Training Catalogue
25/05/2020

KAÏNA-COM
TRAINING CATALOGUE

Android Security

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

KSE010 – Android Security

Reference	KSE010
Experience	☒ Beginner ☒ Intermediate ☐ Advanced
Duration	Training Program: • 1 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
Price	668,50 € HT
Prerequisite	Some experience in Java development and understanding of the Android development platform. There is an advantage to having attended the "Building secure applications" course.
Audience	Android developers, team leaders, software system engineers and system architects, who are interested to learn more about Android Security aspects.

Continued on next page

KSE010 – Android Security, Continued

Objective

Android is an open source platform developed by Google for mobile development. Applications for the Android platform are developed in Java. The course overviews Android's fundamental topics and presents its security model and guidelines in coding secure Android applications.

Continued on next page

KSE010 – Android Security, Continued

Course Contents

Course Contents :

Table 1: KSE010 - Course Contents

Chapter	Description
Introduction	• What is Android? • Android development • Why deal with Android security
Android Applications	• Artifacts • Basic system tools • Installing user applications
Android Challenges	• Battery life • Android market • Services • External access
Android Architecture	• Linux kernel • Java and Native • Dalvik VM • SQLite • Binder component framework • Components • Middleware • Application layer
Components	• Component model • Activities • Services • Content providers • Broadcasts • Intents

Continued on next page

KSE010 – Android Security, Continued

Course Contents, continued

Chapter	Description
Security Enforcement	• Protect application • Dalvik VM • Reference monitor • Access permission logic • Signing application • Pros and cons
Manifest Files	• AndroidManifest.xml • Defining security policy • Public and private components • Implicit open components • Content provider permissions • Intent broadcast permissions • Service hooks • Protected APIs • Pending intents • Permission protection levels • Permission granularity
The End	• Summary • Q&A • Course's Evaluation