WVS Security Scan Report

Found 7 issue(s):

Issue: Cookie without `Secure` flag

Severity: Medium
Description: `Set-Cookie` header `nevercache-b39818=Y; Max-Age=0` lacks the `Secure` attribute. The cookie can be transmitted over unencrypted channels.
Remediation: Add the `Secure` attribute to all sensitive cookies. This ensures they are only sent over HTTPS.

Issue: Cookie without `HttpOnly` flag

Severity: Medium
Description: `Set-Cookie` header `nevercache-b39818=Y; Max-Age=0` lacks the `HttpOnly` attribute. The cookie can be accessed by client-side scripts, increasing XSS risk.
Remediation: Add the `HttpOnly` attribute to all cookies that do not need to be accessed by JavaScript. This mitigates the risk of cookie theft via XSS.

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.