Creating Secure Android Code in Java (COD 318)

BUNDLING AND PRICING:

Curriculum: Mobile Developer Curriculum.

Pricing : $550 single class, per user.

Target Audience: Mobile Developer writing Android application in Java.

Mobile Developer Curriculum	AWA 105. Fundamentals of Security Awareness - Mobile and Social Media
	COD 110. Fundamentals Secure Mobile Development
	COD 218. Creating Secure Code – Android Foundations
	COD 217. Creating Secure Code – iPhone Foundations
	COD 317. Creating Secure iPhone Code in Objective-C
	COD 318. Creating Secure Android Code in Java
	ENG 301. How to Create an Application Security Threat Model
	ENG 312. How to Perform a Security Code Review

ABOUT OUR COURSE:

Course Length- 1.5 hours, 67 slides

Prerequisite: COD 218 Creating Secure Code - Android Foundations.

Course Description

Users will learn about the various developer tools used for securing Android applications and the types of Java memory and how the memory is managed automatically by Java. In addition, students will learn about the various functions of the bytecode verifier.

Users will learn about common Android application security vulnerabilities and various threats to data, including theft of data-at-rest and in transit, and the best practices for mitigating these threats. Also, SQL injection, XSS, and session hijacking attacks and the best practices for mitigating these vulnerabilities are reviewed.

This course teaches about the threats to user privacy and confidentiality, and about web-based attacks and malware, as well as encrypting sensitive data by using the javax.crypto package to make a hacker's task as difficult as possible.

Users will learn about the different methods of storing and protecting confidential data on the Android OS, and learn about implementing input validation and the different vulnerabilities that can result from not performing input validation. The course teaches how to use parameterized queries to help protect the database from malicious attacks and the different methods that can help prevent the risks associated with unauthorized access.

Course Objectives:

- Describe the open-source developer tools available for securing Android applications.
- Introduce the different types of Android application security vulnerabilities and attack vectors.
- Describe how to protect confidential data by using secure UUIDs.
- Describe how to use parameterized queries and implement input validation to prevent malicious attacks on a database.
- Explain how to use the AccountManager class to avoid the risks associated with unauthorized access.
- Describe how to use different methods and cryptography to secure the WebView class.