Konferenční systém – správa článků a recenzního řízení

Matěj Šulič

Zadání práce a účel aplikace

Cílem semestrální práce bylo vytvořit plně funkční webovou aplikaci, která slouží pro správu konferenčních článků, jejich recenzního řízení a administraci uživatelů.
Aplikace umožňuje tři role uživatelů:

- **Autor** – může nahrávat vlastní články, upravovat je, sledovat stav recenzního řízení.
- **Recenzent** – hodnotí přiřazené články, udává technické, odborné a jazykové skóre a píše slovní komentář.
- **Administrátor** – spravuje uživatele, články, přiděluje recenzenty, mění stav článků a má přehled nad celým procesem.

Aplikace je inspirována jednoduchými CMT systémy (Conference Management Tools) a slouží jako demonstrační příklad MVC webové aplikace s datovým úložištěm, uživatelskými rolemi a víceúrovňovým workflow.

Použité technologie

Back-end

- **PHP 8+** – hlavní logika aplikace, MVC struktura, routování, validace, session management.
- **PDO (PHP Data Objects)** – bezpečná komunikace s databází, prepared statements pro ochranu proti SQL injection.
- **MySQL/MariaDB** – relační databázové úložiště, tabulky: users, articles, reviews.
- **Sessions** – správa uživatelských stavů (role, přihlášení).

Front-end

- **HTML5 & Bootstrap 5** – tvorba rozhraní, grid systém, responzivita.
- **CSS3 + vlastní styly** – úprava vzhledu, ikonky, barvy, rozložení.
- **JavaScript (minimálně)** – drobné interakce, potvrzení akcí.

Další technologie

- **MVC architektura** – oddělení logiky, dat a prezentace.
- **Prepared Statements + htmlspecialchars()** – ochrana proti SQL injection a XSS.

Každá část technologie je využita přímo v konkrétní části aplikace:

- MVC – řízení pohledů v `Controller.php`, `ArticleController.php`, `AdminController.php`.
- Bootstrap – tabulky článků, přihlašovací formulář, dashboard.
- PDO – všechny CRUD operace v modelech (UserModel, ArticleModel, ReviewModel).
- Ochrana XSS – všechny dynamické výpisy přes `htmlspecialchars()`.

Architektura aplikace

Aplikace používá **jednoduchý MVC architektonický vzor**:

Model (UserModel, ArticleModel, ReviewModel)

- Obsahuje logiku přístupu k databázi.
- Realizuje operace: registrace, login, vytvoření článku, recenze, změny stavů.
- Všechny SQL dotazy jsou implementovány pomocí **prepare + execute**, což zajišťuje bezpečnost.

Controller

- Ovládá logiku konkrétních stránek.
- Každý controller je spojený s jednou oblastí aplikace:
  - `AuthController` – login, registrace, odhlášení
  - `ArticleController` – nahrávání článků, úpravy, výpis seznamů
  - `ReviewController` – vyplnění recenzí
  - `AdminController` – dashboard, uživatelé, přiřazování recenzí
- V controlleru se načítají modely a předávají data do view.

View

- HTML šablony (*.phtml)
- Používají `htmlspecialchars()` pro bezpečný výpis dat.
- Bootstrap pro layout.

Popis hlavních složek

- **/Controllers** – zpracování požadavků, komunikace s modely a zobrazení odpovídajících pohledů.
- **/Models** – práce s databází, CRUD operace, validace dat.
- **/Views** – šablony stránek, HTML s vloženými PHP výpisy.
- **/Core** – základ aplikace: připojení k databázi a controller engine.
- **/public/uploads** – uložené PDF článků.

Bezpečnostní opatření

Aplikace splňuje požadavky na ochranu proti útokům:

Ochrana proti SQL Injection

- Všechny SQL dotazy používají **PDO prepared statements**, např.:

```
$stmt = $db->prepare("SELECT * FROM users WHERE username = :user");
$stmt->execute(['user' => $username]);
```

Ochrana proti XSS

- Každý dynamický výpis je ošetřen přes:

```
<?= htmlspecialchars($variable) ?>
```

Např. u názvu článku, uživatelského jména, komentáře recenzenta atd.

Ochrana hesel

- Hesla nejsou ukládána v plaintextu.
- Používám:

```
password_hash($password, PASSWORD_BCRYPT)
```

Závěr

Aplikace splňuje požadavky zadání předmětu KIV/WEB.
Podporuje správu uživatelů, článků, recenzí, 3 uživatelské role, bezpečné přihlášení, nahrávání PDF, jednoduchý administrační panel a veřejný seznam publikovaných článků.

Celý projekt je strukturován v přehledném MVC modelu a dodržuje bezpečnostní standardy pro práci s databází a uživatelskými vstupy.