KOENIG SOLUTIONS · COURSE OUTLINE

Web AppSec: OWASP Top 10, SQLi & XSS

Learn to identify, exploit and fix web application vulnerabilities including SQL injection, XSS and the OWASP Top 10.

5 Days	8	35	1
40 HOURS	MODULES	TOPICS	HANDS-ON ACTIVITIES

COURSE OVERVIEW

This course introduces penetration testing methodologies, ethical and legal considerations, and tools such as Nmap, Wireshark and Burp Suite. It covers vulnerability assessment with scanners like Nessus and OpenVAS and the Metasploit framework, before moving into hands-on exploitation of SQL injection, XSS, OS command injection, file inclusion and CSRF. It then works through the OWASP Top 10, from broken access control and cryptographic failures to authentication failures and SSRF, followed by remediation of common findings such as missing security headers and verbose errors. It closes with pen test practices for thick clients, including privilege escalation, DLL hijacking and reverse engineering.

WHO THIS COURSE IS FOR

Penetration Testers | **Ethical Hackers** | **Security Analysts** | **Web Developers** | **Application Security Engineers**

LEARNING OBJECTIVES

- Explain penetration testing methodologies and legal considerations
- Apply tools such as Nmap, Wireshark and Burp Suite
- Assess vulnerabilities using scanners like Nessus and OpenVAS
- Exploit SQL injection, XSS and OS command injection flaws
- Analyse OWASP Top 10 risks including broken access control
- Identify authentication failures and server-side request forgery
- Implement fixes for common web application findings
- Evaluate thick client applications for privilege escalation risks

COURSE SYLLABUS

8 Modules, 35 Topics

01

Introduction to Ethical Hacking & Penetration Testing

TOPICS

- What is Penetration Testing?
- Difference Between Ethical Hacking & Cybercrime
- Pen Testing Methodologies (PTES, OWASP, NIST)
- Legal & Ethical Considerations

02

Introduction to Tools Useful for Web Application Pen Testing

TOPICS

WHOIS, nslookup, Ping · Nmap, Wireshark, Burp suite

03

Vulnerability Assessment

TOPICS

- Understanding CVEs & Vulnerabilities
- Using Vulnerability Scanners (Nessus, OpenVAS)
- Introduction to Metasploit Framework

04

Exploitation & Gaining Access (Theory + Hands-on)

TOPICS

- Exploiting Common Vulnerabilities
- **SQL Injection (use cases:** Data breaches, database access, account takeover)
- **XSS (Reflected, Stored, DOM-based) Use case:** Stealing cookies, session hijacking, phishing attacks
- OS Command Injection
- File Inclusion
- Cross-Site Request Forgery (CSRF)

HANDS-ON

- Hand on using the sample application using all common vulnerabilities

05

OWASP Top 10 for Web Application (Theory + Hands-on) - Top 5

Explain the theory and use sample web applications to show the vulnerabilities, how to identify using tools, damages caused

TOPICS

- Broken access control
- Cryptographic Failures
- Injections (only overview, already covered in module 4)
- Insecure Design
- Security misconfiguration

06

OWASP Top 10 for Web Application

Explain the theory and use sample web applications to show the vulnerabilities, how to identify using tools

TOPICS

Identification and Authentication Failures · Software and Data Integrity Failures · Security Logging and Monitoring Failures · Server-Side Request Forgery (SSRF)

07

How to Fix Common Web Application Pen Test Findings

(Examples given)

TOPICS

- Distributed Denial Of Service Attacks (DDoS)
- HTML Injection Validation (UI & API)
- Missing HTTP security headers
- Verbose errors with detailed backend information
- **Cloud related:** Removing public access for PaaS resources, WAF
- No sensitive information in URL/query params

08

Pen Test Best Practices for Thick Clients

Should include Tools used, penTest approach for the exploit and mitigation measures

TOPICS

- Registry / File monitoring
- Privilege escalation
- DLL Hijacking / Remote Code Execution
- Reverse Engineering (considering C#/java as programming language)
- **Tools:** TCP View, CFF Explorer, Regshot, Winhex

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