

# Objednávkový systém

Semestrální práce KIV/WEB

Tomáš Klepač

`klepact@students.zcu.cz`

A23B0048P

5. října 2025

# Úvod

Cílem této semestrální práce bylo vytvořit webovou aplikaci v jazyce PHP, která implementuje objednávkový systém s podporou více uživatelských rolí. Aplikace je založená na MVC architektuře a komunikuje s databází pomocí PDO. Součástí projektu je i responzivní webové rozhraní vytvořené pomocí Bootstrapu a vlastních stylů.

## Použité technologie

- PHP 8 - objektově orientované programování, MVC architektura
- MySQL/MariaDB - databáze, přístup přes PDO
- HTML5, CSS3 - responzivní design
- Bootstrap 5 + vlastní styl `app.css`
- JavaScript - potvrzovací dialogy a interaktivní prvky

## Architektura aplikace

Projekt je rozdělen do adresářů:

- `public` - vstupní soubor `index.php`, routery
- `app/Controllers` - controllery
- `app/Models` - modely
- `app/Views` - pohledy
- `app/Views/partials` - společné části (header, footer)
- `config` - konfigurace databáze
- `sql` - export databáze

Celková struktura projektu:

```
objednavkovy-system/  
  app  
    Controllers  
    Models  
    Views  
  config  
  public  
  sql  
  dokumentace.pdf  
  Readme.md
```

# Funkcionalita

Aplikace podporuje následující funkce:

- Registrace, přihlášení a odhlášení uživatelů
- Tři role uživatelů:
  - **Admin** - správa uživatelů, všech produktů a objednávek
  - **Dodavatel** - správa vlastních produktů, zobrazení objednávek jeho položek
  - **Zákazník** - prohlížení produktů, práce s košíkem, tvorba objednávek
- Správa produktů (CRUD), včetně nahrávání obrázků
- Košík - přidávání, mazání, změna množství
- Objednávky - vytvoření, potvrzení administrátorem, změna stavu

# Bezpečnost

- Hesla jsou ukládána hashovaná pomocí Bcrypt.
- Přístup k databázi je řešen přes PDO a prepared statements (ochrana proti SQL Injection).
- Všechny výstupy jsou ošetřeny funkcí `htmlspecialchars` (ochrana proti XSS).
- Session jsou použity pro správu přihlášení a rolí uživatele.
- Formuláře využívají CSRF tokeny pro ověření původu požadavků (ochrana proti Cross-Site Request Forgery).
- Při nahrávání souborů se kontroluje přípona a velikost obrázku.

# Databázový model

Databáze obsahuje následující tabulky:

- **users** - informace o uživatelích (jméno, email, heslo, stav účtu)
- **roles** - definice jednotlivých rolí (Admin, Dodavatel, Zákazník)
- **user\_role** - propojovací tabulka mezi uživateli a rolemi (N:M vztah)
- **products** - seznam produktů, včetně názvu, ceny, popisu a obrázku
- **orders** - základní údaje o objednávkách (uživatel, datum, stav)
- **order\_items** - jednotlivé položky objednávky (produkt, množství, cena)

Export databáze ve formátu SQL je součástí odevzdaného archivu ve složce `sql/`.

## Popis implementace

Backend je rozdělen do controllerů podle typu dat - uživatelé, produkty a objednávky. Každý controller komunikuje s příslušným modelem a zobrazuje výstup pomocí view šablon. Aplikace využívá směrování přes parametr `action` v souboru `index.php`.

## Uživatelské rozhraní

Rozhraní je vytvořeno pomocí Bootstrap 5 a doplněno o vlastní minimalistické styly. Aplikace obsahuje responzivní layout, přehledné tabulky, barevné zvýraznění stavů objednávek a akční tlačítka.

## Testování

Aplikace byla testována lokálně na serveru XAMPP v prohlížeči Google Chrome. Bylo ověřeno správné fungování autentizace, práce s databází a správa rolí. Nebyla zjištěna žádná kritická chyba v běžném provozu.

## Architektura a třídy

Aplikace je rozdělena podle principu MVC.

- `user_controller.php` - zajišťuje registraci, přihlášení, odhlášení a správu uživatelů.
- `product_controller.php` - obsluhuje CRUD operace s produkty, včetně nahrávání obrázků.
- `order_controller.php` - spravuje objednávky, jejich tvorbu, potvrzování a změnu stavu.
- `user_model.php`, `product_model.php`, `order_model.php` - přístup do databáze přes PDO.
- `views/` - HTML šablony s vloženými PHP proměnnými.

## Seznam testovacích uživatelů

Role	Email	Heslo
Admin	admin@local.test	Admin123!
Dodavatel	supplier@local.test	Supplier123!
Zákazník	customer@local.test	Customer123!

## Umístění aplikace

Aplikace byla testována lokálně v prostředí XAMPP (PHP 8.2, MariaDB 10.4). Po rozbalení archivu stačí importovat databázi ze složky `sql/`, upravit připojení v `config/db.php` a otevřít `http://localhost/objednavkovy-system/public/`.

## **Závěr**

Aplikace splňuje všechny požadavky zadání - MVC architekturu, databázovou komunikaci, autentizaci, role uživatelů, bezpečnostní opatření a responzivní design.