Délicious - Food Delivery Ordering System

Dokumentace semestrální práce

Jméno:	Oldřich Jan Švehla
Email:	tmwmf@students.zcu.cz
Datum vytvoření:	9. prosince 2025
Předmět:	KIV/WEB (Webové aplikace)
Název aplikace:	Délicious

1 URL aplikace

Aplikace běží lokálně na XAMPP serveru: http://localhost/web-foodapp/

2 Zadání práce

2.1 Oficiální zadání

Objednávkový systém (např. rozvoz potravin)

Jako příklad lze využít (zjednodušený) web některé z firem pro rozvoz potravin zákazníkům. Role: nepřihlášený uživatel, konzument, dodavatel, administrátor. Nepřihlášený uživatel vidí seznam produktů a může se do systému registrovat jako konzument nebo jako dodavatel (ten by měl být schválen administrátorem). Konzument vidí seznam produktů, které může vkládat do košíku a ten následně objednat. Dále vidí své historické objednávky, včetně produktů a data objednání. Dodavatel může do systému vkládat produkty (a např. může vidět, kolikrát byl který produkt objednán) a vidí nevyřízené objednávky, které může označit za vyřízené. Administrátor spravuje uživatele a může upravit vše potřebné.

2.2 Realizace

Aplikace **Délicious** (slovní hříčka: Delicious + Delivery) je webová aplikace pro rozvoz jídla, která implementuje zadání s následujícími funkcemi:

- **Nepřihlášený uživatel:** může procházet seznam produktů, registrovat se jako konzument nebo dodavatel
- **Konzument:** procházení produktů, přidávání do košíku, vytváření objednávek, zobrazení historických objednávek s produkty a datem
- **Dodavatel:** správa vlastních produktů (vytváření, editace, mazání s nahráváním obrázků), zobrazení objednávek obsahujících jejich produkty
- **Administrátor:** schvalování nových dodavatelů, správa všech uživatelů, produktů a objednávek
- Hashování hesel (bcrypt), ochrana proti XSS a SQL injection
- Responsivní design pro mobilní zařízení i PC

3 Použité technologie

3.1 Backend

- **PHP 8.2.12** - implementace MVC architektury, business logika v Controllers, datová vrstva v Models
- **MySQL/MariaDB** - relační databáze se 4 tabulkami (users, products, orders, order_items)
- **PDO** - databázová vrstva s prepared statements pro ochranu proti SQL injection
- **Twig 3.22** - template engine pro všechny Views s auto-escapingem (XSS ochrana)
- **Composer** - správa závislostí (Twig)

3.2 Frontend

- **HTML5 + CSS3** - moderní minimalistický design s custom CSS properties
- **Bootstrap 5.3** - responzivní grid systém, utility třídy, komponenty
- **Bootstrap Icons** - ikonová sada použitá v celé aplikaci
- **JavaScript (Vanilla)** - AJAX operace pro košík, správu produktů (fetch API)

3.3 Vývojové prostředí

- **XAMPP** - Apache server + MySQL databáze
- **Git/GitHub** - verzování kódu
- **.htaccess** - URL rewriting, směrování všech požadavků do public/index.php

4 Adresářová struktura

`app/Controllers/`
: MVC Controllers - obsahuje 8 controllerů (AdminController, CartController, HomeController, LoginController, OrderController, ProductController, RegisterController, SupplierController). Každý má metodu index() pro GET a specifické metody pro POST požadavky.

`app/Models/`
: MVC Models - obsahuje 4 modely (Database.php pro PDO singleton, User.php, Product.php, Order.php). Zajišťují komunikaci s databází pomocí prepared statements.

`app/Views/templates/`
: Twig templates - 13 šablon (base.twig jako master layout, home.twig, login.twig, register.twig, products.twig, cart.twig, checkout.twig, orders.twig, order_detail.twig, supplier.twig, admin_dashboard.twig, admin_users.twig, admin_products.twig, admin_orders.twig).

`app/Helpers/`
: Pomocné třídy - TwigHelper.php pro inicializaci Twig s konfigurací (cache, autoescape).

`app/autoload.php`
: Autoloader pro automatické načítání tříd.

`public/index.php`
: Jediný vstupní bod aplikace (single entry point). Obsahuje switch-based router, který na základě parametru `?page=` načítá příslušný controller. Inicializuje session.

`public/css/style.css`
: Vlastní CSS styly - moderní minimalistický design, responzivní pravidla pro mobilní zařízení.

`public/uploads/`
: Adresář pro nahrané obrázky produktů.

`database/install.sql`
: Kompletní instalační SQL skript - vytvoří databázi, všechny tabulky a naplní je testovacími daty.

`vendor/` Composer závislosti (Twig).

`.htaccess`
: Root htaccess - přesměrování všech požadavků do `public/` adresáře.

5 Architektura aplikace

5.1 MVC Pattern s Single Entry Point

Aplikace používá architektonický vzor Model-View-Controller:

- **Router (public/index.php):** Veškerý HTTP provoz směřuje do tohoto souboru díky .htaccess. Switch-case na parametr `$_GET['page']` určuje, který controller se načte. Session je inicializována globálně.
- **Models (app/Models/):**
  - `Database.php` - Singleton pattern pro PDO připojení
  - `User.php` - správa uživatelů (registrace, přihlášení, seznam, schvalování)
  - `Product.php` - CRUD operace pro produkty (create, read, update, delete)
  - `Order.php` - správa objednávek (vytváření včetně položek, seznam, detail, změna stavu)
- **Views (app/Views/templates/):** Twig šablony s auto-escapingem. `base.twig` je master layout s navbar a bloky (title, content, extra_js). Ostatní templates z něj dědí. AJAX logika je implementována v block extra_js.
- **Controllers (app/Controllers/):** Každý má metodu `index()` pro GET (zobrazení view) a specifické metody pro POST (zpracování formulářů, AJAX). Kontrolují oprávnění na základě `$_SESSION['role']`.
  - `HomeController` - úvodní stránka
  - `LoginController` - přihlášení/odhlášení, kontrola schválení dodavatele
  - `RegisterController` - registrace s volbou role
  - `ProductController` - seznam produktů schválených dodavatelů
  - `CartController` - košík v session, AJAX operace (add, update, remove, clear)
  - `OrderController` - checkout, vytvoření objednávky, seznam, detail
  - `SupplierController` - dashboard dodavatele, CRUD produktů s upload obrázků
  - `AdminController` - dashboard, správa uživatelů/produktů/objednávek, schvalování dodavatelů

5.2 Bezpečnost

- **SQL Injection:** Všechny dotazy používají PDO prepared statements
- **XSS:** Twig autoescape='html' v TwigHelper.php
- **Hesla:** `password_hash(PASSWORD_BCRYPT)`
- **Upload souborů:** Validace typu (JPG, PNG, GIF, WEBP), velikosti (max 5MB), unikátní názvy
- **RBAC:** Kontrola role v session před přístupem k chráněným částem

5.3 Databázový model

- **users** - PK: user_id, obsahuje email (UNIQUE), password (bcrypt), jmeno, role (konzument/dodavatel/admin), is_approved, is_super_admin
- **products** - PK: product_id, FK: supplier_id -¿ users, obsahuje name, description, price, image
- **orders** - PK: order_id, FK: customer_id -¿ users, obsahuje customer_name, email, delivery_address, phone, note, status, total_price
- **order_items** - PK: order_item_id, FK: order_id -¿ orders, FK: product_id -¿ products, obsahuje quantity, price

6 Výchozí uživatelské účty

Všichni uživatelé mají heslo: **heslo123**

6.1 Super Administrátor

- Email: `superadmin@test.cz`
- Heslo: `heslo123`
- Oprávnění: správa všech uživatelů včetně ostatních administrátorů, nelze smazat, nejvyšší oprávnění v systému

6.2 Administrátor

- Email: `admin@test.cz`
- Heslo: `heslo123`
- Oprávnění: správa uživatelů, schvalování dodavatelů, správa všech produktů a objednávek

6.3 Dodavatelé (schválení)

- Email: `dodavatel@test.cz` - Pizza House (4 produkty)
- Email: `dodavatel2@test.cz` - Burger King (4 produkty)
- Heslo: `heslo123`
- Oprávnění: správa vlastních produktů, zobrazení objednávek vlastních produktů

6.4 Dodavatel (neschválený)

- Email: `dodavatel3@test.cz` - Sushi Bar
- Heslo: `heslo123`
- Stav: čeká na schválení administrátorem, nemůže se přihlásit

6.5 Zákazníci

- Email: `zakaznik@test.cz` - Jan Novák (2 testovací objednávky)
- Email: `zakaznik2@test.cz` - Marie Svobodová (2 testovací objednávky)
- Heslo: `heslo123`
- Oprávnění: procházení produktů, košík, vytváření objednávek