API SECURITY WORKSHOP

How to Defend your APIs

If you are involved in designing or securing APIs within your organization then this complimentary half-day workshop is a must attend.

This workshop combines insightful educational sessions on the latest API threats and vulnerabilities and the OWASP API Top 10 with practical hands-on tutorials and drills using the 42Crunch API Security platform testing and runtime protection tooling.

WORKSHOP **AGENDA**

INTRODUCTION TO API SECURITY
Why API security matters, and the challenges it poses

OWASP API SECURITY TOP 10
Understanding the Top vulnerabilities facing APIs, with real use cases and remediation

AUTHENTICATION & AUTHORIZATION
Understand the key concepts

DATA INTEGRITY
Protect your API data

API SECURITY TESTING
Testing APIs with Postman and 42Crunch

SECURING APIS ON GITHUB
Automated API testing with GitHub Actions

API RUNTIME PROTECTION
How to use an API firewall to protect and monitor APIs

WORKSHOP **LEADERS**

Tutor led, classroom environment, practical hands-on workshop

COLIN DOMONEY
Author: Defending APIs

AXEL GROSSE
Head of Presales 42Crunch

WHO SHOULD **ATTEND?**

This workshop gives API and security professionals an in-depth understanding of the essentials of API security, how it is different to traditional application security and gain hands-on practical exposure to tooling designed specifically to address the challenges of API security. So whether you're involved in development, security, operations or indeed API management, then this event is designed for you.

WHAT TO **BRING?**

Laptop (Windows, Linux or Mac)

Software & Tools

- Postman
- VS Code
- GitHub account
- Docker (optional)

42crunch