

Master Web Application Security, Become a Penetration Testing Expert

Web applications power the digital world — and they are also prime targets for attackers. This comprehensive training program helps you learn how to find, exploit, and report real-world web application vulnerabilities using industry-standard methodologies and tools.



Hands-On Learning

Real-world labs, practical exercises and live application testing.



OWASP Methodology

Follow industry-standard OWASP framework and best practices.



Industry Tools

Work with Burp Suite, Nmap, Kali Linux, Hashcat, John the Ripper, BEEF and more.



Expert Guidance

Learn from experienced cybersecurity professional with practical industry experience.



Certificate of Completion

Get certified as a Web-Application Penetration Tester.



BUILD YOUR SKILLS.
EXPLORE REAL-WORLD SCENARIOS.
BE JOB READY.

What You'll Learn

A structured and practical approach to web application penetration testing, covering every critical aspect.

- 01 Introduction to Web Application Security**
Architecture, attack surface, OWASP Top 10 overview
- 02 Web Application Penetration Testing Methodology**
Reconnaissance, enumeration, attack phases
- 03 Information Gathering & Enumeration**
Passive/active recon, tools, endpoints, parameters
- 04 Authentication Testing**
Password attacks, MFA, reset flows, account takeover
- 05 Authorization Testing**
IDOR, privilege escalation, access control
- 06 Session Management**
Cookies, tokens, fixation, timeouts, CSRF, session hijacking
- 07 Input Validation & Injection**
SQLi, XSS, command injection, XXE, SSTI and more
- 08 Error Handling**
Information disclosure, stack traces, debug errors
- 09 Cryptography**
TLS, hashing, secrets, JWT, weak crypto
- 10 Business Logic Flaws**
Price manipulation, coupon abuse, workflow attacks
- 11 Client-Side Testing**
DOM XSS, CORS, browser storage, JavaScript analysis
- 12 API Security Testing**
REST, GraphQL, BOLA, API authentication
- 13 Reporting & Remediation**
Evidence collection, professional report writing, fixes and mitigations

Tools You'll Use



Burp Suite



Nmap



Kali Linux



Hashcat



John the Ripper



BEEF



Who Should Join?

- ✓ Aspiring cybersecurity professionals
- ✓ IT professionals looking to upskill
- ✓ Developers & QA engineers
- ✓ Anyone interested in web application security



Duration
2 Months



Mode
Online Only
(Live Interactive Sessions)



LabYard.in

PRACTICE | LEARN | GROW

WEB-APPLICATION PENETRATION TESTER

FROM RECON TO REPORT — MASTER WEB SECURITY

Real-World Labs

OWASP Methodology

Industry Tools

Expert Guidance



Gain the skills. Find the vulnerabilities.
Build a safer web.



www.labyard.in

LEARN | PRACTICE | GROW