Securing Web Applications 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

In the current digital landscape, modern software architectures, primarily driven by Cloud-Native technologies, have ushered in an era of rapid deployment and immense scalability through Microservices and powerful Web Applications. However, this shift has also expanded the Attack Surface significantly. Organizations must move beyond perimeter defenses to adopt a "Shift Left" approach, integrating security into every phase of the CI/CD pipeline. Securing Web Applications and Microservices Training Course provides the comprehensive knowledge and Hands-on Labs necessary to defend against the latest threats, from the OWASP Top 10 to sophisticated API Security and supply chain vulnerabilities, ensuring your applications are resilient, compliant, and Zero-Trust ready.

The complexity of interconnected services, ephemeral environments like Containers and Serverless functions, and reliance on Third-Party Dependencies demands advanced security expertise. Security professionals and developers need to master modern defense strategies like Runtime Application Self-Protection (RASP), secure Authentication and Authorization for distributed systems, and implementing Mutual TLS for inter-service communication. By focusing on practical application of DevSecOps principles and leveraging AI-Driven Threat Detection, this training empowers teams to build and maintain Secure-by-Design applications that meet critical Governance, Risk, and Compliance standards in a rapidly evolving threat landscape.

Programme Curriculum

Securing Web Applications and Microservices Training Course

Introduction

In the current digital landscape, modern software architectures, primarily driven by Cloud-Native technologies, have ushered in an era of rapid deployment and immense scalability through Microservices and powerful Web

Applications. However, this shift has also expanded the Attack Surface significantly. Organizations must move beyond perimeter defenses to adopt a "Shift Left" approach, integrating security into every phase of the CI/CD pipeline. Securing Web Applications and Microservices Training Course provides the comprehensive knowledge and Hands-on Labs necessary to defend against the latest threats, from the OWASP Top 10 to sophisticated API Security and supply chain vulnerabilities, ensuring your applications are resilient, compliant, and Zero-Trust ready.

The complexity of interconnected services, ephemeral environments like Containers and Serverless functions, and reliance on Third-Party Dependencies demands advanced security expertise. Security professionals and developers need to master modern defense strategies like Runtime Application Self-Protection (RASP), secure Authentication and Authorization for distributed systems, and implementing Mutual TLS for inter-service communication. By focusing on practical application of DevSecOps principles and leveraging AI-Driven Threat Detection, this training empowers teams to build and maintain Secure-by-Design applications that meet critical Governance, Risk, and Compliance standards in a rapidly evolving threat landscape.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Analyze the Threat Landscape for distributed, cloud-native applications.
2. Implement OWASP Top 10 mitigations in modern Web and API codebases.
3. Design and secure RESTful and GraphQL APIs using best practices.
4. Apply the Zero-Trust Architecture model to Microservices communication.
5. Master secure Authentication and Authorization protocols like OAuth 2.0 and OpenID Connect.
6. "Shift Left" by integrating SAST, DAST, and SCA tools into the CI/CD Pipeline.
7. Harden Container and Kubernetes environments for Microservices deployment.
8. Implement Secrets Management and secure configuration for distributed systems.
9. Defend against Supply Chain Attacks and manage Third-Party Dependencies securely.
10. Deploy and configure Web Application Firewalls (WAF) and API Gateways.
11. Design robust Logging, Monitoring, and Incident Response for Microservices.
12. Utilize Runtime Application Self-Protection (RASP) to defend live applications.
13. Ensure compliance with data protection and regulatory frameworks like PCI DSS and GDPR.

Target Audience

1. Software Developers
2. Application Security Engineers
3. DevSecOps Engineers
4. Security Architects
5. Cloud Security Engineers
6. Penetration Testers/Ethical Hackers
7. Technical Project/Product Managers
8. Quality Assurance (QA) Engineers with a security focus

Course Modules

Module 1: Web Application Fundamentals & OWASP Top 10

- Review modern Web Application architecture, HTTP, and TLS/SSL.
- Deep dive into the current OWASP Top 10
- Secure coding practices for input validation and output encoding.
- Understanding and mitigating Cross-Site Scripting and Cross-Site Request Forgery
- Case Study: Analyzing the Equifax breach to highlight severe "Broken Access Control" and improper asset management.

Module 2: Security in Microservices Architecture

- Introduction to Microservices, service discovery, and inter-service communication.
- Key security challenges.
- Implementing Mutual TLS for secure inter-service communication.
- Applying the Principle of Least Privilege to service accounts and permissions.
- Case Study: Examining a scenario where a container misconfiguration led to lateral movement across a staging environment's microservices cluster.

Module 3: Authentication and Authorization

- Securing the perimeter with OAuth 2.0 and OpenID Connect flows.
- Implementing JWT securely and managing their expiration.
- Understanding and using API Gateways for centralized authentication and rate limiting.
- Implementing fine-grained authorization within microservices.
- Case Study: The Capital One breach analysis to understand the failure of a misconfigured WAF/API Gateway and its impact on authorization.

Module 4: DevSecOps and the "Shift Left" Approach

- Integrating security tools into the CI/CD Pipeline.
- Using SAST to find flaws in code pre-deployment.
- Running DAST and I-AST in test environments.
- Automated Vulnerability Scanning and Configuration Management checks.
- Case Study: Implementing an automated pipeline for a financial service where a high-severity bug was caught by SAST and blocked from deployment.

Module 5: API Security and Hardening

- Securing RESTful APIs against common threats
- Protecting GraphQL APIs from excessive data exposure and DoS attacks.
- Implementing strong validation, rate limiting, and request payload controls.
- Understanding and defending against API-specific injections.
- Case Study: Analyzing a public report of a major retail API where BOLA allowed unauthorized data access to other users' records.

Module 6: Container and Cloud-Native Security

- Docker and Container Hardening best practices
- Securing Kubernetes clusters
- Managing container images with Software Composition Analysis.
- Implementing Cloud Security Posture Management for IaaS/PaaS.
- Case Study: Investigating a public vulnerability where a misconfigured Kubernetes RBAC role allowed an attacker to create new privileged containers.

Module 7: Data Protection and Secrets Management

- Secure handling of sensitive data: Encryption in transit and at rest.
- Best practices for Secrets Management using tools like HashiCorp Vault or AWS Secrets Manager.
- Implementing secure Logging and Monitoring to detect unauthorized data access.
- Data validation, sanitization, and the principle of Data Minimization.
- Case Study: Discussing the impact of the Uber 2016 breach where hard-coded credentials in a GitHub repository led to massive data exfiltration.

Module 8: Advanced Defenses and Compliance

- Deploying and tuning WAFs and RASP solutions for real-time protection.
- Integrating AI/ML-Driven Threat Detection for anomaly identification.
- Building an effective Vulnerability Management and patch cadence program.
- Compliance requirements: mapping security controls to PCI DSS, GDPR, and HIPAA.
- Case Study: Reviewing how an organization used a RASP tool to instantly block a zero-day deserialization attack before an official patch was available.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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