Web App Vulnerability Scan Report for http://xss-game.appspot.com/

[+] No Heartbleed vulnerability detected. Error: [Errno 11001] getaddrinfo failed

Severity: Critical. Remediation: Upgrade OpenSSL to a non-vulnerable version.

[+] SSL Certificate valid until: 2025-06-12 11:18:19

Severity: Unknown. Remediation: Review manually.

[+] Secure Protocol in use: TLSv1.3

Severity: Unknown. Remediation: Review manually.

[!] No Perfect Forward Secrecy (PFS). Cipher used: TLS_AES_256_GCM_SHA384

Severity: Unknown. Remediation: Review manually.

[+] No cookies detected.

Severity: Medium. Remediation: Set Secure, HttpOnly, and SameSite attributes on cookies.

[+] Final URL after redirects: https://xss-game.appspot.com/

Severity: High. Remediation: Encode outputs and use Content Security Policy (CSP).

[!] Missing Strict-Transport-Security: HSTS (Enforces HTTPS)

Severity: Unknown. Remediation: Review manually.

[!] Missing X-Frame-Options: Prevents Clickjacking

Severity: Unknown. Remediation: Review manually.

[!] Missing Content-Security-Policy: Prevents XSS & Data Injection

Severity: High. Remediation: Encode outputs and use Content Security Policy (CSP).

[!] Missing X-Content-Type-Options: Blocks MIME-type attacks

Severity: Unknown. Remediation: Review manually.

[!] Server Information Leakage Detected: Server: Google Frontend

Severity: Low. Remediation: Configure your server to hide version info and sensitive headers.

[!] Possible SQL Injection detected with payload: '

Severity: High. Remediation: Use parameterized queries and input validation.

[!] Possible SQL Injection detected with payload: ' OR '1'='1

Severity: High. Remediation: Use parameterized queries and input validation.

[!] Possible SQL Injection detected with payload: ' OR '1'='1' --

Severity: High. Remediation: Use parameterized queries and input validation.

[!] Possible SQL Injection detected with payload: ' OR '1'='1' /*

Severity: High. Remediation: Use parameterized queries and input validation.

[+] No DOM-Based XSS detected.

Severity: High. Remediation: Encode outputs and use Content Security Policy (CSP).

[+] No stored XSS detected.

Severity: High. Remediation: Encode outputs and use Content Security Policy (CSP).

[+] No reflected XSS detected.

Severity: High. Remediation: Encode outputs and use Content Security Policy (CSP).

[+] Open Ports: 80, 443

Severity: Unknown. Remediation: Review manually.

[!] Unable to grab banner for xss-game.appspot.com:80

Severity: High. Remediation: Encode outputs and use Content Security Policy (CSP).

[!] Unable to grab banner for xss-game.appspot.com:443

Severity: High. Remediation: Encode outputs and use Content Security Policy (CSP).

[+] Allowed HTTP Methods: GET

Severity: Unknown. Remediation: Review manually.

[+] No directory traversal vulnerabilities detected.

Severity: Critical. Remediation: Sanitize file path inputs and use whitelist-based validation.