

## KOENIG SOLUTIONS • COURSE OUTLINE

# Web Application Hacking and Security (WAHS)

Learn to identify, exploit and remediate web application vulnerabilities, from SQL injection and XSS to access control and file inclusion flaws.

## COURSE OVERVIEW

This course covers advanced web application penetration testing techniques, beginning with injection and cross-site scripting flaws such as SQLi, reflected, stored and DOM-based XSS, CSRF and SSRF. It then addresses security misconfigurations, directory bruteforcing, CMS and network scanning, authentication bypass, enumeration and dictionary attacks. Further topics include insecure direct object references, broken access control, local and remote file inclusion, arbitrary file upload and download, and the use of components with known vulnerabilities. The course concludes with command injection, remote code execution, privilege escalation, log poisoning, weak SSL ciphers, cookie and header modification, session fixation and clickjacking.

## WHO THIS COURSE IS FOR

Penetration Testers

Security Analysts

Web Developers

Security Consultants

Ethical Hackers

## LEARNING OBJECTIVES

- Apply advanced SQL injection techniques against web applications
- Identify reflected, stored and DOM-based cross-site scripting flaws
- Exploit cross-site request forgery using GET and POST methods
- Analyse server-side request forgery and security misconfigurations
- Assess authentication mechanisms for bypass and privilege escalation
- Evaluate broken access control and insecure direct object references
- Implement local and remote file inclusion attacks
- Explain risks of using components with known vulnerabilities

## 30 Topics

### TOPICS

- Advanced Web Application Penetration Testing
- Advanced SQL Injection (SQLi)
- Reflected, Stored and DOM-based Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF) - GET and POST Methods
- Server-Side Request Forgery (SSRF)
- Security Misconfigurations
- Directory Browsing/Bruteforcing
- CMS Vulnerability Scanning
- Network Scanning
- Auth Bypass
- Web App Enumeration
- Dictionary Attack
- Insecure Direct Object Reference Prevention (IDOR)
- Broken Access Control
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Arbitrary File Download
- Arbitrary File Upload
- Using Components with Known Vulnerabilities
- Command Injection
- Remote Code Execution
- File Tampering
- Privilege Escalation
- Log Poisoning
- Weak SSL Ciphers
- Cookie Modification
- Source Code Analysis
- HTTP Header Modification
- Session Fixation
- Clickjacking

#### 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](https://koenig-solutions.com)

✉ [info@koenig-solutions.com](mailto:info@koenig-solutions.com)