

SERVICE DATA SHEET

API Security Testing

Secure the APIs behind your applications, partners and mobile apps

APIs now carry most of the traffic behind web and mobile applications, partner integrations and microservices. They expose business logic and data directly, often with less scrutiny than the interface in front of them.

The most damaging API flaws are rarely bugs a scanner can find. They are authorisation gaps: one customer reading another's invoices by changing an ID, a regular user calling an admin function, or an endpoint returning far more data than the app displays.

SentryArk's API assessments find these flaws with manual, role-aware testing that goes beyond the OWASP API Security Top 10, covering REST, GraphQL, gRPC and SOAP services.

AUTHORISATION AND BUSINESS LOGIC TESTING

We test every endpoint with multiple user roles and tenants, comparing what each can see and do. This is how we uncover broken object-level authorisation (BOLA), broken function-level authorisation and mass assignment, the flaws behind many large API data breaches.

- Object-level authorisation
- Function-level access control
- Authentication and tokens
- Excessive data exposure
- Rate limiting and abuse
- Injection and input validation

BUILT AROUND YOUR DOCUMENTATION

Testing starts from your OpenAPI or Swagger specification, Postman collections or captured traffic, so every documented endpoint is covered. We also look for the undocumented and legacy versions an attacker would find.

Findings are verified by hand and reported with the exact requests and responses, so your developers can reproduce and fix them quickly.

ASSESSMENT DETAILS AND METHODOLOGY

Our API methodology follows the OWASP API Security Top 10 and the OWASP Web Security Testing Guide, with greater emphasis on authorisation and business logic than automated tools can give.

**Planning and
information gathering**

01

We collect specifications, collections and test accounts for each role, and agree environments and rate limits.

Discovery and mapping

02

We map endpoints, parameters, versions and data objects, including undocumented routes found through traffic analysis and fuzzing.

Vulnerability analysis

03

Automated scanning plus manual testing of authentication, token handling, input validation and configuration.

**Authorisation and logic
testing**

04

Role- and tenant-differential testing of every endpoint to find BOLA, BFLA, mass assignment and workflow abuse.

Reporting and retest

05

Findings with full request and response evidence, risk ratings and remediation, then a retest to confirm the fixes.

The assessment includes

- Executive summary
- Findings mapped to OWASP API Top 10
- Detailed remediation steps
- Endpoint coverage map
- Request and response evidence
- Retest of fixed issues

ABOUT SENTRYARK

SentryArk is a team of security engineers and offensive security specialists. Our consultants hold OSCE, CRYPTO and CEH certifications. We have secured 20+ organisations, assessed 8K+ devices and 30+ applications, and reported 250+ vulnerabilities. Our focus is offensive security that shows the real-world risk to your business.