DAWAN

Plan de la formation

www.dawan.fr

# Formation Tests d’intrusion d’applications Web et API : Initiation

| | |
|---|---|
| **Durée :** | 3 jours (21 heures) |
| **Tarifs inter-entreprise :** | 2 775,00 € HT (standard)<br>2 220,00 € HT (remisé) |
| **Public :** | Pentesters et auditeurs sécurité Développeurs et architectes souhaitant renforcer la sécurité Web/API Ingénieurs sécurité, RSSI et consultants techniques impliqués dans des audits applicatifs |
| **Pré-requis :** | Bonnes bases en HTTP/HTTPS, API REST et JSON - Connaissances en sécurité Web (OWASP Top 10) et notions de pentest - Aisance avec un environnement Linux et l’utilisation d’outils en ligne de commande |
| **Objectifs :** | Mettre en œuvre une méthodologie de test d’intrusion Web et API<br> - Tester l’authentification, la session et les contrôles d’accès principaux - Identifier les vulnérabilités majeures et leurs impacts - Formuler des recommandations correctives et exploitables |
| **Modalités pédagogiques, techniques et d’encadrement :** | • Formation synchrone en présentiel et distanciel.<br>• Méthodologie basée sur l’Active Learning : 75 % de pratique minimum.<br>• Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat.<br>• Un formateur expert. |

| | |
|---|---|
| **Modalités d’évaluation :** | • Définition des besoins et attentes des apprenants en amont de la formation.<br>• Auto-positionnement à l'entrée et la sortie de la formation.<br>• Suivi continu par les formateurs durant les ateliers pratiques.<br>• 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 :** | CYB102865-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 |

## Jour 1 – Comprendre et cadrer un test d’intrusion Web et API

Analyser les architectures Web modernes et les flux applicatifs
Revoir HTTP/HTTPS, cookies, sessions, en-têtes, CORS et CSRF
Comprendre les principes des API REST, endpoints, verbes HTTP et codes de retour
Appliquer une méthodologie de test d’intrusion applicatif
Réaliser la reconnaissance, la cartographie et la définition du périmètre
Mettre en place l’environnement de test et les outils d’analyse

**Atelier fil rouge : cartographier une application Web et une API, établir une checklist initiale et prioriser les tests**

## Jour 2 – Tester l’authentification et la gestion de session

Identifier et analyser les mécanismes d’authentification
Tester la robustesse des mots de passe, des erreurs et des protections anti-brute force
Évaluer la gestion de session, cookies, tokens, expiration et renouvellement
Analyser les mécanismes de réinitialisation de mot de passe

Comprendre et tester les JWT, leur structure, validation et signature
Introduire OAuth2 et OpenID Connect dans le cadre d’un audit applicatif

**Atelier fil rouge : tester l’authentification et la session, identifier les failles et proposer des mesures correctives**

## Jour 3 – Tester les autorisations et les contrôles d’accès

Distinguer authentification et autorisation dans une application
Tester les contrôles d’accès horizontaux et verticaux
Identifier les vulnérabilités de type IDOR et fuites de données
Analyser la séparation des rôles et les contournements possibles
Comparer contrôles côté client et contrôles côté serveur
Évaluer les impacts métiers et prioriser les risques

**Atelier fil rouge : mettre en œuvre des scénarios de contournement de droits et formuler des recommandations**