Actividad 2.5: Manejo de elementos de seguridad

Nombre: Marcelo Valenzuela

Carrera: Ingeniería en Informática

Fecha: 22-10-2024

Docente: Manuel Merino

Análisis de vulnerabilidades

1. Identificación de vulnerabilidades:

- **Herramienta utilizada:** Se utilizó MobSF para realizar un análisis estático de la aplicación.

-Resultados del análisis estático:

- **App Security Score:** 31/100, clasificado como alto riesgo (grado C).
- **Problemas en el certificado:** La aplicación está firmada con un certificado de depuración, lo cual es un riesgo para un entorno de producción.
- **Uso de algoritmos débiles:** El certificado utiliza SHA1, conocido por problemas de colisión.
- **Configuración de depuración activa:** El apk permite la depuración (android:debuggable=true), lo que facilita el trabajo de los atacantes para obtener información sensible.
- **Compatibilidad con versiones vulnerables de Android:** La aplicación puede instalarse en dispositivos Android con versiones vulnerables, ya que la minSdk es 24 (Android 7.0).

2. Test de vulnerabilidad

-Áreas críticas identificadas:

- **Exportación de componentes sin la debida protección:** Un receptor de difusión (BroadcastReceiver) está accesible para otras aplicaciones, lo que podría permitir un acceso no autorizado.
- **Permiso no definido:** El receptor está protegido por un permiso que no está claramente especificado, lo que puede representar un riesgo.

-Recomendación de mejoras:

- **Eliminar el certificado de depuración:** Firmar la aplicación con un certificado de producción seguro.

- **Actualizar el algoritmo de firma:** Cambiar a un algoritmo más seguro como SHA-256 o superior.

- **Deshabilitar la depuración:** Remover la opción android:debuggable=true en versiones finales.

- **Compatibilidad:** Establecer la compatibilidad mínima con versiones más recientes de Android (API 29 o superior).

Implementación de Best Practices

1. **Cifrado de datos sensibles:** No se detectó la implementación de cifrado en los resultados del análisis.

2. **Uso de HTTPS:** El análisis de seguridad no encontró detalles explícitos sobre la implementación de HTTPS, lo cual es una mejora recomendada para la comunicación segura de la app.

3. **Validación y sanitización:** No se mencionó validación de entradas, pero es fundamental para evitar inyecciones de código o ataques similares.

Security Tips

1. **Autenticación y autorización:** No se detallan mecanismos de autenticación robustos como OAuth2 o JWT en los resultados del análisis, por lo que sería ideal implementarlos para asegurar el acceso a la app.

2. **Protección contra ataques de red:** Se recomienda proteger la aplicación contra ataques como Man-in-the-Middle (MITM) mediante el uso de certificados SSL/TLS apropiados y configuraciones estrictas de red.

Programa de Mejora de Seguridad

1. **Proceso de revisión:**

- Implementar un proceso continuo de revisión de seguridad que incluya pruebas de vulnerabilidades antes de cada lanzamiento.

- Realizar análisis periódicos con herramientas como MobSF y OWASP ZAP.

- **Métricas clave:** Medir la cantidad de vulnerabilidades críticas, el tiempo de respuesta para corregirlas y la mejora del puntaje de seguridad general.