+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 Expert (CWEE)

3 jours (21 heures)

Présentation

La certification HTB Certified Web Exploitation Expert (CWEE) valide votre capacité à identifier, exploiter et documenter des vulnérabilités web avancées. Elle s’adresse aux profils qui veulent passer d’une approche “scan” à une démarche offensive structurée, applicable en pentest, bug bounty et audit applicatif.

La formation vise à maîtriser une chaîne complète d’exploitation : reconnaissance, analyse du comportement applicatif, exploitation, élévation d’impact et recommandations. Vous travaillez sur des scénarios réalistes (authentification, API, logique métier, sessions) avec une méthodologie reproductible.

L’approche est 100% pratique : ateliers guidés, démos d’exploitation, exercices chronométrés et corrections. Les livrables incluent des checklists, des templates de rapport, des playbooks Burp et des notes de méthodologie pour préparer l’examen.

Objectifs

- Cartographier une surface d’attaque web et API de façon fiable.
- Exploiter des failles OWASP et des vulnérabilités de logique métier.
- Analyser et contourner des contrôles d’accès et mécanismes de session.
- Automatiser des tests ciblés avec Burp Suite et scripts.
- Rédiger des preuves d’exploitation et des remédiations actionnables.

Public visé

- Pentesters et consultants sécurité applicative
- Développeurs souhaitant renforcer la sécurité de leurs applications
- Analystes SOC/CSIRT orientés investigation web
- Profils bug bounty intermédiaires

Pré-requis

- Bon niveau en HTTP/HTTPS, cookies, sessions, CORS
- Pratique de base de JavaScript et d'au moins un langage (Python, PHP, Node)
- Connaissances des vulnérabilités web courantes (OWASP Top 10)
- Notions de SQL et d'authentification (JWT, OAuth2)

Pré-requis techniques

- Linux (Kali/Ubuntu) ou Windows avec WSL2, ou macOS
- Burp Suite, navigateur Chromium/Firefox, Docker ou VM
- Outils : Git, Python 3, curl, jq, éditeur de code

Programme de notre formation Certification HTB Certified Web Exploitation Expert (CWEE)

[Jour 1 - Matin]

Reconnaissance web et cartographie de surface d'attaque

- Identifier technologies, frameworks et versions (headers, fingerprints, erreurs)
- Cartographier l'application : endpoints, paramètres, flux, rôles et permissions
- Énumération ciblée : contenus cachés, fichiers sensibles, endpoints non documentés
- Mettre en place un workflow Burp Suite : proxy, scope, repeater, intruder, logger
- Atelier pratique : Construire une cartographie complète d'une application cible et prioriser les vecteurs.

[Jour 1 - Après-midi]

Contrôle d'accès : IDOR, BOLA et escalades horizontales/verticales

- Détecter et exploiter les IDOR (objets, ressources, multi-tenant)
- Tester BOLA/BFLA sur APIs : endpoints, méthodes, champs et filtres
- Bypass d'autorisations : paramètres, chemins alternatifs, confusion d'identifiants
- Validation des impacts : lecture/écriture, suppression, prise de contrôle de compte
- Atelier pratique : Exploiter une faille d'accès non autorisé et produire une preuve d'impact reproductible.

[Jour 2 - Matin]

Injections côté serveur : SQLi, NoSQLi et injections de commandes

- Identifier points d’injection : paramètres, JSON, headers, cookies, fichiers
- SQLi : error-based, union-based, blind (boolean/time) et extraction contrôlée
- NoSQLi : opérateurs, contournements de filtres et impacts sur l’authentification
- Command injection : détection, encodages, séparateurs et contraintes d’exécution
- Atelier pratique : Obtenir une extraction de données via injection (SQL/NoSQL) et démontrer une exécution de commande contrôlée.

[Jour 2 - Après-midi]

Failles de logique et attaques sur l’authentification

- Analyser les workflows : inscription, reset, changement d’email, validation d’actions
- Bypass d’authentification : failles de logique, états incohérents, endpoints oubliés
- Attaques sur sessions : fixation, invalidation, rotation, gestion multi-device
- Bruteforce et rate limiting : contournements, verrouillages, protections et preuves
- Atelier pratique : Exploiter une faille de logique pour prendre le contrôle d’un compte sans connaître le mot de passe.

[Jour 3 - Matin]

Exploitation avancée : SSRF, XXE et désérialisation

- SSRF : détection, contournements (DNS rebinding, encodages), pivot vers services internes
- Accès metadata cloud : validation d’exposition et extraction de secrets
- XXE : vecteurs (XML/SOAP), exfiltration, SSRF via entités externes
- Désérialisation : identification, gadgets, impacts (RCE, auth bypass, data tampering)
- Atelier pratique : Chaîner une SSRF/XXE pour atteindre un service interne et récupérer une information sensible.

[Jour 3 - Après-midi]

Chaînage, post-exploitation web et préparation à l’examen

- Construire une chaîne d’attaque réaliste : du foothold à l’impact métier
- Exfiltration et preuves : collecte minimale, traçabilité, reproductibilité des étapes
- Durcissement des rapports : description, risque, conditions, recommandations actionnables
- Stratégie CWEE : gestion du temps, priorisation, checklists et erreurs fréquentes
- Atelier pratique : Mini-simulation type examen (scénario complet) avec rédaction d’un rapport d’exploitation.

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.