

Web App Security: OWASP Testing, SQL Injection & XSS

Learn to test web applications for security flaws using the OWASP framework, covering SQL injection, XSS, authentication and session management.

5 Days

40 HOURS

10

MODULES

75

TOPICS

COURSE OVERVIEW

The Advanced Web Application Security Testing Course is designed to equip learners with the skills necessary to identify, analyze, and mitigate security vulnerabilities in web applications. This comprehensive course covers a wide range of topics, from understanding the OWASP Testing Framework in Module 1 to the complexities of AJAX Testing in Module 11. Learners will gain hands-on experience with various types of security testing, including Configuration Management, Authentication, Session Management, Authorization, and Data Validation Testing. By delving into the intricacies of Business Logic, Denial of Service, and Web Services Testing, participants will be well-prepared to tackle real-world security challenges. The course concludes with guidance on Writing Reports, ensuring that learners can effectively communicate their findings. Upon completion, individuals can pursue Web Application Security testing certification, demonstrating their expertise to employers. This Web Application Security testing course is an invaluable resource for anyone looking to advance their knowledge and protect web applications from emerging security threats.

WHO THIS COURSE IS FOR

The Advanced Web Application Security Testing course by Koenig Solutions is designed for IT professionals focused on safeguarding web applications.

Security Analysts

Penetration Testers

Web Application Developers

Security Consultants

IT Security Managers

System Administrators

Risk Management Professionals

Quality Assurance Testers

Software Architects

Ethical Hackers

Cybersecurity Enthusiasts

Network Engineers with a focus on security

Compliance Auditors looking to understand technical risks

CISOs and other senior security officers

Anyone aspiring to attain a certification in Web Application Security

What You Will Learn

- Identify application entry points through information gathering and fingerprinting
- Assess configuration management including SSL/TLS and admin interfaces
- Evaluate authentication mechanisms for brute force and bypass weaknesses
- Analyse session management for fixation, CSRF and exposed variables
- Identify authorization flaws such as path traversal and privilege escalation
- Apply data validation testing to detect SQL injection and XSS flaws
- Assess web services and AJAX components for structural vulnerabilities
- Plan and write security testing reports that convey real risk

COURSE SYLLABUS

10 Modules, 75 Topics

01

Introduction and Objective of OWASP Testing Framework

TOPICS

- Information Gathering
- **Testing:** Spiders, robots, and Crawlers
- Search engine discovery/Reconnaissance
- Identify application entry points
- Testing for Web Application Fingerprint
- Application Discovery
- Analysis of Error Codes

02

Configuration Management Testing

TOPICS

- SSL/TLS Testing
- DB Listener Testing
- Infrastructure configuration management testing
- Application configuration management testing
- Testing for File extensions handling
- Old, backup and unreferenced files
- Infrastructure and Application Admin Interfaces
- Testing for HTTP Methods and XST

03

Authentication Testing

TOPICS

- Credentials transport over an encrypted channel
- Testing for user enumeration
- Default or guessable (dictionary) user account
- Testing For Brute Force
- Testing for Bypassing authentication schema
- Testing for Vulnerable remember password and pwd reset
- Testing for Logout and Browser Cache Management
- Testing for CAPTCHA
- Testing for Multiple factors Authentication
- Testing for Race Conditions

04

Session Management Testing

TOPICS

Testing for Session Management Schema · Testing for Cookies attributes · Testing for Session Fixation · Testing for Exposed Session Variables · Testing for CSRF

05

Authorization Testing

TOPICS

Testing for path traversal · Testing for bypassing authorization schema · Testing for Privilege Escalation

06

Business Logic Testing

TOPICS

- Data Validation Testing
- Testing for Reflected Cross Site Scripting
- Testing for Stored Cross Site Scripting
- Testing for DOM based Cross Site Scripting
- Testing for Cross Site Flashing
- SQL Injection
- Oracle Testing
- MySQL Testing
- SQL Server Testing
- MS Access Testing
- Testing PostgreSQL
- LDAP Injection
- ORM Injection
- XML Injection
- SSI Injection
- XPath Injection
- IMAP/SMTP Injection
- Code Injection
- OS Commanding
- Buffer overflow Testing
- Heap overflow
- Stack overflow
- Format string

07

Denial of Service Testing

TOPICS

- Testing for SQL Wildcard Attacks
- Locking Customer Accounts
- Buffer Overflows
- User Specified Object Allocation
- User Input as a Loop Counter
- Writing User Provided Data to Disk
- Failure to Release Resources
- Storing too Much Data in Session

08

Web Services Testing

TOPICS

WS Information Gathering · Testing WSDL · XML Structural Testing · XML Content-level Testing · HTTP GET parameters/REST Testing · Naughty SOAP attachments · Replay Testing

09

AJAX Testing

TOPICS

AJAX Vulnerabilities · Testing For AJAX

10

Writing Reports

TOPICS

How to value the real risk · How to write the report of the testing

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