API Vulnerability Report

Scanned URL: http://www.testingmcafeesites.com/testcat_an.html

Date: 2025-05-05 08:58:13

API2 Vulnerabilities

API is NOT using HTTPS! (Risk of data interception) [OWASP API2:2023]

Insecure protocol (HTTPS missing) [OWASP API2:2023]

No Authorization token in headers [OWASP API2:2023]

API3 Vulnerabilities

Usage of MD5 - Collision attacks [OWASP API3:2023]

Usage of SHA-1 - Weak hash strength [OWASP API3:2023]

RSA keys < 2048 bits - Easily breakable [OWASP API3:2023]

AES keys < 128 bits - Weak symmetric encryption [OWASP API3:2023]

API4 Vulnerabilities

Missing X-RateLimit-Limit - may indicate lack of rate limiting [OWASP API4:2023]

Missing X-RateLimit-Remaining - may indicate lack of rate limiting [OWASP API4:2023]

Missing Retry-After - may indicate lack of rate limiting [OWASP API4:2023]

API7 Vulnerabilities

Missing Strict-Transport-Security (Enforce HTTPS) [OWASP API7:2023]

Missing Expect-CT (Ensures Certificate Transparency) [OWASP API7:2023]

API8 Vulnerabilities

Missing Content-Security-Policy (Mitigates XSS) [OWASP API8:2023]

Missing X-Frame-Options (Clickjacking prevention) [OWASP API8:2023]

Missing X-Content-Type-Options (Prevent MIME sniffing) [OWASP API8:2023]

□□ Missing Permissions-Policy (Restricts features like camera, geolocation) [OWASP API8:2023]

□□ Missing Cross-Origin-Embedder-Policy (Prevents cross-origin resources) [OWASP API8:2023]

□□ Missing Cross-Origin-Opener-Policy (Isolates browsing context group) [OWASP API8:2023]

□□ Missing Cross-Origin-Resource-Policy (CORS policy enforcement) [OWASP API8:2023]

Uncategorized Vulnerabilities

□ SSL/TLS Check Failed: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'www.testingmcafeesites.com'. (_ssl.c:1028)

□ Strict-Transport-Security is missing! (Protects against protocol downgrade attacks [OWASP API7])

□ Content-Security-Policy is missing! (Prevents XSS attacks [OWASP API8])

□ X-Content-Type-Options is missing! (Prevents MIME-sniffing [OWASP API8])

□ X-Frame-Options is missing! (Protects against clickjacking [OWASP API8])

□ Referrer-Policy is missing! (Controls referer info [OWASP API7])

□ Permissions-Policy is missing! (Restricts powerful features [OWASP API8])

□ Cross-Origin-Embedder-Policy is missing! (Prevents cross-origin issues [OWASP API8])

□ Cross-Origin-Opener-Policy is missing! (Isolates browsing context [OWASP API8])

□ Cross-Origin-Resource-Policy is missing! (Prevents cross-origin sharing [OWASP API8])

□ Expect-CT is missing! (Certificate transparency enforcement [OWASP API7])

Generated by API Security Scanner