# Triple Bottom Line Grocery Scanning API - Analysis

## Overview

This FastAPI application evaluates consumer products based on a Triple Bottom Line (TBL) framework, scoring brands across social, environmental, and economic dimensions. Users can scan products, compare brands, and track their sustainable purchasing history.

## Architecture

### Core Components

**Framework & Dependencies**: Uses FastAPI for REST endpoints, with Pydantic for data validation, httpx for async HTTP requests, and hashlib for password hashing. CORS middleware enables cross-origin access.

**Data Storage**: Implements three in-memory databases—USERS_DB for authentication, PURCHASE_HISTORY_DB for user transaction logs, and PRODUCT_CACHE for barcode lookups. The CERTIFIED_BRANDS_DB contains hardcoded TBL scores for 21 brands.

**Scoring System**: Calculates overall TBL scores using weighted averages (35% social, 40% environmental, 25% economic). Grades range from A (≥8.5) to F (<4.0).

## Key Features

**Product Lookup**: The `/product/{barcode}` endpoint integrates with Open Food Facts API to retrieve product metadata, then normalizes brand names for matching against the certified database using both exact and partial matching strategies.

**Brand Comparison**: The `/compare` endpoint ranks multiple brands by overall TBL score, enabling side-by-side analysis of social, environmental, and economic metrics.

**Purchase Tracking**: Users can record purchases with `/purchase`, which calculates TBL scores and maintains history. The `/history/{username}` endpoint returns purchase logs with average TBL score across the user's history.

**User Management**: Basic registration and login with SHA-256 password hashing. Session management uses simple "token_" prefixed usernames (not production-ready).

## Database Schema

**Users**: Username, email, hashed password, creation timestamp

**Purchases**: Barcode, brand, product name, category, price, TBL score, timestamp

**Brands**: Social/environmental/economic scores (0-10 scale), certifications array

## Security & Design Considerations

**Vulnerabilities**:

- Passwords hashed with SHA-256 without salt—vulnerable to rainbow table attacks
- In-memory databases lose all data on server restart
- No JWT tokens or session management beyond basic string tokens
- No rate limiting on API endpoints
- Brand database is static and not updated from authoritative sources

**Quality Assurance**:

- Includes disclaimer on health check and `/brands` endpoint acknowledging prototype-quality data
- Normalizes brand names (removes apostrophes, standardizes case) to improve matching accuracy
- Fallback scores (5.5/5.0/7.0) for unrecognized brands prevent errors

## API Endpoints

| Method | Endpoint | Purpose |
|---|---|---|
| POST | /auth/register | Create new user account |
| POST | /auth/login | Authenticate user |
| POST | /scan | Score a product by brand |
| POST | /compare | Rank multiple brands |
| POST | /purchase | Record purchase transaction |
| GET | /product/{barcode} | Retrieve product with TBL score |
| GET | /history/{username} | View purchase history & averages |
| GET | /brands | List all rated brands |
| GET | /health | System status check |
| GET | / | Serve HTML frontend |

## Production Recommendations

1. **Authentication**: Replace SHA-256 with bcrypt or argon2; implement proper JWT tokens with expiration
2. **Persistence**: Migrate to PostgreSQL or MongoDB; implement database migrations
3. **Data Sourcing**: Integrate official certification APIs (B-Corp, Fair Trade organizations) instead of hardcoded scores
4. **Rate Limiting**: Add throttling per IP/user to prevent abuse

5. **Caching**: Implement Redis for distributed caching and session management
6. **Validation**: Add input validation for barcode format, email verification for registration
7. **Error Handling**: Implement comprehensive error logging and user-friendly error messages
8. **API Documentation**: Add OpenAPI schema customization for Swagger UI clarity
9. **Testing**: Implement unit tests for score calculations and integration tests for Open Food Facts connectivity