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

Mis à jour le 19/05/2026

S'inscrire

Formation Burp Suite Certified Practitioner

4 jours (28 heures)

Présentation

La formation Burp Suite Certified Practitioner vous prépare à utiliser Burp Suite de façon méthodique pour auditer des applications web et API. Vous gagnerez en efficacité sur les cas d'usage concrets : interception, manipulation de requêtes, automatisation, validation de vulnérabilités et rédaction de preuves.

La finalité est de vous rendre opérationnel pour conduire un test d'intrusion applicatif complet avec Burp Suite : cartographie, identification des points d'entrée, exploitation contrôlée et priorisation des risques. L'accent est mis sur les vulnérabilités fréquentes (authentification, sessions, injections, logique métier) et sur la reproductibilité des résultats.

L'approche est pratique : ateliers guidés, démos pas à pas, exercices chronométrés et corrections. Vous repartez avec des checklists d'audit, une configuration Burp optimisée, des scripts/recettes Repeater/Intruder, et un modèle de rapport incluant preuves, impact et recommandations.

Objectifs

- Configurer Burp Suite (proxy, CA, scope) et sécuriser l'environnement de test.
- Cartographier une application et identifier les surfaces d'attaque web/API.
- Exploiter Repeater, Intruder et Sequencer pour valider des hypothèses.
- Détecter et démontrer des vulnérabilités (auth, session, injections, accès).
- Produire des preuves reproductibles et formuler des recommandations actionnables.

Public visé

- Pentesters et consultants sécurité applicative
- Développeurs/DevSecOps souhaitant renforcer les tests de sécurité
- Analystes SOC/AppSec en charge de la validation des correctifs

Pré-requis

- Bases solides en HTTP/HTTPS, cookies, en-têtes et codes de statut
- Notions de sécurité web (OWASP Top 10) et d’authentification
- Lecture/édition de JSON et compréhension des API REST
- Connaissances Linux/Windows et usage d’un terminal

Pré-requis techniques

- PC avec 8 Go RAM minimum (16 Go recommandé) et 10 Go d’espace libre
- Windows, macOS ou Linux (navigateur Chromium/Firefox)
- Burp Suite (Community ou Professional selon contexte) et Java si requis
- Outils complémentaires : curl, un éditeur de code, Docker ou VM pour labs

Programme de notre formation Burp Suite Certified Practitioner

[Jour 1 - Matin]

Prise en main de Burp Suite et mise en place du proxy

- Comprendre le rôle de Burp dans un test d’intrusion Web (proxy, interception, modification)
- Configurer le navigateur et le certificat CA pour intercepter le trafic HTTPS
- Maîtriser les vues essentielles : Proxy, HTTP history, Target, Logger
- Définir le périmètre (scope) et filtrer efficacement le trafic utile
- Atelier pratique : Configurer Burp + navigateur et intercepter un parcours de connexion.

[Jour 1 - Après-midi]

Cartographier l’application : Target, crawling et analyse des requêtes

- Construire une cartographie : arborescence, endpoints, paramètres, méthodes HTTP
- Identifier les zones sensibles : authentification, administration, API, upload, recherche
- Analyser les sessions (cookies, tokens) et les en-têtes de sécurité
- Reproduire et comparer des requêtes (Repeater) pour valider des hypothèses
- Atelier pratique : Cartographier une application cible et isoler 10 endpoints prioritaires.

[Jour 2 - Matin]

Tester l’authentification et la gestion de session avec Burp

- Contrôler la robustesse des mécanismes de login (messages d’erreur, verrouillage, MFA)
- Vérifier la sécurité des cookies (Secure, HttpOnly, SameSite) et la rotation de session

- Détecter les faiblesses courantes : fixation, réutilisation, expiration, logout incomplet
- Manipuler les jetons (JWT, tokens opaques) et valider les impacts côté serveur
- Atelier pratique : Rejouer un flux d'authentification et démontrer un problème de session.

[Jour 2 - Après-midi]

Automatiser les attaques : Intruder, payloads et règles de détection

- Configurer Intruder : positions, types d'attaque, gestion des encodages
- Construire des payloads efficaces (listes, règles, transformations, grep/extract)
- Détecter rapidement des anomalies : codes, tailles, temps de réponse, redirections
- Optimiser les tests (throttling, exclusions, gestion des erreurs, anti-bruit)
- Atelier pratique : Mener un fuzzing ciblé sur paramètres et identifier un comportement anormal.

[Jour 3 - Matin]

Exploiter les vulnérabilités Web avec Repeater et les outils Burp

- Tester les injections (SQLi, NoSQLi, command injection) par variations contrôlées
- Valider les failles XSS (reflected/stored) et les contraintes de contexte/encodage
- Analyser les contrôles d'accès (IDOR, BOLA) via changements d'identifiants et rôles
- Identifier les failles de logique (workflow, contournements, validations côté client)
- Atelier pratique : Exploiter une IDOR et démontrer un accès non autorisé à une ressource.

[Jour 3 - Après-midi]

Scanner Burp et validation manuelle : prioriser, confirmer, réduire les faux positifs

- Lancer des scans ciblés selon le scope et interpréter les résultats (sévérité, confiance)
- Confirmer manuellement une alerte : preuve, impact, conditions de reproductibilité
- Exploiter les issues types : SSRF, path traversal, open redirect, CORS, headers
- Documenter les requêtes/réponses de preuve et préparer des recommandations correctives
- Atelier pratique : Scanner une zone définie et produire 3 preuves validées (PoC) avec Repeater.

[Jour 4 - Matin]

Extensions, macros et workflows avancés pour gagner en efficacité

- Installer et utiliser des extensions (BApp Store) adaptées aux besoins (auth, JWT, logging)

- Configurer des macros et règles de session handling pour automatiser l’authentification
- Chaîner des tests : extraction de token, réinjection, maintien de session sur Intruder/Repeater
- Améliorer l’analyse : Comparer, Decoder, Sequencer, recherche et annotations
- Atelier pratique : Mettre en place une macro de login et l’utiliser dans un test Intruder.

[Jour 4 - Après-midi]

Préparation à la certification : méthodologie, reporting et examen blanc

- Structurer une approche “exam-ready” : reconnaissance, priorisation, exploitation, preuves
- Gérer le temps et le scope : checklists, notes, reproduction fiable des vulnérabilités
- Rédiger des constats exploitables : description, étapes, impact, correctifs, références techniques
- Consolider les acquis : erreurs fréquentes, pièges, bonnes pratiques Burp
- Atelier pratique : Examen blanc guidé + mini-rapport (preuves, impacts, remédiations).

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