# Business Requirement Document (BRD)

## 1. Business Overview

The e-commerce application enables users to browse products, manage their profiles and addresses, add products to carts, place orders, and receive notifications for key events. The system also includes **authentication features**, such as secure login, session management, and **forgot password functionality via OTP verification** to verified mobile numbers.

## 2. Key Business Requirements

* **Authentication Management:** Secure login, session handling, and OTP-based forgot password functionality.
* **Product Management:** Users and admins can manage products and categories.
* **Cart and Order Management:** Users can add products to carts, place orders, and view order histories.
* **Profile and Address Management:** Users can view and edit their profile and addresses.
* **Notifications:** Notifications are sent upon key events like order placement.
* **Forgot Password:** Users can reset passwords using OTPs sent to verified mobile numbers.

## 3. Microservices Overview

**Total Microservices:**

1. **Authentication Service** (NEW)
2. **Profile Service**
3. **Address Service**
4. **Product Service**
5. **Cart Service**
6. **Order Service**
7. **Notification Service**
8. **Session Service**

## 4. Tables and APIs

### 4.1 Authentication Service

**Description:** Handles user authentication, OTP generation for password recovery, and password management.

**Tables:**

* **auth (NEW):**
  + Stores user authentication data, such as hashed passwords and authentication status.
  + Columns: user\_id (FK), password\_hash, is\_locked, failed\_attempts, otp\_code, otp\_expiry.

**APIs:**

* **User Authentication:**
  + POST /auth/login: Authenticate a user with username and password.
  + POST /auth/logout: Logout a user and invalidate their session.
* **Forgot Password:**
  + POST /auth/forgot-password: Trigger OTP generation and send to verified mobile number.
  + POST /auth/verify-otp: Verify OTP and reset the password.
* **Account Lockout and Management:**
  + Automatically lock accounts after a configurable number of failed login attempts.

### 4.2 Profile Service

**Description:** Handles user profile management, including email and phone verification.

**Tables:**

* **Existing Tables:**
  + profile, privs, profprivs, users, phone, email.
* **APIs:**
  + POST /users/verify-phone: Verify a phone number via OTP (sent by the Notification Service).
  + POST /users/verify-email: Verify an email via confirmation link or code.
  + Other APIs as defined earlier.

### 4.3 Address Service

No changes; handles address and location data.

**Tables:**

* countries, states, district, address.

### 4.4 Product Service

No changes; manages products and categories.

**Tables:**

* prodtypes, products, prodstocks.

### 4.5 Cart Service

No changes; manages user carts.

**Tables:**

* cart.

### 4.6 Order Service

No changes; handles order placement and details.

**Tables:**

* orders, orderdetails.

### 4.7 Notification Service

No changes; handles notifications for order placements and OTPs.

**Tables:**

* notification.

**Additional API for OTP Notifications:**

* POST /notifications/otp: Send an OTP to the user’s verified phone number.

### 4.8 Session Service

No changes; manages user sessions.

**Tables:**

* usession.

## 5. Functional Flow

### Authentication Workflow:

1. **User Login:**
   * A user sends their username and password via the POST /auth/login API.
   * The system authenticates credentials and creates a session via the Session Service.
2. **Forgot Password:**
   * The user provides their username or verified mobile number via the POST /auth/forgot-password API.
   * The system generates an OTP and sends it via the Notification Service.
   * The user submits the OTP and new password via POST /auth/verify-otp to reset the password.
3. **Phone Verification:**
   * A user provides their phone number for verification via POST /users/verify-phone.
   * An OTP is sent via the Notification Service.
   * The user submits the OTP for verification, enabling their phone for future use.

### 6. API Gateway Routes

The API Gateway ensures seamless routing for all services:

| **Route** | **Service** | **Description** |
| --- | --- | --- |
| /auth/\*\* | Authentication Service | Login, logout, password management |
| /users/\*\* | Profile Service | Profile and verification management |
| /addresses/\*\* | Address Service | Address management APIs |
| /products/\*\* | Product Service | Product and category management |
| /cart/\*\* | Cart Service | Cart management APIs |
| /orders/\*\* | Order Service | Order placement and details |
| /notifications/\*\* | Notification Service | Notifications and OTP APIs |
| /sessions/\*\* | Session Service | Session management APIs |

### 7. Additional Security Considerations

* **Password Hashing:**  
  Use strong hashing algorithms (e.g., bcrypt) to store passwords securely.
* **OTP Expiry:**  
  OTPs should have a short expiry (e.g., 5 minutes) and single-use restrictions.
* **Rate Limiting:**  
  Protect endpoints like forgot-password and verify-otp from abuse using rate limiting.
* **JWT Authentication:**  
  Use JWT tokens to secure user sessions.

### 8. Tables Summary

| **Table** | **Purpose** |
| --- | --- |
| **auth** | Stores authentication and OTP-related data. |
| **profile** | Stores profile information for users. |
| **privs** | Maintains privileges available in the system. |
| **profprivs** | Links profiles with privileges. |
| **users** | Stores user-specific details like name, email, and profile. |
| **phone** | Stores verified phone numbers for users. |
| **email** | Stores verified email addresses for users. |
| **countries** | Stores country information for addresses. |
| **states** | Stores state information linked to countries. |
| **district** | Stores district details linked to states. |
| **address** | Stores address information linked to users. |
| **prodtypes** | Stores product categories. |
| **products** | Stores product details linked to categories. |
| **prodstocks** | Tracks stock availability for products. |
| **cart** | Tracks products added to user carts. |
| **orders** | Stores order summaries linked to users. |
| **orderdetails** | Tracks product details for each order. |
| **notification** | Stores notifications for users, including OTP-related messages. |
| **usession** | Tracks active user sessions. |