

# Tabla de Contenido

<b>1. Introducción</b>	<b>1</b>
1.1. Antecedentes . . . . .	1
1.2. Motivación . . . . .	1
1.3. Objetivos . . . . .	2
1.4. Solución Propuesta . . . . .	2
<b>2. Marco teórico</b>	<b>4</b>
2.1. Sistema operativo Android . . . . .	4
2.1.1. Arquitectura . . . . .	4
2.2. Aplicaciones Android . . . . .	5
2.2.1. Android Application Package (APK) . . . . .	5
2.2.2. Componentes . . . . .	5
2.2.3. Archivo Manifiesto AndroidManifest.xml . . . . .	8
<b>3. Tipos de vulnerabilidades y herramientas de detección</b>	<b>10</b>
3.1. Tipos de vulnerabilidades comunes . . . . .	10
3.1.1. Inyección de parámetros en intents . . . . .	10
3.1.2. Redirección de intents . . . . .	11
3.1.3. Intercepción de emisiones de intents . . . . .	11
3.1.4. Acceso a proveedores de contenido . . . . .	11
3.1.5. Errores en la asignación de permisos . . . . .	12
3.1.6. Componentes sin protección . . . . .	12

3.1.7.	Conexiones inseguras . . . . .	12
3.1.8.	Secretos incrustados . . . . .	13
3.2.	Herramientas . . . . .	13
3.2.1.	Decompilador de APK . . . . .	13
3.2.2.	Emulador de dispositivos Android . . . . .	14
3.2.3.	Proxy . . . . .	14
3.2.4.	Android Debug Bridge - ADB . . . . .	14
<b>4.</b>	<b>Metodología</b>	<b>15</b>
4.0.1.	Decompilación de la aplicación . . . . .	16
4.0.2.	Análisis general de la aplicación . . . . .	16
4.0.3.	Análisis general de componentes . . . . .	16
4.0.4.	Particularidades de la aplicación . . . . .	17
4.0.5.	Monitoreo de conexiones y logs generados por la aplicación . . . . .	17
<b>5.</b>	<b>Pruebas de seguridad</b>	<b>19</b>
5.1.	Configuraciones iniciales . . . . .	19
5.1.1.	Dispositivo Android . . . . .	19
5.1.2.	Instalación de aplicaciones . . . . .	19
5.2.	Análisis de aplicación AFP Modelo . . . . .	20
5.2.1.	Decompilación de la aplicación . . . . .	20
5.2.2.	Análisis general de la aplicación . . . . .	20
5.2.3.	Análisis general de componentes . . . . .	21
5.2.4.	Particularidades de la aplicación . . . . .	22
5.2.5.	Revisión de conexiones . . . . .	25
5.2.6.	Resumen de resultados . . . . .	27
<b>6.</b>	<b>Conclusión</b>	<b>28</b>
6.0.1.	Trabajo a futuro . . . . .	29

<b>7. Bibliografía</b>	<b>30</b>
<b>Anexos</b>	<b>35</b>
<b>Anexo A.</b>	<b>35</b>
A.1. Ejemplos de vulnerabilidades . . . . .	35
A.1.1. Ejemplo de inyección de parámetros en Intents . . . . .	35
A.1.2. Ejemplo de redirección de Intents . . . . .	36
A.1.3. Ejemplo de interceptación de emisiones de intents . . . . .	37
A.1.4. Ejemplo de acceso a los proveedores de contenido . . . . .	38
A.1.5. Ejemplo de errores en al asignación de permisos . . . . .	39
A.1.6. Ejemplo de errores en componentes sin protección . . . . .	40
A.1.7. Ejemplo de conexiones inseguras . . . . .	40
A.1.8. Ejemplos de secretos incrustados . . . . .	41
A.2. Procedimientos . . . . .	42
A.2.1. Configuración de proxy . . . . .	42
A.2.2. Decompilar APK . . . . .	45
A.2.3. Comandos ADB . . . . .	46
A.3. Aplicaciones estudiadas . . . . .	48
A.3.1. AFP Modelo . . . . .	48