Training Catalogue
02/07/2020

KAÏNA-COM
TRAINING CATALOGUE

Building Secure Applications - Advanced

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 – Building Secure Applications - Advanced

Reference

KSE011

Experience

☒ Beginner

☒ Intermediate

☐ Advanced

Duration

Training Program:

- 32 hours (4 hours/day)

Training Method

☐ I: i-learning, individual training (web-based training)

☒ V: v-learning, virtual class

☐ C: c-learning, classroom training

KAÏNA-COM

LE CARRÉ HAUSSMANN II,

6 Allée de la Connaissance

77127 Lieusaint - France

Prerequisite

Experience and comprehension of application development

Audience

Application developers and Everyone who seeks to better understand how to build Secure Applications.

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Objective

Most of the focus when dealing with security has been on securing the network infrastructure (firewalls, VPNs etc.) and the server OS (e.g. patch management systems). However, in the last few years the focus has shifted to the application layer. This is because infrastructure (network and OS) security has improved significantly while applications have remained vulnerable. The application layer has become the main target of attack, while secure applications have become synonymous with higher quality.

The course covers the different aspects of application security including authentication, authorization, auditing, confidentiality, and data-integrity, as well as the different technologies addressing these requirements. It includes the risk analysis model and explains how to use it to analyze the risks associated with application vulnerabilities.

Participants learn how to build secure applications: starting from including security in the application development life cycle and continuing to secure coding practices and security testing tools.

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Course Contents

Course Contents :

Table 1: KSE011 - Course Contents

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

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Course Contents, continued

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

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Course Contents, continued

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

Continued on next page

KSE011 – Building Secure Applications - Advanced, Continued

Course Contents, continued

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