My E-Commerce API

GitHub: user/my-ecommerce-api

Generated: February 15, 2026

Ø=ÜÊ Statistics

Total Findings: 15
Critical: 2
High: 3
Medium: 4
Low: 2

Ø=Ý' Security Findings

Ø=Ý4 1. SQL Injection Vulnerability

Severity: CRITICAL
Description: SQL injection vulnerability detected in user authentication query. Input from "user_input" parameter is directly concatenated with SQL query.
Location: src/controllers/authController.js
Line: 45

Ø=ßà 2. Password Hashing Weak Algorithm

Severity: HIGH
Description: Using MD5 for password hashing - deprecated and insecure. Should use bcrypt or Argon2.
Location: src/models/User.js
Line: 78

Ø=ßà 3. Missing CSRF Protection

Severity: HIGH
Description: Critical endpoint /api/transfer does not implement CSRF token validation.
Location: src/routes/transfer.js
Line: 123

Ø=ßá 4. Weak CORS Policy

Severity: MEDIUM
Description: CORS origin set to * allowing any origin to access API.
Location: src/app.js
Line: 67

Ø=ßá 5. Unused Dependency: mkdirp

Severity: MEDIUM
Description: Package "mkdirp" is imported but never used in codebase.
Location: src/utils/file.js
Line: 15

Ø=ßá 6. Missing HTTPS Headers

Severity: MEDIUM
Description: Missing X-Content-Type-Options header - potential XSS risk.
Location: src/app.js
Line: 72

Ø=Ý5 7. Server Time Information Leak

Severity: LOW
Description: X-Powered-By header exposes server technology.
Location: src/app.js
Line: 69

Ø=Ý5 8. Hardcoded Database URL
Severity: LOW
Description: Database connection URL is hardcoded in environment variable configuration.
Location: src/config/db.js
Line: 34

&ª 9. TODO Comment
Severity: INFO
Description: Code has TODO comment: "Implement rate limiting for API endpoints".
Location: src/middleware/rateLimit.js
Line: 89

&ª 10. Console.log in Production Code
Severity: INFO
Description: Debug console.log statements found in production code.
Location: src/utils/logger.js
Line: 102

&ª 11. Deprecated npm Package
Severity: INFO
Description: Package "lodash" version 4.17.21 is deprecated.
Location: package.json
Line: 18

&ª 12. Long Function
Severity: INFO
Description: Function "processOrder" has 150 lines - consider refactoring.
Location: src/controllers/orderController.js
Line: 456

Ø=ßá 13. Potential Race Condition
Severity: MEDIUM
Description: No locking mechanism for shared resource access in file operations.
Location: src/utils/fileHandler.js
Line: 78

Ø=ßà 14. Missing Rate Limiting
Severity: HIGH
Description: Login endpoint has no rate limiting - vulnerable to brute force attacks.
Location: src/routes/auth.js
Line: 234

Ø=Ý4 15. Insecure Random Number Generation
Severity: CRITICAL
Description: Using Math.random() for session ID generation - predictable.
Location: src/middleware/session.js
Line: 45

IAL