Automatización de la certificación de seguridad para aplicaciones Android

Realizado por: Manuel Ruiz Ruiz

Dirigido por: Rubén Ríos del Pozo

Codirigido por: Rodrigo Román Castro

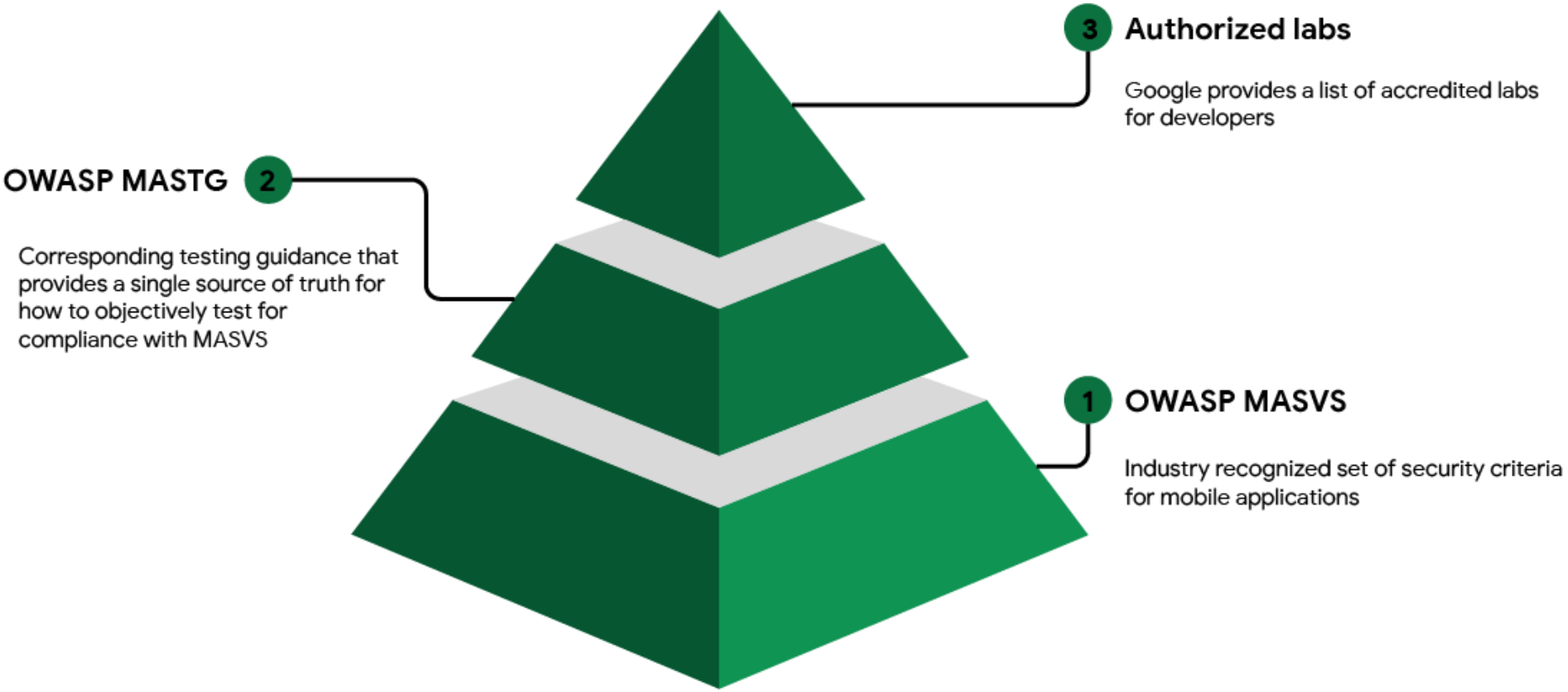
Lenguajes y Ciencias de la Computación - UNIVERSIDAD DE MALAGA

Introducción

- En 2020 había más de **1000 millones de usuarios** en Android.
- Google Play, el proveedor oficial de aplicaciones en Android, cuenta con más de **2,5 millones de aplicaciones.**
  - El **40%** son aplicaciones de **baja calidad e inseguras**.
- Existe un problema de reputación, seguridad y privacidad.

Introducción

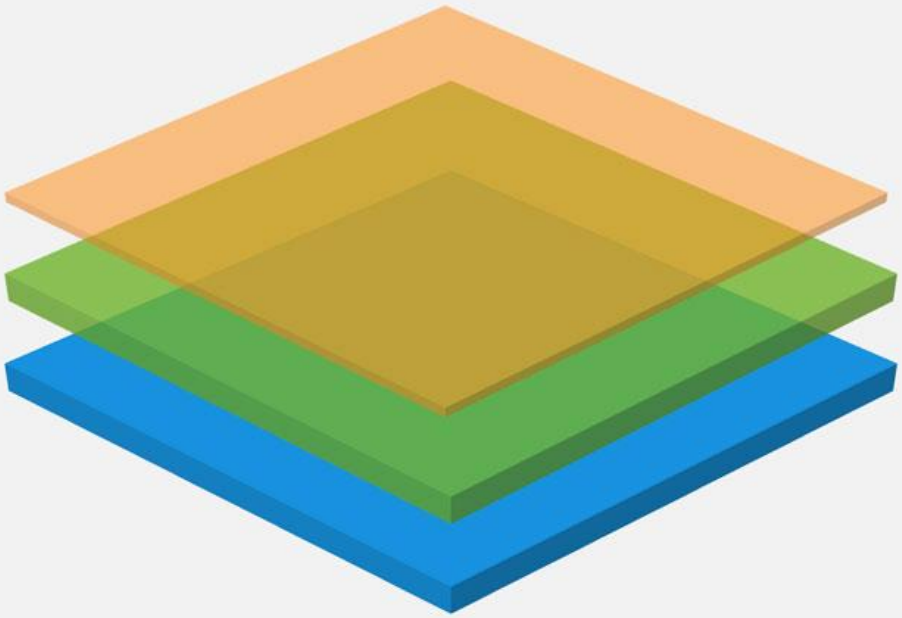
- Google MASA: Programa de seguridad en aplicaciones basado en **OWASP MASVS y MASTG.**



Introducción

- MASVS (STORAGE-2):
  - No se debe almacenar información sensible fuera del contenedor de la aplicación o del almacenamiento de credenciales del sistema.
- MASTG (STORAGE-2):
  - No se declaran permisos de escritura en memoria externa.
  - No se generan ficheros temporales.

OWASP MASVS



R – Resiliency Against Reverse Engineering and Tampering

L2 – Defense-in-Depth

L1 – Standard Security

Objetivos

- **Reducir el tiempo** y esfuerzo empleado **en la evaluación de aplicaciones móviles** por el equipo de certificación.
- Combinar, **clasificar y categorizar la información** procedente de varias herramientas **de análisis**, en función de los casos de prueba establecidos por los diferentes estándares.
- Presentar un **veredicto automatizado** o, en su defecto, agrupar toda la información necesaria para que el experto pueda realizar un veredicto con facilidad.

Estado de la técnica

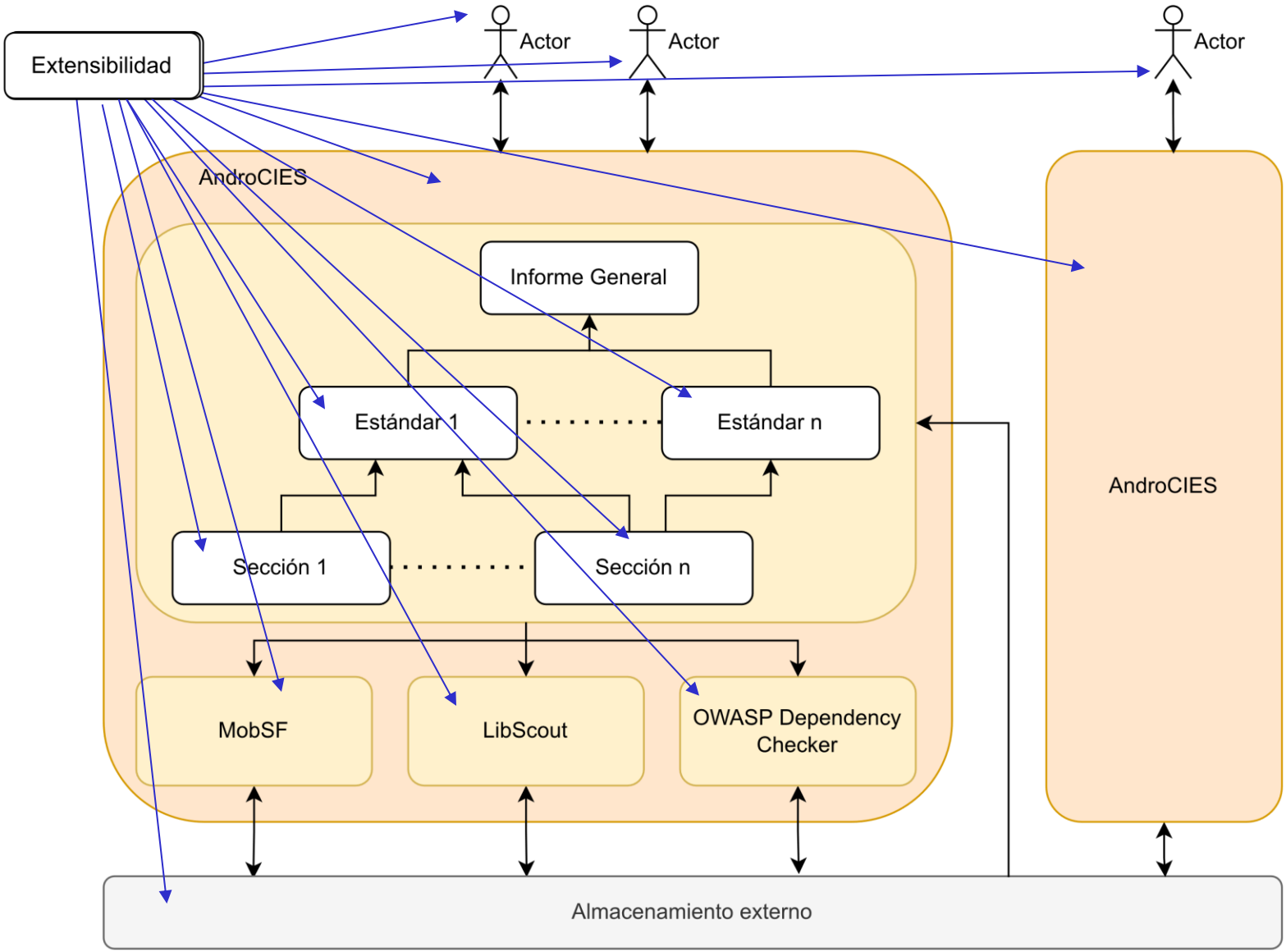
	Análisis					
	Permisos	Manifest	Código	Certificados	URLs	Librerías ext
AndroShield	✗	✓	✓	✗	✗	✗
Androtomsit Lite	✗	✓	✓	✓	✗	✗
MARA Framework	✓	✓	✓	✓	✓	✗
MobSF	✓	✓	✓	✓	✓	✓*
Ostorlab	✓	✓	✓	✓	✓	✓
Kryptowire	✓	✓	✓	✓	✓	✓
NowSecure	✓	✓	✓	✓	✓	✓

	SaaS	Clasificación de severidad	Formato de salida
AndroShield	✗	✓	Página Web
Androtomsit Lite	✗	✗	Fichero txt
MARA Framework	✗	✓	Ficheros json y txt
MobSF	✗	✓	Base de datos MySQL
Ostorlab	✓	✓	Página Web
Kryptowire	✓	✓	Página Web
NowSecure	✓	✓	Página Web

Requisitos

- **Completitud**: se evaluarán todos los casos de prueba del MASVS L1 que DEKRA considera relevantes, alineados con Google MASA.
- **Extensibilidad**: se adaptará a los estándares actuales y futuros.
- **Portabilidad**: se desplegará en diferentes entornos y sistemas operativos.
- **Persistencia**: se garantizará la permanencia de los datos tras los análisis.
- **Soporte multi-usuario**: se ofrecerá el servicio a varios usuarios a la vez.
- **Usabilidad**: ofrecerá una interfaz sencilla, clara y concisa.

Diseño


Extensibilidad
Actor
Actor
Actor
AndroCIES
Informe General
Estándar 1
Estándar n
Sección 1
Sección n
MobSF
LibScout
OWASP Dependency Checker
AndroCIES
Almacenamiento externo

Caso de uso

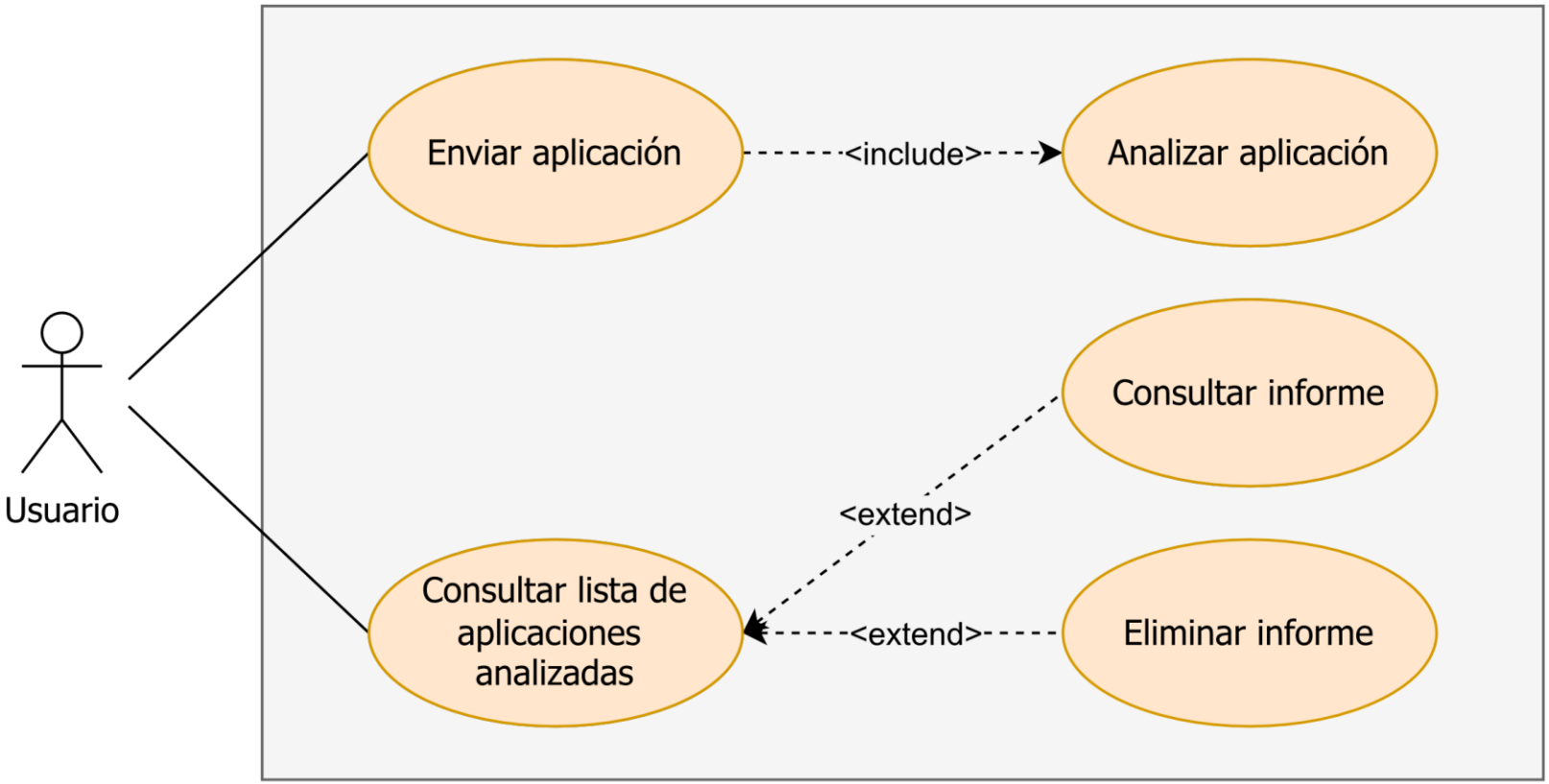

Usuario
Enviar aplicación
<include>
Analizar aplicación
Consultar informe
<extend>
Consultar lista de aplicaciones analizadas
<extend>
Eliminar informe

Diagrama de secuencia

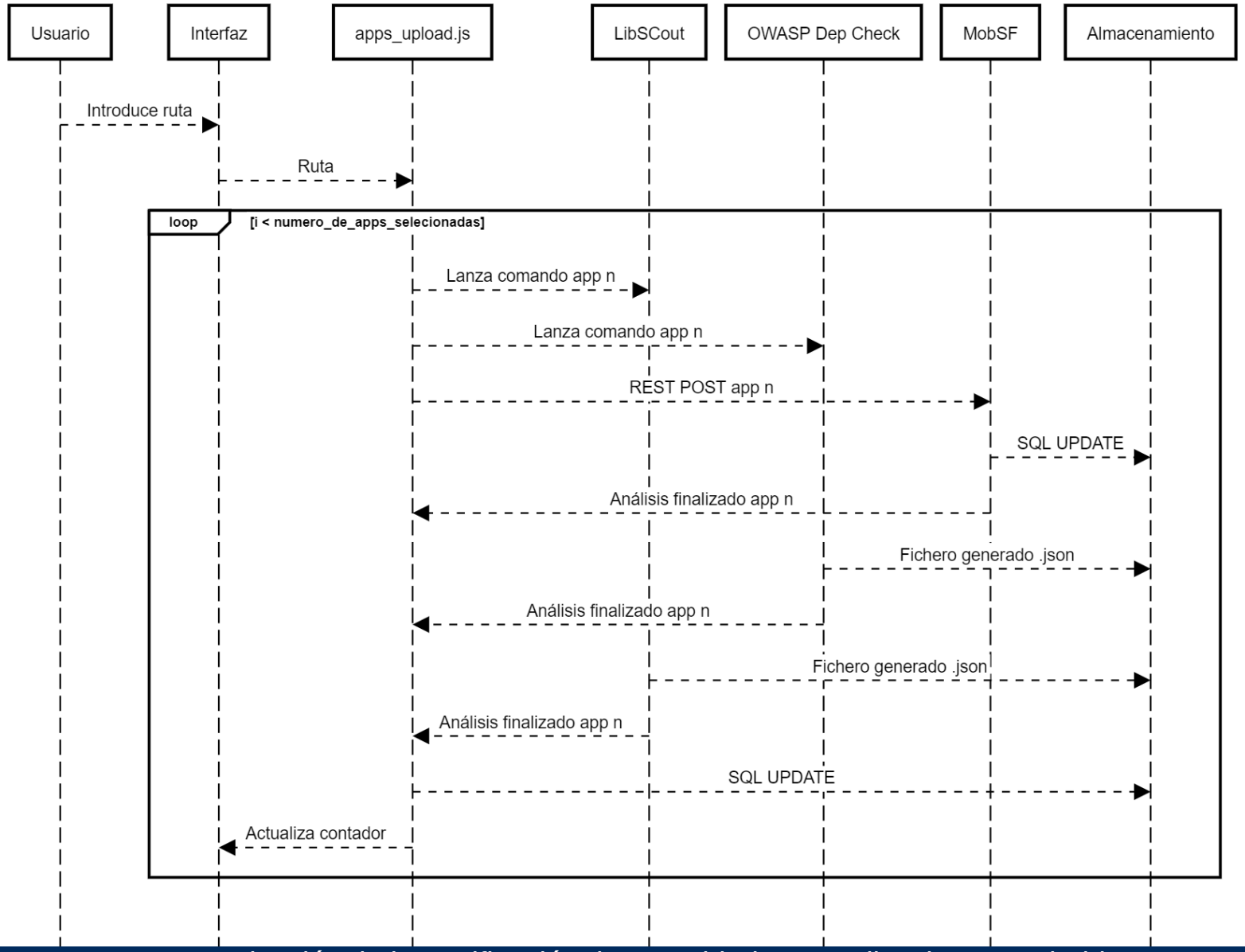
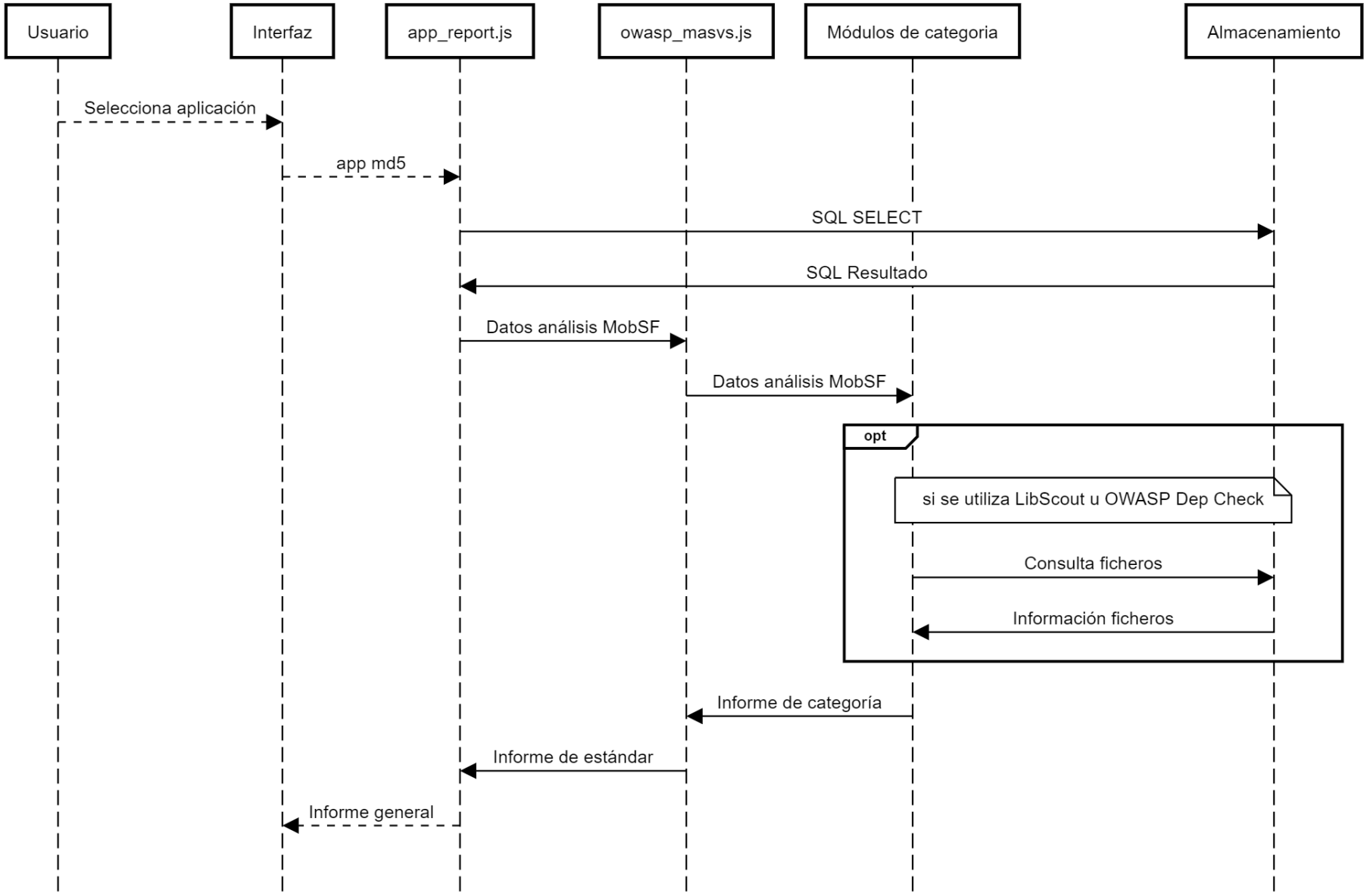
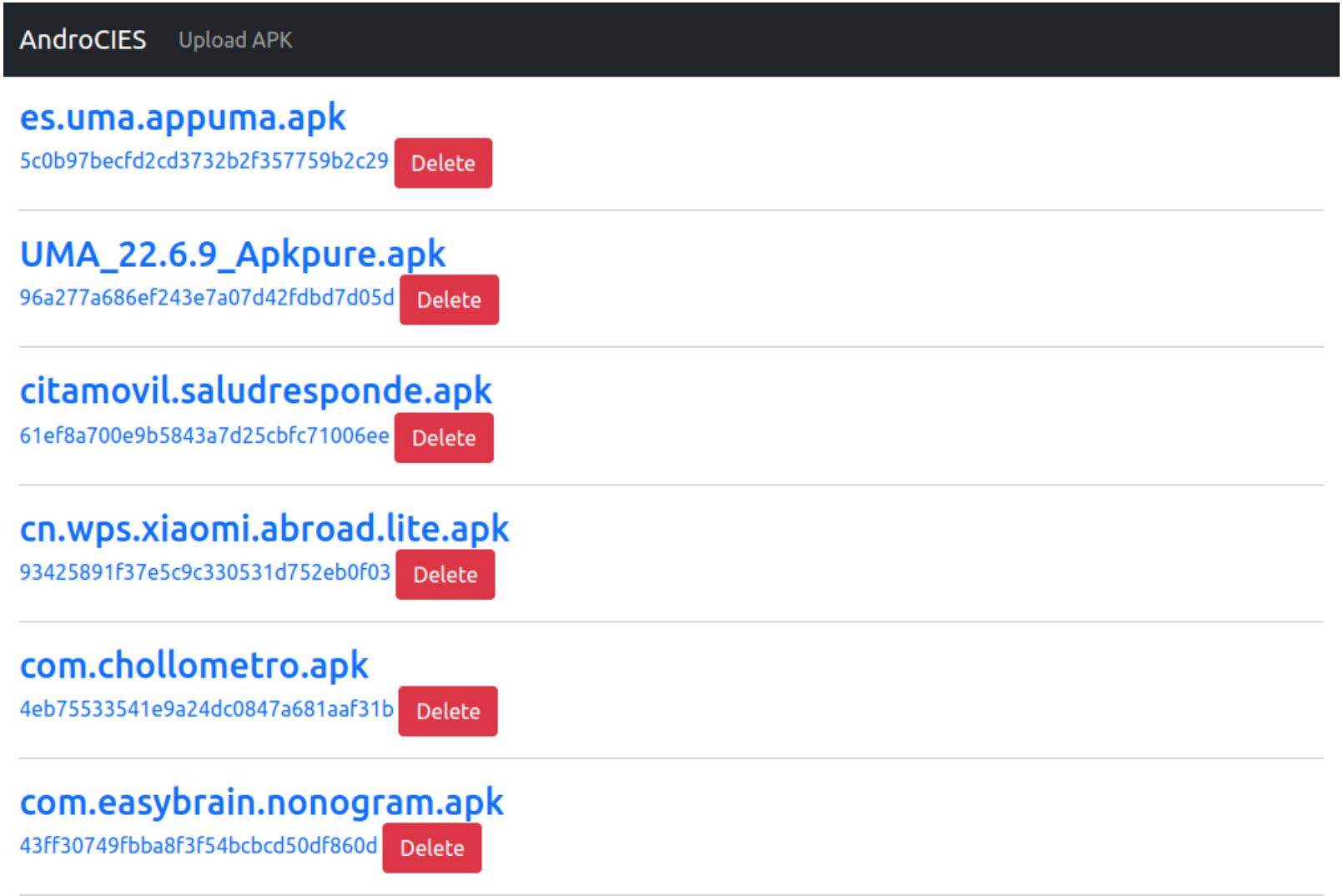


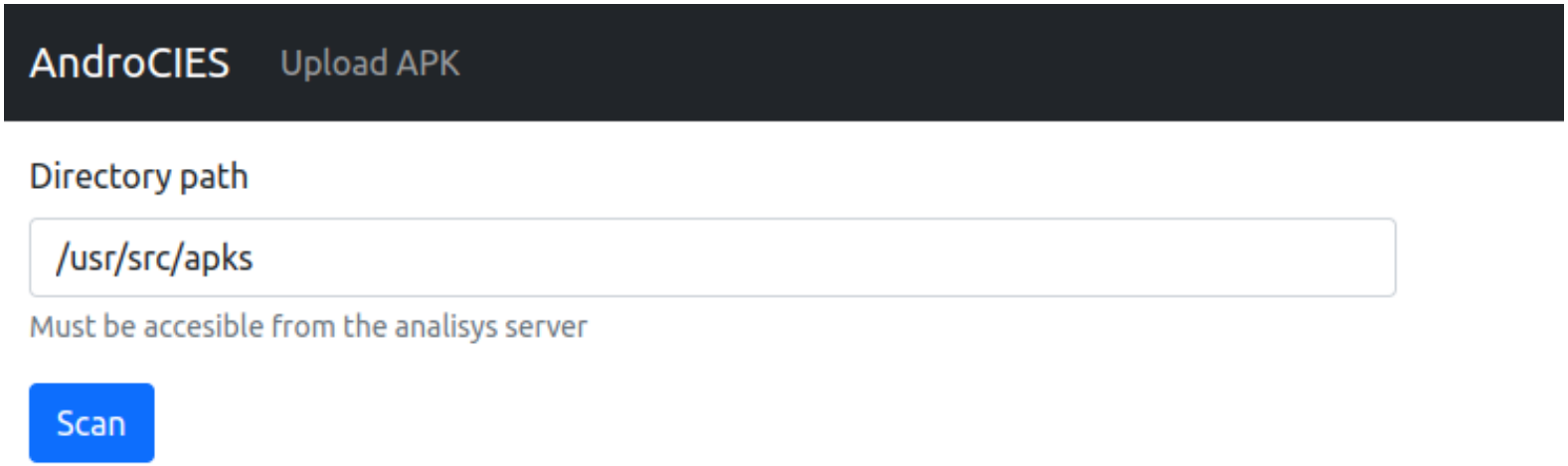
Diagrama de secuencia



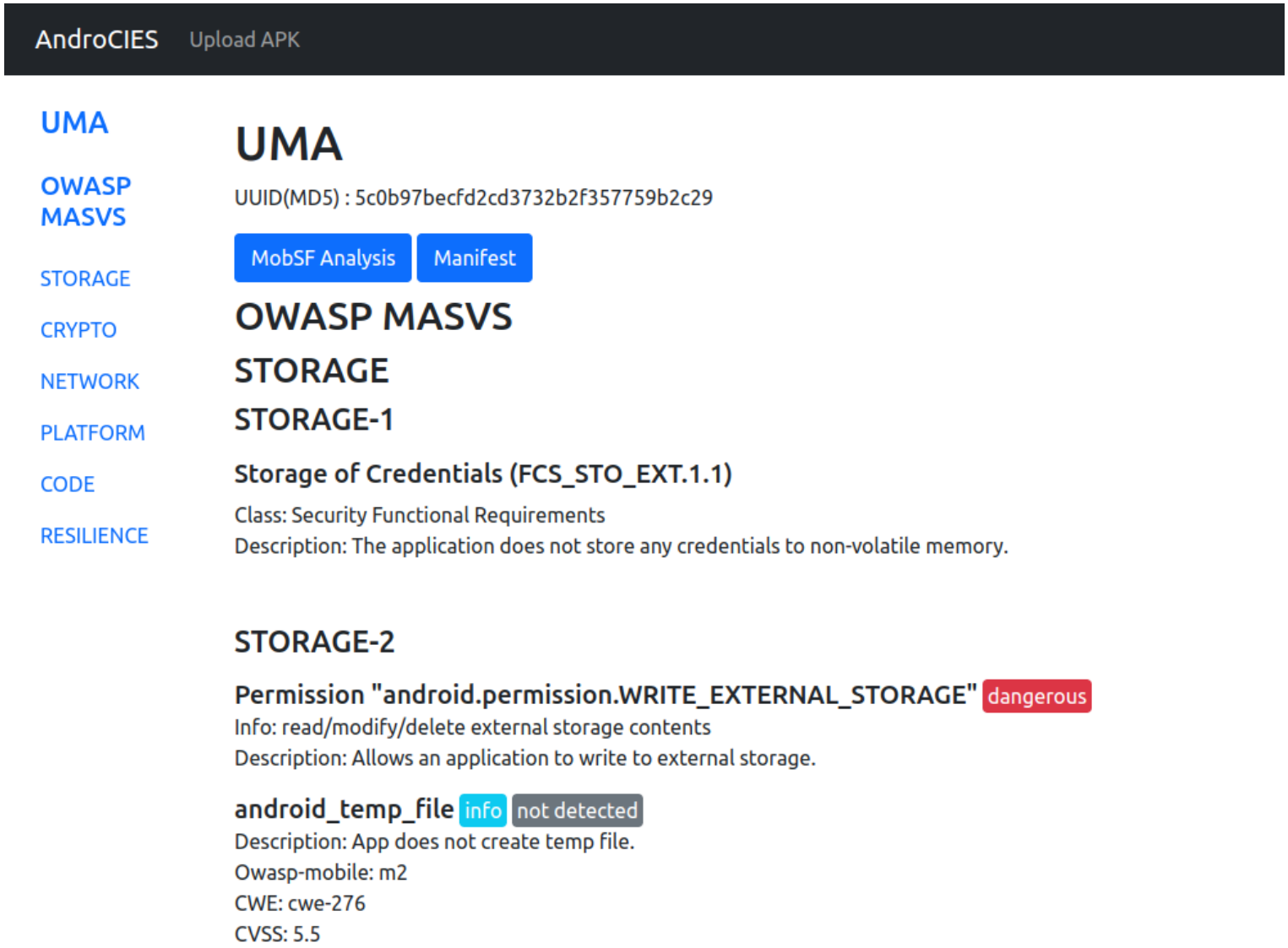
Interfaz


AndroCIES
Upload APK
es.uma.appuma.apk
5c0b97becfd2cd3732b2f357759b2c29
Delete
UMA_22.6.9_Apkpure.apk
96a277a686ef243e7a07d42fdbd7d05d
Delete
citamovil.saludresponde.apk
61ef8a700e9b5843a7d25cbfc71006ee
Delete
cn.wps.xiaomi.abroad.lite.apk
93425891f37e5c9c330531d752eb0f03
Delete
com.chollometro.apk
4eb75533541e9a24dc0847a681aaf31b
Delete
com.easybrain.nonogram.apk
43ff30749fbba8f3f54bcbcd50df860d
Delete

Interfaz


AndroCIES
Upload APK
Directory path
/usr/src/apks
Must be accesible from the analisys server
Scan

Interfaz


AndroCIES
Upload APK
UMA
OWASP MASVS
STORAGE
CRYPTO
NETWORK
PLATFORM
CODE
RESILIENCE
UMA
UUID(MD5) : 5c0b97becfd2cd3732b2f357759b2c29
MobSF Analysis
Manifest
OWASP MASVS
STORAGE
STORAGE-1
Storage of Credentials (FCS_STO_EXT.1.1)
Class: Security Functional Requirements
Description: The application does not store any credentials to non-volatile memory.
STORAGE-2
Permission "android.permission.WRITE_EXTERNAL_STORAGE" dangerous
Info: read/modify/delete external storage contents
Description: Allows an application to write to external storage.
android_temp_file info not detected
Description: App does not create temp file.
Owasp-mobile: m2
CWE: cwe-276
CVSS: 5.5

Conclusiones

- El mercado de los móviles es uno de los más numerosos en la actualidad.
- El interés de Google por una Play Store más segura y transparente está empujando a los laboratorios especializados a **mejorar sus procesos de certificación** de seguridad de aplicaciones.
- En promedio, se ha determinado **una reducción del 20% del tiempo empleado** para la evaluación respecto al estándar OWASP MASVS siguiendo la metodología de OWASP MASTG.

Líneas Futuras

- Incorporación de más estándares.
- Incorporación de técnicas de **análisis dinámico** de código.
- Incorporación de **inteligencia artificial** para diferentes características como la **detección de falsos positivos**.

Gracias por su atención.