DAWAN

Plan de la formation

www.dawan.fr

Formation Tests d’intrusion d’applications Web et API : Niveau expert

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 975,00 € HT (standard) 3 180,00 € HT (remisé)
Public :	Consultants en sécurité, pentesters Ingénieurs / techniciens sécurité - Administrateurs systèmes / réseaux impliqués dans la sécurité Web - Développeurs souhaitant comprendre la logique offensive pour mieux sécuriser leurs applications
Pré-requis :	Bonne connaissance du modèle HTTP, des architectures Web et des concepts d’API - Connaissances de base en tests d’intrusion (ou suivi de « Hacking et sécurité – Les fondamentaux » / « Niveau avancé ») - À l’aise avec les environnements Linux et les outils d’analyse Web (proxy, logs, etc.)
Objectifs :	Comprendre en profondeur les spécificités de la sécurité des applications Web et des API - Identifier les faiblesses logiques et techniques des applis Web modernes et des API (authentification, autorisation, session, données) - Disposer des compétences nécessaires pour conduire des tests d’intrusion avancés en environnement contrôlé et interpréter les résultats - Être en mesure de proposer des contre-mesures concrètes et de dialoguer efficacement avec les équipes de développement
Modalités pédagogiques, techniques et d’encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l’Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat. • Un formateur expert.

Modalités d’évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102748-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre le paysage des menaces sur les applications Web et les API

Identifier les spécificités des attaques ciblant les applications Web et les API par rapport aux attaques infrastructurelles
Revoir les grands principes du protocole HTTP, des sessions, des cookies, des jetons et des APIs REST / GraphQL
Comprendre les catégories de vulnérabilités les plus courantes (injection, authentification, autorisation, gestion des sessions, exfiltration de données)
Relier chaque type de vulnérabilité à des risques métiers concrets (fuite de données, fraude, prise de contrôle de comptes, atteinte à l’image)
Atelier fil rouge : cartographier une application Web ou une API type (zones fonctionnelles, chemins critiques, données sensibles)

Mettre en place une méthodologie de test d’intrusion Web et API

Structurer les étapes d’un test : reconnaissance fonctionnelle, cartographie, identification des surfaces d’attaque, priorisation des tests
Utiliser des proxies d’analyse de trafic pour observer, manipuler et rejouer les

requêtes dans un contexte de laboratoire
Différencier tests automatisés (scans) et tests manuels ciblés sur la logique métier
Organiser la collecte des éléments observés pour faciliter l'analyse et le reporting
Atelier fil rouge : définir une checklist de test adaptée à une application Web donnée, en fonction de ses fonctionnalités et de ses données

Analyser les faiblesses d'authentification, de gestion de session et d'autorisation

Comprendre les mécanismes d'authentification modernes : formulaires, SSO, OAuth / OpenID Connect, jetons, MFA
Identifier les faiblesses typiques : contournement de login, récupération inappropriée de mot de passe, verrouillage insuffisant, gestion défaillante des sessions
Étudier les problèmes d'autorisation : contrôle d'accès horizontal et vertical, exposition de données d'autres utilisateurs, API mal filtrées
Proposer des stratégies de renforcement en lien avec les équipes de développement et d'archi
Atelier fil rouge : à partir de cas de tests en labo, identifier les symptômes de faiblesses d'authentification / autorisation et proposer des mesures de remédiation

Approfondir l'analyse des données et des entrées utilisateur

Revoir les risques liés aux entrées utilisateurs non maîtrisées : injections, exfiltration, exposition de données sensibles
Comprendre les problématiques d'injections dans différents contextes (SQL, commandes, gabarits, etc.) dans un cadre pédagogique
Identifier les défauts de validation côté client vs côté serveur et leurs conséquences
Relier ces vulnérabilités aux bonnes pratiques de développement sécurisé (validation d'entrées, requêtes paramétrées, gestion des erreurs, logs)
Atelier fil rouge : analyser des scénarios de vulnérabilités d'injection dans un environnement de test et rédiger des recommandations orientées développeurs

Tester les API : logique métier, exposition des données et erreurs de conception

Comprendre les spécificités de la sécurité des API : endpoints, ressources, verbes HTTP, payloads, versioning
Identifier les risques liés aux API : sur-exposition fonctionnelle, absence de filtrage, documentation publique, erreurs de design

Analyser les réponses API : codes, messages d’erreur, métadonnées, structure des données, fuites d’information involontaires
Évaluer la robustesse des mécanismes d’autorisation côté API (jetons, scopes, claims, filtrage côté serveur)
Atelier fil rouge : travailler sur une API de démonstration, identifier les points de fragilité et proposer des correctifs organisationnels et techniques

Observer les traces et exploiter les journaux pour renforcer la défense

Comprendre comment les tentatives d’attaque se traduisent dans les journaux applicatifs et d’accès Web
Identifier les indicateurs de comportement suspect : séquences de requêtes, patterns d’erreurs, volumes anormaux
Articuler les journaux applicatifs avec la supervision (SIEM, alertes) et la détection des attaques Web
Utiliser ces analyses pour ajuster les règles de sécurité applicatives (WAF, filtrage logique, limitations de débit, surveillance ciblée)
Atelier fil rouge : à partir de journaux simplifiés, reconstituer un scénario d’attaque sur une application Web et en tirer des actions de durcissement

Concevoir des contre-mesures et dialoguer avec les équipes de développement

Relier les vulnérabilités constatées aux principes de sécurité applicative (OWASP, bonnes pratiques de dev sécurisé)
Prioriser les recommandations selon l’impact, la facilité de mise en œuvre et le contexte métier
Adapter le niveau de détail des préconisations aux publics visés : développeurs, architectes, managers
Intégrer progressivement les tests d’intrusion dans le cycle de vie applicatif (CI/CD, revues de code, tests réguliers)
Atelier fil rouge : rédiger un extrait de rapport orienté « développeurs » et un extrait orienté « direction / MOA » pour une même vulnérabilité

Construire une démarche continue de test et d’amélioration

Définir les périmètres applicatifs à tester régulièrement (applis critiques, API exposées, nouvelles fonctionnalités)
Articuler tests ponctuels, revues de code, scans réguliers et exercices de défense (blue team)
Intégrer les retours des tests dans les référentiels internes (guides de développement, standards d’architecture)

Planifier sa propre montée en compétences (hacking Web avancé, API, mobile, bug bounty, etc.)

Atelier fil rouge final : élaborer une feuille de route annuelle de tests Web / API et d’amélioration continue pour une organisation type