

DAST Scan Report

Target URL: https://google.com

Scan Date: 2025-04-06 17:03:37
Scan ID: dast_f02b28d4

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: https://www.google.com/

Solution: Implement a Content Security Policy header to restrict resource loading to trusted sources.

AI Recommendations:

- Start with CSP Report-Only mode to fix issues.
- Set up a reporting endpoint to monitor CSP violations.
- Use nonce or hash-based CSP methods.

2. 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://www.google.com/

Solution: Set the X-Content-Type-Options header to 'nosniff'.

AI Recommendations:

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

3. 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://www.google.com/>

Solution: Add Strict-Transport-Security header with appropriate max-age value.

AI Recommendations:

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

4. Cookie Without Secure Flag (Medium Risk)

Description: A cookie (NID) is set without the Secure flag, which means it can be transmitted over unencrypted connections.

URL: <https://google.com>

Solution: Set the Secure flag on all cookies that are sent over HTTPS.

AI Recommendations:

- Encrypt or sign cookie values.
- Set Same-Site attribute to Strict or Lax.
- Use HttpOnly flag for sensitive cookies.

Report generated at: 2025-04-06 17:03:50

This report was automatically generated by AlronSafe DAST Scanner