Pentesting API Gateways and Microservices Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Modern application architectures rely heavily on Microservices and API Gateways to deliver fast, scalable, and resilient services, making them a primary target for sophisticated cyberattacks. Pentesting API Gateways and Microservices Training Course is meticulously designed to equip security professionals and developers with the critical offensive skills necessary to identify, exploit, and remediate security vulnerabilities unique to these distributed environments. You will dive deep into the OWASP API Security Top 10 (2023), learning to bypass centralized controls at the Gateway and uncover hidden flaws within individual microservices. By mastering the art of API Penetration Testing within a complex, cloud-native landscape, you will significantly strengthen your organization's security posture against real-world data breaches and business logic flaws.

This course emphasizes a DevSecOps-focused methodology, translating theoretical attack vectors into actionable defense strategies. You will move beyond traditional web application testing, focusing on the nuances of Broken Object Level Authorization (BOLA), Unrestricted Resource Consumption, and securing East-West traffic within the service mesh. Utilizing industry-standard tools and realistic lab environments, you will gain practical expertise in both Black-Box and Grey-Box testing of modern APIs, ensuring you can effectively secure the entire application ecosystem from the perimeter (API Gateway) to the core. Graduate ready to champion API-first security and drive a shift-left security culture within your development lifecycle.

Programme Curriculum

Pentesting API Gateways and Microservices Training Course

Introduction

Modern application architectures rely heavily on Microservices and API Gateways to deliver fast, scalable, and resilient services, making them a primary target for sophisticated cyberattacks. Pentesting API Gateways and

Microservices Training Course is meticulously designed to equip security professionals and developers with the critical offensive skills necessary to identify, exploit, and remediate security vulnerabilities unique to these distributed environments. You will dive deep into the OWASP API Security Top 10 (2023), learning to bypass centralized controls at the Gateway and uncover hidden flaws within individual microservices. By mastering the art of API Penetration Testing within a complex, cloud-native landscape, you will significantly strengthen your organization's security posture against real-world data breaches and business logic flaws.

This course emphasizes a DevSecOps-focused methodology, translating theoretical attack vectors into actionable defense strategies. You will move beyond traditional web application testing, focusing on the nuances of Broken Object Level Authorization (BOLA), Unrestricted Resource Consumption, and securing East-West traffic within the service mesh. Utilizing industry-standard tools and realistic lab environments, you will gain practical expertise in both Black-Box and Grey-Box testing of modern APIs, ensuring you can effectively secure the entire application ecosystem from the perimeter (API Gateway) to the core. Graduate ready to champion API-first security and drive a shift-left security culture within your development lifecycle.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Master the OWASP API Security Top 10 (2023) and implement effective countermeasures.
2. Perform Advanced API Reconnaissance to map microservice architecture and discover hidden endpoints.
3. Execute Broken Object Level Authorization (BOLA) and BFLA exploitation on REST and GraphQL APIs.
4. Conduct comprehensive API Gateway Security Assessment, focusing on authentication, rate limiting, and policy bypasses.
5. Identify and exploit Business Logic Flaws and Unrestricted Access to Sensitive Business Flows in microservices.
6. Analyze and test security controls for JSON Web Tokens (JWT) and OAuth 2.0 implementations.
7. Secure East-West Traffic and inter-service communication within a Service Mesh
8. Discover and mitigate Server-Side Request Forgery (SSRF) vulnerabilities targeting internal microservices.
9. Apply Mass Assignment and Excessive Data Exposure techniques to demonstrate data leakage.
10. Integrate API Penetration Testing into a CI/CD pipeline.
11. Test for Unrestricted Resource Consumption flaws to prevent denial-of-service (DoS) attacks.
12. Generate High-Impact Penetration Test Reports with clear, actionable remediation guidance.
13. Implement Zero Trust Architecture principles within a Microservices environment.

Target Audience

1. Penetration Testers and Security Analysts.
2. API Developers and Software Engineers.
3. Security Architects.
4. DevSecOps Engineers.
5. Application Security team members.
6. Cloud Security Professionals.
7. IT Auditors.
8. Red Team and Blue Team members.

Course Modules

Module 1: Microservices and API Gateway Security Fundamentals

- Understanding the distributed Microservices Architecture and the role of the API Gateway
- Mapping East-West and North-South traffic and associated security risks.
- Introduction to OWASP API Security Top 10 (2023) as the core testing methodology.
- Lab Setup: Deploying the vulnerable multi-service environment
- Case Study: Analyzing a major data breach caused by a misconfigured API Gateway proxying internal services.

Module 2: Advanced API Reconnaissance and Endpoint Discovery

- Techniques for Passive and Active API Reconnaissance
- Tools and methods for discovering undocumented or hidden API endpoints and service schemas.
- Analyzing OpenAPI/Swagger documentation for exploitable information disclosures.
- Testing for Improper Assets Management and versioning flaws.
- Case Study: Using a public Swagger file to map a bank's internal microservice endpoints, revealing sensitive operations.

Module 3: Authentication and Authorization Flaws (BOLA/BFLA)

- In-depth exploitation of Broken Object Level Authorization via ID parameter manipulation.
- Identifying and exploiting Broken Function Level Authorization in administrative functions.
- Attacking Broken Authentication mechanisms, including weak password flows and user enumeration.
- Advanced techniques for testing role-based access controls across services.
- Case Study: The infamous Uber BOLA attack.

Module 4: JWT, OAuth, and Identity Management Security

- Analyzing and exploiting flaws in JSON Web Tokens, including weak secrets and algorithm manipulation
- Attacking OAuth 2.0 and OpenID Connect flows in a Microservices context
- Testing for token-handling vulnerabilities like token reuse and lack of proper revocation.
- Implementing secure token validation and centralizing authorization at the API Gateway.
- Case Study: A breach where an attacker exploited a "none" algorithm JWT to impersonate an administrator and change user roles.

Module 5: Injection and Data Integrity Attacks

- Exploiting traditional injection flaws in API payloads.
- Testing for and mitigating Mass Assignment by over-posting or manipulating request object properties.
- Detecting Excessive Data Exposure by observing sensitive fields returned in default responses.
- Advanced payload construction for various content types
- Case Study: Exploiting a Mass Assignment flaw to escalate privileges by adding an is_admin.

Module 6: Business Logic and Resource Consumption Flaws

- Identifying and exploiting Unrestricted Access to Sensitive Business Flows via automation and rate-limit bypass.
- Testing and fixing Unrestricted Resource Consumption by manipulating request size, frequency, or resource pointers.
- Finding logic flaws in multi-step transactions and checkout processes spanning multiple microservices.

- Techniques for effective Rate Limiting and Throttling bypass on the API Gateway.
- Case Study: A case of an e-commerce API allowing a user to repeatedly use a one-time coupon code by manipulating the flow between the checkout and inventory microservices.

Module 7: Attacking the Service Mesh and Lateral Movement

- Exploitation of internal East-West communication and default-open network policies.
- Executing Server-Side Request Forgery to pivot into internal microservices and cloud metadata endpoints.
- Understanding and exploiting Security Misconfiguration in container and service mesh settings
- Techniques for securing mTLS and implementing a full Zero Trust model between services.
- Case Study: An attacker using an SSRF vulnerability in a public API endpoint to access the AWS metadata service to steal IAM credentials.

Module 8: Reporting, Remediation, and DevSecOps Integration

- Crafting a professional, high-impact API Penetration Test Report for both executive and technical audiences.
- Prioritizing vulnerabilities and providing actionable remediation strategies and secure coding practices.
- Integrating security testing tools and policies into the CI/CD pipeline for a Shift-Left approach.
- Implementing robust Logging & Monitoring and building API-specific WAF/Gateway rules.
- Case Study: Reviewing a final report and proposed remediation plan for a company whose microservices were leaking customer PII.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org **or call** +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com