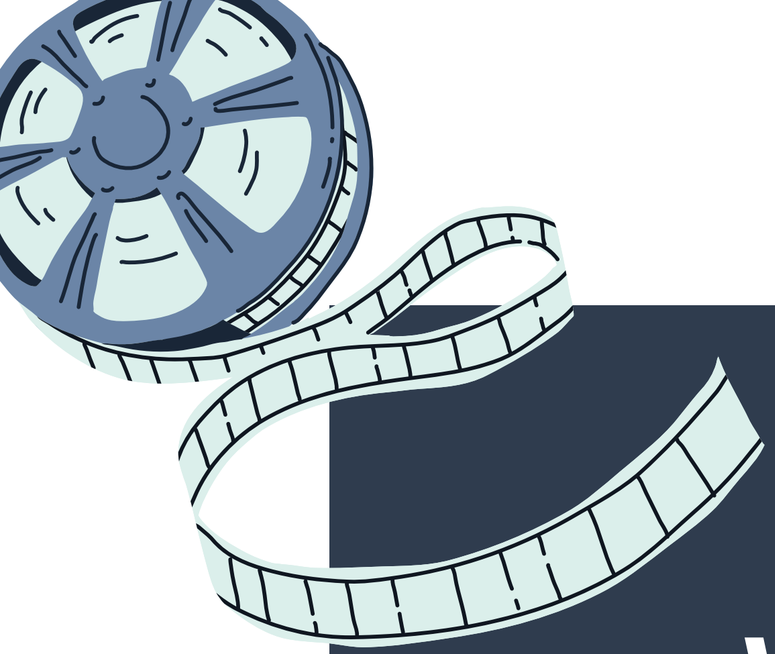
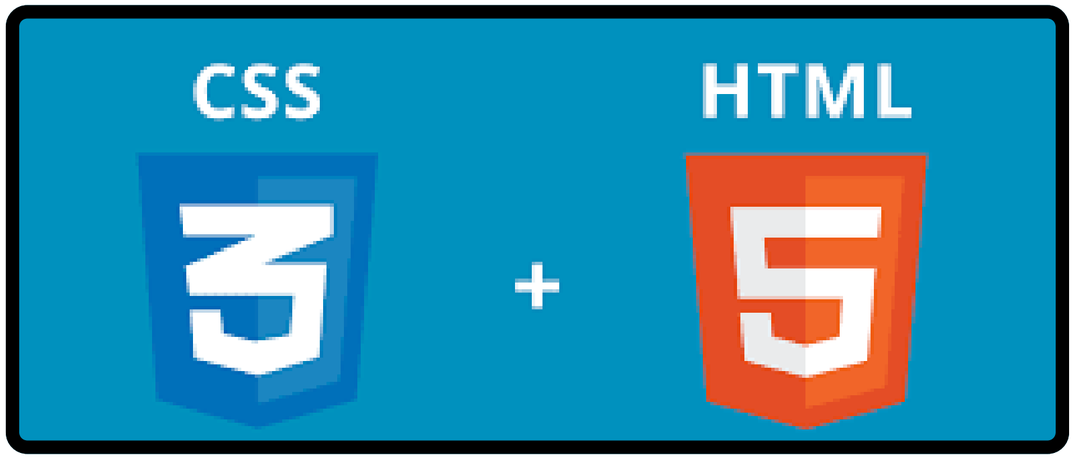
Web Phim



CÔNG NGHỆ

Backend: PHP + MySQL

Frontend: HTML/CSS



TÍNH NĂNG CHÍNH CỦA WEBSITE

Trang quản trị (admin)

- Giao diện thống nhất với trang người dùng
- Vào trang quản trị
- Quản lý phim: thêm / sửa / xóa phim
- Quản lý Nạp
- Quản lý bình luận: xóa bình luận không phù hợp

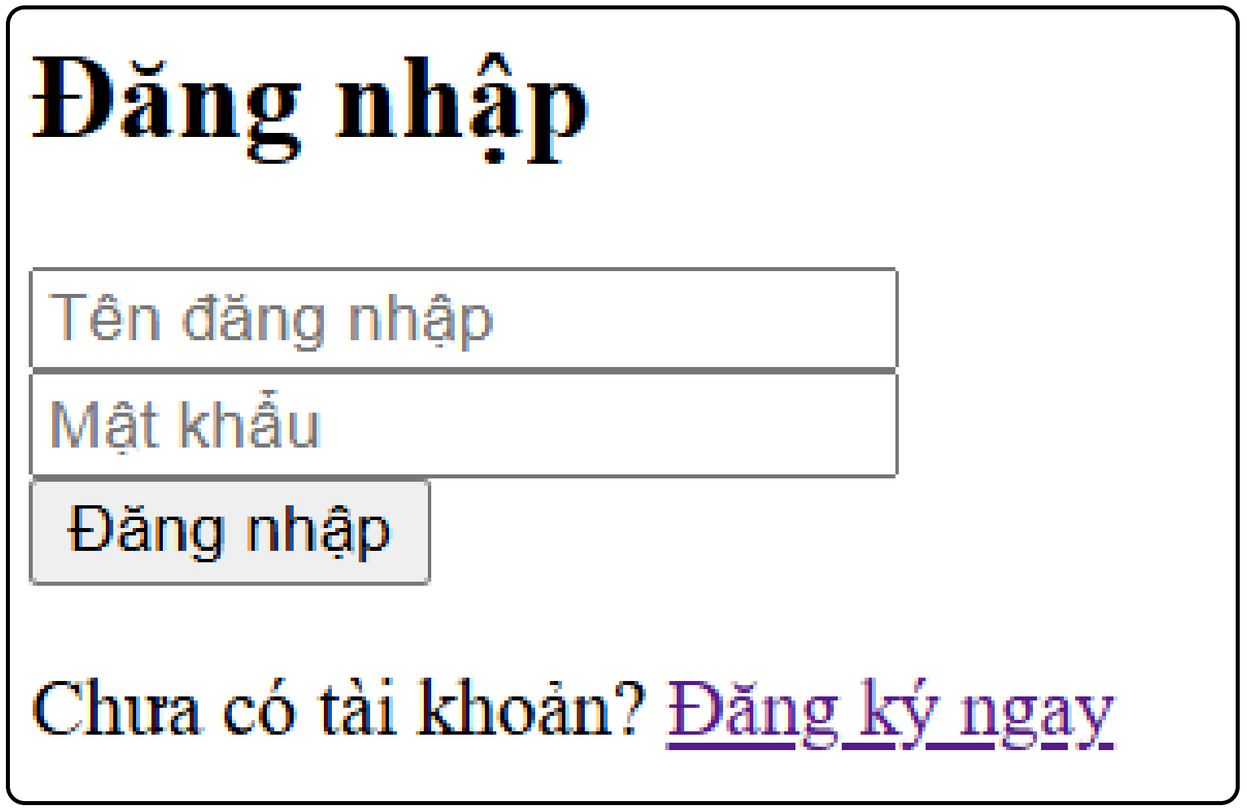
Trang người dùng (user)

- Đăng ký / Đăng nhập
- Trang chủ (Xem danh sách phim)
- Tìm kiếm phim theo tên
- Xem chi tiết phim, danh sách các tập
- Mua phim vip
- Bình luận phim
- VÍ, Trang hồ sơ

Trang người dùng (user)

Đăng ký / Đăng nhập

Giao diện trang Đăng nhập



code login.php

Truy vấn người dùng theo username

```php
$username = addslashes(trim($_POST['username']));
$sql = "SELECT * FROM users WHERE username = '$username'";
$result = mysqli_query($conn, $sql);
```

Nhận dữ liệu từ form đăng nhập

```php
if (isset($_POST['login'])) {
    $username = trim($_POST['username']);
    $password = $_POST['password'];
```

Lưu thông tin đăng nhập vào session

```php
$_SESSION['user_id'] = $user['id'];
$_SESSION['username'] = $user['username'];
$_SESSION['role'] = $user['role'];
header("Location: ../pages/index.php");
```

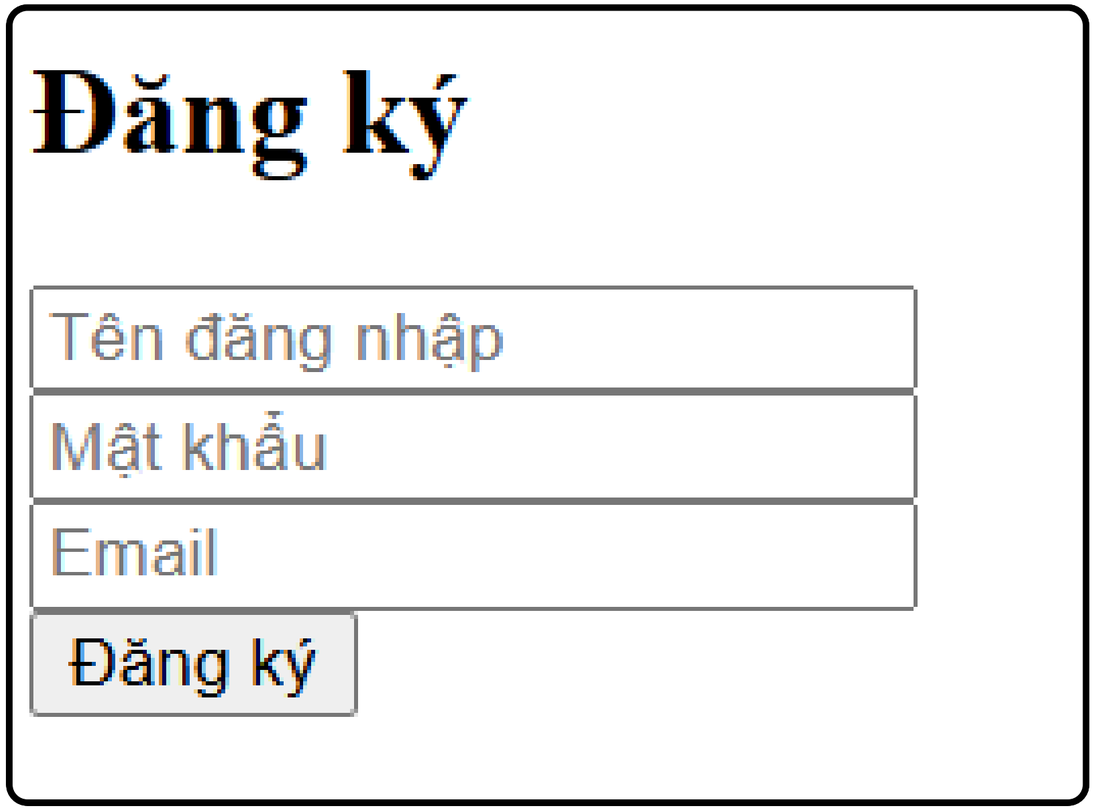
Trường hợp không tìm thấy tài khoản

```php
} else {
    $error = "⚠️ Không tìm thấy người dùng.";
}
```

Trang người dùng (user)

Đăng ký / Đăng nhập

Giao diện trang Đăng ký



code register.php

Nhận thông tin đăng ký:

- Lấy dữ liệu từ form: username, password, email.

```php
$username = trim($_POST['username']);
$password = trim($_POST['password']);
$email = trim($_POST['email']);
```

Kiểm tra trùng tài khoản:

- Dùng prepared statement để kiểm tra:
- Trùng username
- Hoặc email đã tồn tại với vai trò user

```php
$stmt = $conn->prepare("SELECT * FROM users WHERE username = ?
OR (email = ? AND role = ?)");
$stmt->bind_param("sss", $username, $email, $role);
```

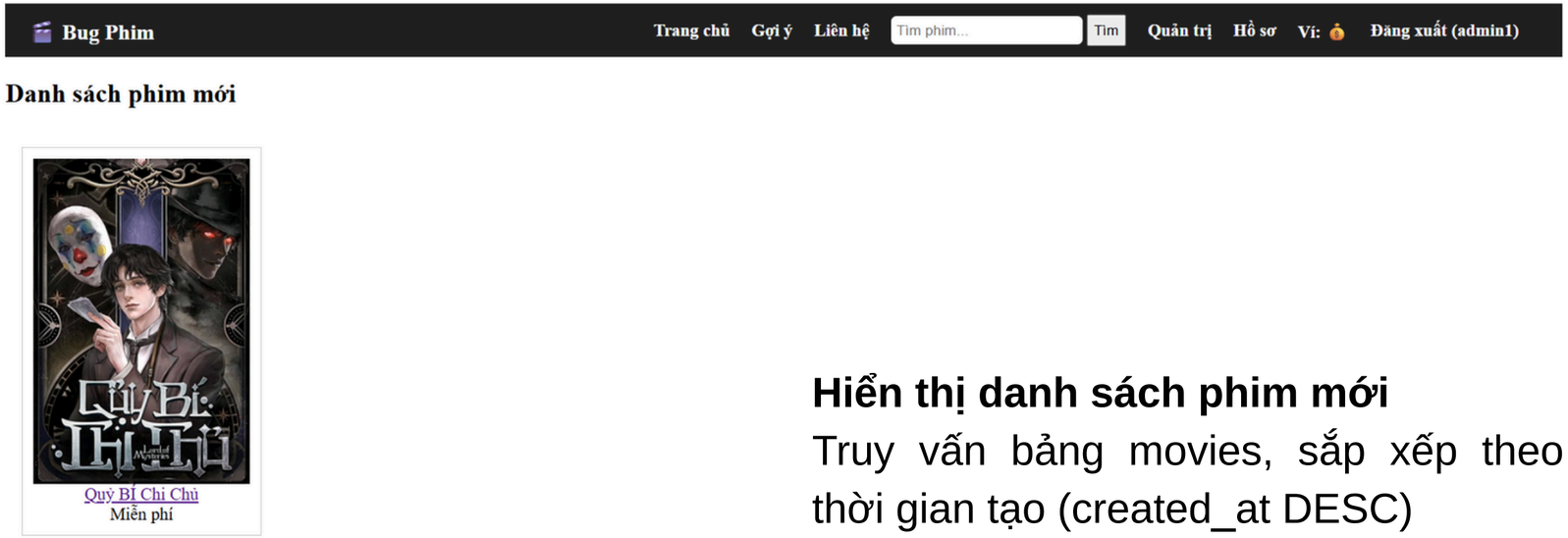
Mã hóa mật khẩu và lưu vào CSDL:

- Sử dụng password_hash() để bảo mật mật khẩu.
- Chèn người dùng mới vào bảng users.

```php
$hashed_password = password_hash($password, PASSWORD_DEFAULT);
$stmt = $conn->prepare("INSERT INTO users (username, password, email, role)
VALUES (?, ?, ?, ?)");
$stmt->bind_param("ssss", $username, $hashed_password, $email, $role);
```

Trang người dùng (user)

Trang chủ (Xem danh sách phim)



Hiển thị danh sách phim mới

Truy vấn bảng movies, sắp xếp theo thời gian tạo (created_at DESC)

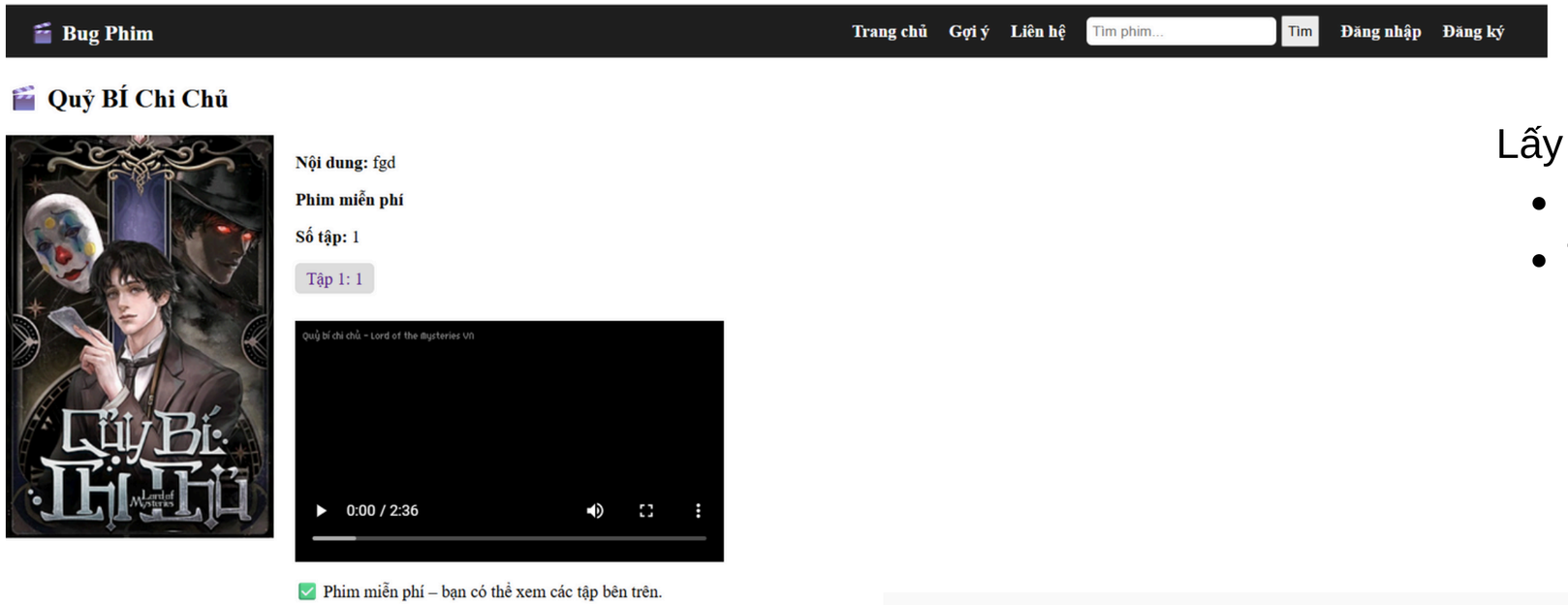
Mỗi phim hiển thị:

- Ảnh poster
- Tên phim
- Thông báo là phim VIP (hiện giá) hoặc phim miễn phí
- Link đến trang movie.php?id=..

```php
$movies = mysqli_query($conn, "SELECT * FROM movies ORDER BY created_at DESC");
```

Trang người dùng (user)

Xem chi tiết phim



code movie.php

Lấy và hiển thị thông tin phim

- Nhận movie_id từ URL ($_GET['id'])
- Truy vấn bảng movies để lấy thông tin:
  - Tiêu đề
  - Mô tả
  - Ảnh poster
  - Trailer (nếu có)
  - Phân loại: thường hay VIP (trả phí)

```
$result = mysqli_query($conn, "SELECT * FROM movies WHERE id = $movie_id");
```

Bình luận phim

- Hiển thị tất cả bình luận từ bảng comments (tập 0 là bình luận chung phim)
- Người dùng đăng nhập mới được phép gửi bình luận

```
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_POST['comment']) && $user_id
    ...
    mysqli_query($conn, "INSERT INTO comments ...");
```

Trang người dùng (user)

Xem chi tiết phim

Phim miễn phí

✅ Phim miễn phí – bạn có thể xem các tập bên trên.

Phim vip

🔒 Đăng nhập để mua phim.

code movie.php

Xem tập phim

- Lấy danh sách tập từ bảng episodes
- Nếu phim VIP → xem được khi đã mua
- Nếu phim miễn phí → hiển thị link tất cả các tập

```
$result = mysqli_query($conn, "SELECT * FROM movies WHERE id = $movie_id");
```

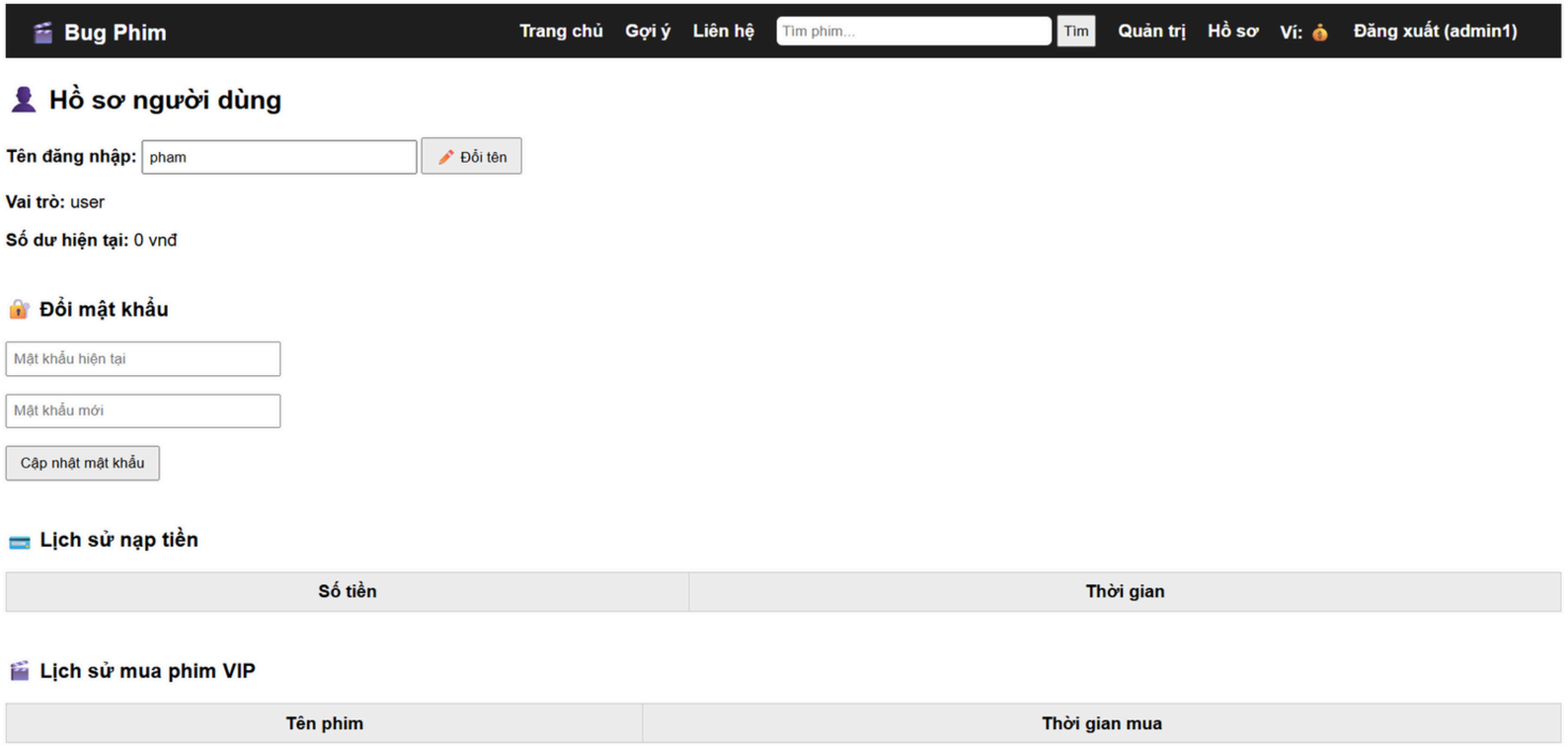
Xem phim VIP

- Nếu chưa mua:
  - Hiển thị nút "💰 Mua phim"
  - Kiểm tra số dư ví
  - Trừ tiền, lưu giao dịch vào bảng purchases

```
if (isset($_POST['buy']) && $user_id && !$has_bought) {
    ...
    mysqli_query($conn, "INSERT INTO purchases ...");
    mysqli_query($conn, "UPDATE wallets SET balance = ...");
}
```

Trang người dùng (user)

VÍ, Trang hồ sơ



Chức năng

Xem thông tin hồ sơ

Hiển thị:

Tên đăng nhập

Vai trò: user hoặc admin

Số dư tài khoản

Đổi tên người dùng

Cho phép người dùng (hoặc admin) đổi tên tài khoản.

Nếu người dùng đang chỉnh sửa chính mình, cập nhật cả $_SESSION['username']

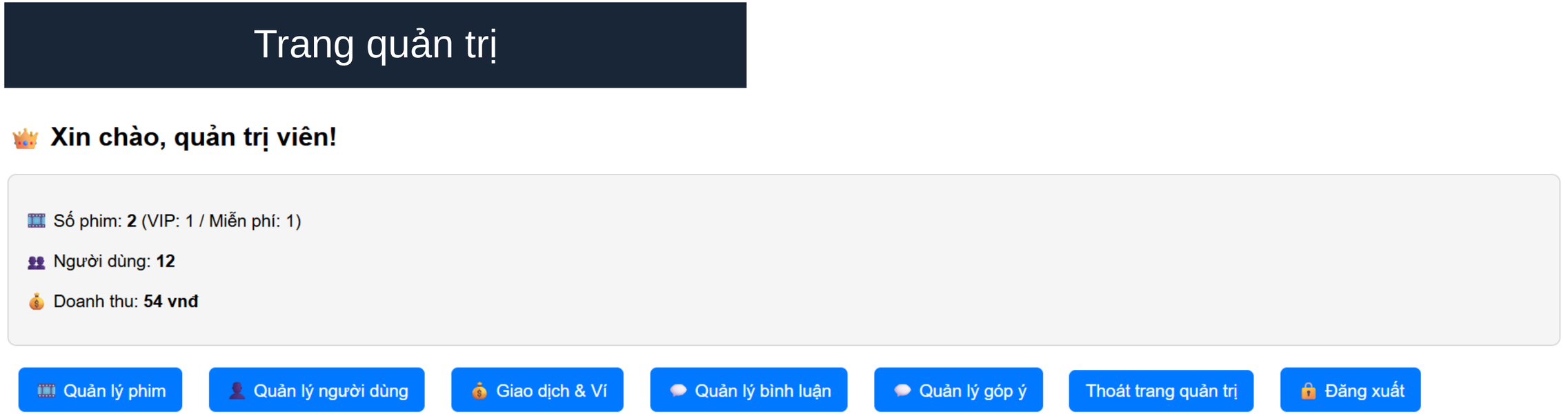
Lịch sử nạp tiền

Hiển thị các khoản tiền đã nạp, thời gian nạp.

Lịch sử mua phim

Hiển thị tên phim VIP và thời gian mua của người dùng.

Trang quản trị (admin)



chức năng

Kiểm tra quyền truy cập

Chỉ cho phép admin truy cập.

Nếu người dùng chưa đăng nhập hoặc không phải admin → chặn truy cập.

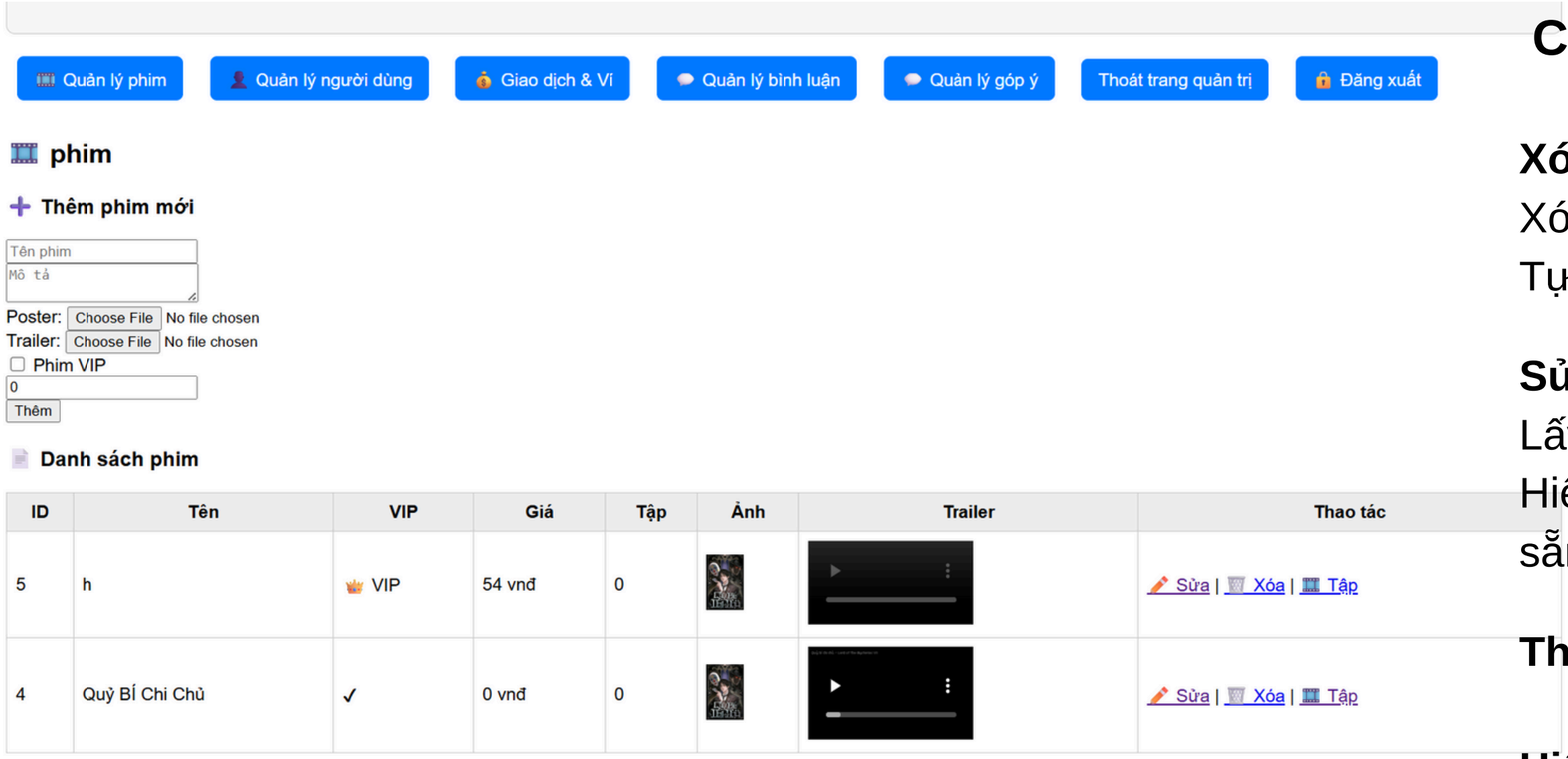
Thống kê tổng quan

Dữ liệu được truy vấn từ cơ sở dữ liệu

Điều hướng quản trị

Trang quản trị (admin)

Quản lý phim



Chức năng

Xóa phim

Xóa phim khỏi CSDL

Tự động load lại trang

Sửa phim

Lấy thông tin phim cần sửa

Hiển thị form cập nhật, kèm thông tin sẵn có

Thêm phim mới

Hiển thị danh sách phim

Trang quản trị (admin)

Quản lý bình luận

Chức năng

Xóa bình luận

Khi admin bấm xóa, bình luận tương ứng sẽ bị xóa và reload lại trang.

```php
if (isset($_GET['delete'])) {
    $id = intval($_GET['delete']);
    mysqli_query($conn, "DELETE FROM comments WHERE id = $id");
    header("Location: comment_manage.php");
    exit();
}
```

Bảng bình luận

Bộ lọc bình luận

Từ khóa:

Phim:

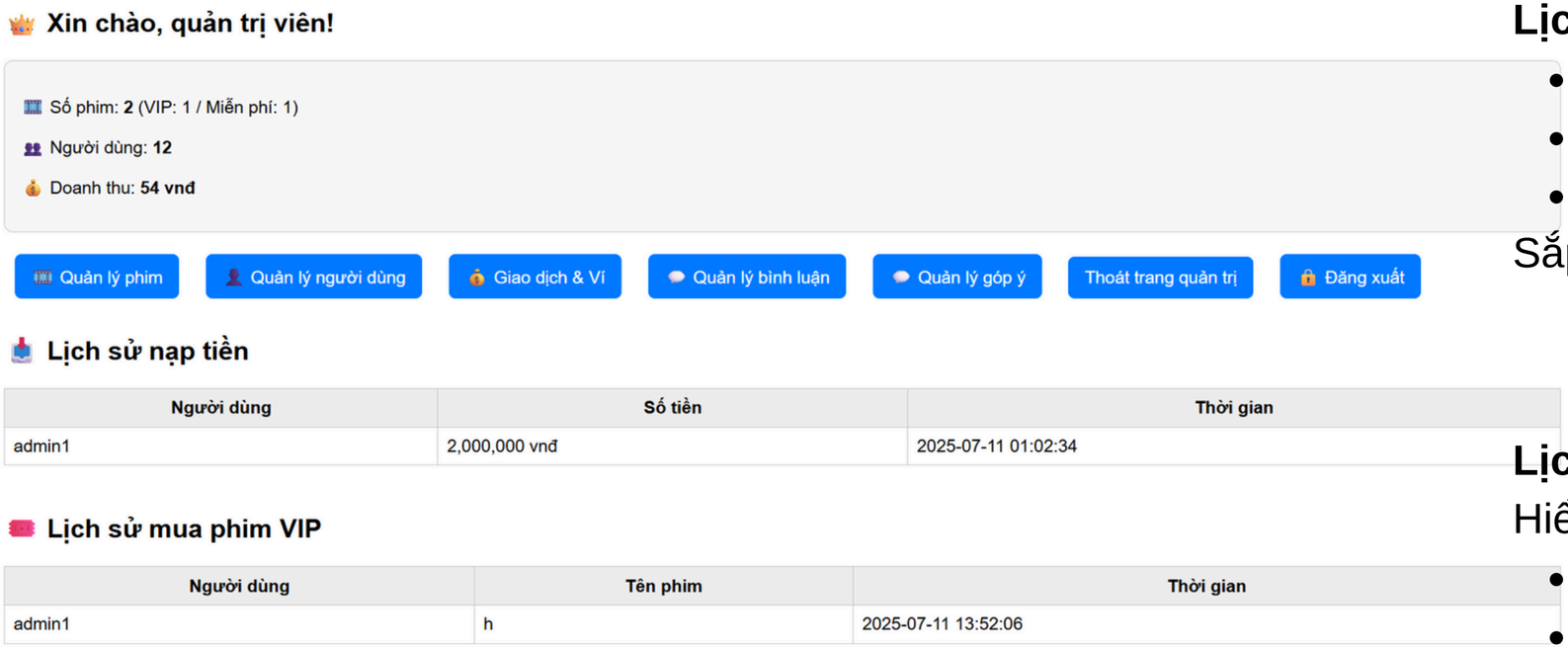
Chỉ hiện bình luận thuộc 1 phim cụ thể.

Nếu movie_id = 0 sẽ hiển thị tất cả.

```php
$movie_id = $_GET['movie_id'] ?? 0;
$sql .= " AND comments.movie_id = $movie_id";
```

Trang quản trị (admin)

Quản lý nạp



Chức năng

Lịch sử nạp tiền Hiển thị danh sách:

- Người nạp
- Số tiền đã nạp
- Thời gian nạp

Sắp xếp theo thời gian gần nhất.

Lịch sử mua phim

Hiển thị danh sách:

- Người mua
- Số tiền đã mua
- Thời gian mua

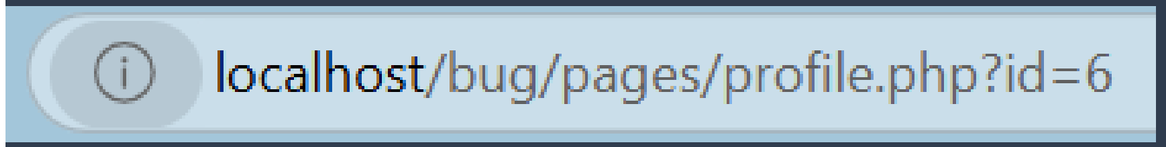
Sắp xếp theo thời gian gần nhất.

Lỗi

Mã	Tên lỗi	Vị trí cụ thể	Mô tả lỗi
A01	Broken Access Control *(Kiểm soát truy cập bị phá vỡ)*	profile.php	Người dùng có thể thay đổi ?id=... để xem hồ sơ người khác, kể cả khi không có quyền.
A02	Cryptographic Failures *(Thiếu mã hóa an toàn)*	login.php, users table	Mật khẩu người dùng lưu dưới dạng MD5 không muối (md5('password')) – dễ bị dò bằng từ điển hoặc rainbow table.
A03	Injection *(Chèn mã độc)*	login.php	Không sử dụng Prepared Statements khi xử lý đầu vào, có thể bị tấn công SQL Injection thông qua username, search (VD: ' OR '1'='1 → đăng nhập không cần mật khẩu).
A07	Identification and Authentication Failures (Xác thực không đúng cách)	login.php	Đăng nhập không giới hạn số lần thử – dễ bị tấn công brute force.
A08	Software and Data Integrity Failures *(Không kiểm soát tính toàn vẹn)*	episode_manage.php	Cho phép upload tập phim .mp4 mà không kiểm tra MIME, có thể upload mã độc (VD: .php.mp4, shell.php), dễ bị chiếm quyền điều khiển máy chủ.

Lỗi

Broken Access Control (Kiểm soát truy cập bị phá vỡ)



Có thể xem được hồ sơ của người khác bằng cách thay đổi id trên link

```
$logged_user_id = $_SESSION['user_id'];
$requested_id = isset($_GET['id']) ? intval($_GET['id']) : $logged_user_id;

// Nếu không phải admin, chỉ được xem hồ sơ của chính mình
if ($_SESSION['role'] != 'admin' && $requested_id != $logged_user_id) {
    echo "❌ Không có quyền truy cập hồ sơ người khác.";
    exit();
}
```

Lỗi

Cryptographic Failures (Thiếu mã hóa an toàn)

Lỗi: Mật khẩu lưu bằng MD5 → dễ bị bẻ khóa.

```
// Khi đăng ký
$hashed = password_hash($password, PASSWORD_DEFAULT);
mysqli_query($conn, "INSERT INTO users (username, password) VALUES ('$username', '$hashed')");
```

Lỗi

Injection (Chèn mã độc)

Lỗi: Không dùng câu lệch chuẩn → dễ bị SQL Injection.

Ví dụ:

$sql = "SELECT * FROM users WHERE username = '$username' AND password = '$password'"

Nếu người dùng nhập:

- Username: ' OR '1'='1
- Password: bất kỳ

SELECT * FROM users WHERE username = '' OR '1'='1' AND password = '';

```
$stmt = $conn->prepare("SELECT * FROM users WHERE username = ?");
$stmt->bind_param("s", $username);
$stmt->execute();
```

Đoạn mã này sử dụng Prepared Statements với mysqli_prepare() và bind_param(), giúp ngăn chặn SQL Injection bằng cách tách biệt dữ liệu đầu vào ($username) khỏi câu lệnh SQL.

Lỗi

Identification and Authentication Failures (Xác thực không đúng cách)

Lỗi: Cho đăng nhập sai không giới hạn số lần

Giới hạn số lần đăng nhập sai, ví dụ: 5 lần trong 15 phút.
Ghi lại số lần sai vào session hoặc database.

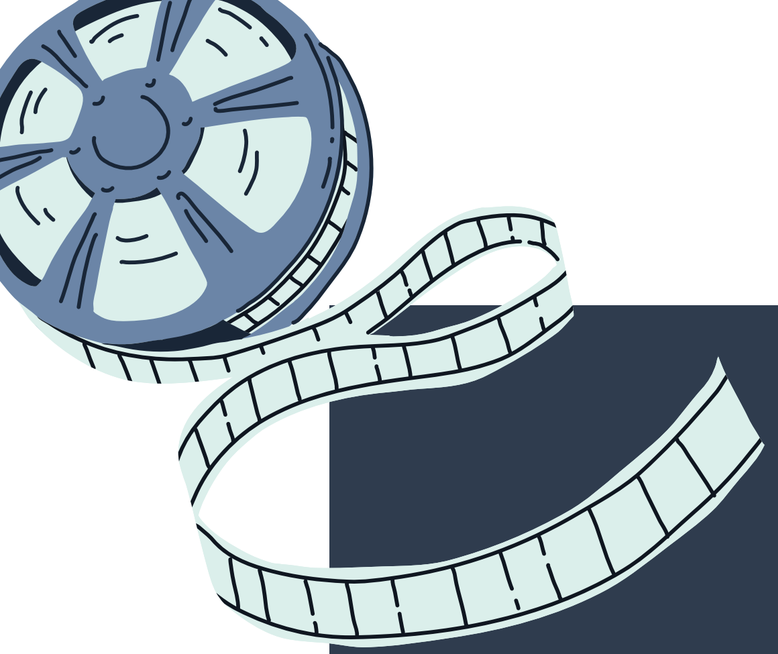
```
if (!isset($_SESSION['login_attempts'])) $_SESSION['login_attempts'] = 0;
if ($_SESSION['login_attempts'] >= 5) {
    echo " Quá nhiều lần đăng nhập sai. Hãy thử lại sau 15 phút.";
    exit();
}
```

Lỗi

Software and Data Integrity Failures (Không kiểm soát tính toàn vẹn)

Lỗi: Upload .mp4 nhưng không kiểm tra loại file → dễ upload mã độc .php.mp4.

```
$allowed_types = ['video/mp4'];
$finfo = finfo_open(FILEINFO_MIME_TYPE);
$mime_type = finfo_file($finfo, $_FILES['episode']['tmp_name']);
finfo_close($finfo);
if (!in_array($mime_type, $allowed_types)) {
    echo "Chỉ cho phép tập phim .mp4.";
    exit();
}
```



the end