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

Mis à jour le 09/06/2026

S'inscrire

Formation Certification Web Exploitation Specialist (CWES)

3 jours (21 heures)

Présentation

La certification HTB Certified Web Exploitation Specialist (CWES) valide votre capacité à identifier et exploiter des vulnérabilités web dans des environnements réalistes. Elle est particulièrement utile pour mener des tests d'intrusion applicatifs, qualifier des risques et proposer des correctifs actionnables.

Cette formation vous prépare de façon opérationnelle aux exigences CWES : méthodologie, enchaînement des attaques, collecte de preuves et rédaction. Vous travaillerez sur des scénarios proches du terrain (applications vulnérables, endpoints API, authentification, gestion de sessions) afin de reproduire les conditions d'un audit.

L'approche est centrée sur des ateliers guidés et des démos : reconnaissance, exploitation, post-exploitation web et durcissement. Les livrables incluent des checklists de test, des templates de rapport, des notes de commandes/outils et un plan de révision orienté examen.

Objectifs

- Cartographier une surface d'attaque web et prioriser les vecteurs.
- Exploiter des failles courantes (injections, XSS, contrôle d'accès, SSRF).
- Analyser l'authentification, les sessions et les mécanismes anti-CSRF.
- Tester des APIs (REST) et valider les contrôles côté serveur.
- Rédiger des preuves d'exploitation et recommander des remédiations.

Public visé

- Pentesters et consultants sécurité applicative
- Développeurs souhaitant renforcer la sécurité de leurs apps
- Analystes SOC/Blue Team impliqués dans la détection web
- Chefs de projet sécurité en charge de la validation des correctifs

Pré-requis

- Bases solides en HTTP, cookies, sessions et en-têtes
- Notions de HTML/JavaScript et d'un langage back-end (PHP, Python ou Node.js)
- Compréhension des bases de données et du SQL
- Connaissances Linux et usage du terminal

Pré-requis techniques

- Linux recommandé (ou Windows avec WSL2, ou macOS)
- Outils : navigateur, Burp Suite, curl, nmap, éditeur de code
- Accès Internet stable et possibilité d'exécuter des environnements de lab

Programme de notre formation Certification HTB Certified Web Exploitation Specialist (CWES)

[Jour 1 - Matin]

Fondamentaux de l'exploitation Web et méthodologie CWES

- Rappels HTTP/HTTPS : méthodes, en-têtes, cookies, sessions et codes de statut
- Cartographier une application : endpoints, paramètres, flux d'authentification, rôles
- Chaîne d'attaque Web : reconnaissance, identification, exploitation, post-exploitation
- Hygiène d'analyse : notes, preuves, reproductibilité, gestion des risques
- Atelier pratique : Mettre en place un workflow Burp Suite (proxy, scope, repeater) et tracer un parcours applicatif.

[Jour 1 - Après-midi]

Contrôles d'accès et attaques d'authentification

- Identifier IDOR/BOLA : objets, références, contrôles côté serveur, impacts
- Bypass d'authentification : logique, endpoints oubliés, paramètres cachés, reset password
- Gestion de session : fixation, invalidation, rotation, cookies (Secure/HttpOnly/SameSite)
- Forcer la navigation : découverte de fonctionnalités et escalade horizontale/verticale
- Atelier pratique : Exploiter un IDOR et démontrer une escalade de privilèges avec preuves et correctifs.

[Jour 2 - Matin]

Injection SQL : détection, exploitation et contournements

- Détecter une SQLi : erreurs, time-based, boolean-based, différences de réponses
- Exploitation manuelle : UNION, extraction ciblée, enumeration minimale
- Contournements : filtrage, encodages, commentaires, variations de syntaxe
- Impacts : lecture/écriture, exfiltration, pivot applicatif, prise de contrôle logique
- Atelier pratique : Réaliser une extraction de données via SQLi (boolean/time) et rédiger un PoC reproductible.

[Jour 2 - Après-midi]

Injections côté serveur : Command Injection, SSTI et désérialisation

- Command Injection : points d'entrée, séparateurs, blind RCE, validation des sorties
- SSTI : identification des moteurs, primitives d'évasion, lecture de fichiers et exécution
- Désérialisation : signatures, gadgets, impacts, contraintes d'environnement
- Durcissement : validation stricte, listes blanches, sandboxing, suppression des fonctionnalités dangereuses
- Atelier pratique : Obtenir une exécution de commande contrôlée (RCE) sur une cible de labo et proposer une remédiation.

[Jour 3 - Matin]

Vulnérabilités de fichiers : upload, LFI/RFI et path traversal

- Path traversal : normalisation, encodages, contournements et tests systématiques
- LFI/RFI : inclusion, wrappers, logs poisoning, contraintes de configuration
- Upload : validations faibles, double extensions, content-type, polyglots, stockage public
- Chaînage : upload ? exécution, LFI ? secrets, traversal ? configuration
- Atelier pratique : Exploiter un upload pour obtenir l'exécution ou l'accès à des secrets, puis produire un plan de correction.

[Jour 3 - Après-midi]

SSRF, XSS et préparation à l'examen CWES

- SSRF : détection, contournement des filtres, accès metadata, pivot interne
- XSS : reflet/stocké/DOM, contextes (HTML/JS/URL), impact sur sessions et actions
- Chaînes réalistes : SSRF ? fuite de secrets ? prise de compte, XSS ? actions CSRF-like
- Stratégie d'examen : gestion du temps, priorisation, collecte de preuves, rapport final
- Atelier pratique : Mini-simulation CWES (2 vulnérabilités à chaîner) avec livrables : PoC, impact, correctifs.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.