WVS Security Scan Report

Found 7 issue(s):

Issue: Missing security header: x-frame-options (and no CSP frame-ancestors)

Severity: Medium
Description: The response lacks `x-frame-options` and `content-security-policy` with `frame-ancestors` directive. This could expose the application to clickjacking attacks.
Remediation: Implement `x-frame-options` (e.g., DENY or SAMEORIGIN) or use `content-security-policy` with the `frame-ancestors` directive to control framing.

Issue: Missing security header: strict-transport-security

Severity: Medium
Description: The response lacks the `strict-transport-security` header. This could expose the application to various attacks depending on the missing header.
Remediation: Implement the `strict-transport-security` HTTP security header. Consult OWASP Secure Headers Project for specific recommendations.

Issue: Missing security header: content-security-policy

Severity: Medium
Description: The response lacks the `content-security-policy` header. This could expose the application to various attacks depending on the missing header.
Remediation: Implement the `content-security-policy` HTTP security header. Consult OWASP Secure Headers Project for specific recommendations.

Issue: Missing security header: x-content-type-options

Severity: Medium
Description: The response lacks the `x-content-type-options` header. This could expose the application to various attacks depending on the missing header.
Remediation: Implement the `x-content-type-options` HTTP security header. Consult OWASP Secure Headers Project for specific recommendations.

Issue: Missing security header: referrer-policy

Severity: Medium
Description: The response lacks the `referrer-policy` header. This could expose the application to various attacks depending on the missing header.
Remediation: Implement the `referrer-policy` HTTP security header. Consult OWASP Secure Headers Project for specific recommendations.

Issue: Outdated component: jquery 1.6.2

Severity: Medium
Description: Detected jquery version 1.6.2, which is older than the recommended secure baseline of 3.6.0. Outdated components can contain known vulnerabilities that could be exploited.
Remediation: Upgrade jquery from version 1.6.2 to the latest stable release (at least 3.6.0 or newer). Regularly check for and apply updates to all third-party components. Consider using Software Composition Analysis (SCA) tools.

Issue: Unable to determine version of jquery

Severity: Low
Description: The scanner found an indication of `jquery` but could not extract a semantic version string. Manual verification is recommended to ensure it's not an outdated or vulnerable version.
Remediation: Manually verify the version of jquery in use. If it's outdated or known to be vulnerable, update it to a secure version. Ensure version information is consistently available in asset metadata or filenames.