API Cryptography Vulnerability Report

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

Scan Date: 2025-04-29 22:28:39

Findings

Analyzing SSL/TLS Version and Cipher...
âœ” Secure SSL/TLS Version: TLSv1.3
âœ” Cipher Used: TLS_AES_256_GCM_SHA384 (TLSv1.3 bits)
âš SSL/TLS Check Failed: '<' not supported between instances of 'str' and 'int'
Checking Important Security Headers...
âŒ Strict-Transport-Security is missing! (Protects against protocol downgrade attacks [OWASP A6])
âŒ Content-Security-Policy is missing! (Prevents XSS attacks [OWASP A7])
âŒ X-Content-Type-Options is missing! (Prevents MIME-sniffing [OWASP A5])
âŒ X-Frame-Options is missing! (Protects against clickjacking [OWASP A5])
âŒ Referrer-Policy is missing! (Controls information sent in Referer header [OWASP A6])
Checking Common Cryptographic Weaknesses (Theoretical)...
âš Usage of MD5 for hashing - Collision attacks [OWASP A3:2017]
âš Usage of SHA-1 instead of SHA-256 - Weak hash strength [OWASP A3:2017]
âš RSA keys < 2048 bits - Easier to break with modern computing [OWASP A3:2017]
âš AES keys < 128 bits - Insufficient symmetric key strength [OWASP A3:2017]

Mapped to OWASP API Top 10 and OWASP Web Top 10 vulnerabilities where applicable.