Stephen Akinrodoye_CA-AWTEC_Assignment 1 - Registration & Login System

Auth Service (Internal Staff Authentication)

This Auth Service is a standalone authentication and authorization microservice designed to support the internal staff and admin dashboard for the QBridge Athleisure Order Management System (OMS). It is not customer-facing and is intentionally restricted to company personnel such as the owner and warehouse/operations staff.

The service is built with Node.js, Express, and MongoDB and is responsible for managing staff identities, enforcing secure access control, and issuing authenticated sessions for internal tools. Public self-registration is disabled; all staff accounts are created and managed by the system owner to maintain strict operational security.

Core Responsibilities

- **Staff Authentication**
  Authenticates internal users (owner, ops, viewer) using email and password, passwords are securely hashed using bcrypt and never stored in plaintext, issues signed JWTs upon successful login.

- **Session Management**
  JWTs are stored in HTTP-only cookies to protect against XSS attacks; provides login, logout, and session validation endpoints, and supports stateless authentication suitable for microservice architectures.

- **Role-Based Access Control (RBAC)**
  Enforces access levels using predefined roles (`owner`, `ops`, `viewer`), restricts sensitive operations (e.g., creating staff accounts) to the owner role; middleware ensures protected routes are accessible only to authorized users.

- **Internal User Management**
  Allows the owner to create and manage staff accounts; supports account activation/deactivation without deleting historical data; designed for small, trusted internal teams rather than public users.

- **Service Isolation**
  Runs as a separate service alongside the Python-based OMS; can be queried by internal dashboards or backend services to validate sessions, and decouples authentication concerns from business logic and order processing.

Security Design Principles

No public signup endpoints, strong password requirements for staff accounts, HTTP-only cookies to prevent token leakage, centralized authentication service to reduce attack surface, and minimal data exposure in authenticated responses.

Intended Usage

This Auth Service acts as the security gateway for internal admin dashboards, warehouse and operations tools, protected OMS endpoints, as well as future internal analytics or reporting services. It ensures that only authorized staff can access operational systems while keeping authentication logic cleanly separated from order management and inventory workflows.