



API Security Checklist

Authentication, authorisation, rate limiting, validation and monitoring for your APIs.

Version 1.0 · October 2026 · switech-solution.com

APIs are the backbone of modern apps and a popular target. This checklist follows the OWASP API Security Top 10 (2023 edition). The labels API1 to API10 refer to the respective category.

HOW TO USE THIS CHECKLIST

Work through the items in order and tick off what is done. Start with everything marked "Critical". Repeat the review before every major release and at least once per quarter.

Priorities: **CRITICAL** **IMPORTANT** **RECOMMENDED**

1 AUTHENTICATION

- ☐ **Use proven standards** **CRITICAL**
OAuth 2.0 / OpenID Connect or established auth providers. No home-made cryptography (API2).
- ☐ **Validate tokens fully** **CRITICAL**
For JWTs, check signature, expiry (exp), issuer (iss) and audience (aud). Reject the "none" algorithm.
- ☐ **Short-lived tokens** **IMPORTANT**
Short-lived access tokens, revocable refresh tokens.
- ☐ **Use API keys correctly** **IMPORTANT**
Send them in headers, never in URLs. Rotatable, separate per customer, with minimal permissions. Do not use them as the only authentication for user data.

2 AUTHORISATION

- ☐ **Check object level (API1)** **CRITICAL**
On every access to /orders/{id}, check that the object belongs to the requesting user. The most common API vulnerability.
- ☐ **Check property level (API3)** **CRITICAL**
Return only the fields needed. Prevent mass assignment: users must not be able to set fields like "role" or "isAdmin" themselves.
- ☐ **Check function level (API5)** **CRITICAL**
Check the role on the server for admin and management endpoints, rather than just hiding them in the frontend.
- ☐ **Protect sensitive business flows (API6)** **IMPORTANT**
Secure sign-up, vouchers, orders and bookings against automated abuse.

3 INPUT & VALIDATION

☐ Schema validation **CRITICAL**

Validate every request against a schema (e.g. JSON Schema, zod). Define types, lengths and value ranges, and reject unknown fields.

☐ Limit sizes and formats **IMPORTANT**

Maximum payload size, allowed content types, limits for arrays and uploads.

☐ Prevent server-side request forgery (API7) **CRITICAL**

If you fetch URLs supplied by users: check destinations against an allowlist and block internal addresses and metadata services.

4 RESOURCES & RATE LIMITING (API4)

☐ Rate limiting **CRITICAL**

Limits per user, API key and IP. When exceeded, return status 429 with a Retry-After header.

☐ Enforce pagination **IMPORTANT**

Set a maximum page size. Never return an unlimited number of records.

☐ Timeouts and cost limits **IMPORTANT**

Set timeouts for requests and queries. Set budget limits for paid services (e.g. AI APIs, SMS).

5 CONFIGURATION (API8)

☐ HTTPS only **CRITICAL**

Reject unencrypted connections and enable HSTS.

☐ Restrictive CORS **IMPORTANT**

Only allow known origins, and no "*" wildcard with credentials.

☐ Error messages without internals **IMPORTANT**

Do not send stack traces, SQL errors or version numbers to clients.

☐ Disable what you do not need **RECOMMENDED**

Switch off unused HTTP methods, debug modes and default accounts.

6 INVENTORY & VERSIONS (API9)

☐ Document the API **IMPORTANT**

Document all endpoints, e.g. with OpenAPI, including authentication and data types.

☐ Retire old versions **IMPORTANT**

Decommission outdated API versions and test endpoints in a planned way.

☐ Separate environments **RECOMMENDED**

Do not expose test and staging APIs publicly and never run them with production data.

7 THIRD-PARTY APIS (API10)

- ☐ **Do not trust responses blindly** **IMPORTANT**
Validate data from third parties just like user input.
- ☐ **Timeouts and redirects** **IMPORTANT**
Set timeouts and do not follow redirects unchecked.
- ☐ **Store keys securely** **CRITICAL**
Keep third-party credentials on the server only, in a secret manager or environment variables.

8 LOGGING & MONITORING

- ☐ **Log security events** **IMPORTANT**
Failed logins, denied access and rate-limit hits.
- ☐ **No secrets in logs** **CRITICAL**
Mask or omit tokens, passwords and full personal data.
- ☐ **Alerts and request IDs** **RECOMMENDED**
Alerts for anomalies. Request IDs make incident analysis easier.

9 TESTING

- ☐ **Test authorisation automatically** **CRITICAL**
Tests that make sure user A cannot access user B's data.
- ☐ **Scan dependencies** **IMPORTANT**
Automatically check libraries for known vulnerabilities.
- ☐ **Penetration test** **RECOMMENDED**
Have an external test carried out before major releases or when handling sensitive data.

This checklist does not replace an individual security assessment. More details: OWASP API Security Project (owasp.org).

Questions or need support?

I help small businesses and founders build secure AI tools and automations. The intro call is free.

www.switech-solution.com