Android Security Essentials V8

Course Duration: 16 Hours **Course code: ASE-V8**

1. Course Overview

This course provides a comprehensive understanding of Android security architecture, threats, and best practices. Participants will learn to secure Android applications, safeguard sensitive data, apply cryptography, and implement secure communication. It also covers real-world vulnerabilities, app hardening, and secure coding techniques to protect apps against attacks.

2. What you'll learn?

- Understand Android security architecture and application sandboxing.
- Secure Android apps with permissions, encryption, and secure storage.
- Implement secure coding practices to prevent vulnerabilities.
- Protect data with cryptography and secure communication protocols.
- Identify and mitigate OWASP Mobile Top 10 security risks.
- Use testing tools for penetration testing and vulnerability assessment.
- Apply app hardening, obfuscation, and anti-tampering techniques.

3. Target Audience

- QA/security testers specializing in mobile security.
- IT professionals responsible for mobile security in organizations.
- Students interested in cybersecurity and mobile application security.

4. Pre-Requisites

- Basic knowledge of Android app development (Java/Kotlin, Android Studio).
- Familiarity with networking concepts and mobile ecosystems.
- Awareness of general application security concepts.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

5. Course content

Lesson 1: Permissions

- Introduction
- Android Platform Architecture
- Android Security Architecture
- Application Signing
- Installing Applications
- Permissions
- Why Permissions?
    - Enforcing Permissions
    - Levels of Permission Protection
    - Application-Level Permissions
    - Component-Level Permissions
    - Extending Android Permissions

Lab 1: Permissions

- Creating and Accessing App Permissions
- Configuring Permissions Among Different Apps

Lesson 2: Managing the Policy File

- Introduction
- The Manifest File
    - Manifest Tag Attributes
    - Application Tag Attributes
- Modifying the Application Policy
    - Application Running with the Same Linux ID
    - Setting Application Permissions
    - Permissions for External Applications
    - External Storage
    - Debugging Mode

- Backup

Lab 2:

- Creating Two Applications with the Same Linux ID
- Backing up Data on Cloud Storage

Lesson 3: Users' Data Privacy and Protection

- Introduction
- Data Security Principles
  - Confidentiality
  - Integrity
  - Availability
- The Mobile Environment
- Data States
- Vulnerabilities and Attacks Against Stored Data
  - Vulnerabilities of Stored Data
  - Threats on Stored Data
- Protection Principles
- Tips for Avoiding Android Coding Vulnerabilities

Lab 3:

- Ensuring Data Confidentiality - Hacking Application
- Protecting Application Data with Permissions

Lesson 4: Securing Storage

- Introduction
- Data Storage Decisions
  - Privacy
  - Data Storage Period
- Storage Mechanisms

  - SharedPreferences
  - File
- File Operations on an External Storage
- Cache
- Database

Lab 4: Data Storage Applications

- Using SharedPreferences
- File Storage Operations
- Storing Data in Cache
- SQLite Database Storage