Certified Web Penetration Tester Program

The objective of this program is to equip learners with practical offensive security skills in web application penetration testing, including vulnerability assessment, exploitation, and professional reporting, preparing them for Red Team and Web Penetration Tester roles and the Certified Web Penetration Tester certification.

100 HOURS | <DATE> | FULLY ONLINE

- Provides practical training for professionals transitioning into offensive security and Red Team roles.
- Builds hands-on skills in web application vulnerability discovery, exploitation, and reporting.
- Includes applied labs, real-world case studies, and certification assessments.
- Covers web architecture, injection attacks, server-side exploitation, authentication testing, and professional reporting.
- Delivered through an online learning platform with guided instruction and practical exercises.
- Designed for professionals seeking Web Penetration Tester and Penetration Tester roles.

TARGET AUDIENCE

- Security professionals transitioning from defensive to offensive security
- Blue team and SOC analysts with prior experience
- Professionals launching careers in Red Team operations and offensive cybersecurity
- IT and security staff with intermediate technical proficiency
- Anyone preparing for Web Penetration Tester or Penetration Tester roles

THE INSTRUCTOR

This program is delivered through a dedicated learning platform and supported by experienced instructors with strong backgrounds in cybersecurity, IT systems, and digital technologies.

The training combines guided instruction, hands-on labs, case studies, and applied assessments to help participants build practical skills and prepare for certification.

ABOUT ECS ETHIOPIA

ECS Ethiopia is a technology-driven company working with government bodies, municipalities, and large corporations to bring advanced global solutions to Ethiopia. As part of the ECS Group (UK), we help finance and execute major projects while fostering strong partnerships and innovation across the country.

GLOBAL TRAINING PARTNERSHIPS

Our training programs and learning platform were developed in close collaboration with leading international training organisations. Thousands of professionals worldwide have successfully completed these programs using this training content and learning system.

WEB SECURITY TESTING FOUNDATIONS COURSE

This course builds essential web application security testing fundamentals, covering web basics, architecture, and reconnaissance. You will learn how modern web applications work, how to analyze them systematically, and how to use tools like Burp Suite for professional security testing.

MODULE 1

WEB FUNDAMENTALS AND CLIENT-SIDE TECHNOLOGY

This module introduces the core web technologies and the attacker mindset behind exploiting them, covering HTTP, HTML, JavaScript, and how browser architecture becomes an attack surface.

Topics Covered:

- How Attackers Think: Behavior Before Exploits
- HTTP – The Main Protocol Behind the Web
- HTML and the Structure of Input
- JavaScript Fundamentals
- Browser Architecture and Capabilities

MODULE 2

WEB ARCHITECTURE AND CLIENT-SIDE STORAGE

This module examines how modern web applications are built and how client-side data is stored, covering server structures, authentication flows, and storage mechanisms where vulnerabilities commonly emerge.

Topics Covered:

- Web Server Basics
- Browser Storage
- Web Application Architecture
- Authentication Flow

MODULE 3

WEB INTERCEPTION AND RECONNAISSANCE TECHNIQUES

This module gives learners hands-on experience intercepting and analyzing web communications, identifying technologies in use, and evaluating security headers to uncover perimeter weaknesses.

Topics Covered:

- HTTP Interception and Modification Concepts
- Interception & Testing Setup
- Technology Identification & Security Headers
- Web Application Perimeter Evaluation

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Basic HTML Coding
- Basic JavaScript Coding
- Browser Architecture and Capabilities
- Simple Website Serverside Exploration
- Browser Storage Analysis
- Intercept and Access with Burp Suite
- Web Server Reconnaissance

CASE STUDY

- The Pizza Index
- The Curious Case of DefendNot
- A Hidden Field with Too Much Power

WEB VULNERABILITY EXPLOITATION COURSE

This course builds a strong foundation in vulnerability discovery and exploitation, exposing you to a wide range of common and critical web application flaws. From injection attacks to server-side exploitation and file system vulnerabilities, you will learn how these weaknesses arise, how attackers leverage them, and how to identify them systematically.

MODULE 1

VULNERABILITY FOUNDATIONS AND INJECTION ATTACKS

This module covers the core principles of web application vulnerabilities, focusing on injection-based attacks like XSS and SQL injection, with hands-on labs reinforcing secure coding and defensive validation.

Topics Covered:

- Vulnerability Fundamentals
- Cross Site Scripting (XSS)
- SQL Injection (SQLi)

MODULE 2

SERVER-SIDE EXPLOITATION AND FILE SYSTEM ATTACKS

This module covers attacks targeting server-side execution and file system access, including command injection, directory traversal, and insecure file uploads, with a focus on exploitation paths and mitigation practices.

Topics Covered:

- Command Injection Basics
- Local File Inclusion and Path Traversal
- Insecure File Upload Vulnerabilities

MODULE 3

HTTP SECURITY AND CONFIGURATION FLAWS

This module examines HTTP and server configuration weaknesses that enable attackers to bypass controls, covering CSRF and SSRF attack vectors and best practices for hardening through secure headers and policy enforcement.

Topics Covered:

- Cross-Site Request Forgery (CSRF)
- HTTP Security Headers
- Server-Side Request Forgery (SSRF)

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Comprehensive XSS Discovery and Exploitation
- Building Your First Database
- SQL Injection Playground
- Command Injection 101
- File Inclusion Assessment
- Insecure File Upload Exploitation
- CSRF Discovery and Exploitation
- SSRF Discovery

CASE STUDY

- The Log4Shell Attack (CVE-2021-44228)
- The MySpace Samy Worm
- Mutation XSS – When Sanitization Backfires
- The GLPI Vulnerability (CVE-2025-24799)
- Sophos Command Injection
- Node.js Path Traversal
- Casdoor Identity Management CSRF

WEB APPLICATION PENETRATION TESTING COURSE

This course builds skills in identifying and exploiting authentication, authorization, and logic flaws. From username enumeration and brute force bypasses to access control weaknesses, privilege escalation, and business logic attacks, you will learn how these vulnerabilities emerge, how they are exploited, and how to detect them effectively.

MODULE 1

WEB LOGIC AND AUTHENTICATION TESTING

This module examines authentication and logic flaws attackers exploit to bypass credentials, covering username enumeration, brute-force bypasses, and token/password-recovery vulnerabilities, with labs reinforcing practical defenses.

Topics Covered:

- Username Enumeration & Authentication Logic Bypass
- Brute Force Protection Bypass & Rate Limiting
- Password Recovery and Token Exploitation

MODULE 2

AUTHORIZATION AND ACCESS CONTROL EXPLOITATION

This module covers authorization weaknesses and access-control failures, including IDOR exploitation, privilege escalation, and business-logic vulnerabilities that allow attackers to access data or functions beyond their privileges.

Topics Covered:

- Access Control Foundations & Basic Bypasses
- Insecure Direct Object References (IDOR)
- Privilege Escalation Testing
- Business Logic Vulnerabilities

MODULE 3

PROFESSIONAL ASSESSMENT AND REPORTING

This module teaches the professional practices for conducting and communicating web application penetration tests, covering advanced scenarios like JWT attacks, CVSS-based risk scoring, and building clear, actionable reports for technical and non-technical stakeholders.

Topics Covered:

- JWT Attacks
- Professional Testing Methodology
- CVSS Scoring and Risk Classification
- Professional Report Structure

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Authentication Testing
- Anti-Automation Testing
- Password Recovery Exploitation
- IDOR Exploitation
- JWT Exploitation End-to-End

CASE STUDY

- Equifax Breach (2017)
- National Public Data Breach
- 2024 CDK Global Cyberattack
- Red Scenario Analysis and Rule Tuning – Part 1
- Red Scenario Analysis and Rule Tuning – Part 2