



API Security Testing

Protect your APIs,
protect your business



Ensure APIs are robust against cyber threats, safeguarding sensitive data and system integrity.

Fujitsu Cyber's API Security Testing ensures your APIs are robust against cyber threats. We assess authentication and authorisation, identify injection vulnerabilities (SQL, XML, NoSQL), evaluate data protection, test rate limiting and throttling, and detect business logic flaws. All testing is aligned with the OWASP API Security Top 10.



Vulnerability identification

Uncover security flaws before they can be exploited.



Strengthen risk posture

Reduce the likelihood of breaches, data leaks, and service disruptions.



Ensure compliance

Validate that APIs meet industry and regulatory security standards.



Build stakeholder confidence

Demonstrate a proactive approach to protecting systems and data.

The risks it uncovers



Gaps in endpoint and network detection



Injection attacks (SQL, XML, NoSQL)



Sensitive data exposure and weak encryption



Insufficient rate limiting and throttling



Business logic and workflow flaws



Detecting workflow and login weaknesses.

Gain clarity, confidence, and control over your environment

Our approach

Reconnaissance:

Gather and analyse API documentation, endpoints, and authentication mechanisms.

Automated and manual testing:

Use automated tools and manual validation for thorough analysis.

Exploitation and validation:

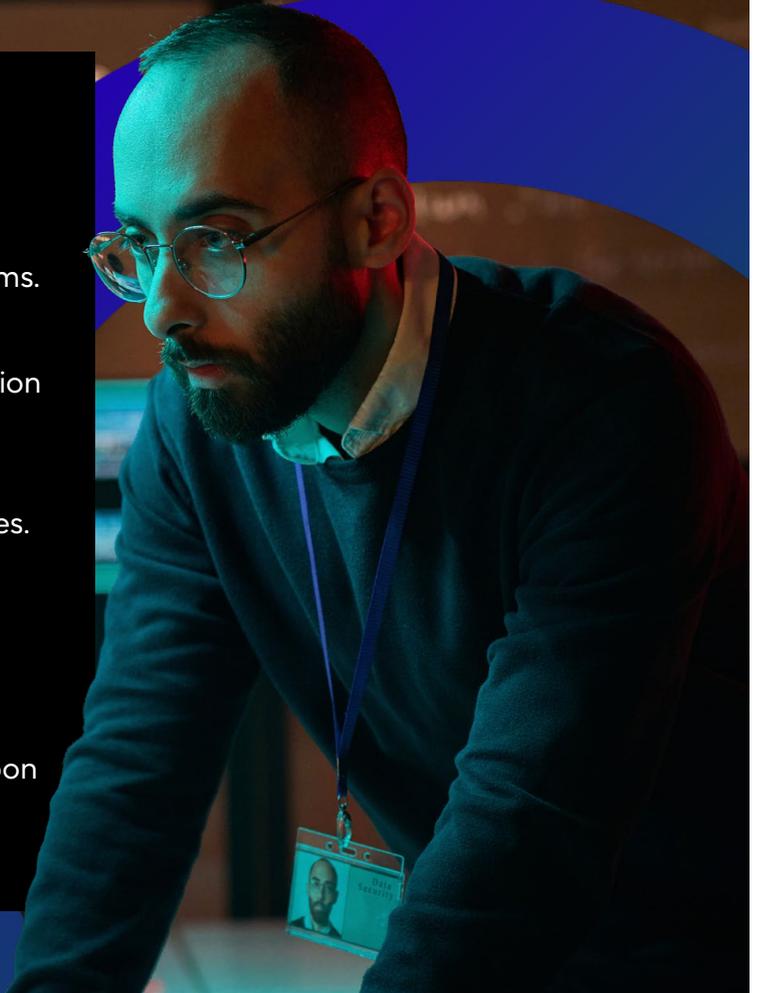
Simulate attacks to confirm vulnerabilities.

Reporting and recommendations:

Provide actionable insights and security improvements.

Retesting support:

Verification of high-impact issue fixes upon request.



Choose Fujitsu for expert-led API security testing, decades of cross-industry experience, proven OWASP-aligned methodologies, and actionable insights that strengthen your security posture every step of the way. You'll receive a comprehensive report including a detailed security assessment with vulnerabilities and impact analysis.



Comprehensive report:

Technical findings with MITRE ATT&CK mapping and business risk context.



Expert-led testing:

Cyber specialists with decades of experience across industries.



Remediation guidance:

Steps to resolve identified security flaws.

Ready to get started?

Let's work together to uncover vulnerabilities before they become threats

