

## Programme de formation Sécurité des applications Web

### • Objectifs pédagogiques

La sécurité des applications web est devenue un véritable enjeu. Administrations, structures publiques ou entreprises privées sont aujourd'hui des cibles potentielles d'attaques. Suite à cette formation, vous serez capable de comprendre et d'anticiper les risques pour pouvoir mettre en place des procédures de sécurité efficaces. Vous maîtriserez aussi la modélisation des menaces et les outils de contrôle permettant de repérer les failles de vos applications web.

### • Prérequis

Connaissances de base en système, réseau et Web

### • Durée

3 jours

### • Public

Développeurs, chefs de projet

### • Programme de formation

#### Introduction

Définition du concept de sécurité des applications web  
Présentation du contexte et des chiffres clés  
Base de la sécurité web : le triangle CIA, l'authentification...

#### Principaux risques d'attaques selon l'OWASP

Présentation de l'OWASP  
Injection : définition, scénarios d'attaques, prévention  
Violation de sessions: cookie, poisoning, session hijacking...  
Cross-site Scripting (XSS) : Un type d'attaque en pleine expansion  
Références directes non sécurisées à un objet  
Défaut de configuration de sécurité : bonnes pratiques  
Exposition de données sensibles : cryptographie  
Violation d'accès au niveau fonctionnel  
Falsification de requête inter-sites (CSRF)

Présence de composants ayant des vulnérabilités connues  
Redirections et renvois non validés

#### Bonnes pratiques de sécurité

Sécuriser les interactions entre bases de données et applications  
Se protéger contre le détournement de session  
Contrôler les fuites d'informations  
Sécuriser la validation des saisies

#### Comment sécuriser une API REST ?

Repérer et gérer les vulnérabilités  
Protocoles et meilleures pratiques

#### Repérer les faiblesses grâce aux Scans d'application

Savoir configurer et utiliser les scanners  
Maîtriser les tests d'intrusion de l'OWASP et de tiers

#### Conclusion



Bonnes pratiques

Connaitre et adopter les normes de protection

Gérer les données à risque (personnelles,  
financières...)

Savoir modéliser les menaces pour diminuer  
les risques