API Security Checklist

OWASP API Security Top 10 — practical self-assessment

Prepared by	Nazline Mwita, CompTIA Security+
Practice	HarLyn Digital Partners
Scope	Self-assessment starting point — not a substitute for a scoped audit

Authentication & Authorization

- Every endpoint enforces authentication — no implicitly-public internal endpoints.
- Object-level authorization is checked per request (a user can't fetch another user's record by changing an ID).
- Admin/privileged endpoints are separated from the general API surface, not just hidden.

Input & Rate Handling

- Request payloads are validated against a schema, not just “happy path” checked.
- Rate limiting exists on authentication, search, and any expensive/AI-backed endpoint.
- Mass-assignment is prevented — clients can't set fields like `role` or `isAdmin` via request body.

Data Exposure

- API responses return only the fields the client actually needs, not full internal objects.
- Verbose error messages/stack traces are not returned to the client in production.
- API documentation doesn't expose internal-only or deprecated endpoints publicly.

Configuration & Inventory

- There is a current inventory of all live API versions — no forgotten v1 still accepting traffic.
- CORS policy is scoped to known origins, not a wildcard in production.
- Security headers (HSTS, CSP, X-Content-Type-Options) are set on API responses where applicable.

How to use this checklist

This is a starting-point self-assessment, not a substitute for a scoped engagement. Items checked “no” or “unsure” are candidates for a Secure Digital Workflow Assessment.

Nazline Mwita, CompTIA Security+ certified Cybersecurity Assurance Lead and Co-Founder at HarLyn Digital Partners. Specializing in authorized web & API security assessments, KDPA compliance reviews, and defensive cloud architecture in Nairobi, Kenya.