

Sécurité des applications .Net

Objectif :

Le Framework .NET intègre des fonctionnalités de sécurité très évoluées, qui s'appliquent aussi bien aux applications distribuées, qu'aux applications Web ASP.NET ou aux applications de bureau Windows. L'écriture d'un code sécurisé, l'utilisation d'un certificat, le chiffrement de données sont autant de challenges que le bon développeur .Net doit relever.

Cette formation Sécurité .net vous permettra de:

- Comprendre comment tirer parti des fonctionnalités de sécurités intégrées au Framework .Net
- Savoir les mettre en oeuvre, plus particulièrement en ce qui concerne le chiffrement et la signature des données
- Savoir gérer un certificat numérique aussi bien sur un serveur Web qu'à partir du client

Participants :

Cette formation Sécurité .NET s'adresse aux chefs de projet informatique et aux développeurs .net avec une bonne expérience.

Pré-requis :

Expérience dans le développement d'application .NET

Durée : 3 jours (21 heures) **Référence : SDNE**

Contenu de la formation :

Sécurité des applications .NET

Principes - La sécurité
Les différents types de menace
Gestion de la sécurité dans le Framework .Net pour les différents types d'application : applications distribuées, applications mobiles, applications Web, applications de bureau

Sécurité dans le framework .NET

Concepts fondamentaux
Sécurité d'accès du code
Sécurité basée sur les rôles
Services de chiffrement

Les bases de la cryptographie

Cryptographie - Les définitions
Types de chiffrement : chiffrement à clés partagées, chiffrement à clés publique

Symétrique vs. asymétrique, combinaisons symétrique / asymétrique, fonctions de Hachage, signatures numériques, processus de signature, processus de vérification

Chiffrement, hash, et signature des données en .NET

Cryptographic Service Providers (CSP)

System, security, cryptography

Choix des algorithmes de chiffrement

Chiffrement symétrique en .Net : algorithme (DES, 3DES, RC2, AES), chiffrement de flux, mode de chiffrement (CBC, ECB, CFB)

Algorithmes asymétriques en .Net

Algorithme : RSA, DSA

Algorithme de hachage : SHA-1, MD-5

Vue d'ensemble d'une infrastructure à clé publique (PKI)

Certificat numérique : certificat X.509

PKI - Les définitions

Les fonctions PKI

PKI - Les composants

PKI - Le fonctionnement

Applications de PKI : SSL, VPN, IPSec

IPSec et SSL en entreprise

Smart Cards (cartes intelligentes)

Autorité de certification

SSL et certificat de serveur

Certificat de serveur SSL : présentation, autorité de certification d'entreprise, autorité de certification autonome

Utilisation de SSL et des certificats clients

Certificats clients

Fonctionnement de SSL : phase I, II, III et IV

Classe X509 Certificate

Classe HttpClient Certificate

Sécurité des services Web

Objectifs de la sécurisation des services Web : authentification, autorisation, confidentialité et intégrité

Limitations liées à SSL

Sécurité des services Web : WSE 2.0, sécurisation des messages SOAP

Jetons de sécurité

Jetons de sécurité : UserName Token, Binary Token, XML Token

Certificats X.509

Signature des messages SOAP : création d'un jeton de sécurité, vérification des messages

SOAP, chiffrement des messages SOAP, déchiffrement du message

Vue d'ensemble de DPAPI (Data Protection API)

Qu'est-ce que DPAPI ?
Stockage utilisateur
Stockage machine
DPAPI utilise l'Entropie

Outil de sécurité et d'audit

Outils du SDK liés à la sécurité
Outils pour mener les tests de sécurité