Secure Coding Practices 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 landscape of rapid DevSecOps and pervasive AI-enhanced coding, traditional software development is no longer sufficient. Modern applications face continuous and sophisticated threats like Zero-Day Exploits and advanced Supply Chain Attacks, making Proactive Security a non-negotiable requirement. Secure Coding Practices Training Course is designed to empower developers and engineers to Shift Left integrating robust security principles directly into the Software Development Life Cycle (SDLC) from the very first line of code. Participants will move beyond reactive Vulnerability Patching to master Defensive Programming, ultimately reducing development costs and achieving critical Compliance with standards like PCI DSS and GDPR.

This program goes beyond theoretical concepts, offering hands-on experience in identifying, exploiting, and mitigating the most critical software flaws, including the OWASP Top 10 and CWE/SANS Top 25. By adopting an Offensive Security mindset, you will learn to Threat Model and apply Security Architecture Design to build Resilient Software systems. The focus on Cloud-Native Security and Container Security ensures the skills acquired are immediately applicable to modern, distributed environments, establishing a strong Security-First Culture within your development teams and protecting your organization's most valuable digital assets.

Programme Curriculum

Secure Coding Practices Training Course

Introduction

In the current landscape of rapid DevSecOps and pervasive AI-enhanced coding, traditional software development is no longer sufficient. Modern applications face continuous and sophisticated threats like Zero-Day Exploits and advanced Supply Chain Attacks, making Proactive Security a non-negotiable requirement. Secure Coding Practices Training Course is designed to empower developers and engineers to Shift Left

integrating robust security principles directly into the Software Development Life Cycle (SDLC) from the very first line of code. Participants will move beyond reactive Vulnerability Patching to master Defensive Programming, ultimately reducing development costs and achieving critical Compliance with standards like PCI DSS and GDPR.

This program goes beyond theoretical concepts, offering hands-on experience in identifying, exploiting, and mitigating the most critical software flaws, including the OWASP Top 10 and CWE/SANS Top 25. By adopting an Offensive Security mindset, you will learn to Threat Model and apply Security Architecture Design to build Resilient Software systems. The focus on Cloud-Native Security and Container Security ensures the skills acquired are immediately applicable to modern, distributed environments, establishing a strong Security-First Culture within your development teams and protecting your organization's most valuable digital assets.

Course Duration

5 days

Course Objectives

1. Master DevSecOps principles for seamlessly integrating Security Automation into the CI/CD pipeline.
2. Apply Threat Modeling techniques to identify and prioritize risks early in the SDLC.
3. Implement robust controls to prevent the latest OWASP Top 10 web application vulnerabilities.
4. Develop Input Validation and Output Encoding strategies to neutralize Cross-Site Scripting (XSS) and SQL Injection attacks.
5. Design and implement Secure Authentication and Authorization flows, including Multi-Factor Authentication and Zero Trust principles.
6. Understand and correctly use Cryptographic controls for Data Protection at rest and in transit.
7. Employ Memory Management and defensive coding techniques to mitigate Buffer Overflows in low-level languages.
8. Conduct effective Static and Dynamic Application Security Testing as part of the development workflow.
9. Securely manage and audit Third-Party Dependencies to prevent Software Supply Chain compromises.
10. Secure Cloud-Native Applications by implementing Container Security and secret management best practices.
11. Practice Defensive Programming principles like Least Privilege and Fail-Safe Defaults in all code.
12. Design Secure APIs and microservices using principles like rate limiting and secure data format handling.
13. Establish a Security-First Culture and implement effective Vulnerability Remediation processes.

Target Audience

1. Software Developers
2. DevOps and DevSecOps Engineers
3. Software Architects and Security Architects
4. QA Engineers and Penetration Testers
5. Application Security Professionals
6. Engineering Managers and Team Leads
7. Cloud Engineers
8. Product Managers

Course Modules

Module 1: Introduction to Secure SDLC and Threat Modeling

- The Shift Left Imperative.
- Core Secure Design Principles.
- Methodologies for Threat Modeling and risk assessment
- Understanding the attack surface for modern Microservices and API architectures.
- Case Study: Analyzing the development process failure in the Equifax Data Breach traced to a known vulnerability in an unpatched third-party component, highlighting the need for early dependency management and "shift left."

Module 2: Injection Vulnerabilities

- Deep dive into SQL Injection, NoSQL Injection, and Command Injection attacks.
- Implementing parameterized queries and Prepared Statements to eliminate SQLi.
- Best practices for robust Input Validation, sanitization, and context-aware output encoding.
- Securely handling user input in modern frameworks and preventing dangerous function calls.
- Case Study: The Heartland Payment Systems breach, one of the largest early credit card breaches, where a SQL Injection attack was a key vector, demonstrating the critical impact of improper data/command separation.

Module 3: Authentication and Access Control

- Secure practices for Password Storage and avoiding Sensitive Data Exposure.
- Implementing and enforcing strong Broken Authentication and Session Management controls
- Mitigating Insecure Direct Object Reference and enforcing fine-grained Authorization checks.
- Understanding and protecting against Cross-Site Request Forgery attacks.
- Case Study: Examining the 2021 Twitch Source Code Leak, primarily enabled by an insecure server configuration allowing broken access control, underscoring the risk of internal exposure.

Module 4: Cross-Site Scripting and Client-Side Flaws

- Identifying and mitigating the three types of XSS.
- Implementing Output Encoding and context-sensitive sanitization for HTML, JavaScript, and CSS.
- Using modern browser security features.
- Securing client-side JavaScript and framework vulnerabilities
- Case Study: A major 2018 British Airways breach where a vulnerability in a third-party JavaScript library led to a sophisticated XSS attack, allowing attackers to skim payment data, illustrating the danger of client-side supply chain risk.

Module 5: Cryptography and Sensitive Data Protection

- Best practices for secure key management, generation, and storage.
- Correctly applying symmetric and asymmetric Cryptography
- Protecting data in transit using TLS/SSL and securing API communication.
- Data classification, Data Masking, and secure logging to prevent Sensitive Data Exposure.
- Case Study: The Target Data Breach (2013), which involved insecure network segmentation and exposed payment data that was not properly encrypted in transit or at rest, emphasizing the need for end-to-end data security.

Module 6: Error Handling, Logging, and Configuration Security

- Implementing secure, non-verbose Error Handling to prevent information leakage to attackers.
- Creating a robust Security Logging strategy for detection and incident response

- Hardening application and server Security Configuration to prevent Security Misconfigurations.
- Secure File Upload handling and preventing Unvalidated Redirects and Forwards.
- Case Study: Analyzing the security flaw in the Optus API (2022) which exposed millions of customer records due to an unsecured API endpoint that allowed data to be collected without authentication/proper logging, highlighting the consequences of poor configuration and logging.

Module 7: Dependency and Supply Chain Security

- Managing and auditing Third-Party Libraries and components for known vulnerabilities.
- Implementing automated Vulnerability Scanning into the build process.
- Tools and practices for secure Software Composition Analysis.
- Code signing, artifact integrity, and securing the build pipeline.
- Case Study: The SolarWinds Supply Chain Attack (2020), where a compromised software update introduced a backdoor into thousands of organizations, providing a critical example of the devastating impact of a sophisticated software supply chain attack.

Module 8: Modern Application Security Trends & Future Threats

- Securing REST and GraphQL APIs
- Container Security best practices and image hardening.
- Introduction to AI-Enhanced Secure Coding tools for vulnerability detection and remediation.
- Writing secure code in specific modern languages and frameworks
- Case Study: Examining a recent Cloud Misconfiguration incident to illustrate how developer-level configuration choices directly translate to massive cloud-native security risks.

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