DAST Scan Report

Target URL: http://host.docker.internal:4545

Scan Date: 2025-04-06 17:03:11
Scan ID: dast_c2d56858

Summary

Risk Level	Count
High	0
Medium	3
Low	1
Info	0

Detailed Findings

1. Content Security Policy Not Set (Medium Risk)

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks.
URL: http://host.docker.internal:4545/
Solution: Implement a Content Security Policy header to restrict resource loading to trusted sources.

AI Recommendations:

• Add CSP headers and specify trusted sources.
• Use nonce or hash-based CSP methods.
• Set up a reporting endpoint to monitor CSP violations.

2. Missing X-Frame-Options Header (Medium Risk)

Description: The X-Frame-Options header is not set, which means the site could be at risk from clickjacking attacks.
URL: http://host.docker.internal:4545/
Solution: Set the X-Frame-Options header to DENY or SAMEORIGIN.

AI Recommendations:

• Set X-Frame-Options to DENY on critical pages.
• Set X-Frame-Options header to DENY or SAMEORIGIN.
• Add frame-busting JavaScript to prevent clickjacking attacks.

3. Missing X-Content-Type-Options Header (Low Risk)

Description: The X-Content-Type-Options header is not set to 'nosniff', which means browsers could MIME-sniff the content type, potentially leading to security issues.
URL: http://host.docker.internal:4545/
Solution: Set the X-Content-Type-Options header to 'nosniff'.

AI Recommendations:

• Regularly update third-party libraries and dependencies.
• Integrate security testing into your CI/CD pipeline.
• Prioritize security in the software development process.

4. No HTTPS Enforcement (Medium Risk)

Description: The application does not use HTTPS, allowing insecure communication over plain HTTP.
URL: http://host.docker.internal:4545
Solution: Enforce HTTPS using HSTS headers. Redirect all HTTP traffic to HTTPS. Configure secure cookies.

AI Recommendations:

• Regularly scan for and patch security vulnerabilities.
• Integrate security testing into your CI/CD pipeline.
• Prioritize security in the software development process.