

TECHNICKÁ DOKUMENTACE — NESTLYHOMES

Autor: Ivan Shcherbatiuk

1. ARCHITEKTURA A TECHNOLOGIE

Projekt je implementován jako webová aplikace pro inzerci a pronájem nemovitostí. Aplikace je postavena na klasickém technologickém zásobníku **LAMP** (Linux, Apache, MySQL, PHP) a dodržuje principy čistého kódu bez použití externích frameworků (tzv. "Vanilla" řešení).

Použité technologie:

- **Backend:** Nativní PHP 8.x (využívá striktní typování `declare(strict_types=1)`).
- **Databáze:** MySQL (komunikace přes rozhraní PDO s využitím *Prepared Statements*).
- **Frontend:** HTML5 (sémantické), CSS3 (Flexbox/Grid, responzivní design, tiskové styly), Vanilla JavaScript (ES6+).
- **Návrhový vzor:** MVC (Model-View-Controller). Aplikace je strukturována do logických modulů, kde jsou striktně odděleny:
 - **Model (*_model.inc.php):** Přímá komunikace s databází.
 - **View (*_view.inc.php):** Generování HTML výstupu.
 - **Controller (*_contr.inc.php):** Validace vstupů a aplikační logika.
 - **Router/Handler (*.inc.php):** Zpracování formulářů a přesměrování.

2. DATOVÉ SCHÉMA

Data jsou uložena v relační databázi MySQL. Schéma se skládá ze tří hlavních entit propojených relacemi 1:N. Integrita dat je zajištěna cizími klíči s kaskádovým mazáním (ON DELETE CASCADE).

A. Tabulka users

Uchovává údaje o registrovaných uživateli a administrátorech.

- **Atributy:** id (PK), firstname, surname, email (Unique), pwd (Hash), role ('user'/'admin'), created_at.
- **Role:** Sloupec role určuje oprávnění (běžný uživatel vs. administrátor).

B. Tabulka listings

Hlavní entita reprezentující inzerát nemovitosti.

- **Atributy:** id (PK), user_id (FK -> users), praha (Obvod 1-10), district (Čtvrť), price, area, layout (Dispozice), listing_description, created_at.
- **Vazba:** Inzerát je vázán na tvůrce. Při smazání uživatele se smažou i jeho inzeráty.

C. Tabulka listing_images

Uchovává cesty k nahraným fotografiím.

- **Atributy:** id (PK), listing_id (FK -> listings), image_path.
- **Ukládání:** V DB je pouze název souboru (např. listing_5_uniqueID.jpg). Fyzické soubory jsou ve složce uploads/.

3. SERVEROVÁ ČÁST (BACKEND)

Aplikace je členěna do adresářů podle funkčních celků.

3.1. Hlavní stránka a Vyhledávání (mainpage/)

- **index.php:** Vstupní bod. Inicializuje session a renderuje základní rozložení.
- **includes/ajax_load_listings.php:** Handler pro asynchronní požadavky (AJAX). Přijímá filtry (cena, lokalita, řazení), dotazuje se databáze a vrací HTML fragment se seznamem bytů.
- **Dynamické SQL:** Funkce setConditionForQuery dynamicky sestavuje podmínky WHERE na základě vyplněných filtrů, což umožňuje kombinovat libovolná kritéria.

3.2. Správa inzerátů (newlisting/, editlisting/, deletelisting/)

- **Vytvoření (newlisting):**
 - Implementuje upload souborů s kontrolou MIME typu (finfo) a velikosti.
 - **Zpracování obrazu:** Skript image_resize.inc.php využívá knihovnu **GD** k automatickému zmenšení a optimalizaci nahraných fotografií (zachování poměru stran).
- **Úprava (editlisting):** Formulář je předvyplněn stávajícími daty z DB. Uživatel může měnit texty a spravovat fotografie.
- **Mazání (deletelisting):** Bezpečné smazání záznamu z DB a fyzické odstranění souborů ze serveru.

3.3. Uživatel a Autentizace (login/, registration/, myprofile/)

- **Registrace/Login:** Validace vstupů (regex pro jména, formát emailu). Hesla jsou hashována algoritmem **Bcrypt** (password_hash).
- **Profil:** Uživatel může měnit své údaje (editprofile.php), heslo (changepwd.php) nebo smazat účet.
- **Session Management:** Implementováno v config_session.php. Zahrnuje regeneraci ID session a nastavení bezpečných cookie parametrů (HttpOnly, Secure).

3.4. Administrace (admin/)

- Chráněná sekce dostupná pouze uživatelům s role = 'admin'.
- Umožňuje přehled všech uživatelů a hromadnou správu inzerátů (mazání libovolného inzerátu).

4. KLIENTSKÁ ČÁST (FRONTEND)

Frontend klade důraz na uživatelskou přívětivost (UX) a moderní přístupy bez závislosti na jQuery.

JavaScript (Vanilla JS)

- **AJAX Filtrování (filter.js):** Odesílá formulář filtrů na pozadí pomocí Fetch API. Aktualizuje seznam inzerátů bez reloadu stránky a upravuje URL v prohlížeči pomocí History API (umožňuje sdílení odkazu s filtry).
- **Závislé selecty (prague_district_input.js, select.js):** Dynamicky mění nabídku čtvrtí (district) podle vybraného obvodu Prahy (praha), aby uživatel nemohl vybrat neexistující kombinaci.
- **Image Slider (imageslider.js):** Vlastní implementace galerie obrázků na kartě inzerátu s cyklickým procházením.
- **Klientská validace (formcheck.js, editprofile.js):** Okamžitá zpětná vazba uživateli při vyplňování formulářů (obarvení chybných polí).

CSS a Design

- **Responzivita:** Layout se přizpůsobuje mobilním zařízením pomocí Media Queries.
- **Tiskové styly (print.css):** Definice @media print, která při tisku skryje navigaci, filtry a patičku, a optimalizuje výpis inzerátů pro tisk na papír (černobílé, odstranění stínů).

5. ZABEZPEČENÍ

Aplikace splňuje bezpečnostní standardy vyžadované zadáním:

1. **Ochrana proti SQL Injection:** Důsledné použití PDO a Prepared Statements (bindování parametrů) ve všech modelech.
2. **Ochrana proti XSS (Cross-Site Scripting):** Veškerý uživatelský vstup vypisovaný do HTML je ošetřen funkcí htmlspecialchars().
3. **Ochrana proti CSRF (Cross-Site Request Forgery):** Implementována v csrf.inc.php. Formuláře obsahují skrytý token, který se ověřuje při zpracování POST požadavku.
4. **Bezpečný upload:** Validace typu souboru na serveru (nikoliv jen přípony), přejmenování souborů unikátním identifikátorem (uniqid), limit velikosti souboru.
5. **Řízení přístupu (ACL):** Kontrola \$_SESSION['user_id'] a \$_SESSION['user_role'] na začátku každého chráněného skriptu.

6. INSTALACE

1. Nahrajte soubory na webový server.
2. Importujte soubor database_structure.sql do vaší databáze.
3. Upravte přihlašovací údaje k DB v souboru includes/dbh.inc.php.
4. Nastavte práva pro zápis (chmod 777) pro složku uploads/.