Security Pipeline Report

Repository: projectman14/test-repo-ddos
Branch: main
Commit: 7ad12bd71f88d620014e8f74f4ed36e9ad7f6379
Generated: 11/25/2025, 4:36:46 AM

Executive Summary

72	3	0
Dependencies	**Code Issues**	**Secrets**
Vulnerabilities	Semgrep	Leaked

Security Pipeline Report

Dependency Vulnerabilities

Total Dependencies: 73

Vulnerable Dependencies: 72

Severity Breakdown:

moderate: 21
critical: 10
high: 29
low: 12

Top Vulnerabilities:

Package	Severity	CVE	CVSS Score
@babel/helpers:7.18.2	MODERATE	GHSA-968p-4wvh-cqc8	6.2
@babel/runtime-corejs3:7.18.3	MODERATE	GHSA-968p-4wvh-cqc8	6.2
@babel/runtime:7.24.4	MODERATE	GHSA-968p-4wvh-cqc8	6.2
@babel/traverse:7.18.2	CRITICAL	GHSA-67hx-6x53-jw92	9.4
axios:0.21.4	HIGH	GHSA-4hjh-wcwx-xvwj	7.5
axios:0.21.4	HIGH	GHSA-jr5f-v2jv-69x6	N/A
axios:0.21.4	MODERATE	GHSA-wf5p-g6vw-rhxx	6.5
axios:1.6.8	HIGH	GHSA-4hjh-wcwx-xvwj	7.5
axios:1.6.8	HIGH	GHSA-8hc4-vh64-cxmj	N/A
axios:1.6.8	HIGH	GHSA-jr5f-v2jv-69x6	N/A
base-x:3.0.9	HIGH	GHSA-xq7p-g2vc-g82p	N/A
body-parser:1.20.0	HIGH	GHSA-qwcr-r2fm-qrc7	7.5
brace-expansion:1.1.11	LOW	GHSA-v6h2-p8h4-qcjw	3.1
brace-expansion:2.0.1	LOW	GHSA-v6h2-p8h4-qcjw	3.1
braces:3.0.2	HIGH	GHSA-grv7-fg5c-xmjg	7.5

... and 57 more vulnerabilities

Security Pipeline Report

Code Security Analysis (Semgrep)

Total Findings: 3

Severity Breakdown:

INFO: 1
WARNING: 2

Findings:

1. javascript.express.security.audit.express-check-csurf-middleware-usage.express-check-csurf-middleware-usage

INFO

File: N/A
Message: A CSRF middleware was not detected in your express application. Ensure you are either using one such as `csurf` or `csrf` (see rule references) and/or you are properly doing CSRF validation in your ro...

2. javascript.express.security.injection.raw-html-format.raw-html-format

WARNING

File: N/A
Message: User data flows into the host portion of this manually-constructed HTML. This can introduce a Cross-Site-Scripting (XSS) vulnerability if this comes from user-provided input. Consider using a sanitiza...

3. javascript.express.security.injection.raw-html-format.raw-html-format

WARNING

File: N/A
Message: User data flows into the host portion of this manually-constructed HTML. This can introduce a Cross-Site-Scripting (XSS) vulnerability if this comes from user-provided input. Consider using a sanitiza...

Security Pipeline Report

Threat Model Analysis

Total Threats: 4

Technology Stack:

Languages: JavaScript

Frameworks: Express, React

Identified Threats:

1. HTTP used instead of HTTPS for external calls

MEDIUM

Using plain HTTP can allow traffic sniffing and man-in-the-middle attacks....

2. Use of random without cryptographic security

LOW

Using predictable random sources for security tokens may allow guessing of values....

3. Express app without Helmet middleware

MEDIUM

Express application does not appear to use Helmet, which helps set secure HTTP headers....

4. Express app without rate limiting

LOW

Express application does not appear to use any basic rate limiting, which can help mitigate brute-force or DoS attacks....

Security Pipeline Report

Secret Detection (Gitleaks)

' No secrets or credentials detected

Security Pipeline Report

Recommendations

1. **Update Vulnerable Dependencies**
   72 vulnerable dependencies detected. Run 'npm audit fix' or update packages manually to patch known vulnerabilities.

2. **Address Code Security Issues**
   3 security issues found by static analysis. Review and fix issues related to injection, authentication, and unsafe patterns.

3. **Implement CI/CD Security Checks**
   Integrate these security scans into your CI/CD pipeline to catch vulnerabilities before they reach production.

4. **Regular Security Audits**
   Schedule regular security scans and code reviews. Keep dependencies updated and monitor security advisories.