

## Formation Tests d'intrusion d'applications Web et API : Approfondissement

<b>Durée :</b>	2 jours (14 heures)
<b>Tarifs inter-entreprise :</b>	1 575,00 CHF HT (standard) 1 260,00 CHF HT (remisé)
<b>Public :</b>	Participants ayant suivi le socle 3 jours ou disposant d'une pratique du pentest Web et API - Pentesters et auditeurs souhaitant approfondir les tests avancés - Développeurs sécurité et architectes impliqués dans la remédiation
<b>Pré-requis :</b>	Avoir suivi la formation socle 3 jours ou posséder un niveau équivalent - Maîtriser les notions d'authentification, autorisation et vulnérabilités majeures Web - Savoir analyser et manipuler des requêtes Web et API
<b>Objectifs :</b>	Approfondir l'exploitation des vulnérabilités Web et API - Tester des scénarios avancés et des mécanismes complexes - Renforcer la restitution et la priorisation des risques - Intégrer les tests dans une démarche sécurité continue
<b>Modalités pédagogiques, techniques et d'encadrement :</b>	<ul style="list-style-type: none"><li>Formation synchrone en présentiel et distanciel.</li><li>Méthodologie basée sur l'Active Learning : 75 % de pratique minimum.</li><li>Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat.</li><li>Un formateur expert.</li></ul>
<b>Modalités d'évaluation :</b>	<ul style="list-style-type: none"><li>Définition des besoins et attentes des apprenants en amont de la formation.</li><li>Auto-positionnement à l'entrée et la sortie de la formation.</li><li>Suivi continu par les formateurs durant les ateliers pratiques.</li><li>Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.</li></ul>

<b>■ Sanction :</b>	Attestation de fin de formation mentionnant le résultat des acquis
<b>■ Référence :</b>	CYB102866-F
<b>■ Note de satisfaction des participants:</b>	Pas de données disponibles
<b>■ Contacts :</b>	commercial@dawan.fr - 09 72 37 73 73
<b>■ Modalités d'accès :</b>	Possibilité de faire un devis en ligne ( <a href="http://www.dawan.fr">www.dawan.fr</a> , <a href="http://moncompteformation.gouv.fr">moncompteformation.gouv.fr</a> , <a href="http://maformation.fr">maformation.fr</a> , etc.) ou en appelant au standard.
<b>■ Délais d'accès :</b>	Variable selon le type de financement.
<b>■ Accessibilité :</b>	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à <a href="mailto:referenthandicap@dawan.fr">referenthandicap@dawan.fr</a> , nous étudierons ensemble vos besoins

## Jour 1 - Exploiter les vulnérabilités Web avancées

Analyser en profondeur les points d'entrée utilisateur  
 Exploiter des injections avancées et chaînes d'attaque  
 Tester des scénarios XSS complexes et leurs impacts  
 Identifier et exploiter les vulnérabilités SSRF et orientées flux  
 Construire des preuves reproductibles et exploitables

## Atelier fil rouge : exploiter des scénarios avancés et documenter les preuves

### Jour 2 - Tester la sécurité des API et industrialiser les tests

Tester des API complexes et l'exposition fonctionnelle  
 Analyser et tester OAuth2, OpenID Connect, scopes et claims  
 Tester les mécanismes anti-abus et le rate limiting  
 Analyser les logs, la détection et l'alerting  
 Intégrer les tests dans le cycle de vie applicatif  
 Structurer une restitution avancée et un plan de remédiation

## Atelier fil rouge final : définir un plan de tests API avancé et une feuille de route sécurité