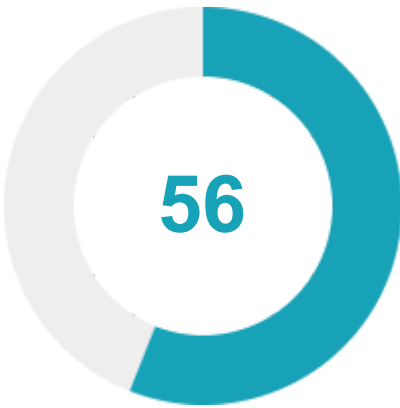


★Puntuación de seguridad



Puntuación de seguridad 56/100

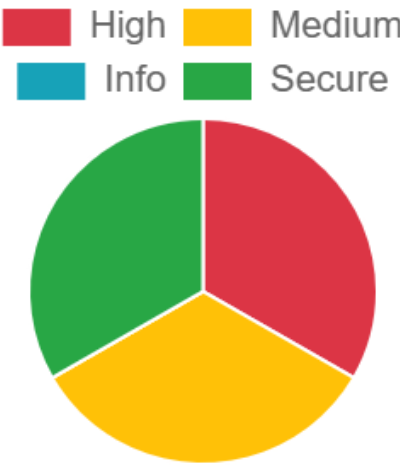
🚧Clasificación de riesgo



Calificación



📊 Distribución de la gravedad (%)



👤 Riesgo de privacidad



Rastreadores de usuarios y dispositivos

Recomendaciones



Alto
1



Medio
1



Información
0



Seguro
1



Punto de acceso
1

alto

La actividad (.MainActivity) es vulnerable a StrandHogg 2.0

[MANIFIESTO](#)

medio

Se pueden realizar copias de seguridad de los datos de la aplicación

[MANIFIESTO](#)

seguro



Esta aplicación no tiene rastreadores de privacidad.

[Rastreadores](#)

punto de acceso

Se encontraron 2 permisos críticos

[PERMISOS](#)

Cuadro de mando de seguridad de aplicaciones MobSF generado para  (GPSMapApp) 

Reporte de Análisis Dinámico de Seguridad

Detalles del Análisis Dinámico

1. Prueba de Vulnerabilidad StrandHogg 2.0:

- Objetivo: Evaluar si se puede explotar la vulnerabilidad de MainActivity.
- Metodología: Ejecutar la app en un entorno controlado de MobSF para detectar suplantación de actividades.
- Resultado esperado: Verificar si MainActivity es susceptible a redirigir usuarios hacia apps falsas.

2. Prueba de Copias de Seguridad de Datos:

- Objetivo: Confirmar si se pueden realizar copias de seguridad no autorizadas de los datos de la app.
- Metodología: Intentar realizar copia de seguridad desde el sistema operativo y verificar permisos.
- Resultado esperado: Determinar si el sistema restringe la exportación no autorizada de datos de la app.

3. Monitoreo de Permisos Críticos:

- Objetivo: Observar el uso de permisos críticos identificados como puntos de acceso.
- Metodología: Análisis en tiempo real con permisos otorgados y revocados.
- Resultado esperado: Confirmar dependencia de permisos y detectar solicitudes excesivas.

4. Pruebas de Seguridad en Tiempo de Ejecución:

- Objetivo: Observar comportamientos inusuales en condiciones de uso variadas, especialmente en actividades de red.
- Metodología: Monitoreo de actividad de red y uso de APIs para evitar llamadas innecesarias.
- Resultado esperado: Asegurar que no existan fugas de datos o accesos no autorizados a APIs.