**Project Security & Delivery Report**

Overview

--------

This document summarizes the security measures, delivery contents, and setup instructions for the Todo Web API project. It is written in clear, human language for easy understanding by both technical and non-technical readers.

---

**What Was Implemented (And Why)**

------------------------------

In this project, we made sure that all the important secrets—like passwords and API keys—are never written directly into the code or shared in places where they could be seen by accident. Instead, we set things up so that these secrets are stored safely in a tool called Vault. When the app or the CI/CD pipeline needs a secret, it asks Vault for it, just for that moment, and then moves on. This way, secrets aren't left lying around where someone could find them.

Why did we do it this way? Because it's way safer! If secrets are hidden away in Vault, there's much less chance of them leaking out or being stolen. It also means we can change them easily if we ever need to, without having to dig through code or configuration files. Basically, it keeps our project secure and makes life a lot easier for everyone working on it.

---

Project Delivery

-------------------------

Here's what you'll get when you receive this project, all packed up and ready to go:

1. The Code Bundle

  - The Dockerfile (so you can build and run the app easily)

  - The pipeline configuration (for automated builds and deployments)

  - All the application code (the heart of the project)

2. **The PDF Report**

  - You'll also get a PDF report that sums up what was done, why it was done that way, and any important details you should know. It's written in plain language, so you don't need to be a tech expert to understand it.

With all these pieces, you'll have a complete package: the code, the instructions, and the story behind the project. If you ever need help or have questions, everything you need is right there in the bundle.

---

Setup Instructions (from README)

--------------------------------

To run locally:

```
  npm install
  npm start
```

To run tests:

```
  npm test
```

---

**Security Hardening Summary**

- Minimal Docker base image (node:lts-alpine) for reduced attack surface.

- Multi-stage Docker build to keep the final image small and clean.

- Non-root user (appuser) runs the app in the container.

- Trivy scan: No high/critical vulnerabilities found. Only low: missing HEALTHCHECK (to be added).

- No hardcoded secrets: All secrets managed via Vault.

- CI/CD pipeline: Security gates in place; images only pushed if all checks pass.

---

**Recommendations for Production**

- Add a HEALTHCHECK to the Dockerfile for better container health monitoring.

- Regularly update dependencies and base images.

- Enable runtime security tools (e.g., Falco, AppArmor) for extra protection.

- Review and restrict IAM permissions to least privilege.

- Monitor logs and set up alerts for suspicious activity.