

API Security Report

Scanned URL: <https://example.com/api>

- ✓ API is using HTTPS. [OWASP API2:2023 - Broken User Authentication]
- ✓ Secure SSL/TLS Version: TLSv1.3
- ✓ Cipher Used: TLS_AES_256_GCM_SHA384 (TLSv1.3 bits)
- ☐ SSL/TLS Check Failed: '<' not supported between instances of 'str' and 'int'
- ☐ 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])
- ☐ 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]
- ☐ Shodan scan failed with status 403: {"error": "Requires membership or higher to access"}