OWASP Top 10 Application Security Training Course

4 – 8 January 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

OWASP Top 10 Application Security Training Course

Ref: 771_223989 **Date:** 4 – 8 January 2027 **Location:** Addis Ababa **Fees:** 4500 Euro

Overview

OWASP Top 10 Application Security Training Course is a one-week intermediate course for application security analysts, developers, security testers, DevSecOps engineers, and technical risk teams who leave with an Application Security Improvement Plan. Participants apply OWASP Top 10 risk assessment, secure design decisions, application security verification, evidence-based remediation, and remediation prioritization across software delivery. The course distinguishes risk-led application improvement from broad penetration testing and certification preparation. Agile Leaders Training Center develops practical OWASP application security capability.

Who Should Attend

- Application security functions responsible for identifying and treating software risks
- Software development functions responsible for secure design and coding decisions
- Security testing functions responsible for producing verification evidence
- DevSecOps functions responsible for integrating controls into delivery pipelines
- Technical risk functions responsible for prioritizing remediation and ownership

The course assumes participants can interpret web application architecture, HTTP behavior, code findings, and security test results, and leaves out exploit development, unrestricted penetration testing, and certification exam preparation.

Departments and Industries

The course supports departments and industries that build, acquire, test, or operate web applications.

- Banking digital channels and software assurance
- Retail and e-commerce engineering
- Healthcare application delivery
- Telecommunications digital platforms
- Technology product and managed security services

Learning Objectives

By the end of this course, participants will be able to:

- Apply the OWASP Top 10 to application risk recognition
- Analyze design, code, configuration, and dependency weaknesses
- Use ASVS requirements to define verification evidence
- Evaluate findings with WSTG-aligned testing methods
- Prioritize remediation by exposure, impact, and ownership
- Build an Application Security Improvement Plan

Course Agenda

Day 1: Frame OWASP Application Risk

- OWASP Top 10 Risk Category Map
- Application Architecture and Trust Boundary Diagram
- Data Flow and Attack Surface Inventory
- Risk Evidence and Business Impact Worksheet
- Application Security Responsibility Matrix

Day 2: Control Access and Input Risks

- Broken Access Control Abuse-Case Method
- Authentication and Session Failure Review
- Injection Source-to-Sink Analysis
- Input Validation and Output Encoding Decision Table
- Authorization Test Evidence Record

Day 3: Address Design and Supply Risks

- Insecure Design Threat Scenario Canvas
- Security Misconfiguration Baseline Checklist
- Cryptographic Failure Data Protection Map
- Software Supply Chain Dependency Register
- Software and Data Integrity Control Matrix

Day 4: Verify, Remediate, and Monitor

- OWASP ASVS Requirement Selection Method
- OWASP WSTG Test Evidence Worksheet
- Security Logging and Alerting Coverage Map
- Exceptional Condition Handling Review
- Remediation Priority and Ownership Matrix

Day 5: Practice the Improvement Cycle

- Exercise: Map Findings to OWASP Top 10 Risks
- Exercise: Review Access, Input, and Design Evidence
- Exercise: Evaluate Configuration and Dependency Controls
- Exercise: Prioritize Remediation and Verification Actions
- Capstone: Application Security Improvement Plan

Practical Exercises

The course uses suggested activities based on banking, retail, healthcare, telecommunications, and software-product applications.

- Suggested activity: map observed weaknesses to the current OWASP Top 10 risk categories and affected trust boundaries.
- Suggested activity: convert a risk scenario into secure design, coding, and verification decisions.
- Suggested activity: compare test evidence with selected ASVS requirements and document coverage gaps.
- Suggested activity: rank remediation actions, assign owners, and define evidence needed for closure.

FAQs

Who suits OWASP Top 10 application security training, and what does it assume?

Application security, development, testing, DevSecOps, and technical risk functions suit the training; it assumes familiarity with web architecture, HTTP behavior, and common software findings.

How does OWASP Top 10 application security differ from general penetration testing?

OWASP Top 10 application security organizes risk recognition, design decisions, verification, and remediation, while general penetration testing focuses on discovering and demonstrating exploitable weaknesses within an authorized scope.

How should teams use the OWASP Top 10 in secure software delivery?

Teams should use the OWASP Top 10 as a risk-awareness frame, connect relevant categories to requirements and controls, verify implementation, record evidence, and prioritize unresolved exposure.

Why connect OWASP Top 10 risks with ASVS requirements?

Connecting risks with ASVS requirements turns broad awareness into testable expectations, helping teams define what evidence is needed and where verification depth should increase.

AGILE LEADERS
Training Center

How should OWASP Top 10 remediation be prioritized?

Remediation should be prioritized using exposure, business impact, exploit conditions, control gaps, affected assets, dependencies, ownership, and the evidence required to confirm closure.

Conclusion

Participants take back an Application Security Improvement Plan linking OWASP risks, trust boundaries, control decisions, verification evidence, remediation priorities, owners, and closure criteria. It changes scattered findings into a risk-led improvement cycle. The plan supports coordinated decisions across development, testing, operations, security, and technical risk functions.