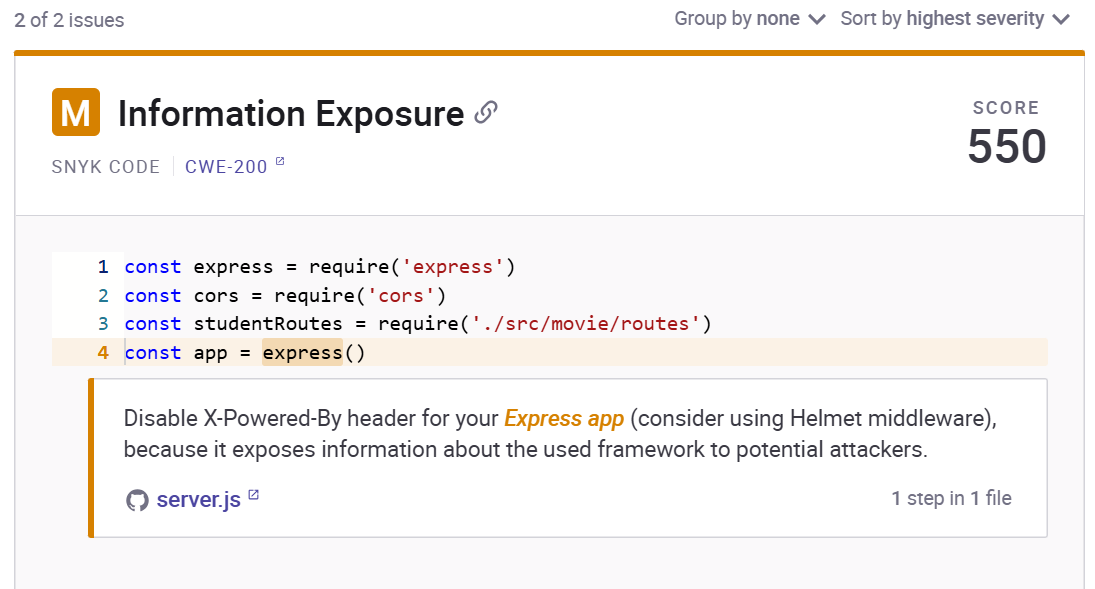
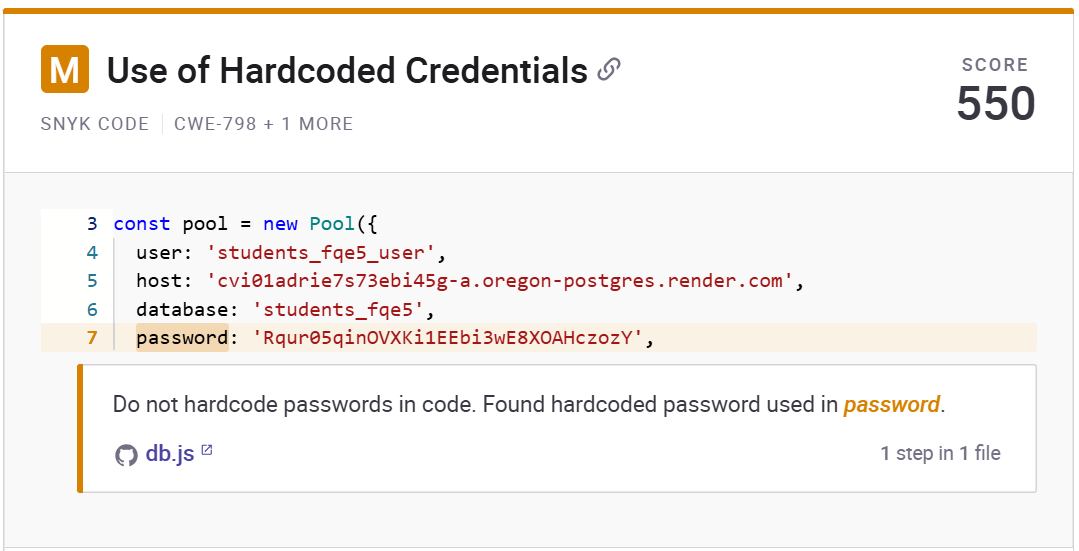
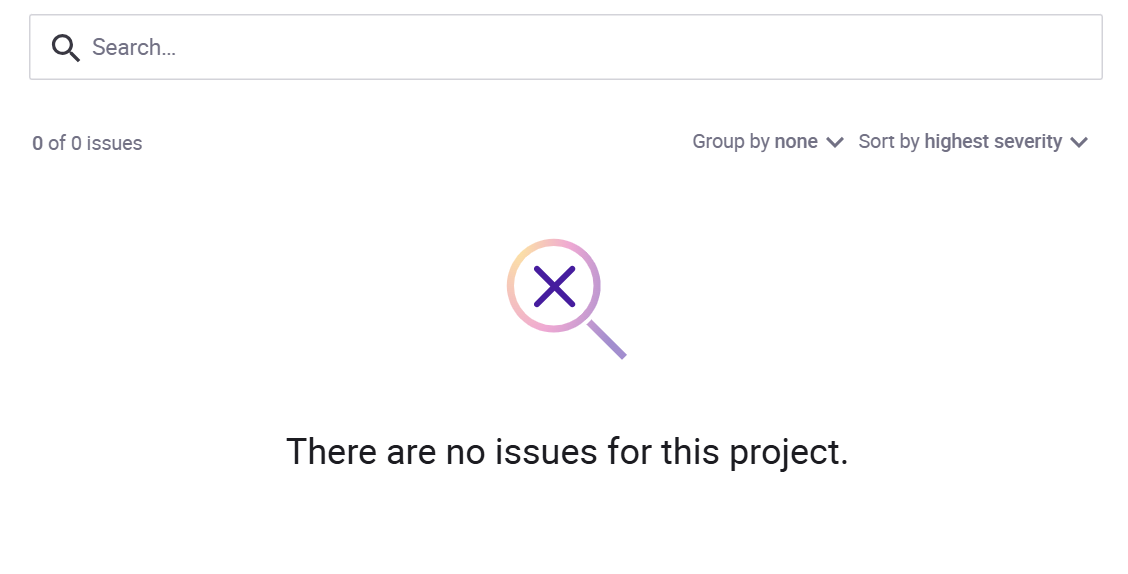
Initially, I had 2 issues, Information Exposure and Hardcoded credentials as shown below.



During an initial Snyk scan of the Express application, a medium-severity vulnerability was identified related to information exposure. Specifically, the application was automatically sending the X-Powered-By HTTP header in all responses. This header reveals that the backend is built with Express, which is unnecessary and potentially dangerous. Exposing implementation details like this can provide attackers with clues about the technologies in use, allowing them to tailor their attacks based on known vulnerabilities in those technologies. Disabling this header is a widely recommended best practice to reduce the attack surface and make the application less identifiable.

Additionally, the scan and manual review highlighted a security concern related to hardcoded credentials. The PostgreSQL database password was embedded directly in the source code. This practice significantly increases the risk of credential exposure, especially if the code is ever shared publicly or stored in a version control system without proper access restrictions. Hardcoding secrets makes it difficult to rotate credentials and violates principles of secure software development. To address this, the application was updated to load sensitive configuration such as database credentials from environment variables using a .env file. This change not only improves security but also enhances maintainability and makes the application more adaptable across different deployment environments.

This Left me with no issue remaining.