Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de Magister en Ciberseguridad

AUTORES:

CALDERON SANTANDER CRISTIAN ISRAEL

ESPIN LEIVA VALERIA CAROLINA

GARCIA VITERI DAMIAN ISAIAS

MANTILLA LOPEZ KEVIN DAVID

TUTORES:

Iván Reyes Chacón

Paulina Vizcaíno

TEMA

Auditoría de seguridad a la aplicación Android "Cyber Password Manager" para la identificación de vulnerabilidades mediante análisis estático y dinámico alineado con OWASP MASVS e ISO/IEC 27034

Quito - Ecuador

Junio – 20206

REINVENTEMOS EL FUTURO

Resumen

La creciente utilización de aplicaciones móviles para la gestión de información sensible ha incrementado la necesidad de implementar mecanismos que garanticen la seguridad de los datos y credenciales de los usuarios. En este contexto, la presente investigación desarrolla una auditoría de seguridad informática de caja blanca a la aplicación Android *Cyber Password Manager*, desarrollada en Flutter y orientada al almacenamiento seguro de credenciales corporativas.

El estudio tuvo como objetivo evaluar la efectividad de los controles de seguridad implementados mediante técnicas de análisis estático y dinámico, tomando como referencia los estándares OWASP MASVS e ISO/IEC 27034. Para ello, se diseñó un laboratorio de pruebas que permitió analizar aspectos relacionados con la criptografía, el almacenamiento seguro de información mediante Hive, la gestión de claves criptográficas y las comunicaciones de red.

Los resultados permitieron determinar el nivel de cumplimiento de los controles de seguridad evaluados, identificar oportunidades de mejora y formular recomendaciones orientadas al fortalecimiento de la protección de la información sensible. Finalmente, la investigación destaca la importancia de incorporar procesos de evaluación de seguridad durante el ciclo de vida de desarrollo de aplicaciones móviles, contribuyendo a la reducción de riesgos y a la adopción de buenas prácticas de ciberseguridad.

Palabras clave: ciberseguridad, aplicaciones móviles, Android, OWASP MASVS, ISO/IEC 27034, análisis estático, análisis dinámico.

Abstract

The increasing use of mobile applications for managing sensitive information has highlighted the need to implement mechanisms that ensure the security of users' data and credentials. In this context, this research presents a white-box security audit of the Android application *Cyber Password Manager*, developed in Flutter and designed for the secure storage of corporate credentials.

The objective of this study was to evaluate the effectiveness of the application's security controls through static and dynamic analysis techniques, using the OWASP Mobile Application Security Verification Standard (MASVS) and ISO/IEC 27034 as reference frameworks. To achieve this, a controlled testing environment was designed to assess cryptographic mechanisms, secure data storage through Hive, cryptographic key management, and network communications.

The results made it possible to determine the level of compliance with the evaluated security controls, identify opportunities for improvement, and propose recommendations aimed at strengthening the protection of sensitive information. Finally, the study highlights the importance of incorporating security assessment processes throughout the mobile application development lifecycle, contributing to risk reduction and the adoption of cybersecurity best practices.

Keywords: cybersecurity, mobile applications, Android, OWASP MASVS, ISO/IEC 27034, static analysis, dynamic analysis.