Here's an automated AI-generated review to support your development workflow.

📝 Summary

- Introduces JWT-based authentication for the API layer
- Adds login and token refresh endpoints with rate limiting
- Secures sensitive routes behind an auth middleware

⚠️ Potential Issues

- JWT secret is read from env but not validated at startup; a misconfiguration could lead to weak or missing signing
- Refresh token is stored in memory only; server restart invalidates all sessions with no user feedback
- No explicit token expiry is documented; recommend aligning with a short access token and longer refresh window

🚀 Potential Optimizations

- Consider moving secret validation into an app bootstrap step so misconfig fails fast
- Use a dedicated store (e.g. Redis) for refresh tokens if you need revocability and durability
- Add structured logging (without secrets) for auth failures to help debugging and security audits

💡 Suggestions

- Good separation of login vs refresh logic; keeps responsibilities clear
- Consider adding a short doc comment or README section on expected env vars and token lifetimes
- Add integration tests that assert 401 on missing/invalid token and 200 with a valid token

— This review was generated by **Gitzoid**, an AI-powered code review assistant.