Christian Schneider
Security Architect, Hacker, Trainer

SERVICE INFO
Fixed-scope engagement · Remote or on-site

API SECURITY CHECK

A focused security review of the APIs *your business runs on*.

A pragmatic, fixed-scope assessment of your REST, GraphQL or gRPC interfaces — combining manual exploitation and targeted tooling. You receive findings prioritized by business impact, with remediation guidance your developers can act on the same week.

christian-schneider.net/service/api-security-check ↗

WHAT GETS TESTED

- **OWASP API Security Top 10**
  BOLA, broken authentication, BFLA, mass assignment, unrestricted resource consumption, SSRF — each probed against your real endpoints, not a checklist.
- **Authentication & authorization**
  OAuth2 / OIDC flows, JWT validation, scope enforcement, tenant isolation, session handling — the layer where most real-world breaches happen.
- **Business-logic abuse**
  Workflow bypasses, race conditions, quota and pricing manipulation, replay scenarios — the bugs scanners cannot see.
- **Input handling & injection**
  Injection across SQL, NoSQL, command, template and GraphQL contexts. SSRF, deserialization, XXE where applicable.
- **Data exposure & tenant isolation**
  Excessive data in responses, IDOR across tenants, leakage through verbose errors, debug endpoints and forgotten admin routes.
- **Transport & configuration**
  TLS posture, CORS, rate limits, error-handling leakage, header hygiene, gateway and WAF bypasses.

HOW IT WORKS

Kick-off and scoping → guided test phase against staging with full visibility → live debrief with engineering → written report with executive summary and per-finding remediation. Optional retest after fixes.

YOU RECEIVE

- → Written report — executive + technical
- → Findings ranked by business impact, not CVSS alone
- → Concrete remediation guidance per finding
- → Live debrief with your engineering team
- → Optional retest of fixed issues

TO GET STARTED

- → Reachable staging environment with representative data
- → API specification (OpenAPI / GraphQL schema) or Postman collection
- → Test accounts covering relevant roles and tenants

Let's scope your API Security Check.
Every engagement starts with a free scoping call to align on attack surface, access requirements and reporting depth. Fixed price once the scope is clear.

GET IN TOUCH
mail@christian-schneider.net
christian-schneider.net