# Formation : Campus Atlas - Sécurité des applications

*Cours pratique - 3j - 21h00 - Réf. LAN*
*Prix : 1940 CHF H.T.*

NEW

À l'issue de la formation, le participant sera capable de développer des applications web et mobiles sécurisées. Tous les points fondamentaux de la sécurité des applications seront abordés, des modèles de maturité aux bonnes pratiques en Java incluant un tour d'horizon des vulnérabilités courantes et spécifiques pour mieux les gérer.

## Objectifs pédagogiques

**À l'issue de la formation, le participant sera en mesure de :**

- Comprendre les problématiques de la sécurité des applications
- Identifier les principales menaces et vulnérabilités affectant les applications web et mobiles
- Appliquer les bonnes pratiques de sécurité dans le développement d'applications
- Utiliser des outils et techniques pour détecter et corriger les failles de sécurité
- Découvrir les principes de base de la cybersécurité et leur impact sur la sécurité des applications

## Public concerné

Architectes, développeurs, analystes, chefs de projet…

## Prérequis

Posséder une bonne connaissance de la programmation objet et de la programmation d'applications web.

## Méthodes et moyens pédagogiques

**Travaux pratiques**

Exercices pratiques et/ou études de cas.

**Méthodes pédagogiques**

60% pratique – 40% théorie. Pour optimiser le parcours d'apprentissage, des modules e-learning peuvent être fournis avant et après la session présentielle ou la classe virtuelle, sur simple demande du participant.

**PARTICIPANTS**

Architectes, développeurs, analystes, chefs de projet…

**PRÉREQUIS**

Posséder une bonne connaissance de la programmation objet et de la programmation d'applications web.

**COMPÉTENCES DU FORMATEUR**

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

**MODALITÉS D'ÉVALUATION**

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

## Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

## Programme de la formation

### 1 Top OWASP – Les vulnérabilités d'une application web

**partie 1 – OPTION digital learning préformation**

- Introduction.
- Manque de contrôle d'accès.
- Mauvaise configuration de sécurité.
- Cross-site scripting (XSS).
- Désérialisation non sécurisée.
- Utilisation de composants avec des vulnérabilités connues.
- Manque de log et de monitoring.

#### Activités digitales

Dans cette formation en ligne, vous découvrirez les 6 dernières vulnérabilités du top 10 OWASP, les principes de sécurité à connaître pour les prévenir, les techniques utilisées par les hackers pour les exploiter, ainsi que les bonnes pratiques et contre-mesures à mettre en place pour protéger des applications web.

### 2 Sécurité informatique, concepts essentiels et techniques de protection

**pour l'utilisateur - OPTION digital learning préformation**

- Concepts de sécurité.
- Logiciels malveillants.
- Sécurité réseau.
- Utilisation sécurisée du web.
- Utilisation sécurisée de la messagerie.
- Gestion de la sécurité des données.

#### Activités digitales

Dans cette formation en ligne, vous découvrirez les principaux risques liés à la sécurité informatique, leurs causes et leurs conséquences, ainsi que les bonnes pratiques pour les prévenir. Après une introduction aux concepts fondamentaux, vous explorerez les menaces associées aux logiciels malveillants, aux réseaux, à la navigation Internet, aux messageries et à la protection des données stockées, afin d'utiliser votre ordinateur en toute confiance.

### 3 Introduction à la sécurité des applications

- Définitions clés : vulnérabilité, menace, risque, attaque.
- Acteurs de la sécurité : CERT, OWASP, BSIMM.
- Risques liés au développement d'une application.
- Traces laissées par les développeurs : mémoire, journaux…

#### Démonstration

Analyse d'une application vulnérable pour identifier les traces laissées par les développeurs.

**MOYENS PÉDAGOGIQUES ET TECHNIQUES**

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

**MODALITÉS ET DÉLAIS D'ACCÈS**

L'inscription doit être finalisée 24 heures avant le début de la formation.

**ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES**

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

## 4 Modèles de maturité en sécurité

- Présentation du modèle OpenSAMM.
- Les 4 niveaux de maturité.
- Introduction au BSIMM (Building Security In Maturity Model).

**Travaux pratiques**
Calcul du niveau de maturité d'une organisation à l'aide d'OpenSAMM.

## 5 Vulnérabilités courantes des applications web

- Le guide pratique Application Security Verification Standard (ASVS).
- Un écosystème d'outils open source.
- OWASP Top 10 : Broken Access Control, Cryptographic Failures, Injection (ex. SQL Injection)...

**Travaux pratiques**
Exploitation simple d'une faille SQL Injection ou XSS sur une mini appli Java. Comment aurait-on pu l'éviter ?

## 6 Vulnérabilités spécifiques aux applications mobiles

- Stockage non sécurisé.
- Authentification faible.
- Exposition des API.

**Travaux pratiques**
Analyse d'une application mobile pour identifier des vulnérabilités spécifiques.

## 7 Sécurité dès la conception

- Principes du Security by Design.
- Intégration de la sécurité dans le cycle de développement (DevSecOps).

**Démonstration**
Étude d'un cas de conception sécurisée d'une application.

## 8 Bonnes pratiques en Java

- Validation des entrées utilisateurs.
- Gestion des erreurs et des exceptions.
- Sécurisation des API REST avec Spring Security ou Jakarta Security.

**Travaux pratiques**
Mise en œuvre de Spring Security ou Jakarta Security pour sécuriser une API REST.

## 9 Sécurité des configurations et des dépendances

- Gestion des configurations sensibles.
- Mise à jour des dépendances et gestion des vulnérabilités connues.

**Démonstration**
Utilisation de Dependency-Check pour identifier des vulnérabilités dans les dépendances d'un projet Java.

### 10 Sécurisation des applications mobiles

- Bonnes pratiques pour le développement mobile sécurisé.
- Outils et techniques spécifiques aux plateformes mobiles.

**Travaux pratiques**
Application des bonnes pratiques de sécurité sur une application mobile existante.

### 11 Introduction aux tests de sécurité

- Objectifs des tests de sécurité : détection proactive.
- Revue de code statique (SAST).
- Tests dynamiques (DAST).
- Tests interactifs (IAST).

**Démonstration**
Analyse outillée d'une application pour identifier des vulnérabilités.

### 12 Gestion des vulnérabilités

- Processus de gestion des vulnérabilités.
- Mise en place de correctifs et suivi.

**Travaux pratiques**
Élaboration d'un plan de gestion des vulnérabilités pour une application existante.

### 13 Atelier final – Mise en pratique

- Application des connaissances acquises sur un projet complet.
- Identification et correction des vulnérabilités.
- Présentation des solutions mises en œuvre.

**Travaux pratiques**
Projet de sécurisation d'une application web ou mobile, de l'identification des failles à leur correction.

### 14 Top 10 OWASP—Les vulnérabilités d'une application web partie 2—

**OPTION digital learning post-formation**

- Introduction.
- Les injections.
- La violation de gestion d'authentification et de session.
- L'exposition des données sensibles.
- L'attaque XXE (XML Entité Externe).

**Activités digitales**
Dans cette formation en ligne, vous découvrirez les 4 premières vulnérabilités du Top 10 OWASP, dont les injections (SQL, XPath, code), les failles d'authentification et de gestion de session, l'exposition de données sensibles et les attaques XXE. Vous apprendrez comment les hackers les exploitent et quelles bonnes pratiques appliquer pour sécuriser vos applications web.

## Dates et lieux

**CLASSE À DISTANCE**
2026 : 24 mars, 16 juin, 22 sep., 24 nov.