

Web & Mobile Security: OWASP Top 10 & Burp Suite

Learn to identify and test OWASP Top 10 web and mobile vulnerabilities using Burp Suite and secure development practices.

5 Days

DURATION

5

MODULES

36

TOPICS

1

HANDS-ON ACTIVITIES

COURSE OVERVIEW

This course covers the foundations of web and mobile application security, including common attack surfaces and the OWASP Top 10 vulnerabilities for web applications. It then addresses web application testing and vulnerability analysis, covering threat modelling, testing methodologies, and tools such as Burp Suite and OWASP ZAP, along with authentication and session security testing. It continues into mobile application security, examining the OWASP Top 10 Mobile Risks and mobile testing frameworks, before moving into advanced concepts such as integrating security into the secure software development lifecycle and secure coding practices. It concludes with incident detection, response and best practices for securing web and mobile applications.

WHO THIS COURSE IS FOR

Security Testers

Web Developers

Mobile Developers

Application Security Analysts

Penetration Testers

DevOps Engineers

LEARNING OBJECTIVES

- Identify common attack surfaces in web and mobile applications
- Explain the OWASP Top 10 web application vulnerabilities
- Analyse web application architecture and perform threat modelling
- Apply Burp Suite and OWASP ZAP for vulnerability scanning
- Assess authentication, authorization and session security weaknesses
- Identify OWASP Top 10 Mobile Risks in mobile applications
- Describe integration of security into the SDLC and CI/CD pipelines
- Plan incident detection and response for application attacks

5 Modules, 36 Topics

01

Foundations of Web and Mobile Application Security

INTRODUCTION TO WEB AND MOBILE SECURITY

- Importance of securing applications in today's digital landscape
- Common attack surfaces and security challenges

UNDERSTANDING OWASP TOP 10 VULNERABILITIES (WEB APPLICATIONS)

- Injection flaws (e.g., SQL Injection)
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfigurations
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

SETTING UP THE SECURITY ENVIRONMENT

- Tools and configurations needed for web security testing

02

Web Application Testing and Vulnerability Analysis

WEB APPLICATION ARCHITECTURE AND THREAT MODELLING

- Overview of web app components (Frontend, Backend, APIs)
- Identifying and prioritizing threats

TESTING METHODOLOGIES AND TOOLS

- Static and Dynamic Analysis Tools (e.g., Burp Suite, OWASP ZAP)
- Manual testing strategies

AUTHENTICATION, AUTHORIZATION, AND SESSION SECURITY TESTING

- Common vulnerabilities in login systems and session handling

HANDS-ON LABS

- Conducting vulnerability scans using Burp Suite and OWASP ZAP

03

Mobile Application Security (Without Lab)

UNDERSTANDING OWASP TOP 10 MOBILE RISKS

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communication
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality Issues
- Code Tampering
- Reverse Engineering
- Extraneous Functionality
- Introduction to Mobile Application Testing Frameworks

MOBILE APPLICATION VULNERABILITY IDENTIFICATION

- Identifying risks in mobile apps based on OWASP guidelines

04

Advanced Application Security Concepts

SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC)

- Integrating security into the SDLC
- Automated security testing in CI/CD pipelines

TOOLS AND TECHNIQUES FOR SECURE DEVELOPMENT

- Secure coding practices and vulnerability remediation techniques

05

Incident Handling and Best Practices

INCIDENT DETECTION AND RESPONSE FOR WEB AND MOBILE APPLICATIONS

Identifying security incidents · Steps to respond to and recover from attacks

SECURITY BEST PRACTICES FOR WEB AND MOBILE APPLICATIONS

Checklist for securing web and mobile apps

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com