



THE XSS RAT · CERTIFICATION

Issued by Wesley Thijs · ratcerts.com

EXPERT

CAPIE

CERTIFIED API HACKING EXPERT

This certifies that

Ariful Islam Anik

has demonstrated expert-level practical competence in API security testing, covering authentication, authorisation, business-logic and injection flaws in real-world APIs.

DATE OF AWARD

7 February 2024

ISSUED BY

The XSS Rat



CERTIFICATE ID

CECC-0A2A-380C-9F7B

VERIFY AT

ratcerts.com/verify?code=CECC-0A2A-380C-9F7B

Wesley Thijs · Founder & Lead Examiner
OSCP · CNWPP · CAPIE · CWAP



THE XSS RAT · CERTIFICATION

Issued by Wesley Thijs · ratcerts.com

SYLLABUS · PAGE 2 OF 3

CAPIE - What was taught

CERTIFIED API HACKING EXPERT

HOW IT WAS EXAMINED

A 4-hour practical exam on a live API seeded with 10 medium, high and critical vulnerabilities. The candidate must find and exploit at least 7 of the 10 to pass. Chapter MCQs and assignments gate entry to the exam.

Chapter 1 · An introduction to APIs

- What is an API
- SOAP vs REST
- Authentication & authorisation: API keys, Basic, JWT, OAuth 2.0, OpenID Connect
- Code review of each auth scheme
- API architectures
- Reading API documentation

Chapter 2 · How to talk to an API

- curl
- Postman
- SoapUI
- Python for API testing
- Fuzzing an API
- Hackxpert-brute: our open-source API hacking tool

Chapter 3 · OWASP API Top 10 (2019)

- BOLA
- Broken user authentication
- Excessive data exposure
- Lack of rate limiting
- Broken function level authorisation
- Mass assignment
- Security misconfiguration
- Injection
- Improper asset management
- Insufficient logging & monitoring
- Recorded demo per category



THE XSS RAT · CERTIFICATION

Issued by Wesley Thijs · ratcerts.com

SYLLABUS · PAGE 3 OF 3

CAPIE - What was taught

CERTIFIED API HACKING EXPERT

CONTINUED

Chapter 4 · OWASP API Top 10 (2023)

- BOLA
- Broken authentication
- Broken object property level authorisation
- Unrestricted resource consumption
- Broken function level authorisation
- Unrestricted access to sensitive business flows
- SSRF
- Security misconfiguration
- Improper inventory management
- Unsafe consumption of APIs

Chapter 5 · Pentesting API documentation

- Writing the test plan
- Writing the test report
- Running the debrief meeting
- Worked examples: API pentest plan and report

Chapter 6 · API firewalls & security

- What an API firewall is
- Installing your own API firewall
- Bypassing an API firewall
- Securing a REST API: best practices

Chapter 7 · Build your own API to hack

- The basics
- Faking it before making it
- Information disclosure
- Business logic
- Emulating wonky behaviour
- API roulette: name the issues

Chapter 8 · API practice labs

- Running the labs in Docker
- OWASP API Top 10 2019 & 2023 lab machines
- Authentication API labs
- Practice exams and the exam machine walkthrough