CYBERSECURITY · SHORT COURSE

Secure API Engineering and OWASP API Security Testing

This practical course equips software developers, application security professionals, penetration testers, system administrators, DevSecOps teams, and IT security practitioners with the knowledge and hands-on skills required to design, develop, secure, assess, and test Application Programming Interfaces (APIs).

DATES	30 Nov – 4 Dec 2026	DURATION	5-day course
COURSE FEE	TZS 1,200,000 · per participant	VAT	Fee excludes VAT
VENUE	Arusha, Tanzania	DAILY HOURS	8:30 AM – 4:30 PM
FEE INCLUDES	Course materials, lunch and refreshments	CERTIFICATE	Certificate of attendance
TRAINER	Elly International training team	APPLICATIONS	Open for applications

Overview

This practical course equips software developers, application security professionals, penetration testers, system administrators, DevSecOps teams, and IT security practitioners with the knowledge and hands-on skills required to design, develop, secure, assess, and test Application Programming Interfaces (APIs).

Participants will explore secure API architecture, authentication and authorization, input validation, access control, data protection, secure coding practices, API gateway security, logging, monitoring, and secure API lifecycle management. The course places particular emphasis on identifying and addressing vulnerabilities described in the OWASP API Security Top 10, using controlled and authorised testing environments.

Through practical laboratory exercises, secure coding activities, API assessment scenarios, case studies, and guided security testing workflows, participants will learn how to identify weaknesses, validate security controls, document findings, and recommend appropriate remediation measures for enterprise APIs.

The course also covers API security within modern architectures, including REST APIs, JSON-based services, microservices, API gateways, cloud environments, and DevSecOps pipelines.

Course content

Module 1: API Architecture and Security Fundamentals

- Introduction to APIs and modern API architectures
- REST, HTTP, JSON, and web service fundamentals
- API endpoints, resources, methods, and parameters
- API request and response structures
- RESTful API design principles
- API lifecycle and security considerations
- Common API security threats

- Security-by-design principles
- Threat modelling for APIs
- API attack surface identification

Module 2: Secure API Engineering and Design

- Secure API architecture principles
- Designing secure API endpoints
- Input validation and output encoding
- Secure error handling
- Data minimisation and exposure control
- Secure HTTP methods and status codes
- API versioning and backward compatibility
- Rate limiting and resource consumption controls
- Secure API documentation
- Secure coding standards for API development
- Security requirements throughout the API lifecycle

Module 3: API Authentication and Authorization

- Authentication versus authorization
- Session-based and token-based authentication
- API keys and their security considerations
- OAuth 2.0 concepts
- OpenID Connect fundamentals
- JSON Web Tokens (JWT)
- Token lifecycle and validation
- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Object-level and function-level authorization
- Secure credential and secret management

Module 4: OWASP API Security Top 10

- Introduction to the OWASP API Security Top 10
- Broken Object Level Authorization (BOLA)
- Broken Authentication
- Broken Object Property Level Authorization
- Unrestricted Resource Consumption
- Broken Function Level Authorization
- Unrestricted Access to Sensitive Business Flows
- Server-Side Request Forgery (SSRF)
- Security Misconfiguration
- Improper Inventory Management
- Unsafe Consumption of APIs
- Understanding vulnerability impact and remediation

Module 5: API Security Testing Methodology

- API security testing principles
- Defining scope and authorised testing boundaries
- API reconnaissance and endpoint discovery
- Reviewing API documentation
- Identifying authentication and authorization controls

- Request and response analysis
- Parameter and input testing
- Testing access control mechanisms
- Testing error handling and security configurations
- Evidence collection and vulnerability documentation
- Risk assessment and remediation recommendations

Module 6: API Testing Tools and Techniques

- Introduction to API security testing tools
- Using API documentation for security assessment
- Intercepting and analysing HTTP requests
- Testing APIs using controlled testing environments
- API request modification and validation
- Automated and manual API security testing
- Authentication and authorization testing
- Testing rate limiting and resource controls
- Analysing API responses and error messages
- Developing repeatable API security test cases
- Practical API testing laboratory exercises

Module 7: API Data Protection and Secure Communication

- HTTPS and TLS for API communication
- Certificate and encryption considerations
- Protecting sensitive API data
- Secure handling of personal and confidential information
- Data exposure and excessive data return
- Secure storage of API credentials and secrets
- Secure configuration management
- Preventing information leakage
- Secure logging and sensitive-data handling
- API privacy and data protection considerations

Module 8: API Gateway, Microservices and Cloud Security

- API gateway architecture
- Gateway authentication and authorization
- Rate limiting and traffic management
- API routing and access policies
- Microservices security considerations
- Service-to-service authentication
- Zero Trust principles for APIs
- Containerised API security
- Cloud API security concepts
- Managing API keys and secrets
- Monitoring API traffic and security events

Module 9: API Security Monitoring and Incident Response

- API security logging and monitoring
- Identifying suspicious API activity
- Authentication and authorization event monitoring
- Detecting abnormal API usage

- Rate-limit and abuse monitoring
- Security alerts and incident investigation
- API audit trails
- Security incident response for APIs
- Vulnerability management and remediation tracking
- Continuous API security assessment
- Security metrics and reporting

Module 10: Secure API Testing Capstone and Remediation

- Developing an API security assessment plan
- Mapping endpoints against OWASP API Security risks
- Conducting a controlled API security assessment
- Identifying authentication and authorization weaknesses
- Testing input validation and access controls
- Assessing API configuration and data exposure
- Prioritising identified security findings
- Developing remediation recommendations
- Preparing a professional API security testing report
- Re-testing remediated vulnerabilities
- Building an API security testing checklist
- Developing an API security improvement action plan

Who should attend

This course is designed for:

- Software developers
- API developers and engineers
- Application security professionals
- Cybersecurity professionals
- Penetration testers
- Ethical hackers
- Security analysts
- DevSecOps engineers
- DevOps engineers
- Cloud security professionals
- System administrators
- Network and infrastructure professionals
- Security architects
- Application architects
- QA and software testing professionals
- IT auditors
- SOC and incident response professionals
- ICT managers and security managers
- Professionals responsible for API development, deployment, and security

Suitable Sectors

The course is particularly relevant to banks and financial institutions, telecommunications companies, government ministries and agencies, universities and educational institutions, hospitals and healthcare organisations, e-commerce companies, fintech companies, technology companies, insurance organisations, NGOs, development organisations, and enterprises that develop or operate APIs, web applications, mobile applications, cloud services, and microservices.

How to apply

Apply online at ellyinternational.co.tz. Your place is confirmed only after we review your application and contact you, within 1 working day.

Apply for this course | Ask on WhatsApp | Email us

+255 757 066 880 · training@ellyinternational.co.tz · Boma Road, Arusha, Tanzania · P.O. Box 13424

Details correct as of 28 November 2026.