DAST Scan Report

Target URL: https://aironsafe.com

Scan Date: 2025-04-06 16:53:44
Scan ID: dast_c46dcae1

Summary

Risk Level	Count
High	0
Medium	3
Low	2
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: https://aironsafe.com/
Solution: Implement a Content Security Policy header to restrict resource loading to trusted sources.

AI Recommendations:

• Restrict inline script and style usage.
• Add CSP headers and specify trusted sources.
• Start with CSP Report-Only mode to fix issues.

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: https://aironsafe.com/
Solution: Set the X-Frame-Options header to DENY or SAMEORIGIN.

AI Recommendations:

• Use CSP frame-ancestors directive for modern browsers.
• Set X-Frame-Options to DENY on critical pages.
• 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: https://aironsafe.com/
Solution: Set the X-Content-Type-Options header to 'nosniff'.

AI Recommendations:

• Integrate security testing into your CI/CD pipeline.
• Regularly update third-party libraries and dependencies.
• Regularly scan for and patch security vulnerabilities.

4. Missing HTTP Strict Transport Security Header (Medium Risk)

Description: HSTS is not enabled for this site, which means it could be vulnerable to SSL stripping attacks.
URL: https://aironsafe.com/
Solution: Add Strict-Transport-Security header with appropriate max-age value.

AI Recommendations:

• Integrate security testing into your CI/CD pipeline.
• Regularly review the OWASP Top 10 list for application security.
• Prioritize security in the software development process.

5. Server Technology Information Disclosure (Low Risk)

Description: The server reveals technology information via headers: Express
URL: https://aironsafe.com
Solution: Configure the server to suppress the X-Powered-By header.

AI Recommendations:

• Integrate security testing into your CI/CD pipeline.
• Regularly review the OWASP Top 10 list for application security.
• Prioritize security in the software development process.

Report generated at: 2025-04-06 16:53:51
This report was automatically generated by AIronSafe DAST Scanner