CAPIE - Certified API Hacking Expert

Shinobi AI

By continuing to learn, you have shown a deep understanding of how applications interact with APIs, and the ability to hack them.

Date of achievement: 27 Aug 2025

Signature

Thijs Wesley
CEO

Signature

M. G.

Martin Greig
CTO

CAPIE - Certified API Hacking Expert

Competencies & Syllabus

Core Competencies

Holders of this certificate have demonstrated:

API identification, enumeration, and documentation analysis.

Mastery of the OWASP API Top 10 categories, including BOLA, Broken Authentication, Excessive Data Exposure, Mass Assignment, Injection, Security Misconfigurations, SSRF, and more.

Practical exploitation of API flaws with both manual and automated techniques.

Application of recon, vulnerability identification, exploitation, and professional reporting in real-world scenarios.

CAPIE - Certified API Hacking Expert

Competencies & Syllabus

Syllabus Coverage

API Fundamentals – REST, SOAP, schema & documentation.

OWASP API Top 10 (2019 & 2021) – full vulnerability coverage.

Offensive Testing Techniques – enumeration, fuzzing, authentication & authorization testing.

Hands-on Labs – guided practice across all vulnerability categories.

Final Exam – 4-hour practical, simulating a vulnerable API with 10 critical flaws. Candidates proved their ability by exploiting at least 7 vulnerabilities and submitting a professional report.

CAPIE - Certified API Hacking Expert

Competencies & Syllabus

Outcome

A CAPIE-certified professional can confidently:

Identify APIs and their attack surfaces.

Exploit and report API vulnerabilities to professional standards.

Apply a structured methodology aligned with real bug bounty and pentesting practices.