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

Mis à jour le 05/06/2026

S'inscrire

Formation Certification GIAC GWEB®

3 jours (21 heures)

Présentation

La certification GIAC Certified Web Application Defender (GWEB) Practitioner vous prépare à défendre des applications web en conditions réelles : analyse de risques, durcissement, tests et réponse aux vulnérabilités. Elle s'adresse aux équipes qui doivent sécuriser des APIs, portails métiers et applications exposées.

Lors de cette formation, vous adoptez une approche pratique et opérationnelle centrée sur les failles courantes (authentification, gestion de session, injections, XSS, configuration) et les contrôles défensifs (validation, encodage, en-têtes, journalisation). Les notions sont systématiquement reliées à des cas d'usage : revue de code, triage d'alertes, correction et vérification.

La formation alterne démos et ateliers guidés : reproduction d'attaques, mise en place de contre-mesures, puis validation via tests. Livrables : checklists de durcissement, grille de revue, plan de remédiation priorisé et scripts/commandes de vérification.

Objectifs

- Identifier les vecteurs d'attaque web et leurs impacts.
- Analyser une application et prioriser les risques.
- Mettre en œuvre des contrôles défensifs (validation, encodage, headers).
- Tester et vérifier les corrections avec des outils adaptés.
- Documenter un plan de remédiation et des preuves de sécurité.

Public visé

- Développeurs web et API
- Ingénieurs sécurité applicative / AppSec
- DevOps / SRE impliqués dans le durcissement
- Testeurs / pentesters orientés défense

Pré-requis

- Bases en HTTP, cookies, sessions, REST
- Notions de sécurité web (OWASP Top 10)
- Lecture de code (au moins un langage web)
- Confort avec ligne de commande

Pré-requis techniques

- Windows (WSL2), macOS ou Linux
- Navigateur récent et éditeur de code
- Burp Suite Community, curl, Docker (ou VM fournie)

Programme de notre formation Certification GIAC GWEB®

[Jour 1 - Matin]

Fondamentaux de la sécurité des applications Web et cartographie des risques

- Comprendre le modèle client/serveur : HTTP/HTTPS, cookies, sessions, en-têtes
- Identifier les surfaces d’attaque : endpoints, paramètres, fichiers, APIs, authentification
- Prioriser les risques avec OWASP Top 10 et scénarios d’exploitation réalistes
- Mettre en place une approche de défense : prévention, détection, réponse
- Atelier pratique : Cartographier une application cible (routes, paramètres, données sensibles) et établir une matrice de risques.

[Jour 1 - Après-midi]

Authentification, sessions et contrôles d’accès

- Durcir l’authentification : politiques mots de passe, MFA, verrouillage, anti-bruteforce
- Sécuriser les sessions : cookies Secure/HttpOnly/SameSite, rotation, expiration
- Éviter les failles de contrôle d’accès : IDOR, élévation de privilèges, séparation des rôles
- Bonnes pratiques d’implémentation : gestion des erreurs, messages, redirections
- Atelier pratique : Tester et corriger des scénarios d’IDOR et de fixation de session sur une application de démonstration.

[Jour 2 - Matin]

Validation des entrées et prévention des injections

- Mettre en place une validation robuste : listes blanches, normalisation, contraintes côté serveur
- Prévenir SQL Injection : requêtes paramétrées, ORM, moindre privilège base de données
- Prévenir les injections système : commandes, chemins, désérialisation, templates
- Gérer l'encodage/sortie : contexte HTML, attributs, URL, JavaScript
- Atelier pratique : Exploiter puis corriger une injection (SQL et commande) via paramétrage et validation.

[Jour 2 - Après-midi]

Protection contre XSS, CSRF et attaques côté navigateur

- Différencier XSS réfléchi, stocké, DOM et appliquer les contre-mesures adaptées
- Mettre en place une CSP pragmatique et gérer les exceptions (nonce, hash)
- Prévenir CSRF : tokens, SameSite, vérification d'origine, double-submit
- Durcir les en-têtes : HSTS, X-Content-Type-Options, Referrer-Policy, Permissions-Policy
- Atelier pratique : Ajouter une CSP et des protections CSRF, puis valider l'efficacité par tests d'attaque.

[Jour 3 - Matin]

Sécurité des APIs et gestion des secrets

- Sécuriser les APIs REST : authentification, autorisation, scopes, contrôle des objets
- Limiter l'exposition : pagination, filtrage, rate limiting, protections anti-énumération
- Valider les schémas : contrats, types, tailles, formats, gestion des erreurs
- Gérer les secrets : variables d'environnement, rotation, coffre-fort, suppression des secrets du code
- Atelier pratique : Auditer une API (contrôles d'accès, rate limit, validation) et corriger les points critiques.

[Jour 3 - Après-midi]

Durcissement, logs, tests et préparation à l'examen GWEB

- Configurer la sécurité applicative : TLS, gestion des erreurs, durcissement serveur et dépendances
- Mettre en place une journalisation exploitable : événements auth, accès, erreurs, corrélation, rétention
- Intégrer la sécurité au cycle de dev : revues, SAST/DAST, scans dépendances, critères de qualité
- Construire un plan de remédiation : priorisation, preuves de correction, non-régression
- Atelier pratique : Réaliser un mini-audit bout en bout (tests + correctifs) et produire une checklist de défense alignée GWEB.

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2026. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg