Proposed Training TOC

Secure Software & Web Application Security Testing with Open Source License Compliance

Duration: 5 days

Module 1: Frontispiece

- About the OWASP Testing Guide Project
- About The Open Web Application Security Project

Module 2: Introduction to Secure Software Testing

- Principles of Security Testing for Application and Embedded Software
- Deriving Security Test Requirements for Device and Web Software
- Integrating Security Tests in Dev/Test Workflows (CI/CD for .NET, firmware, and web apps)
- Security Test Data Analysis and Reporting

Module 3: Secure SDLC Framework

- Overview of Secure Development Lifecycle (SDLC)
- Phase 1: Before Development – Security Risk Analysis / Threat Modeling for Devices & Web Apps
- Phase 2: Definition & Design – Secure Architecture for .NET, Firmware, and Applications
- Phase 3: Development – Code-Level Security Practices
- Phase 4: Deployment – Secure Packaging and Distribution
- Phase 5: Maintenance & Operations – Patch Management and Vulnerability Monitoring
- Typical SDLC Workflow for Application and Firmware Projects

---

Module 4: Application, Firmware & Web Security Testing

- Configuration and Deployment Management Testing (installer security, firmware flashing, secure boot)
- Authentication & Authorization Testing
- Session Management Testing (including device communication scenarios)
- Input Validation (critical for firmware)
- Error Handling and Information Disclosure Testing

- Cryptographic Testing
- Business Logic Testing
- Client-Side Testing (XSS, DOM-based flaws)
- Client-Server Security Testing

Module 5: Penetration Testing for Applications & Device Software

(Currently not practiced, but included as overview)

- Introduction to Penetration Testing in Embedded and Application Software
- Static and Dynamic Analysis Techniques
- Firmware Reverse Engineering and Exploit Discovery
- Penetration Testing of .NET Applications
- Communication Protocol Security Testing
- Tools & Automation for Embedded and Web Pen Testing

- **Hands-on Tools:** Burp Suite, OWASP ZAP, Postman, SAST/DAST Tools
- **Pen Test Topics:**
  - Security Misconfigurations (headers, cookies, etc.)
  - JWT Token Manipulation
  - Insecure Data Exposure
  - GraphQL API Testing (Postman/Burp Suite)
  - API Key Leakage & Hardcoded Secrets
  - API Enumeration & Fuzzing
  - Broken Object Level Authorization (BOLA)
  - Broken Function Level Authorization

Module 6: DAST (Dynamic Application Security Testing)

- Overview of DAST – Complementing SAST with Veracode
- Introduction to DAST and Black-Box Testing
- DAST for .NET Applications and APIs
- DAST for Device Interfaces and Embedded Services
- Tools & Techniques for Runtime Vulnerability Detection
- Integrating DAST in CI/CD Pipelines
- Reporting and Remediation of DAST Findings

Module 7: Advanced Embedded & API Security

- API Security – REST and GraphQL Security Concerns
- Language-Specific Security Guidelines (Java, Python, JavaScript, C)
- OWASP Embedded Application Security (Good to Have)
    - Firmware Update & Cryptographic Signature
    - Securing Sensitive Information
    - Embedded Framework & C-based Hardening

Module 8: Third-Party Licensing and Open-Source Compliance

- Introduction to Licensing and OSS Use
- Overview of Common License Types (GPL, MIT, Apache, BSD, etc.)
- Licensing Obligations, Risks, and Compliance Requirements
- Copyleft vs. Permissive Licenses
- Dual Licensing and Distribution Risks
- Detecting License Conflicts and Compatibility Issues
- Tools for License Detection (FOSSology, ScanCode, Licensee)
- Software Bill of Materials (SBOM) and Software Composition Analysis (SCA)
- Automating Compliance in CI/CD (DevSecOps Integration)
- Governance Models and Audit Readiness

Module 9: Best Practices & Reinforcement

- Secure Logging Practices
- Threat Landscape for Developers
- Security by Design Principles
- Security Checkpoints in Agile Workflows
- Shift-Left Security: Integrating Early in SDLC
- Using Secure Frameworks and Libraries
- Automating Security Testing in CI/CD Pipelines
- Staying Updated with OWASP Top 10 and CVE Feeds

Module 10: Reporting

- Consolidating Security & License Findings
- Risk Categorization and Remediation Planning
- Executive Summary and Technical Reporting
- Recommendations and Next Steps