**Security Scan Report – [Web Application Security Testing]**

**Project:** [Web Application Security Testing]  
**Tested Environment:** <http://127.0.0.1:3000> (Local Development Server)  
**Scan Tool:** ZAP by Checkmarx  
**Scan Date:** 26 August 2025  
**ZAP Version:** 2.16.1

**Executive Summary**  
A security scan was performed on the project hosted at <http://127.0.0.1:3000> using ZAP by Checkmarx. The scan identified several vulnerabilities and security gaps, mainly of medium and low severity. These issues, if unaddressed, could expose the application to threats like cross-origin attacks, information leakage, and code injection.

**Scan Overview**

* Scan Date: 26 August 2025
* Target Site: <http://127.0.0.1:3000>
* Tool Used: ZAP by Checkmarx, Version 2.16.1
* Total Alerts: 8
* High Risk: 0
* Medium Risk: 3
* Low Risk: 2
* Informational: 3

**Findings**

1. **Cross-Domain Misconfiguration**  
   Risk: Medium  
   Confidence: Medium  
   The server allows cross-origin requests that could be exploited by attackers. This was detected when requesting the favicon resource at <http://127.0.0.1:3000/assets/public/favicon_js.ico>. Unauthorized domains might gain access to resources or initiate unwanted requests.  
   Recommendation: Restrict CORS policies to trusted domains and endpoints.
2. **Content Security Policy (CSP) Header Not Set**  
   Risk: Medium  
   Confidence: High  
   The application lacks a CSP header, leaving it open to script injection and cross-site scripting (XSS) attacks.  
   Recommendation: Implement a strict CSP header, such as “default-src 'self'; script-src 'self'”.
3. **Hidden File Found**  
   Risk: Medium  
   Confidence: Low  
   A hidden or backup file was found, potentially containing sensitive configuration or credentials.  
   Recommendation: Remove or restrict access to these files before production deployment.
4. **Cross-Domain JavaScript Source File Inclusion**  
   Risk: Low  
   Confidence: Medium  
   External scripts are included from potentially unsafe sources, increasing the risk of malicious code execution.  
   Recommendation: Allow only scripts from trusted, verified domains.
5. **Timestamp Disclosure – Unix**  
   Risk: Low  
   Confidence: Low  
   The server reveals timestamps in HTTP responses, which attackers can use to map server activity or infer setup details.  
   Recommendation: Mask or remove timestamp information from responses.
6. **Information Disclosure – Suspicious Comments**  
   Risk: Informational  
   Confidence: Medium  
   Code comments containing debug information or internal details were found, which may aid attackers.  
   Recommendation: Review and clean code to remove unnecessary or sensitive comments.
7. **Modern Web Application**  
   Risk: Informational  
   Confidence: Low  
   The scan identified missing best practices or configurations expected in modern applications.  
   Recommendation: Review security configurations, frameworks, and libraries for compliance.
8. **User Agent Fuzzer**  
   Risk: Informational  
   Confidence: Medium  
   The server responds to unusual or malformed user-agent strings, which could be exploited for probing or abuse.Recommendation: Implement input validation and monitor suspicious patterns.

A screenshot of a computer

AI-generated content may be incorrect.

**References**

* MDN CSP Guide: <https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy>
* OWASP CSP Cheat Sheet: <https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html>
* CORS Misconfiguration Guide: <https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy>
* Snallygaster Tool for finding secrets: <https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html>
* OWASP Web Security Testing Guide: <https://owasp.org/wstg>

**Conclusion**  
The scan results highlight several areas where the application’s security posture can be improved. Addressing these issues will help protect the application from common vulnerabilities such as unauthorized access, information disclosure, and injection attacks. It is recommended to implement the suggested security controls and regularly perform scans to ensure ongoing protection.