Security Scan Report

Report generated on: 2025-03-13 09:12:22

Summary

Total Alerts: 7 Critical Alerts: 4 High Alerts: 1 Medium Alerts: 1 Low Alerts: 1

Detailed Findings

Alert: Broken Access Control
Severity: Critical
Risk Score: 9.0
Description: Users can access resources they are not authorized to view, leading to potential data exposure.
URL: http://localhost:3000/admin/dashboard
Solution: Implement proper access controls to restrict user access to resources based on their roles.

Alert: Broken Access Control
Severity: Critical
Risk Score: 9.0
Description: Users can access sensitive user profiles without proper authorization.
URL: http://localhost:3000/user/profile
Solution: Ensure that user profiles are only accessible to authorized users.

Alert: Cryptographic Failures
Severity: High
Risk Score: 5.4
Description: Sensitive data is stored without encryption, making it vulnerable to unauthorized access.
URL: http://localhost:3000/user/profile
Solution: Use strong encryption algorithms to protect sensitive data at rest and in transit.

Alert: Injection
Severity: Critical
Risk Score: 9.0
Description: The application is vulnerable to SQL injection, allowing attackers to execute arbitrary SQL queries.
URL: http://localhost:3000/rest/user/login
Solution: Use parameterized queries or prepared statements to prevent SQL injection.

Alert: Injection
Severity: Critical
Risk Score: 9.0
Description: The search feature is vulnerable to SQL injection, allowing attackers to manipulate search queries.
URL: http://localhost:3000/rest/products/search?q=test
Solution: Implement input validation and use parameterized queries.

Alert: Insecure Design
Severity: Medium
Risk Score: 4.8
Description: The application lacks proper security controls in its design, making it susceptible to various attacks.
URL: http://localhost:3000/
Solution: Adopt secure design principles and conduct threat modeling during the design phase.

Alert: Security Misconfiguration
Severity: Low
Risk Score: 2.1
Description: The server exposes detailed error messages and version information in HTTP headers, which could aid attackers.
URL: http://localhost:3000
Solution: Disable detailed error messages and remove unnecessary server information from headers.

Confidential - For internal use only