SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

WEB APPLICATION SECURITY

ASP TOP 10 . INJECTION . AC
AUTHENTICATION . SESSION
URE CODING . TESTING . FIX

DURATION	LEVEL	MODULES	MODE
50 Hours	**Intermediate to Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A web application security course teaching attack and defence side by side. Every vulnerability class is exploited in a lab application and then fixed in code, so learners leave able to both find and remediate. Coverage follows the current OWASP Top 10 with additional modules on APIs and authentication.

The course ends with a full assessment of a running application plus a remediation pull request.

WHO IT IS FOR

- Web developers and tech leads
- Application security analysts
- QA and testing engineers
- Penetration testers

PREREQUISITES

HTML, HTTP and one server-side language. Basic database knowledge.

02 LEARNING OUTCOMES

01 Read HTTP traffic and manipulate requests deliberately.

02 Exploit and fix injection vulnerabilities.

03 Test authentication, session and access control logic.

04 Assess API endpoints for authorisation flaws.

05 Identify insecure configuration and dependencies.

06 Apply secure coding patterns and framework defences.

07 Report and verify remediation of findings.

03 MODULE STRUCTURE

8 MODULES

01 HTTP AND TOOLING

- Requests and responses
- Proxy interception
- Lab targets
- Cookies and headers
- Browser dev tools

TOOLS

BURP SUITE · OWASP ZAP

02 INJECTION

- SQL injection
- Command injection
- Parameterisation and fixes
- NoSQL injection
- Template injection

LAB

EXPLOIT AND PATCH

03 CROSS-SITE SCRIPTING

- Reflected
- DOM-based
- Output encoding
- Stored
- Content Security Policy

LAB

XSS CHAIN AND FIX

04 AUTHENTICATION AND SESSIONS

- Password storage
- Session fixation
- Password reset flows
- MFA
- JWT pitfalls
- Rate limiting

05 ACCESS CONTROL

- IDOR
- Business logic abuse
- Vertical and horizontal escalation
- Server-side enforcement

LAB

AUTHORISATION TESTING

06 API SECURITY

- REST and GraphQL surfaces
- Excessive data exposure
- API keys and scopes
- Mass assignment
- Rate limits

07 CONFIGURATION AND SUPPLY CHAIN

- Security headers
- File upload handling
- Dependency scanning
- CORS
- Secrets in repos
- SBOM

TOOLS

SNYK · DEPENDENCY-CHECK

08 SECURE DEVELOPMENT

- Threat modelling
- Code review
- Verification
- Secure coding standards
- SAST and DAST in CI

PROJECT

ASSESSMENT REPORT PLUS REMEDIATION COMMIT

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

APPLICATION SECURITY ENGINEER · WEB PENETRATION TESTER · SECURE SOFTWARE DEVELOPER · DEVSECOPS ENGINEER · SECURITY CODE REVIEWER

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com