Sécurité des applications web développées en .NET, Java & C++

Date et durée

Code formation : SEC-APP
Durée : 4 jours
Nombre d'heures : 28 heures

Description

Si les applications web ont réussi à s'imposer sur le marché du numérique, c'est grâce à leur grande flexibilité, leur ergonomie et leur accessibilité. Cependant, les problèmes de sécurité demeurent nombreux aujourd'hui puisque **les apps sont les cibles de multiples cyberattaques**. Que vous soyez développeur, intégrateur ou responsable de la sécurité des systèmes d'information (RSSI), vous devez donc vous interroger sur la façon dont les applications web de votre entreprise sont sécurisées.
En suivant cette formation, vous disposerez de tous **les éléments clés nécessaires pour sécuriser au maximum les applis** de vos systèmes d'information. Pendant 4 jours, vous aborderez dans les détails toutes les composantes et techniques de sécurisation. Que ce soit pour des applications développées en .NET, Java ou C++, vous découvrirez **les différents types d'attaques dont vous pouvez faire l'objet** et quelles sont les meilleures pratiques à adopter.
En plus des cours théoriques indispensables, cette **formation sur la sécurité des applications** inclut de nombreux travaux pratiques à travers 8 modules. Ils vous seront très bénéfiques pour mettre en pratique les techniques acquises lorsque vous réintégrez votre entreprise.

Objectifs

La **formation sécurité des applications web** vous permettra d'atteindre les objectifs suivants :

- connaître les principes de sécurisation pour des applications développées en Java, .Net et C++ ;
- maintenir des applications web sous une forte charge et valider leurs qualités ;
- savoir analyser proprement du code afin de détecter les éventuelles failles de sécurité ;
- savoir appliquer les bonnes pratiques de développement d'applications web ;

Points forts

Un mixte de cours théoriques et de travaux pratiques ; une auto-évaluation de vos connaissances et de vos compétences en développement d’application web; des temps d'échanges et un accompagnement pédagogique individualisé.

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation sécurité des applications web** nécessite le prérequis suivant :

- maitriser les fondamentaux de la programmation orientée objet en langage Java, .Net ou C++.

Public

Cette formation s'adresse aux publics suivants :

- tous les développeurs, concepteurs d'applications ou acteurs impliqués dans les activités de production, de gestion ou d'intégration qui désirent apprendre à mieux sécuriser leurs applications web.

Cette formation s'adresse aux profils suivants

Développeur
Architecte logiciel / Applicatif
Chef de projet / Responsable de projet
Directeur des Systèmes d'Information (DSI)

Programme

Module 1 : comprendre les principes de sécurisation d'une application

- Les 6 éléments composant la sécurité d'une application (authentification, contrôle d'accès, intégrité et confidentialité des données , non-répudiation et protection contre les analyses de trafic).
- L'utilisation des outils de sécurité d'application sous .NET.
- La mise en place de la sécurité du runtime.
- La mise en place d'un système d'authentification.
- La mise en place du contrôle d'accès et de la protection des données.
- Les différentes formes et types de menaces.
- La mise en place de contrôles lors de la saisie des données.

Module 2 : effectuer une revue de code JAVA et le sécuriser

- L'analyse de la qualité et de la sécurité du code avec SonarQube et AST (Abstract Syntax Tree).
- L'installation et l'utilisation de SonarQube sous Eclipse.
- La sécurisation de Java 2 Enterprise Edition avec le fichier web.xml (authentication realm, CAS et SSO).
- L'utilisation du framework Spring Security pour l'authentification (mise en place d'une sécurité par les ressources et par appel de méthode).

Module 3 : effectuer une revue de code C++ et le sécuriser

- La protection du code d'assemblage via une signature et un contrôle des données.
- Les modèles de protection C++.
- Le paramétrage du Common Language Runtime (CLR).
- La mise en place d'une stratégie de sécurité d'accès du code d'intégration du CLR.
- Les bonnes pratiques de déploiement et d'exécution d'applications codées en C++.

Travaux pratiques :

- charger et sécuriser un Code Access Security (CAS) ;
- charger et décharger le code d'un domaine .app.

Module 4 : sécuriser une application .NET avec un chiffrement

- Les principes de la cryptographie (présentation de la méthode symétrique et asymétrique ainsi que le fonctionnement du moteur de chiffrement).
- L'utilisation du chiffrement pour les certificats et la signature d'une application .NET.
- La mise en place des protocoles SSL et HTTPS pour sécuriser les échanges.

Travaux pratiques :

- chiffrer et déchiffrer des données.

Module 5 : mettre en place l'authentification et gérer les accès

- Les systèmes d'authentification fournis par .NET. Les principes d'authentification basés sur les rôles.
- La mise en place de politiques .Net (codes de groupe).
- La mise en place d'un modèle de protection des données.
- Les limitations d'exécution des applications.
- La mise en place d'un stockage de données protégé.

Travaux pratiques :

- créer et modifier un objet d'identité et un objet principal dans .NET ;
- ajouter et supprimer des entrées de liste de contrôle d'accès (ACL et DACL) ;
- créer des politiques de sécurité avec l'outil de configuration mscorcfg.msc.

Module 6 : corriger les failles de sécurité avec ASP.NET

- Les 10 failles majeures identifiées par l'Open Web Application Security Project (OWASP).
- Les attaques par injection SQL.
- Les failles de type Cross-site scripting (XSS).
- Les attaques par détournement de session (Hijacking).
- Les vulnérabilités Insecure Direct Object References (IDOR).
- Les vulnérabilités cross-site request forgery, (CSRF).

Module 7 : sécuriser une application avec du C++

- Le modèle de mémoire C++17.
- La compilation du programme.
- Le cadre de pile de l'appel de fonction.
- Les bonnes pratiques pour écrire du code sécurisé.
- Les chaînes de caractères et les pointeurs en C++.
- La gestion de la mémoire.
- Les fonctions d'entrées et de sorties.
- La protection des accès aux fichiers.

Travaux pratiques :

- analyser du code sécurisé et du code non sécurisé.

Module 8 : appliquer les bonnes pratiques de programmation

- Les règles de codage de base.
- Les macros et les fonctions inline.
- La gestion de la mémoire et la gestion des erreurs.
- La différence entre la structure et la classe.
- La compilation de C++14 à C++17.
- Les normes de sécurité applicative.

- La validation du code.

Contenu de formation proposé en partenariat avec Softeam Institute