+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 06/09/2026

Sign up

# Web Operations Specialist (CWES) Certification Training

3 days (21 hours)

## Overview

The HTB Certified Web Exploitation Specialist (CWES) certification validates your ability to identify and exploit web vulnerabilities in realistic environments. It is particularly useful for conducting application penetration tests, assessing risks, and proposing actionable fixes.

This training course provides hands-on preparation for the CWES requirements: methodology, attack chains, evidence collection, and report writing. You will work on real-world scenarios (vulnerable applications, API endpoints, authentication, session management) to replicate audit conditions.

The approach focuses on guided workshops and demos: reconnaissance, exploitation, post-exploitation, and hardening. Deliverables include test checklists, report templates, command/tool notes, and an exam-oriented review plan.

## Objectives

- Map a web attack surface and prioritize vectors.
- Exploit common vulnerabilities (injections, XSS, access control, SSRF).
- Analyze authentication, sessions, and anti-CSRF mechanisms.
- Test APIs (REST) and validate server-side controls.
- Document proof-of-concept exploits and recommend remediation measures.

## Target Audience

- Penetration testers and application security consultants
- Developers looking to strengthen the security of their apps
- SOC/Blue Team analysts involved in web detection
- Security project managers responsible for patch validation

# Prerequisites

- Solid foundation in HTTP, cookies, sessions, and headers
- Basic knowledge of HTML/JavaScript and a back-end language (PHP, Python, or Node.js)
- Understanding of databases and SQL
- Knowledge of Linux and terminal usage

# Technical prerequisites

- Linux recommended (or Windows with WSL2, or macOS)
- Tools: browser, Burp Suite, curl, nmap, code editor
- Stable internet connection and the ability to run lab environments

# Course outline for our HTB Certified Web Exploitation Specialist (CWES) certification

## [Day 1 - Morning]

### Fundamentals of Web Exploitation and CWES Methodology

- HTTP/HTTPS review: methods, headers, cookies, sessions, and status codes
- Mapping an application: endpoints, parameters, authentication flows, roles
- Web attack chain: reconnaissance, identification, exploitation, post-exploitation
- Analysis best practices: notes, evidence, reproducibility, risk management
- Hands-on workshop: Setting up a Burp Suite workflow (proxy, scope, repeater) and tracing an application flow.

## [Day 1 - Afternoon]

### Access controls and authentication attacks

- Identifying IDOR/BOLA: objects, references, server-side controls, impacts
- Authentication bypass: logic, forgotten endpoints, hidden parameters, password reset
- Session management: pinning, invalidation, rotation, cookies (Secure/HttpOnly/SameSite)
- Forced navigation: feature discovery and horizontal/vertical escalation
- Hands-on workshop: Exploiting an IDOR and demonstrating a privilege escalation with evidence and fixes.

## [Day 2 - Morning]

### SQL injection: detection, exploitation, and workarounds

- Detecting an SQLi: errors, time-based, boolean-based, response differences
- Manual exploitation: UNION, targeted extraction, minimal enumeration
- Workarounds: filtering, encodings, comments, syntax variations
- Impacts: read/write, exfiltration, application pivoting, logical control takeover
- Hands-on workshop: Perform data extraction via SQLi (boolean/time) and write a reproducible PoC.

### [Day 2 - Afternoon]

## Server-side injections: Command Injection, SSTI, and deserialization

- Command Injection: entry points, delimiters, RCE hardcoding, output validation
- SSTI: identifying engines, escape primitives, file reading, and execution
- Deserialization: signatures, gadgets, impacts, environmental constraints
- Hardening: Strict validation, whitelisting, sandboxing, removal of dangerous features
- Hands-on workshop: Achieve controlled command execution (RCE) on a lab target and propose a remediation.

### [Day 3 - Morning]

## File vulnerabilities: upload, LFI/RFI, and path traversal

- Path traversal: normalization, encodings, workarounds, and systematic testing
- LFI/RFI: inclusion, wrappers, log poisoning, configuration constraints
- Upload: weak validations, double extensions, content-type, polyglots, public storage
- Chaining: upload → execution, LFI → secrets, traversal → configuration
- Hands-on workshop: Exploit an upload to gain execution or access to secrets, then develop a remediation plan.

### [Day 3 - Afternoon]

## SSRF, XSS, and preparation for the CWES exam

- SSRF: detection, bypassing filters, metadata access, internal pivoting
- XSS: reflected/stored/DOM, contexts (HTML/JS/URL), impact on sessions and actions
- Realistic scenarios: SSRF? Secret leakage? Account takeover, XSS? CSRF-like actions
- Exam strategy: time management, prioritization, evidence collection, final report
- Hands-on workshop: Mini-CWES simulation (2 vulnerabilities to chain) with deliverables: PoC, impact, fixes.

# Target Audience

This training is designed for both individuals and companies—large or small—that wish to train their teams in new advanced IT technologies or to acquire specific professional knowledge or modern methods.

## Entry-level assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

## Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

## Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

## Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

## Certification

A certificate will be issued to each trainee who has completed the entire training program.