

Matias Armesto, Ruby Bautista

---

# KDrama Website

IS 4460 Final Project

# Authentication/Login

- Password verification and sanitization
- Implementation details (code snippets from login.php)
- Libraries used (e.g., password\_hash, password\_verify)

```
<?php
require_once 'header.html';
require_once 'dbconnection.php';
require_once 'sanitize.php';
require_once 'user.php';

if (session_status() === PHP_SESSION_NONE) {
    session_start();
}

$conn = new mysqli($hn, $un, $pw, $db);
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

if (isset($_POST['username']) && isset($_POST['password'])) {
    $tmp_username = sanitize($conn, $_POST['username']);
    $tmp_password = sanitize($conn, $_POST['password']);

    $query = "SELECT password FROM users WHERE username = ?";
    $stmt = $conn->prepare($query);
    $stmt->bind_param('s', $tmp_username);
    $stmt->execute();
    $stmt->store_result();
```

```
if ($stmt->num_rows > 0) {
    $stmt->bind_result($passwordFromDB);
    $stmt->fetch();

    if (password_verify($tmp_password, $passwordFromDB)) {
        $_SESSION['user'] = new User($tmp_username); // Store username in session
        error_log("Login successful for user: $tmp_username");
        header("Location: viewdramalist.php");
        exit();
    } else {
        $error = "Invalid username or password";
        error_log("Invalid password for user: $tmp_username");
    }
} else {
    $error = "Invalid username or password";
    error_log("Invalid username: $tmp_username");
}

$stmt->close();
```

# Session Management

- Session creation and management (code snippets from `checksession.php`)
- Session destruction and logout (code snippets from `logout.php`)

```
<?php

require_once 'user.php'; // Ensure this file includes the User class definition

// Initialize session if not already started
if (session_status() === PHP_SESSION_NONE) {
    session_start();
}

// Check if user is logged in
if (!isset($_SESSION['user'])) {
    error_log("Session data is not a User object. Type: " . gettype($_SESSION['user']));
    header("Location: login.php");
    exit();
}

// Retrieve user and roles
$user = $_SESSION['user'];
$user_roles = $user->getRoles();
$username = $user->username;

// Define or retrieve $page_roles
// $page_roles = ['user', 'admin'];
$found = false;

// Check if user has one of the required roles
foreach ($user_roles as $urole) {
    if (in_array($urole, $page_roles)) {
        $found = true;
        break;
    }
}

if (!$found) {
    error_log("User $username does not have appropriate roles, unauthorized entry");
    echo "Unauthorized entry";
    exit();
} else {
    error_log("User $username has appropriate roles, access granted");
}
```

```
<?php

session_start();

function destroy_session_and_data() {
    $_SESSION = array();
    if (ini_get("session.use_cookies")) {
        $params = session_get_cookie_params();
        setcookie(session_name(), '', time() - 42000, $params["path"], $params["domain"], $params["secure"], $params["httponly"]);
    }
    session_destroy();
}

destroy_session_and_data();

header("Location: login.php");
exit();
?>
```



# User Use Cases

## CRUD for User:

- **Create:** Users can register for a new account by providing their details (username, password, email, etc.).
- **Read:** Users can view their account details, such as profile information.
- **Update:** Users can update their profile information, including changing their password, email, or other personal details.
- **Delete:** Users can delete their account if they no longer wish to use the service.

## View Drama Details:

- Users can browse a list of dramas available on the platform.
- For each drama, users can view detailed information, including the title, release date, genre, rating, and image.
- Users can also see the list of actors and directors involved in the drama and any awards the drama has won.

## View Actor Details:

- Users can browse a list of actors featured in the dramas.
- For each actor, users can view detailed information including the actor's name and date of birth

## CRUD for Shopping Cart/User

**Create:** Users can add dramas to their shopping cart by selecting the dramas they wish to purchase and specifying the quantity for each drama.

**Read:** Users can view the contents of their shopping cart, including the list of dramas added, their quantities, prices, and the total cost.

**Update:** Users can update the contents of their shopping cart by changing the quantity of dramas or removing items they no longer wish to purchase.

**Delete:** Users can clear their shopping cart by removing all items if they decide not to make a purchase.

# Admin Use Cases

## All Customer Use Cases:

- Admins can perform all actions that customers can, including viewing drama and actor details, and purchasing dramas.

## CRUD for Drama:

- **Create:** Admins can add new dramas to the platform by providing necessary details like title, release date, genre, rating, and associated director.
- **Read:** Admins can view detailed information about any drama, including its cast, awards, and user reviews.
- **Update:** Admins can update drama details, such as changing the title, release date, genre, rating.
- **Delete:** Admins can remove dramas from the platform if they are no longer available or relevant.

## CRUD for Actor:

- **Create:** Admins can add new actors to the platform by providing their details such as name, date of birth, and biography.
- **Read:** Admins can view detailed information about any actor, including their filmography and roles in various dramas.
- **Update:** Admins can update actor details, such as changing their name, date of birth, or biography.
- **Delete:** Admins can remove actors from the platform if they are no longer relevant or available.

## CRUD for Director:

- **Create:** Admins can add new directors to the platform by providing their details such as name.
- **Read:** Admins can view information about who directed the drama.
- **Update:** Admins can update director details, such as changing their name.
- **Delete:** Admins can remove directors from the platform if they are no longer relevant or available.

## CRUD for Awards:

- **Create:** Admins can add new awards to dramas by providing details such as award name and associated drama.
- **Read:** Admins can view detailed information about any award, including the dramas that have won the award.
- **Update:** Admins can update award details, such as changing the award name or associated drama.
- **Delete:** Admins can remove awards from the platform if they are no longer relevant or available.

## CRUD for Shopping Cart

- **Create:** Admins can add items to cart, can specify quantities.
- **Read:** Admins can view the contents of carts, including the list of dramas, quantities, prices, and the total cost.
- **Update:** Admins can update the quantity amount in the cart.
- **Delete:** Admins can clear the contents of carts.

# Generate Reports

## List of Transactions:

- A detailed report of all transactions done on the platform.
- Includes details such as transaction ID, user ID, transaction amount, date of transaction, and user details.
- Helps in tracking and auditing financial activities on the platform.