Security Vulnerabilities in AI Generated Cross - Platform Mobile Applications: A Comparative Empirical Study using the OWASP Mobile Top 10

Ariel Ramos Ortega
General Director, Codingraph, San José, Costa Rica

Abstract

The Artificial intelligence (AI) is changing software development, it allows developers to create cross - platform mobile applications using natural language prompts. However, a functional application is not necessarily secure one. This document examines whether three AI coding models can implement security controls without explicit instructions. For this case, three models are asked to develop the same application using Flutter and Dart for Android and iOS, with Firebase as the backend and database. All models receive identical functional requirements without security instructions and they have full permissions to edit the app. The generated applications are evaluated against the OWASP Mobile Top 10 (2024), supported by MASVS and MASTG, to identify missing, ineffective, and correctly implemented security controls. The research focuses on authentication, authorization, input validation, data storage, credential handling, binary protection and others defined in the OWASP standard. It also examines the effort required to identify and fix vulnerabilities. The goal is to determine whether AI generated applications are secure by default and why security requirements matter from the beginning.

Keywords

Artificial Intelligence, AI-Generated Code, Flutter, Dart, Firebase, Cross - Platform Mobile Applications, OWASP Mobile Top 10, Mobile Application Security, Secure Software Development.