API Security Checklist: OWASP API Top 10

10 essential checks to strengthen API security and reduce exposure.



01

Broken Object-Level Authorization (BOLA)

Verify access permissions for every object.

02

Broken Authentication

Enforce strong authentication and token validation.

03

Broken Object Property-Level Authorization

Restrict access to sensitive data fields.

04

Unrestricted Resource Consumption

Apply rate limits and resource controls.

05

Broken Function-Level Authorization

Enforce role-based access for every API operation.

06

Unrestricted Access to Sensitive Business Flows

Protect critical workflows against automated abuse.

07

Server-Side Request Forgery (SSRF)

Validate destination URLs, enforce allowlists and restrict outbound network access.

08

Security Misconfiguration

Harden API configurations and disable unnecessary services.

09

Improper Inventory Management

Maintain an updated API inventory and retire obsolete endpoints.

10

Unsafe Consumption of APIs

Validate third-party API responses and data.

Reference: OWASP API Security Top 10 – 2023

www.ampcuscyber.com | letsconnect@ampcuscyber.com