Web Application Security

OWASP Security Testing & Compliance

Instructor-led online training | 5 days | 40 hours

Training overview

Parameter	Details
Duration	5 days, 8 hours per day
Methodology	30% theory and 70% practical
Level	Beginner to intermediate
Modules / labs	10 modules / 15 hands-on labs
Software	Open-source tools
Framework alignment	OWASP Top 10, WSTG, ASVS

Course objectives

- Understand web application security fundamentals and OWASP frameworks.
- Identify and assess common web application vulnerabilities.
- Perform manual and automated application security testing.
- Evaluate authentication, authorization and API security mechanisms.
- Understand secure coding and vulnerability remediation techniques.
- Perform OWASP-aligned security verification and compliance gap assessments.
- Prepare professional security assessment reports.

Day 1: Web Application Security Fundamentals and OWASP Framework

Module 1: Introduction to Web Application Security

- Web application architecture and components
- HTTP and HTTPS protocols
- HTTP requests, responses, headers and cookies
- Common web application threats and vulnerabilities
- Web application attack surfaces
- Confidentiality, Integrity and Availability (CIA Triad)
- Secure Software Development Life Cycle (SSDLC)

Module 2: OWASP Framework and Security Testing Methodology

- Introduction to OWASP
- OWASP Top 10: 2025
- OWASP Web Security Testing Guide (WSTG)
- OWASP Application Security Verification Standard (ASVS)
- Black-box, white-box and grey-box testing
- Active and passive security testing
- Introduction to ZAP Proxy
- Vulnerability assessment methodology

Hands-on Labs

Practical 1: Installation and configuration of ZAP Proxy and OWASP Juice Shop.

Practical 2: Inspecting HTTP requests, responses, cookies and security headers.

Practical 3: Application discovery and passive vulnerability scanning.

Day 2: Authentication, Authorization and Session Management Security

Module 3: Authentication and Session Management Testing

- Authentication mechanisms
- Broken authentication vulnerabilities
- Password policy and password security
- Multi-factor authentication
- Password reset security
- Session identifiers and tokens
- Session fixation and session hijacking concepts
- Cookie security attributes
- Session expiration and logout mechanisms
- JSON Web Token (JWT) security

Module 4: Authorization and Access Control Testing

- Broken access control
- Role-Based Access Control (RBAC)
- Insecure Direct Object References (IDOR)
- Horizontal and vertical privilege escalation
- Cross-Site Request Forgery (CSRF)
- Server-side authorization validation
- Principle of least privilege
- Access control vulnerability remediation

Hands-on Labs

Practical 1: Testing authentication mechanisms and password policies.

Practical 2: Identifying broken access control and IDOR vulnerabilities using test accounts.

Practical 3: Testing session management, cookies and token security.

Day 3: Injection Vulnerabilities and Web Application Security Testing

Module 5: Injection and Client-Side Vulnerabilities

- Input validation and sanitization
- SQL Injection (SQLi)
- NoSQL Injection concepts
- Command injection concepts
- Reflected Cross-Site Scripting (XSS)
- Stored Cross-Site Scripting
- DOM-based Cross-Site Scripting
- Path traversal vulnerabilities
- Parameterized queries and prepared statements
- Output encoding and vulnerability remediation

Module 6: Security Misconfiguration and Data Protection

- Security misconfiguration
- Cryptographic failures
- Sensitive data exposure
- Insecure file upload vulnerabilities
- Error handling and information disclosure
- Content Security Policy (CSP)
- Cross-Origin Resource Sharing (CORS)
- Server-Side Request Forgery (SSRF) fundamentals
- Secure HTTP headers
- Secure application configuration practices

Hands-on Labs

Practical 1: Identifying SQL injection vulnerabilities and evaluating remediation techniques.

Practical 2: Testing Cross-Site Scripting vulnerabilities and input validation.

Practical 3: Performing security configuration, file upload and HTTP security header assessments.

Day 4: Automated Security Testing, API Security and DevSecOps

Module 7: Automated Application Security Testing

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Software Composition Analysis (SCA)
- Automated vulnerability scanning
- Vulnerable third-party dependencies
- Software supply chain security
- Software and data integrity failures
- False positives and false negatives
- Vulnerability validation and retesting
- Integration of security testing into CI/CD pipelines

Module 8: API Security and Secure Application Development

- REST API architecture and security
- OWASP API Security Top 10
- Broken Object Level Authorization (BOLA)
- API authentication and authorization
- API input validation
- API rate limiting and resource consumption
- Insecure application design
- Security logging and alerting
- Mishandling of exceptional conditions
- Secure coding best practices

Hands-on Labs

Practical 1: Performing automated DAST scanning using ZAP Proxy.

Practical 2: Performing REST API security testing using Bruno.

Practical 3: Performing source code and dependency vulnerability scanning using Semgrep CE and Trivy.

Day 5: OWASP Compliance, Risk Assessment and Security Reporting

Module 9: OWASP Compliance and Vulnerability Risk Assessment

- Understanding OWASP ASVS requirements
- ASVS Level 1, Level 2 and Level 3
- Application security verification requirements
- Mapping vulnerabilities to OWASP Top 10
- Mapping security tests to OWASP WSTG
- Common Vulnerabilities and Exposures (CVE)
- Common Weakness Enumeration (CWE)
- Common Vulnerability Scoring System (CVSS)
- Vulnerability classification and prioritization
- Security control gap analysis
- Remediation planning and verification

Module 10: Security Assessment and Compliance Reporting

- End-to-end web application security assessment
- Security testing scope and authorization
- Security evidence collection and documentation
- Business impact analysis
- Preparing security verification checklists
- Vulnerability assessment report preparation
- Executive summary and technical findings
- Compliance gap reporting
- Remediation recommendations
- Security assessment review and sign-off

Hands-on Labs

Practical 1: Conducting an end-to-end web application security assessment using OWASP Juice Shop.

Practical 2: Preparing an OWASP ASVS verification checklist and vulnerability risk assessment matrix.

Practical 3: Preparing a final security assessment and compliance gap report with remediation recommendations.

Open-source software requirements

Software	Purpose
ZAP Proxy	Vulnerability scanning and web application security testing
OWASP Juice Shop	Vulnerable web application for hands-on practice
Node.js	Running OWASP Juice Shop locally
Mozilla Firefox	Browser-based security testing
Bruno	REST API security testing
Semgrep CE	Static application security testing
Trivy	Software dependency vulnerability scanning
Git	Source code management
LibreOffice	Security reporting and compliance documentation

Hardware and system requirements

Component	Requirement
Operating system	Windows 11 or Ubuntu Linux
Processor	Intel Core i5 or equivalent
RAM	8 GB minimum; 16 GB recommended
Disk space	30 GB free
Internet	Stable connection
Permissions	Administrator access
WSL2	Required for proposed Semgrep CE setup on Windows

Participant prerequisites

- Basic understanding of web application architecture.
- Basic knowledge of HTML, JavaScript and SQL.
- Familiarity with HTTP, HTTPS and REST APIs.
- Basic networking knowledge.
- No prior penetration testing experience required.

Day-wise training summary

Day	Modules	Labs
1 - Web Application Security Fundamentals and OWASP Framework	2	3
2 - Authentication, Authorization and Session Management Security	2	3
3 - Injection Vulnerabilities and Web Application Security Testing	2	3
4 - Automated Security Testing, API Security and DevSecOps	2	3
5 - OWASP Compliance, Risk Assessment and Security Reporting	2	3
Total	10	15

Note

All practicals will be conducted using open-source software in authorized local lab environments. No paid software licenses or cloud subscriptions are required. OWASP compliance coverage focuses on security verification and gap assessment rather than formal regulatory certification.