ARMOURINFOSEC®

Hands-On Cyber Security Training · Indore, India

Advanced Web Application Security Testing

Course Syllabus

Master web application security testing, OWASP vulnerabilities, authentication attacks, SQL injection, XSS, SSRF, XXE, session attacks, web server exploitation, and advanced web application penetration testing methodologies through hands-on practical labs.

// COURSE INFORMATION

Course Information

DURATION	8 Months / 32 Weeks / 240 Hours
LEVEL	Advanced
MODULES	17
FORMAT	Hands-on Labs / Hybrid (Online + Indore Classroom)

// COURSE OVERVIEW

Course Overview

The Advanced Web Application Penetration Testing course is designed for ethical hackers, penetration testers, bug bounty hunters, red team operators, SOC analysts, and cybersecurity professionals who want to specialize in web application security assessment and exploitation. This course covers web server architecture, HTTP fundamentals, reconnaissance, SQL injection, XSS, SSRF, XXE, authentication attacks, session management, file inclusion, deserialization, CSRF, clickjacking, security misconfigurations, and advanced exploitation techniques.

// LEARNING OBJECTIVES

Learning Objectives

- Identify and exploit web application vulnerabilities following OWASP methodology
- Master Burp Suite for professional web application testing
- Perform advanced injection attacks (SQL, OS command, XXE, SSRF)
- Exploit authentication and session management weaknesses
- Conduct XSS attacks (reflected, stored, DOM-based)
- Exploit file inclusion, path traversal, and file upload vulnerabilities
- Identify and exploit access control flaws and IDOR
- Perform deserialization, CSRF, and clickjacking attacks
- Assess web server security and misconfigurations

- Harden web servers and applications against common attacks
- Write professional web application penetration testing reports

// PREREQUISITES

Prerequisites

- Basic networking knowledge
- Familiarity with HTTP and web technologies
- Understanding of Linux and Windows basics
- Basic cybersecurity concepts
- Familiarity with web applications

// MODULE BREAKDOWN

Module Breakdown

01 Web Server Concepts

- Web Server Concepts
- Web Server Market Shares
- Open-Source Web Server Architecture (Apache)
- IIS Web Server Architecture
- Web Servers vs Web Applications
- The Role of Cloud Infrastructure
- Understanding How Web Servers Are Hacked
- The Impact of Hacking

02 Web Server Hardening & Security

- Managing and Hardening Web Servers
- Patch Management
- Security Updates and Upgrades
- Locking Down Services
- Network Segmentation
- Sandboxing
- Security Verification
- SSL/TLS Configuration

03 Web Server Enumeration & Misconfigurations

- Crawling and Enumeration Techniques
- Website Mirroring
- Directory Traversal
- HTTP Fingerprinting
- Banner Grabbing
- Internal Leakage
- Debug Settings
- Excessive Access Rights
- Misconfigured SSL
- Weak Authentication

- Outdated Components
- Web Server Configuration Files

04 Web Application Security Tools

- Burp Suite Proxy & Testing
- Nuclei Vulnerability Scanner
- Acunetix Web Vulnerability Scanner
- Nmap Service Fingerprinting
- ffuf Directory Fuzzing
- Shodan Internet Asset Discovery
- Curl HTTP Interaction
- Wget Banner Grabbing

05 Web Application Concepts & Architecture

- Introduction to Web Applications
- Web Application Components
- Web Technologies
- Web Application Architecture
- Client-Server Interaction
- HTTP Protocol Basics
- Cookies and Sessions
- Security Headers

06 Web Application Security Fundamentals

- Web Application Security Principles
- Security Breaches
- Browser Security Protections
- Query Strings
- Routing
- HTTP Verbs
- Client-Side Security Constructs
- Browser Security Limitations

07 Web Application Testing Methodology

- Web Application Testing Methodology
- Vulnerable Web Application Lab Setup
- Reconnaissance and Footprinting
- Crawling and Spidering
- Forced Browsing
- Framework Discovery
- Shodan Enumeration
- Fuzzing Techniques

08 Injection Attacks

- SQL Injection
- Blind SQL Injection
- Out-of-Band SQL Injection

- HTML Injection
- IFrame Injection
- OS Command Injection
- Blind OS Command Injection
- PHP Code Injection
- Host Header Injection
- SSI (Server-Side Includes) Injection
- XML/XPath Injection

09 Authentication & Session Attacks

- Broken Authentication
- CAPTCHA Bypassing
- Insecure Login Forms
- Weak Passwords
- Password Attacks
- 2FA Weaknesses
- Change Password Vulnerabilities
- Email Change Exploits
- Session Cookies
- Session IDs in URLs
- Session Hijacking
- Session Fixation
- Secure Session Management

10 Cross-Site Scripting (XSS)

- Reflected XSS
- Stored XSS
- DOM-Based XSS
- XSS Payloads
- Browser-Based Exploitation
- XSS Filter Bypass Techniques
- Advanced Payload Construction

11 Security Misconfiguration

- Weak Credentials
- Default Credentials
- Cross-Domain Policy Files
- CORS Misconfigurations
- XML Bomb Attacks
- WebDAV Misconfiguration
- HTTP Header Misconfigurations
- Directory Listing Exposure

12 Sensitive Data Exposure

- Base64 Encoding Risks
- HTML5 Web Storage

- Sensitive Cookies
- Insecure Data Storage
- Improper Encryption
- Information Disclosure
- Debug Information Leakage

13 File Inclusion & Path Traversal

- Directory Traversal
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Log Poisoning
- PHP Wrapper Exploitation
- File Disclosure
- Access Control Issues

14 SSRF & XXE Attacks

- Server-Side Request Forgery (SSRF)
- Blind SSRF Techniques
- Cloud Metadata Abuse (AWS/GCP)
- XML External Entity (XXE)
- Out-of-Band XXE
- XXE to SSRF Chaining
- Internal Network Access
- File Exfiltration via XXE

15 Access Control & IDOR

- Insecure Direct Object References (IDOR)
- Missing Function Level Access Control
- Privilege Escalation
- Authorization Bypass
- Horizontal Privilege Escalation
- Vertical Privilege Escalation
- Parameter Tampering

16 Advanced Web Exploitation Techniques

- Insecure Deserialization
- Session Hijacking
- Session Fixation
- Automated Security Testing
- Improper Error Handling
- Salted Hashes
- Insecure Cryptographic Storage
- Open Redirects

17 Additional Web Attack Vectors

- Clickjacking
- HTTP Verb Tampering

- HTTP Response Splitting
- HTTP Parameter Pollution
- Information Disclosure
- Client-Side Validation Bypass
- Unrestricted File Uploads
- Cross-Site Request Forgery (CSRF/XSRF)
- Session Donation

// TOOLS & HANDS-ON LABS

Tools & Hands-On Labs

- Custom vulnerable web applications (multiple frameworks)
- Web server exploitation targets (IIS, Apache)
- Burp Suite Pro access during course
- Nuclei and Acunetix scanning environments
- OWASP-based vulnerable application labs
- Progressive difficulty challenges
- Bug bounty simulation platform

// TRAINING MODE

Training Mode

Every Armour Infosec course runs as a unified programme delivered in two parallel modes — the same curriculum, the same trainers, the same certification, regardless of how you join.

- ✓ Online Live Classes — real-time, instructor-led, fully interactive sessions
- ✓ On-Premise Classroom Training — in-person at our Indore centre (Sudama Nagar)
- ✓ Both modes run concurrently in every batch; switch between them as your schedule needs
- ✓ Same syllabus, lab access, and certification track for online and on-premise students

// CERTIFICATIONS & CAREER OUTCOMES

Certifications & Career Outcomes

This course aligns with industry-recognised certifications and prepares graduates for offensive-security, application-security, and infrastructure-security roles.

- OSWE (Offensive Security Web Expert)
- CEH (Certified Ethical Hacker)
- eWPT (eLearnSecurity Web Penetration Tester)
- BSCP (Burp Suite Certified Practitioner)
- GWAPT (GIAC Web App Penetration Tester)

// ENROL WITH ARMOUR INFOSEC

Enrol With Armour Infosec

Reach out to discuss enrolment, batch schedule, and lab access. Our Indore training centre runs both in-person and live online cohorts with placement assistance.

PHONE +91 99777 47168

EMAIL	info@armourinfosec.com
ADDRESS	674, Sudama Dwar, Narendra Tiwari Marg, Sudama Nagar, Indore, Madhya Pradesh 452009
WEBSITE	https://armourinfosec.com

Scan to View Course Online

https://www.armourinfosec.com/training/web-application-security/