

APPLICATION SECURITY

Application security assessment

Manual penetration testing for web apps, APIs, mobile, Backend-as-a-Service platforms like Supabase, and LLM-powered products.

OWASP TOP 10:2025 · API TOP 10:2023 · LLM TOP 10:2026 · ASVS 5.0 · MASVS · CVSS 4.0

Your application is no longer one thing. It is a web front end, a set of APIs, a managed backend and, more and more often, a language model that can call tools. Each layer fails in its own way, and an attacker only needs one.

We test the whole stack the way an attacker would: manually, with an understanding of how your business works, and well beyond the OWASP Top 10. Every finding comes with proof and steps to fix it, and we retest for free once you've patched.

20+

Organisations secured

30+

Applications secured

250+

Vulnerabilities found

8K+

Devices assessed

WHAT YOU GET**■ Manual testing**

Scanners for breadth, people for depth

■ Scored and mapped

CVSS 4.0, CWE and OWASP for each issue

■ Proof for every finding

Evidence and reproduction steps, no guesses

■ Free retest

We confirm the fix once you've patched



Every layer of a modern application

Each engagement is scoped to how your product is actually built. These are the application types we test most, and the standard we map findings to.

01

Web applications

SPAs and multi-tenant SaaS. Access control across roles and tenants, sessions, injection and client-side flaws.

OWASP TOP 10:2025 · ASVS 5.0

02

APIs

REST, GraphQL, gRPC and webhooks. Object and function level authorisation, mass assignment, rate limits, query depth.

OWASP API SECURITY TOP 10:2023

03

Mobile apps

iOS and Android builds and the APIs behind them. Local storage, certificate pinning, deep links, secrets in the binary.

OWASP MASVS · MASTG

04

BaaS and serverless

Supabase, Firebase, Amplify and edge functions. The rules your client trusts: RLS, security rules, storage, exposed keys.

PLATFORM HARDENING · ASVS 5.0

05

LLM and AI features

Chatbots, copilots, RAG, agents and MCP servers. Prompt injection, data leakage, tool abuse and runaway inference cost.

OWASP LLM TOP 10:2026 · AGENTIC TOP 10

06

Thick clients and portals

Desktop apps, admin consoles and partner integrations. Local trust, update channels and hidden admin functions.

OWASP TOP 10:2025 · ASVS 5.0



Business logic testing, in every engagement

Common vulnerability classes are shrinking. Logic flaws are not: a skipped payment step, coupons that stack, an approval a user can grant themselves, a quota that resets under a race condition. No scanner finds these. We sit with your team to model abuse cases for your workflows before we test, and we test every one of them.



Three OWASP lists, one baseline

Our test cases go well past these lists, but every finding we report maps back to the current edition of each one.

WEB APPLICATIONS

OWASP Top 10:2025

A01	Broken Access Control
A02	Security Misconfiguration
A03	Software Supply Chain Failures
A04	Cryptographic Failures
A05	Injection
A06	Insecure Design
A07	Authentication Failures
A08	Software or Data Integrity Failures
A09	Security Logging and Alerting Failures
A10	Mishandling of Exceptional Conditions

APIs

OWASP API Top 10:2023

API1	Broken Object Level Authorization
API2	Broken Authentication
API3	Broken Object Property Level Authorization
API4	Unrestricted Resource Consumption
API5	Broken Function Level Authorization
API6	Unrestricted Access to Sensitive Business Flows
API7	Server Side Request Forgery
API8	Security Misconfiguration
API9	Improper Inventory Management
API10	Unsafe Consumption of APIs

LLM AND AI

OWASP LLM Top 10:2026

LLM01	Prompt Injection
LLM02	Sensitive Information Disclosure
LLM03	Excessive Agency
LLM04	Supply Chain
LLM05	Data and Model Poisoning
LLM06	Unbounded Consumption
LLM07	Misinformation
LLM08	Hidden Context Exposure
LLM09	Vector and Embedding Weaknesses
LLM10	Improper Output Handling

BACKEND-AS-A-SERVICE DEEP DIVE

Supabase, Firebase and friends

On a BaaS app the database is one request away from the browser. We test with the same public key your users hold, then review the policies behind it. The same approach covers Firebase, Appwrite and PocketBase.

- Row Level Security on every exposed table
- Storage bucket policies and public buckets
- Edge Functions: JWT verification and CORS
- Realtime channel and presence authorisation
- service_role key or secrets in client bundles
- SECURITY DEFINER functions exposed over RPC
- Auth redirects, user enumeration, OTP limits
- Views and query filters that bypass RLS



Six phases, start to finish

Every engagement follows the same six phases. Once you've patched, we go back and re-exploit every finding to confirm the fix, at no extra cost.





How we score, and what you receive

RISK SCORING

CVSS 4.0, adjusted for your environment

Every finding carries a full CVSS 4.0 vector, with Threat and Environmental metrics set for your deployment rather than a generic worst case. Where CVSS undersells a logic or AI flaw, we add an OWASP Risk Rating (likelihood times impact) and say so in the finding.

Base	Threat	Environmental	Supplemental
How easy the flaw is to exploit and what it exposes	Whether working exploits exist or are used in the wild	Your compensating controls and how much the asset matters	Automation, recovery and safety context for triage

CVSS 4.0 metric groups. Supplemental metrics add context to a finding but do not change its score.

SEVERITY BANDS

SEVERITY	CVSS 4.0	TYPICAL IMPACT	SUGGESTED FIX
■■■■ Critical	9.0 to 10.0	Remote compromise or mass data exposure	Within 7 days
■■■□ High	7.0 to 8.9	Other users' data or admin functions	Within 30 days
■■□□ Medium	4.0 to 6.9	Needs conditions or user action	Within 90 days
■□□□ Low	0.1 to 3.9	Hard to exploit or minor exposure	Next release
□□□□ Info	0.0	Hardening, no direct risk	As planned

THE REPORT

- Executive summary for leadership
- Findings with CVSS 4.0 vector, CWE and OWASP ID
- Proof of concept and reproduction steps
- Fix guidance for your stack and framework
- Assets and data reached during testing
- Retest report confirming each fix

Plan your next assessment

Tell us what you are building and we'll scope the test with you.

www.sentryark.com

contact@sentryark.com

OSCE · CRT0 · CEH · ISO 27001