Technical Overview  
  
Authentication

JWT is used for stateless authentication. After login, a signed token is returned and verified on each request. The token includes basic user info (id, email, role) and expires after 24 hours.  
  
Role Access

* Employee: can view and create vacation requests.
* Manager: can manage users, review requests, and assign schedules.

## Database

Main tables:

* users
* vacation\_requests
* work\_schedules
* audit\_log
* lookup tables for roles, statuses, and schedule types

API Routes

* `/api/auth` – login, returns JWT token.
* `/api/users` – CRUD for users (manager only).
* `/api/requests` – vacation requests (employee + manager).
* `/api/schedules` – manage schedules (manager).
* `/api/lookups` – fetch enums (public).

Structure

* `src/controllers` – handles business logic.
* `src/models` – DB entities.
* `src/utils` – helpers (JWT, CORS, Validator, Response).
* `public/api` – REST endpoints.

Testing  
  
Basic PHPUnit tests ensure the main logic (validation, auth) runs correctly. Database tests are mocked or isolated.