Protection et sécurisation des applications Web Java

Programme *(Mis à jour le 31/01/2026)*

Concepts de sécurité logicielle (1h)

- Concepts fondamentaux de la sécurité logicielle
- Définitions clés (menace, vulnérabilité, attaque, risque)
- Pourquoi sécuriser vos applications?
- Les mythes sur la sécurité applicative
- Panorama des responsabilités développeur / architecte

Rappels sur les fondements du Web et des échanges (1h)

- Fonctionnement de HTTP / HTTPS
- Notions de session, cookies, headers
- Surface d'attaque d'une application Web moderne
- Travaux pratiques : analyse de requêtes et de réponses HTTP.

Analyse de quelques types d'attaques (2h)

- Attaques « brute-force »
- Attaques par « déni de services » (DOS : Denial Of Service)
- Attaques par analyse de trames IP
- Attaques par « Injection SQL »
- Attaques « XSS » (Cross Site Scripting)
- Attaques « CSRF » (Cross Site Request Forgery)
- Autres types d'attaques (IDOR, manipulation de paramètres, etc.)
- Outils de détection de faille de sécurité
- Travaux pratiques : tests de ces différents types de problèmes sur une application mal développée.

Outils et initiation à l'audit de sécurité Web (1h)

- Principes de base d'un audit de sécurité applicatif
- Présentation d'outils de détection de vulnérabilités
- Travaux pratiques : scan de sécurité d'une application Web
- Lecture et interprétation des résultats
- Limites des outils automatisés
- Travaux pratiques : analyse collective des vulnérabilités détectées

Validation des données entrantes (1h)

- Protection contre les entrées d'utilisateurs nuisibles
- Utilisation d'expressions régulières
- Se prémunir des attaques par « injections SQL »
- Se prémunir des attaques « XSS »
- Se prémunir des attaques « CSRF »
- Détecter et contrer les attaques « brute-force »
- Sécuriser les données en Cookie
- Protection contre les menaces de déni de service
- Ne pas présenter à l'utilisateur les détails des erreurs techniques
- Travaux pratiques : modifications successives du code de l'application initialement proposée pour interdire ces différents types d'attaques

Sécurité des API Web (SOAP / REST) (1h)

Référence

THIS3652

Durée

2 jours / 14 heures

Prix HT / stagiaire

1400€

Objectifs pédagogiques

- Connaître les méthodes courantes utilisées pour compromettre une cible.
- Maîtriser les techniques d'attaque spécifiques aux applications Web.
- Être sensibilisé aux principes et bonnes pratiques pour auditer sa propre application.

Niveau requis

- Maîtriser les technologies web (HTML/JavaScript) et le langage de programmation Java

Public concerné

- Développeurs
- Architectes

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d'émargement (signature électronique privilégiée)
Evaluations formatives et des acquis sous forme de questions orales et/ou écrites (QCM) et/ou mises en situation
Questionnaires de satisfaction (enquête électronique privilégiée)

- Vulnérabilités spécifiques aux API
- Sécurisation des échanges JSON / REST
- Nettoyage et validation des requêtes
- Gestion des erreurs côté API
- Travaux pratiques : nettoyage et sécurisation d’une requête REST/JSON

Les mécanismes de sécurité proposés par la Java (2h)

- Présentation des mécanismes de sécurité Java
- Authentification et autorisation Java / Java EE
- Principes de chiffrement des données
- Protéger vos fichiers JAR (Obfuscation et signature)
- Travaux pratiques : utiliser les mécanismes de sécuriser proposés par Java

Sécuriser les données stockées en base (2h)

- Authentification et Autorisation du SGBDr (Système de Gestion de Base de Données relationnelle)
- Rôles serveur et rôles de base de données
- Propriété et séparation utilisateur-schéma
- Chiffrement de données dans la base de données
- Travaux pratiques : stocker de manière sécurisée les mots de passe en base de données
- Sécurisation par les procédures stockées
- Utilisation de JPA pour l’accès aux données
- Cas des attaques par injection JPQL
- Travaux pratiques : correction d’un code JPA permettant une attaque

Sécuriser le système de fichiers (1h)

- Chiffrer les données sensibles dans les fichiers de configuration
- Détecter les tentatives de remplacement des fichiers sources de l’application
- Signer les fichiers
- Protéger les informations des fichiers de log
- Travaux pratiques : chiffrer des fichiers.

Sécuriser les échanges de données (1h)

- Modèle de chiffrement
- Conception orientée flux
- Configuration du chiffrement
- Choix d’un algorithme
- Mettre en œuvre le chiffrage symétrique
- Mettre en œuvre le chiffrage asymétrique
- Travaux pratiques : réaliser une communication sécurisée à l’aide d’un certificat

OAUTH 2.0 et l’authentification au niveau d’un navigateur (1h)

- Présentation de l’architecture OAuth 2.0
- Utilisation de l’API OAuth 2.0
- Travaux pratiques : mise en œuvre de OAuth