Mobile Secure Coding Awareness

1-Day Seminar

Syllabus

AppSec Labs Ltd.

info@appsec-labs.com | https://appsec-labs.com | 10 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

Mobile secure coding awareness
1-day course

Course description

Secure programming is the last line of defense against attacks targeted toward our systems. This course shows you how to identify security flaws & implement security countermeasures when writing code for Android and iOS mobile devices. Using sound programming techniques and best practices shown in this course, you can produce high-quality code that stands up to attack.
The course covers major security principles when writing Java code for Android and Objective-C code for iOS.

The objectives of the course are to acquaint students with security concepts and terminology, and to provide them with a solid foundation for developing secure software. By course completion, students should be familiar with major secure programming practices and have learnt the basics of security analysis and design.

Target audience

Members of the software development team:

- Android developers
- iOS developers

Prerequisites

Before attending this course, students should be familiar with:

- Basic knowledge of the Android development platform
- Basic knowledge of the iOS development platform

Course topics

Demonstrating the top 10 mobile security attacks

- Insecure Data Storage
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Client Side Injection
- Poor Authorization and Authentication
- Improper Session Handling
- Security Decisions Via Untrusted Inputs
- Side Channel Data Leakage
- Broken Cryptography
- Sensitive Information Disclosure

Secure Coding Best practices

- Creating files with correct ACLs
- Secure memory handling
- Secure data storage
- Erasing Data
- Symmetric encryption
- Asymmetric encryption
- Transport Level Encryption
- Storage Level Encryption
- Key derivation
- The KeyChain
- Validating server certificates and avoiding man-in-the-middle
- SSL Pinning
- Client side certificate authentication
- Application permission isolation
- The permission model
- Permission types & app restrictions
- Application signing
- Permission categories
- Creating custom permissions
- Verifying process permissions during runtime
- Securely activating components
- Avoiding access to restricted screens
- Parameterized queries
- Avoiding hard coded secrets

- Obfuscate the program
- Code Encryption
- Detecting common code level vulnerabilities
- Secure device management