

# Sécurité Web

## Les fondamentaux et l'OWASP

### Programme de la formation

#### Introduction

#### 1. Concepts de base

- Vulnérabilité | Menace | Risque | DICP
- CVE | Exploit | 0-day

#### 2. Rappels techniques

- Mécanismes d'encodage
- HTTP | HTTPS | URL
- HTML | CSS
- JavaScript | API Fetch | JSON
- Applications dynamiques | Cookies

#### 3. OWASP

- Qu'est-ce que l'OWASP ?
- Projets principaux
- OWASP Top10 2021

#### 4. Techniques d'attaque et de défense

- Techniques d'attaque
- Authentification | Les sessions
- Contrôle des accès
- Validation des entrées
- Contrôle des informations | Contrôle des attaques

#### 5. Cycle de développement sécurisé

- Méthodologies
- SAMM
- Intégration dans un projet

#### 6. L'aspect juridique

- Loi Godfrain | LCEN | RGPD

#### Synthèse

### Objectifs de formation

- Comprendre les risques pesant sur les applications web
- Découvrir les contributions et les apports de l'OWASP
- Mettre en œuvre les moyens de protection de son code et de ses développements

### Public

- RSSI | DSI
- Développeurs, Chefs de projet informatique

### Pré-requis

- Disposer des connaissances fondamentales dans le développement applicatif

### Méthodes pédagogiques

- Apports théoriques et pratiques
- Démonstrations

### Livrables

- Support de cours en numérique

### Langue

- Français

### Suivi et Sanction

- Attestation de formation



Code  
DEV-F2



Durée  
1 jour



Prix sur  
demande



3 à 10  
stagiaires



▪ Intra



▪ Présentiel  
▪ À distance