# Web Application Penetration Testing Training Course

Professional Development Training Course Outline

| | | | |
|---|---|---|---|
| **Category** | Data Security | **Duration** | 10 Days |
| **Base Fee** | $3,000 USD | **Delivery Mode** | Online / On-site Hybrid |

## Course Introduction

Web Application Penetration Testing Training Course equips aspiring and established cybersecurity professionals with the offensive security mindset and practical ethical hacking skills needed to secure the digital landscape. As modern enterprises rapidly adopt DevSecOps and leverage complex cloud-native architectures and APIs, the attack surface of web applications has critically expanded. This training provides a hands-on, real-world experience in identifying, exploiting, and mitigating the most critical vulnerabilities, including those outlined in the latest OWASP Top 10 standard. Our focus is on practical mastery of contemporary tools and methodologies, ensuring participants can perform comprehensive, high-value penetration tests and contribute immediately to strengthening an organization's overall security posture.

The program is designed to move beyond theoretical concepts, diving deep into vulnerability research and full-stack exploitation techniques. With the increasing integration of AI/ML into application security and the growing prevalence of threats like Server-Side Request Forgery (SSRF) and Broken Access Control, it is crucial for security practitioners to stay ahead. Upon completion, students will be proficient in utilizing industry-leading frameworks like Burp Suite Professional and Kali Linux, enabling them to conduct detailed security assessments, write professional-grade reports, and implement effective risk prioritization and remediation strategies, driving a necessary "shift-left" approach to application security.

## Programme Curriculum

**Web Application Penetration Testing Training Course**

**Introduction**

Web Application Penetration Testing Training Course equips aspiring and established cybersecurity professionals with the offensive security mindset and practical ethical hacking skills needed to secure the digital

landscape. As modern enterprises rapidly adopt DevSecOps and leverage complex cloud-native architectures and APIs, the attack surface of web applications has critically expanded. This training provides a hands-on, real-world experience in identifying, exploiting, and mitigating the most critical vulnerabilities, including those outlined in the latest OWASP Top 10 standard. Our focus is on practical mastery of contemporary tools and methodologies, ensuring participants can perform comprehensive, high-value penetration tests and contribute immediately to strengthening an organization's overall security posture.

The program is designed to move beyond theoretical concepts, diving deep into vulnerability research and full-stack exploitation techniques. With the increasing integration of AI/ML into application security and the growing prevalence of threats like Server-Side Request Forgery (SSRF) and Broken Access Control, it is crucial for security practitioners to stay ahead. Upon completion, students will be proficient in utilizing industry-leading frameworks like Burp Suite Professional and Kali Linux, enabling them to conduct detailed security assessments, write professional-grade reports, and implement effective risk prioritization and remediation strategies, driving a necessary "shift-left" approach to application security.

**Course Duration**

10 days

**Course Objectives**

The successful participant will be able to:

1. Master the OWASP Top 10 (2021) framework for vulnerability identification and mitigation.
2. Conduct comprehensive Information Gathering and Attack Surface Mapping using passive and active reconnaissance techniques.
3. Execute and defend against advanced Injection Attacks, including SQL Injection and NoSQL Injection.
4. Identify and exploit vulnerabilities in modern API Security.
5. Perform Broken Access Control and Authentication Failures testing to bypass security mechanisms.
6. Exploit complex application logic flaws, including Race Conditions and business logic vulnerabilities.
7. Analyze and exploit common client-side flaws like Cross-Site Scripting and Cross-Site Request Forgery (CSRF).
8. Discover and mitigate Server-Side Request Forgery and XML External Entity injections.
9. Apply DevSecOps principles and a "Shift-Left" approach to embed security throughout the Software Development Life Cycle (SDLC).
10. Test and secure applications deployed in Cloud Environments.
11. Demonstrate proficiency in using industry-standard tools like Burp Suite Professional, Sqlmap, and Nmap.
12. Write professional, actionable Penetration Testing Reports with clear Risk Prioritization and remediation steps.
13. Understand and comply with security standards such as PCI DSS and GDPR as they relate to web application security.

**Target Audience**

1. Aspiring Penetration Testers/Ethical Hackers
2. Security Analysts and Consultants
3. Software Developers and Engineers
4. Security Architects and QA Testers
5. DevOps and DevSecOps Engineers
6. IT Security Professionals.

7. Bug Bounty Hunters
8. Information Security Managers requiring technical oversight.

**Course Modules**

**Module 1: Core Penetration Testing Methodology**

- Penetration Testing Execution Standard and OWASP WSTG frameworks.
- Setting up the Lab Environment.
- Scoping, Rules of Engagement, and different testing types
- Professional Reporting and effective Remediation Tracking.
- Case Study: The Target Data Breach (2013).

**Module 2: Advanced Reconnaissance and Attack Surface Mapping**

- Passive Reconnaissance
- Active Reconnaissance.
- Website structure analysis, technology fingerprinting, and source code review.
- Identifying sensitive information exposure in public repositories.
- Mapping out hidden APIs, subdomains, and cloud-hosted assets.
- Case Study: Casio Cyber Attack (2023).

**Module 3: Proxying, Traffic Analysis, and Burp Suite Mastery**

- Configuring and mastering the Burp Suite Proxy, Repeater, Intruder, and Decoder tools.
- Intercepting, modifying, and analyzing HTTP/HTTPS requests and responses.
- Advanced fuzzing techniques using Burp Intruder for efficient brute-forcing and data extraction.
- Using Burp Collaborator for out-of-band application security testing.
- Writing custom Burp Extensions for specialized tasks.
- Case Study: Real-World SaaS Pentest Findings

**Module 4: Injection Vulnerabilities**

- Deep dive into SQL Injection.
- Automated exploitation using Sqlmap and manual exploitation techniques.
- Understanding and exploiting NoSQL Injection vulnerabilities
- Parameterized Queries, Input Validation, and Principle of Least Privilege.
- Exploiting Time-Based Blind SQLi and Out-of-Band SQLi for advanced data exfiltration.
- Case Study: Large E-commerce Data Breach via SQLi.

**Module 5: Authentication and Session Management Flaws**

- Testing for Brute-Force and credential stuffing vulnerabilities.
- Exploiting weak or predictable session tokens and cookie attributes
- Testing account enumeration, insecure password reset functions, and multifactor authentication bypasses.
- Understanding and exploiting Insecure Direct Object References
- Strong session generation, proper token storage, and secure logout/timeout implementation.
- Case Study: The LinkedIn Breach (2012) on weak hashing.

**Module 6: Broken Access Control**

- Vertical Privilege Escalation testing
- Horizontal Privilege Escalation testing
- Testing for Mass Assignment and function-level access control vulnerabilities.
- Exploiting client-side enforcement of security controls.
- Deny by Default, domain-specific access control checks, and secure authorization mechanisms.
- Case Study: Healthcare Portal Data Leak

**Module 7: Cross-Site Scripting and CSRF**

- Deep dive into Stored XSS, Reflected XSS, and DOM-based XSS and their impacts.
- Bypassing client-side filters and Content Security Policy for exploitation.
- Exploiting Cross-Site Request Forgery vulnerabilities using automated payload generation.
- Context-aware output encoding, Input Sanitization, and Anti-CSRF tokens.
- Testing for Blind XSS exploitation using tools like XSS Hunter.
- Case Study: Twitter/XSS Worm

**Module 8: Server-Side Request Forgery and XXE**

- Understanding and exploiting basic and blind Server-Side Request Forgery
- Bypassing hostname and IP blacklists to access internal resources.
- Exploiting XML External Entity Injection for data disclosure and Denial of Service
- Whitelisting, input validation, and disabling external entity processing.
- Exploiting SSRF to leverage cloud metadata endpoints
- Case Study: Capital One Data Breach (2019) via SSRF/WAF Misconfiguration.

**Module 9: Web API Penetration Testing**

- Understanding API architecture, authentication mechanisms
- Testing for the OWASP API Security Top 10.
- Vulnerabilities specific to APIs.
- Testing GraphQL endpoints for introspection and resource exhaustion attacks.
- Using specialized tools like Postman and Kiterunner for API discovery and testing.
- Case Study: Facebook/Cambridge Analytica Data Exposure.

**Module 10: Advanced Business Logic Flaws**

- Identifying and exploiting flaws in application-specific logic.
- Testing for parameter tampering and inadequate process flow checks.
- Exploiting Race Conditions to gain an unfair advantage
- Testing for insufficient input validation leading to business integrity issues.
- Server-side validation, transactional integrity, and comprehensive state checks.
- Case Study: Airline Ticket Booking Logic Flaw.

**Module 11: Vulnerable and Outdated Components/Misconfiguration**

- Scanning for vulnerable dependencies and outdated software libraries.
- Testing for security Misconfigurations in web servers and containers.
- Analyzing HTTP headers and configuration files for security weaknesses.
- Identifying and exploiting Unvalidated Redirects and Forwards.
- Hardening techniques for web servers, application servers, and load balancers.
- Case Study: Equifax Data Breach (2017) via Apache Struts.

**Module 12: Advanced Exploitation Techniques**

- Remote Code Execution and Command Injection exploitation.
- Bypassing Web Application Firewalls using obfuscation and alternate encoding.
- Exploiting insecure file upload mechanisms and path traversal vulnerabilities.
- Leveraging post-exploitation techniques, including persistence and data exfiltration.
- Exploiting deserialization vulnerabilities
- Case Study: SolarWinds Supply Chain Attack (2020).

**Module 13: Client-Side and Hostile Redirects**

- Deep dive into client-side security mechanisms and weaknesses.
- Exploiting Cross-Origin Resource Sharing misconfigurations.
- Attacks against the application user
- Exploiting Unvalidated Redirects and Forwards to facilitate phishing attacks.
- X-Frame-Options, secure CORS policy, and strict redirect validation.
- Case Study: Phishing Campaign leveraging an Open Redirect.

**Module 14: Cloud & DevOps Security Testing**

- Testing applications in AWS, Azure, and GCP environments.
- Introduction to Infrastructure as Code security analysis
- Testing Container Security for misconfigurations and escape vulnerabilities.
- Integrating security testing into the CI/CD Pipeline
- Scanning and securing CI/CD tools and environments
- Case Study: Docker/Kubernetes Misconfiguration leading to Cryptojacking.

**Module 15: Reporting, Compliance, and Professional Practice**

- Structuring a high-quality, professional Penetration Test Report
- Applying the Common Vulnerability Scoring System for objective risk rating.
- Developing clear, actionable Mitigation and Remediation Strategies.
- Understanding compliance requirements.
- Ethical and legal considerations for penetration testers.
- Case Study: A-LIGN's Social Engineering & Penetration Test Report.

## Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

**Register as a group from 3 participants for a Discount**

**Send us an email: info@fineskilltrainingcenter.org or call** +254769199797

**Certification**

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

**Tailor-Made Course**

We also offer tailor-made courses based on your needs.

**Key Notes**

**a.** The participant must be conversant with English.

**b.** Upon completion of training the participant will be issued with an Authorized Training Certificate

**c.** Course duration is flexible and the contents can be modified to fit any number of days.

**d.** The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

**e.** One-year post-training support Consultation and Coaching provided after the course.

**f.** Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

## Upcoming Scheduled Sessions

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **21 Sep 2026** | 02 Oct 2026 | Online | $2,000 |
| **21 Sep 2026** | 02 Oct 2026 | Physical | $3,000 |
| **21 Sep 2026** | 02 Oct 2026 | Physical | $0 |
| **21 Sep 2026** | 02 Oct 2026 | Physical | $0 |
| **21 Sep 2026** | 02 Oct 2026 | Physical | $0 |
| **21 Sep 2026** | 02 Oct 2026 | Physical | $0 |
| **21 Sep 2026** | 02 Oct 2026 | Physical | $0 |
| **21 Sep 2026** | 02 Oct 2026 | Physical | $0 |

Ready to enroll or request a customized program? Book online or contact us:

**Register Online Now**

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com