ECS Ethiopia

Certified Advanced Web Penetration Tester Program

The objective of this program is to equip experienced security professionals with advanced manual exploitation skills in web application penetration testing, including server-side attacks, protocol-level exploitation, JavaScript object manipulation, and API security, preparing them for senior Web Penetration Tester roles and the Certified Advanced Web Penetration Tester certification.

100 HOURS | <DATE> | FULLY ONLINE

- Provides advanced training for professionals moving beyond foundational web penetration testing.
- Builds specialized skills in manual exploitation techniques that automated scanners routinely miss.
- Includes applied labs, real-world case studies, and certification assessments.
- Covers XXE, SSTI, WordPress security, WebSockets, request smuggling, federated identity attacks, GraphQL, and deserialization.
- Delivered through an online learning platform with guided instruction and practical exercises.
- Designed for professionals advancing to senior Web Penetration Tester and Red Team roles.

TARGET AUDIENCE

- Professionals who completed the Certified Web Penetration Tester (Core Tier) or have equivalent knowledge
- Penetration testers moving beyond foundational web testing into specialized exploitation
- Red Team operators advancing their manual exploitation skills
- Offensive security professionals targeting senior pen tester roles
- Cybersecurity professionals specializing in complex web attack vectors

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.

SERVER-SIDE PROCESSING AND CMS SECURITY COURSE

This course builds advanced server-side exploitation skills, covering XML and template injection, comprehensive WordPress security assessment, and modern transport-layer attacks. You will learn to exploit attack surfaces that automated scanners routinely miss, including XXE, SSTI, CMS vulnerabilities, WebSockets, and PostMessage flaws.

MODULE 1

XXE AND SSTI EXPLOITATION

This module covers advanced server-side injection attacks, focusing on XML External Entity (XXE) and Server-Side Template Injection (SSTI). Learners exploit direct and blind XXE to access local files and internal networks, then identify vulnerable template engines, escape sandboxes, and achieve Remote Code Execution.

Topics Covered:

- XML External Entity (XXE)
- Server-Side Template Injection (SSTI)

MODULE 2

WORDPRESS SECURITY ASSESSMENT

This module provides a comprehensive methodology for assessing WordPress security. Learners explore WordPress architecture, misconfigurations, and XML-RPC abuse, then dive into plugin and theme vulnerabilities, file upload exploitation, and full attack chains from reconnaissance to system compromise.

Topics Covered:

- WordPress Architecture and Reconnaissance
- Authentication Weaknesses and Access Vector Abuse
- Plugin and Theme Vulnerability Assessment
- File Upload, File Access, and Code Execution
- Full Attack Chains and Automation

MODULE 3

WEBSOCKETS AND POSTMESSAGE EXPLOITATION

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:

- WebSocket Fundamentals
- Cross-Site WebSocket Hijacking
- WebSocket Fuzzing and Exploitation
- PostMessage Fundamentals and Discovery
- PostMessage Attack Surface and Exploitation
- Advanced PostMessage Attacks and Defense

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- XXE Detection
- Advanced XXE Exploitation
- SSTI Detection Fundamentals
- SSTI Command Execution
- WordPress Recon
- XML-RPC Attack Chain
- WordPress Professional Assessment
- WebSocket Discovery and Tampering
- CSWSH Attack Implementation
- PostMessage Discovery and Tampering
- PostMessage Exploitation Workshop

WEB PROTOCOL AND IDENTITY EXPLOITATION

This course builds advanced skills in protocol-level attacks and identity exploitation, covering HTTP request smuggling, cache poisoning and deception, open redirects, and federated identity protocols. You will learn how complex architectural flaws and SSO weaknesses are discovered, exploited, and chained for high-impact compromise.

MODULE 1

REQUEST SMUGGLING AND CACHE ATTACKS

This module covers architectural flaws in how servers parse and cache traffic, teaching HTTP Request Smuggling (CL.TE, TE.CL) to bypass security controls and Web Cache Poisoning to affect all application users.

Topics Covered:

- HTTP Request Smuggling Fundamentals
- CL.TE and TE.CL Smuggling Variants
- Obfuscation-Based Smuggling (TE.TE, CL.CL)
- Web Cache Poisoning Techniques
- Request Capture and Credential Theft

MODULE 2

WEB CACHE DECEPTION AND REDIRECT EXPLOITATION

This module covers attacks that trick caches into storing sensitive user data and exploit redirect logic. Learners master path confusion attacks against CDNs and origin servers, and apply advanced Open Redirect chaining to bypass SSRF filters and enable client-side attacks.

Topics Covered:

- Web Cache Deception Fundamentals
- Path Confusion Exploitation
- Cache Deception Methodology
- Open Redirect Fundamentals
- Validation Bypass Techniques
- Attack Chaining and Impact

MODULE 3

ATTACKING FEDERATED IDENTITY PROTOCOLS

This module demystifies the complexity of federated identity used by modern enterprises. Learners examine OAuth 2.0, OpenID Connect (OIDC), and SAML attack surfaces, from stealing OAuth tokens via redirect manipulation to forging SAML assertions using XML Signature Wrapping.

Topics Covered:

- SSO Foundations
- OAuth Fundamentals
- OAuth Attacks and Exploitation
- OIDC Fundamentals
- OIDC Attacks
- SAML Fundamentals
- Signature Attacks and Exploitation

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Classic Smuggling Variants
- Modern Smuggling Variants
- Smuggling Impact Exploitation
- Cache Poisoning Techniques
- Professional Cache Testing
- Web Cache Deception Exploitation
- Open Redirect Exploitation
- OAuth Exploitation Workshop
- OIDC Token Exploitation
- SAML Signature Bypass
- SAML Professional Assessment

ADVANCED EXPLOITATION VECTORS

This course covers the most technically demanding vulnerability classes in modern web applications, including JavaScript object manipulation, GraphQL and Mass Assignment attacks, insecure deserialization, and race conditions. You will learn to exploit deep logic flaws across client and server environments and master techniques used by advanced penetration testers.

MODULE 1

JAVASCRIPT OBJECT EXPLOITATION

This module explores deep JavaScript logic flaws across browser and server environments. Learners master Prototype Pollution to manipulate the prototype chain for XSS or RCE, and use DOM Clobbering to inject HTML that overrides global JavaScript variables and bypasses sanitizers.

Topics Covered:

- Prototype Pollution Foundations
- Browser Analysis for Prototype Pollution
- Client-Side Prototype Pollution
- Server-Side Prototype Pollution
- DOM Clobbering
- DOM Clobbering Exploitation

MODULE 2

GRAPHQL AND OBJECT BINDING ATTACKS

This module covers GraphQL security and Object Binding flaws as APIs evolve beyond REST. Learners perform GraphQL reconnaissance, bypass authorization logic, exploit batching mechanisms, and use Mass Assignment to manipulate autobinding frameworks and modify internal object properties.

Topics Covered:

- GraphQL Foundations
- GraphQL Reconnaissance
- GraphQL Attacks
- Mass Assignment Foundations
- Discovery and Exploitation

MODULE 3

INSECURE DESERIALIZATION AND RACE CONDITIONS

This module covers two of the most technically demanding vulnerability classes. Learners study Insecure Deserialization through PHP object injection, POP chains, and PHAR techniques, then use advanced timing attacks with Turbo Intruder to exploit concurrency flaws in multi-threaded applications.

Topics Covered:

- Insecure Deserialization
- Basic Deserialization Exploitation
- PHAR Deserialization and POP Chains
- Race Condition Basics
- Race Condition Exploitation

MODULE 4

CLOSURE & CERTIFICATION

Course wrap-up and exam readiness.

LABS

- Client-Side Prototype Pollution
- Server-Side Prototype Pollution
- DOM Clobbering Exploitation
- GraphQL Reconnaissance
- GraphQL Authorization Exploitation
- Mass Assignment Exploitation
- PHP Deserialization Basics
- Advanced PHP Deserialization
- Basic Race Conditions
- Advanced Race Conditions