Christian Schneider
Application & AI Security Architect

APPLICATION PENTEST

Breaking in before others do — with a human *actually thinking* about your application.

Automated scanners catch the low-hanging fruit. A manual pentest goes after what they miss: business-logic flaws, chained vulnerabilities, subtle auth bypasses. I run manual and semi-automated attacks against your web apps, backend APIs and mobile apps — with timing and out-of-band (DNS) side-channels to surface blind issues deep inside your backend.

christian-schneider.net/service/application-pentest ↗

WHAT GETS TESTED

- **Client & server-side application logic**
  Injection, XSS in every context, SSRF, deserialization, file-upload traps — across both halves of the stack.
- **Critical business functions**
  Payment, checkout, entitlements, workflow state machines — places where a bypass costs real money.
- **Authentication & authorization**
  BOLA/BFLA, privilege escalation, multi-tenant isolation, SSO and MFA bypass patterns.
- **Sessions, tokens & interfaces**
  Session fixation, JWT pitfalls, exposed and consumed APIs, webhook abuse, rate-limit gaps.
- **Components, dependencies & errors**
  Known-vulnerable libs, misconfigured framework defaults, verbose errors that leak internals.
- **Chained & 2nd-order attacks**
  A minor info-disclosure plus a weak session token is often worse than either alone. Optional backoffice access lets me chase payloads that detonate deeper in your pipeline.

HOW THE ENGAGEMENT RUNS

1. **Scoping call**
   Align on targets, backend systems, exclusions, reporting format and timeframe.
2. **Manual & semi-automated testing**
   Offensive techniques against web, API and mobile — plus side-channels for blind findings.
3. **Detailed report**
   Every finding with evidence, exploit steps, mitigation advice and hardening tips.
4. **Debriefing & optional re-test**
   Walkthrough with the remediation team. Optional follow-up check produces an updated report.

REPORT, ROUTED TO THE RIGHT TEAM

- → Findings categorised by **business**, **architecture**, **dev**, **ops**
- → Evidence, reproduction steps & risk rating
- → Concrete mitigation advice & hardening tips
- → Debriefing with remediation owners + optional re-test

TO START, I NEED

- Access to the app (URLs, clients)
- ≥ 2 test users with different data/tenants
- Sample files for special upload formats (if present)
- For API tests: docs or sample requests

BUNDLE TIP

Pair with an **Attack Tree Quickstart** — the tree maps threats at architecture level, the pentest validates real-world exploitability.

Let's scope your pentest.
Every engagement starts with a free scoping call to align on targets, timeframe and reporting — so testing focuses on your real business risk.

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