API Security Checklist

OWASP API Security Top 10 mitigations

Authentication & Authorization

- ■ API authentication required for all non-public endpoints
- ■ OAuth 2.0 / OIDC used for token-based auth (not API keys for users)
- ■ Object-level authorization enforced (BOLA prevention)
- ■ Function-level authorization checked on every request
- ■ Rate limiting applied per user/IP/API key

Input & Data

- ■ Request body size limits enforced
- ■ Input schema validation applied (JSON Schema or equivalent)
- ■ Mass assignment prevention (explicit allow-lists for writable fields)
- ■ Query parameter injection prevented (parameterized queries)
- ■ File uploads validated and sandboxed

Response & Transport

- ■ Sensitive data filtered from API responses (no over-exposure)
- ■ HTTPS enforced (no HTTP fallback)
- ■ CORS configured with specific origins (no wildcard in production)
- ■ Security headers set (X-Content-Type-Options, X-Frame-Options)
- ■ Error responses don't leak internal details