MOB101 - MOBILE SECURITY FUNDAMENTALS

Course Learning Objectives

Learn to communicate the business risks to developing mobile apps for any platform. Discover risks for mobile apps as it relates to important security concepts of data at rest, data in transit and data in use.

Describe how the threat landscape of a mobile device is different than what we've known for web applications today and the OWASP Mobile Top 10.

Description

In this code-agnostic course, students will learn important mobile security concepts to build more secure mobile applications. We will dive into understanding what the risks are to developing insecure mobile applications and how hackers can target the app, the infrastructure and the mobile device itself.

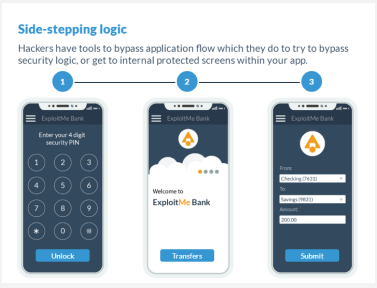
Students will learn about the current threat landscape with different mobile operating systems, un-official means of loading applications on devices and the business risk to developing insecure mobile applications.

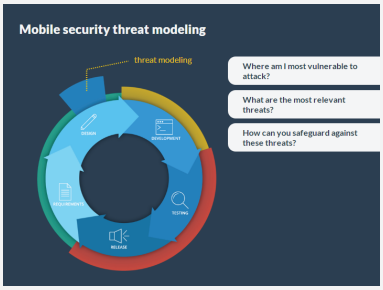
Audience

Mobile application developers
Mobile application architects

Time Required

Tailored learning - 60 minutes total





MOB101 - MOBILE SECURITY FUNDAMENTALS

Course Outline

1. Introduction

- Mobile security architecture and design
- Mobile security threat modeling
- Personal information
- Relevant laws and regulations

2. Risks and vulnerabilities

- Fundamental risks to mobile applications
- Ways of loading applications
- Assume devices and users are untrusted
- Consider the business
- Business minded approach
- Native applications
- Web-based mobile applications
- Native apps vs. web based mobile apps
- Typical mobile architecture
- OWASP Mobile Top 10
- Mapping the top threats
- Application security
- Risk in context

3. Data in transit

- Data in transit
- Information disclosure in transit
- Session token reuse
- Session identifiers in query string
- Dissecting protocol
- Attacker exploits the API
- Network encryption
- Certificate pinning
- Hardening external APIs
- Authorization and session management
- Expire session at logout or timeout
- Invalidating sessions periodically
- Using OAuth

4. Data in use

- Data in use
- Side-stepping logic
- Memory attacks
- Reverse engineering
- URI and resource sharing risks
- Practical sharing example
- Protect your app binaries
- Clear sensitive data in memory
- Secure caching
- Enforce authorization on interna windows

5. Data at rest

- Data at rest
- Insecurely storing data
- The challenge of file system security
- Best practices for user credentials
- Requesting authentication
- Delegating authorization
- Secure file storage
- Secure data storage
- Password-based key derivation function

SecurityCompass