Security Scan Report

Report generated on: 2025-03-12 07:30:08

Summary

Total Alerts: 5 Critical Alerts: 2 High Alerts: 1 Medium Alerts: 1 Low Alerts: 1

Detailed Findings

Alert: SQL Injection
Severity: Critical
Risk Score: 9.0
Description: The login form is vulnerable to SQL injection. Attackers can manipulate the database by injecting malicious SQL queries.
URL: http://localhost:3000/rest/user/login
Solution: Use parameterized queries or prepared statements to prevent SQL injection.

Alert: Cross-Site Scripting (XSS)
Severity: High
Risk Score: 5.4
Description: The search feature does not sanitize user input, allowing attackers to inject malicious JavaScript code.
URL: http://localhost:3000/#/search
Solution: Implement input validation and output encoding to sanitize user inputs.

Alert: Broken Authentication
Severity: Critical
Risk Score: 9.0
Description: The login page does not enforce account lockout after multiple failed attempts, making it vulnerable to brute-force attacks.
URL: http://localhost:3000/rest/user/login
Solution: Implement account lockout mechanisms and enforce strong password policies.

Alert: Sensitive Data Exposure
Severity: Medium
Risk Score: 4.8
Description: User passwords are transmitted over HTTP instead of HTTPS, exposing them to interception.
URL: http://localhost:3000/rest/user/login
Solution: Use HTTPS to encrypt all sensitive data in transit.

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.