Catalogue de formation
20/03/2021

# KAÏNA-COM
## CATALOGUE DE FORMATION

## Développer des applications sécurisées - Avancée

**Nos locaux**
KAÏNA-COM France
LE CARRÉ HAUSSMANN II
6 Allée de la Connaissance
77 127 Lieusaint

**Contact**
+33(0)9 50 20 91 64

**E-mail**
info@kaina-com.fr

**Site Internet**
www.kaina-com.fr

# KSE011 – Développer des applications sécurisées - Avancée

**Référence**

KSE011

**Niveau**

- ☒ Débutant
- ☒ Intermédiaire
- ☐ Expert

**Nombre de jours**

Programme de formation :

- 32 heures (4 heures/jour)

**Lieu de la formation**

- ☐ I: e-learning, Formation individuelle (Formation en ligne)
- ☒ V: v-learning, classe virtuelle
- ☐ C: c-learning, cours présentiel

**KAÏNA-COM**
LE CARRÉ HAUSSMANN II,
6 Allée de la Connaissance
77127 Lieusaint - France

**Prérequis**

Expérience et compréhension du développement d'applications
Un niveau d'anglais business moyen est requis car la formation sera dispensée en anglais.

**Public**

Les développeurs d'applications et tous ceux qui cherchent à mieux comprendre comment créer des applications sécurisées.

*Ce sujet continue à la page suivante*

## KSE011 – Développer des applications sécurisées - Avancée, Suite

**Objectifs**

En matière de sécurité, l'accent a principalement été mis sur la sécurisation de l'infrastructure réseau (pare-feu, VPN, etc.) et du système d'exploitation du serveur (par exemple, les systèmes de gestion des correctifs). Cependant, au cours des dernières années, l'accent s'est déplacé vers la couche application. En effet, la sécurité de l'infrastructure (réseau et système d'exploitation) s'est considérablement améliorée tandis que les applications sont restées vulnérables. La couche application est devenue la principale cible des attaques, tandis que les applications sécurisées sont devenues synonymes de meilleure qualité.
Le cours couvre les différents aspects de la sécurité des applications, y compris l'authentification, l'autorisation, l'audit, la confidentialité et l'intégrité des données, ainsi que les différentes technologies répondant à ces exigences. Il comprend le modèle d'analyse des risques et explique comment l'utiliser pour analyser les risques associés aux vulnérabilités des applications.
Les participants apprennent à créer des applications sécurisées : en commençant par inclure la sécurité dans le cycle de vie de développement d'applications et en continuant à sécuriser les pratiques de codage et les outils de test de sécurité.

*Ce sujet continue à la page suivante*

# KSE011 – Développer des applications sécurisées - Avancée, Suite

**Contenu du cours**

**Contenu du cours :**

**Table 1: KSE011 - Contenu du cours**

| Chapter | Description |
|---|---|
| **Introduction** | • The risks caused by unsecure applications: application vulnerabilities and associated threats<br>• Examples of application layer attacks and associated risks<br>• Security infrastructure and how it helps to protect the application |
| **Encryption and hash functions** | • Ensure data confidentiality and data integrity<br>• Symmetric encryption<br>– Stream encryption algorithms<br>– Block encryption algorithms<br>• Asymmetric encryption<br>• Message hash functions and HMAC<br>• Digital signatures and digital certificates<br>• How to secure the data<br>• Crypto++ examples<br>• Confidentiality best practices |
| **Authentication and Identity Management** | • Passwords including password management<br>• Challenge-resp authentication and tokens<br>• One-time passwords (OTP) and OTP tokens<br>• Smart cards and public key technology<br>• Password storage and management<br>• Brute force and dictionary attacks<br>• Biometric authentication<br>• Two factor authentication<br>• Ticket based authentication<br>• Digital certificates<br>• PKI / PAM / RADIUS / ID Management |

*Ce sujet continue à la page suivante*

# KSE011 – Développer des applications sécurisées - Avancée, Suite

**Contenu du cours**, Suite

| Chapter | Description |
|---|---|
| **Application Layer Vulnerabilities** | • Coding vulnerabilities<br>– Input validation<br>– Injection attacks<br>– Application layer DoS<br>• Business logic vulnerabilities |
| **Input Validation** | • Server side validation<br>• Client side validation<br>• Input validation using positive security logic<br>• Input validation using negative security logic<br>• Canonicalization and evasion<br>• Injection attacks and countermeasures |
| **Authorization and Access Control** | • The principle of least privileges<br>• Access control matrix<br>• Discretionary Access Control (DAC)<br>• Mandatory Access Control (MAC)<br>• Role Based Access Control (RBAC)<br>• Distributed enforcement model with centralized management |
| **Auditing and Logging** | • The need<br>• Central logging<br>• Auditing and log analysis |

*Ce sujet continue à la page suivante*

# KSE011 – Développer des applications sécurisées - Avancée, Suite

**Contenu du cours**, Suite

| Chapter | Description |
|---|---|
| **Risk Analysis and Threats** | • Vulnerability, threat and risk<br>• Risk analysis and risk mitigation<br>• Security risks<br>• Identifying threats<br>• STRIDE threat model and threat modeling<br>• DREAD and risk management<br>• Responding to threats (risk mitigation) |
| **SDLC – Secure Development Life Cycle** | • The Methodology<br>• Integrating security requirements<br>• Secure design<br>• Secure coding<br>• Security testing<br>• Security in deployment, support and maintenance<br>• Security policy management |
| **Secure Design** | • Guidelines to designing secure applications<br>• Reducing the attack surface<br>• Identifying trusts and secrets |
| **Threat Modeling and SDLC Tools** | • Microsoft threat analysis and modeling tool<br>• Pattern and practice check lists<br>• Creating a threat model |

*Ce sujet continue à la page suivante*

# KSE011 – Développer des applications sécurisées - Avancée, Suite

**Contenu du cours**, Suite

| Chapter | Description |
|---|---|
| **Application Layer Vulnerabilities** | • Business logic vulnerabilities<br>• Coding vulnerabilities<br>• Web application vulnerabilities<br>– Injection attacks<br>– Buffer overflow<br>– XSS, cross site scripting<br>– XSRF, cross site request forgery<br>– Application layer DoS and DDoS |
| **Web Services Security Standards** | • XML encryption<br>• XML digital signatures<br>• SAML<br>• XCAML<br>• Web service security |
| **Secure Communication Protocols** | • SSL<br>• IPSec |
| **The End** | • Summary<br>• Q&A<br>• Course's Evaluation |