+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 Expert Certification (CWEE) Training

3 days (21 hours)

Overview

The HTB Certified Web Exploitation Expert (CWEE) certification validates your ability to identify, exploit, and document advanced web vulnerabilities. It is designed for professionals who want to transition from a “scan” approach to a structured offensive methodology applicable to penetration testing, bug bounties, and application audits.

The training aims to master a complete exploitation chain: reconnaissance, application behavior analysis, exploitation, impact escalation, and recommendations. You will work on realistic scenarios (authentication, APIs, business logic, sessions) using a reproducible methodology.

The approach is 100% hands-on: guided workshops, exploitation demos, timed exercises, and feedback. Course materials include checklists, report templates, Burp playbooks, and methodology notes to help you prepare for the exam.

Objectives

- Reliably map a web and API attack surface.
- Exploit OWASP flaws and business logic vulnerabilities.
- Analyze and bypass access controls and session mechanisms.
- Automate targeted tests using Burp Suite and scripts.
- Document proof-of-concept exploits and actionable remediation steps.

Target Audience

- Penetration testers and application security consultants
- Developers looking to strengthen the security of their applications
- SOC/CSIRT analysts focused on web investigations
- Intermediate bug bounty hunters

Prerequisites

- Strong knowledge of HTTP/HTTPS, cookies, sessions, and CORS
- Basic knowledge of JavaScript and at least one programming language (Python, PHP, Node)
- Knowledge of common web vulnerabilities (OWASP Top 10)
- Basic understanding of SQL and authentication (JWT, OAuth2)

Technical prerequisites

- Linux (Kali/Ubuntu) or Windows with WSL2, or macOS
- Burp Suite, Chromium/Firefox browser, Docker, or VM
- Tools: Git, Python 3, curl, jq, code editor

Course outline for our HTB Certified Web Exploitation Expert (CWEE) certification

[Day 1 - Morning]

Web reconnaissance and attack surface mapping

- Identifying technologies, frameworks, and versions (headers, fingerprints, errors)
- Mapping the application: endpoints, parameters, flows, roles, and permissions
- Targeted enumeration: hidden content, sensitive files, undocumented endpoints
- Set up a Burp Suite workflow: proxy, scope, repeater, intruder, logger
- Hands-on workshop: Build a comprehensive map of a target application and prioritize attack vectors.

[Day 1 - Afternoon]

Access control: IDOR, BOLA, and horizontal/vertical escalations

- Detecting and exploiting IDORs (objects, resources, multi-tenant)
- Testing BOLA/BFLA on APIs: endpoints, methods, fields, and filters
- Bypassing authorizations: parameters, alternative paths, credential confusion
- Impact validation: read/write, deletion, account takeover
- Hands-on workshop: Exploiting an unauthorized access vulnerability and producing reproducible proof of impact.

[Day 2 - Morning]

Server-side injections: SQLi, NoSQLi, and command injections

- Identifying injection points: parameters, JSON, headers, cookies, files
- SQLi: error-based, union-based, blind (boolean/time), and controlled extraction
- NoSQLi: operators, filter bypasses, and impacts on authentication
- Command injection: detection, encodings, delimiters, and execution constraints
- Hands-on workshop: Extract data via injection (SQL/NoSQL) and demonstrate controlled command execution.

[Day 2 - Afternoon]

Logic flaws and attacks on authentication

- Analyzing workflows: registration, reset, email change, action validation
- Authentication bypass: logic flaws, inconsistent states, forgotten endpoints
- Session attacks: session fixation, session invalidation, session rotation, multi-device management
- Brute force and rate limiting: workarounds, lockouts, protections, and evidence
- Hands-on workshop: Exploiting a logic flaw to take control of an account without knowing the password.

[Day 3 - Morning]

Advanced exploitation: SSRF, XXE, and deserialization

- SSRF: detection, bypasses (DNS rebinding, encodings), pivoting to internal services
- Cloud metadata access: exposure validation and secret extraction
- XXE: vectors (XML/SOAP), exfiltration, SSRF via external entities
- Deserialization: identification, gadgets, impacts (RCE, auth bypass, data tampering)
- Hands-on workshop: Chaining an SSRF/XXE to reach an internal service and retrieve sensitive information.

[Day 3 - Afternoon]

Chaining, web post-exploitation, and exam preparation

- Building a realistic attack chain: from foothold to business impact
- Exfiltration and evidence: minimal collection, traceability, reproducibility of steps
- Report hardening: description, risk, conditions, actionable recommendations
- CWEE strategy: time management, prioritization, checklists, and common mistakes
- Hands-on workshop: Mini-simulation (full scenario) modeled after an exam, including the drafting of an exploitation report.

Target companies

This training is designed for both individuals and businesses, large and small,

wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Placement at the start of the training

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.