

# Android Security

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **3 Days**

## Overview

Android is an open platform for mobile devices such as handsets and tablets. It has a large variety of security features to make developing secure software easier; however, it is also missing certain security aspects that are present in other hand-held platforms. The course gives a comprehensive overview of these features, and points out the most critical shortcomings to be aware of related to the underlying Linux, the file system and the environment in general, as well as regarding using permissions and other Android software development components.

Typical security pitfalls and vulnerabilities are described both for native code and Java applications, recommendations and best practices to avoid and mitigate them.

## Prerequisites

There are no prerequisites for this course.

## Who Should Attend

Android application developers, architects and testers.

## What You Will Learn

- Understand basic concepts of security, IT security and secure coding
- Learn the security solutions on Android
- Learn to use various security features of the Android platform
- Have a practical understanding of cryptography
- Get information about some recent vulnerabilities in Java on Android
- Learn about typical coding mistakes and how to avoid them
- Get practical knowledge in using security testing tools for Android
- Get sources and further readings on secure coding practices

## Outline

- IT security and secure coding
- Android security overview
- Android application security
- Practical cryptography
- Protecting Android applications
- Input validation
- Improper error and exception handling
- Code quality problems
- Testing Android code
- Principles of security and secure coding
- Knowledge sources