

AppSweep



Índice

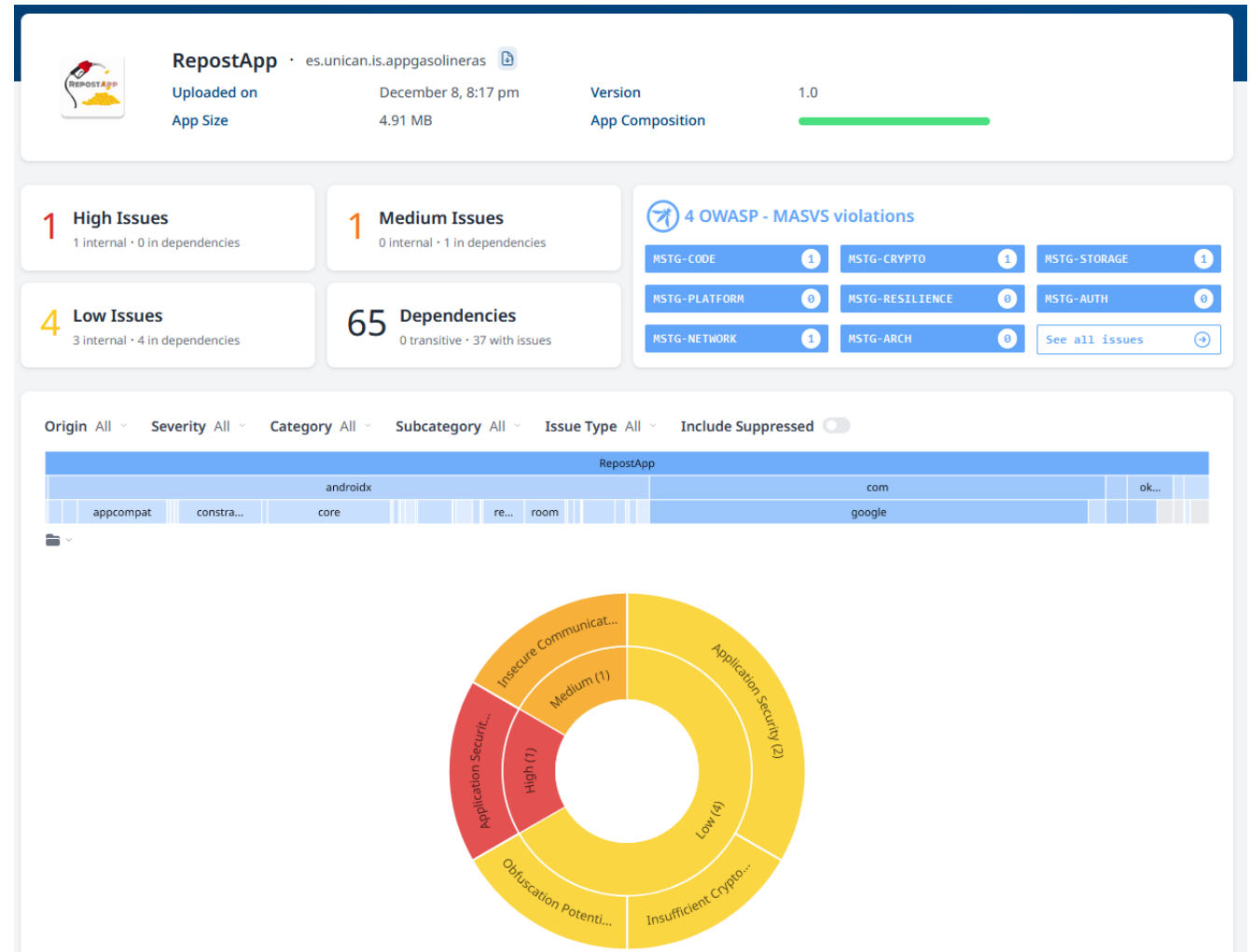
- Características principales
- Escaneo gratis de tu app
- Ventajas de crear una cuenta
- Usar AppSweep con Gradle
- Automatizar los análisis con GitHub action
- Uso de la herramienta
 - Gráfico de versiones
 - Comparador de versiones
 - PDF de análisis
 - Vista principal
 - Vista fallos
 - Vista fallo detallado
- Ventajas de la herramienta
- Tarea

Características principales

- Arreglar problemas: permite arreglar problemas de seguridad rápidamente con acciones de recomendación.
- Pruebas con confianza: el análisis se centra en problemas reales y no en falsos positivos.
- Seguridad continua: permite verificar la seguridad de forma continua mediante la integración en las herramientas DevOps.
- Herramienta de Prueba de Seguridad → crear aplicaciones móviles más seguras.

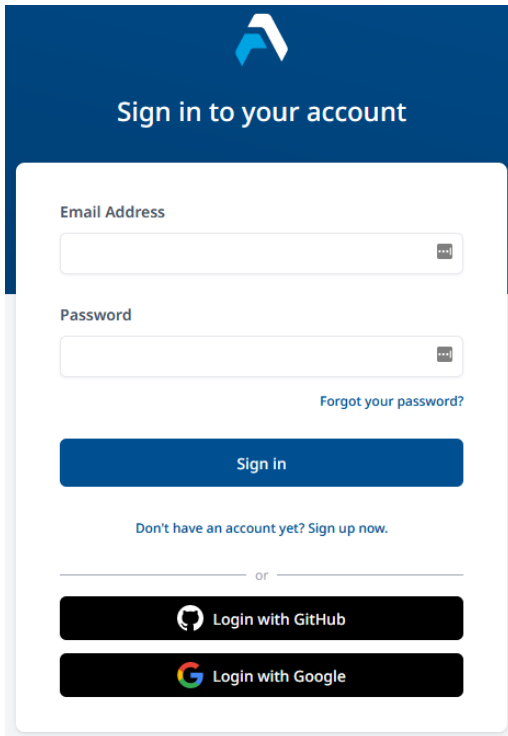
Escaneo gratis de tu app

<https://appsweep.guardsquare.com/>



Ventajas de crear una cuenta

- Crear proyectos
- Trabajar en equipo
- Línea temporal de análisis



Sign in to your account

Email Address


Password


[Forgot your password?](#)

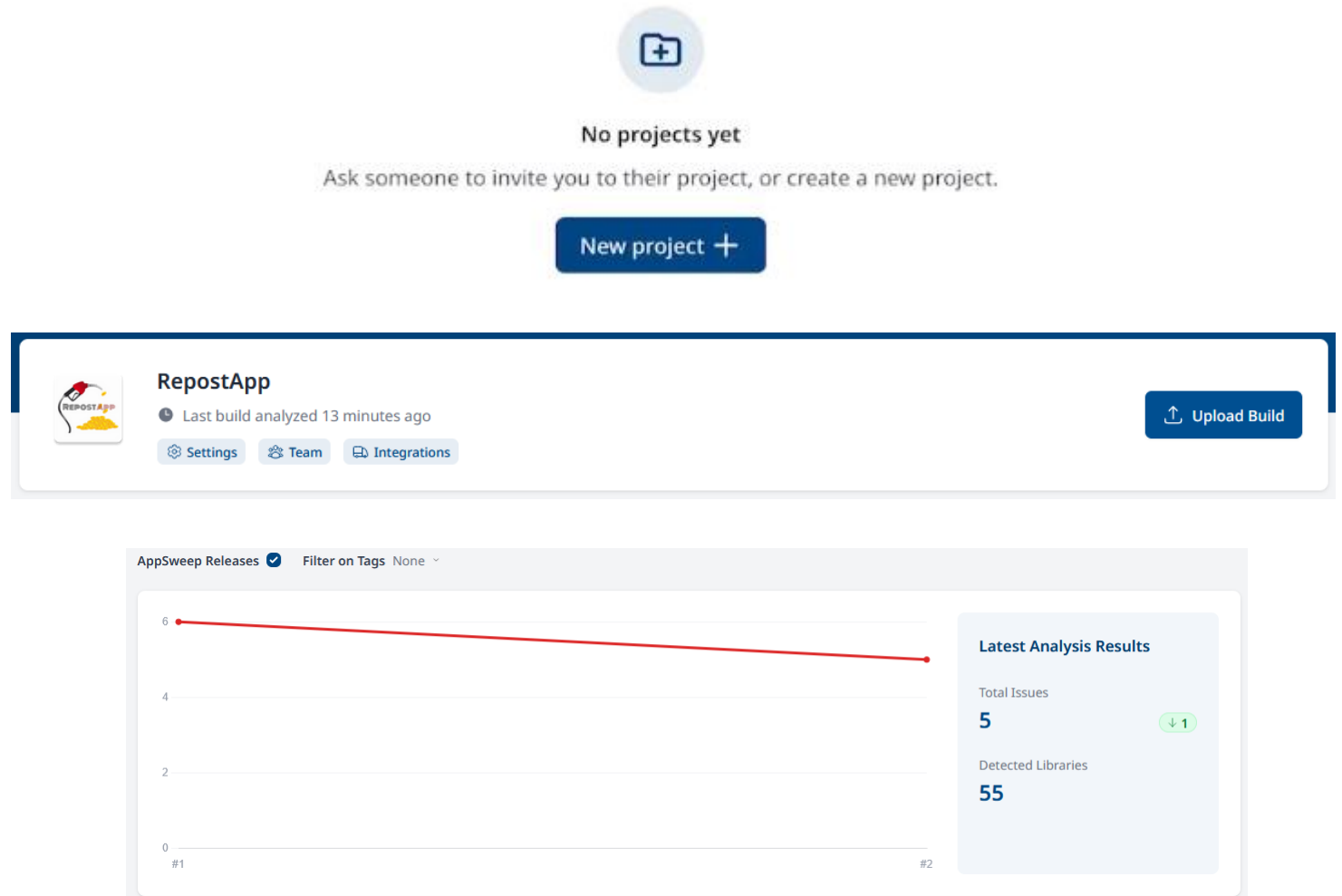
Sign in

[Don't have an account yet? Sign up now.](#)

or

 Login with GitHub

 Login with Google



Usar AppSweep con Gradle (1/3)

- Abrir build.gradle (:app) y añadir la línea roja

```
plugins {  
    id 'com.android.application'  
    id "org.sonarqube" version "3.0"  
    id "com.guardsquare.apsweep" version "latest.release"  
}
```



* Si Gradle < 7.0 : `id "com.guardsquare.apsweep" version "LATEST_RELEASE_VERSION"`

Usar AppSweep con Gradle (2/3)

- Settings -> API Keys -> New API Key



RepostApp

Last build analyzed 11 minutes ago

Settings

Team

Integrations

API Keys

These keys allow you to authenticate API requests. This is useful if you want to integrate AppSweep in your CI pipeline and upload new builds programmatically.

New API Key



API key created!

Make sure to copy your new API key and store it somewhere safe. **It will only be displayed now.** As soon as you navigate away from this page, we won't be able to retrieve the full API key again.

gs_appsweep_xZ1CecH_loZHC0W5irJLnqMbo0LtcXmffcdK3R07



Using our Gradle Plugin?

Update your environment variable

APPSWEEP_API_KEY

to

gs_appsweep_xZ1CecH_loZHC0W5irJLnqMbo0LtcXmffcdK3R07

Usar AppSweep con Gradle (3/3)

- Abrir build.gradle (:app)
- Añadir dentro del android scope tu propia API Key:

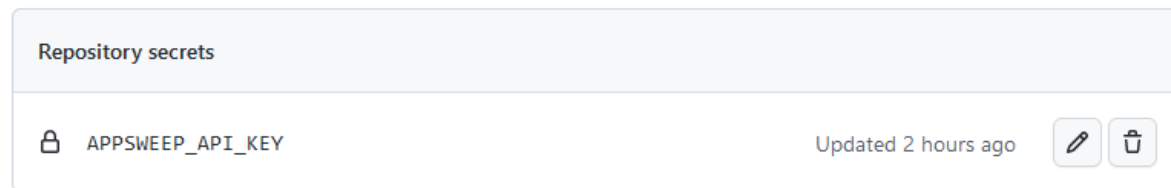
```
appsweep {  
    apiKey "TU API KEY"  
}
```

- Ejecutar desde la propia terminal en AndroidStudio:

```
./gradlew uploadToAppsweepDebug
```


Automatizar los análisis con GitHub action

- Crear un repository secret en GitHub para la API key:
 - Settings -> Secrets -> Actions -> New repository secret
 - Name: APPSWEEP_API_KEY
 - Secret: [TU API key]



- Editar fichero .yaml y añadir a Jobs (en el caso de nuestro proyecto de gasolineras):

Ejecutar analisis de AppSweep

- name: Upload app to AppSweep with Gradle
 - working-directory: ./AndroidProject
 - env:

APPSWEEP_API_KEY: \${ secrets.APPSWEEP_API_KEY }

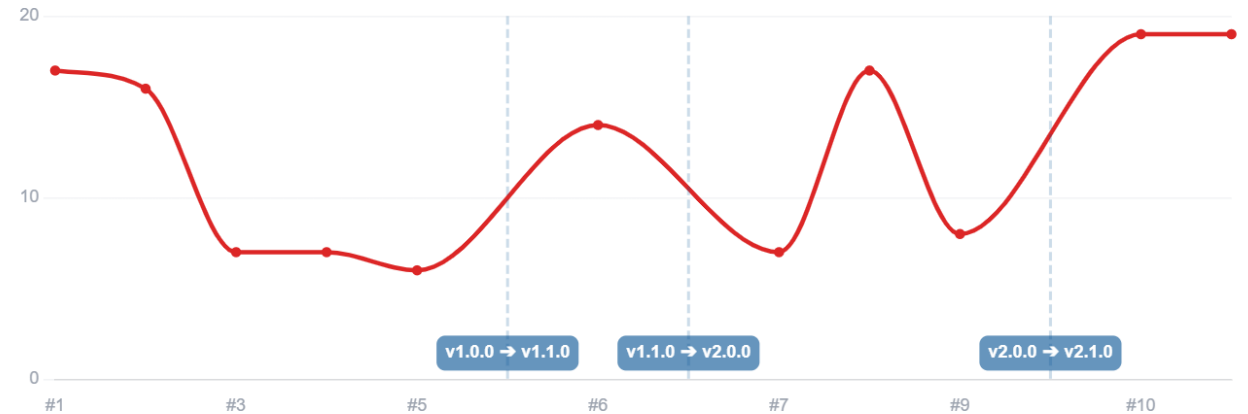
run: ./gradlew uploadToAppSweepRelease

Gráfico de versiones

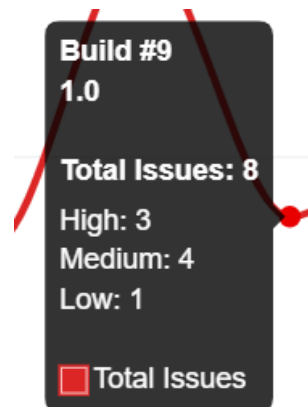
Ofrece una vista global de la evolución (en cuanto a fallos) del proyecto a lo largo de las diferentes versiones.

Permite realizar comparaciones entre versiones.

Comparing: **#9** · 1.0 · September 6, 2:14 pm · 9442f52 · [View Build](#) [Debug](#)
To base: **#10** · 1.0 · November 15, 2:58 pm · b125d37 · [View Build](#) [Debug](#)



Vista en detalle



Comparador de versiones

Selector de versiones a comparar

Compare build

#11

 with build

#10

↔ View Diff

Vista general de cambios

Issues

+ 0 resolved issues

+ 0 improved issues

- 3 new issues

- 0 degraded issues

Libraries

+ 0 added libraries

- 1 removed libraries

App Size

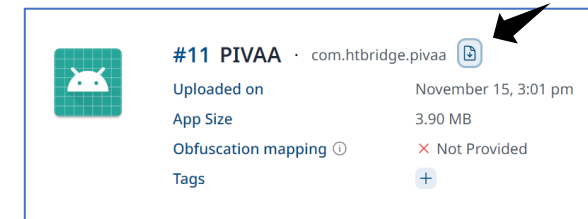
- 3.90 MB (down from 6.62 MB)

Gráfico de fallos nuevos

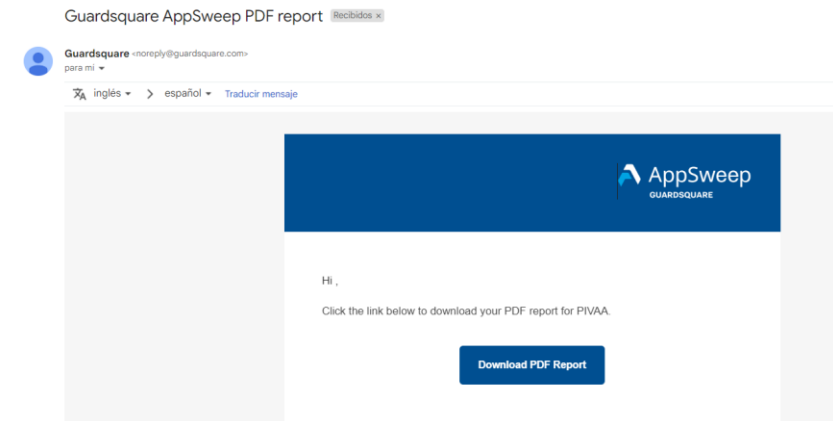


PDF de análisis

Nos da la opción de generar PDFs con un extenso análisis de calidad y seguridad.



Lo envía al correo electrónico con el que hayamos creado la cuenta



Vista principal

Resumen de fallos

5 High Issues
5 internal · 0 in dependencies

13 Medium Issues
13 internal · 0 in dependencies

1 Low Issues
1 internal · 1 in dependencies

39 Dependencies
38 transitive · 18 with issues

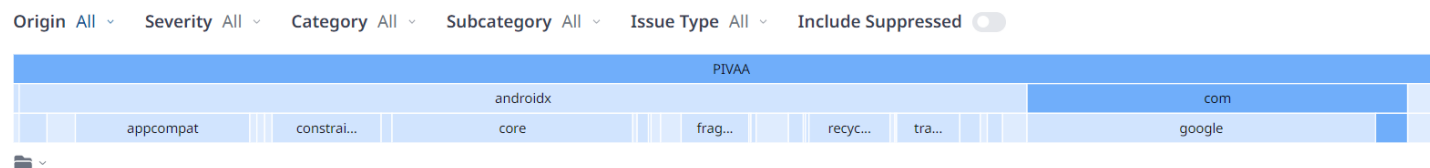
Categorizados según OWASP

 18 OWASP - MASVS violations

MSTG-CODE	1	MSTG-CRYPTO	2	MSTG-STORAGE	1
MSTG-PLATFORM	9	MSTG-RESILIENCE	0	MSTG-AUTH	0
MSTG-NETWORK	4	MSTG-ARCH	1	See all issues 	

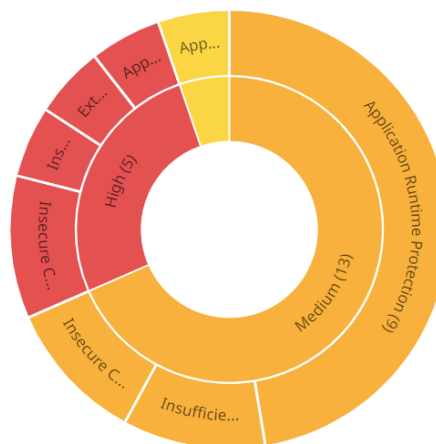
Vista fallos

Filtros por características



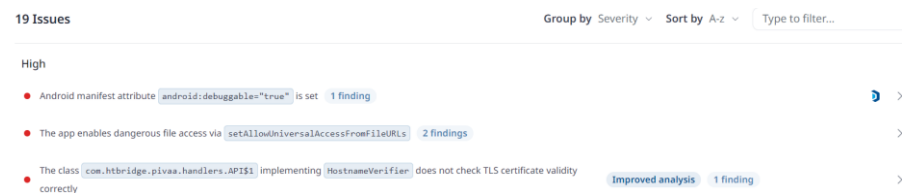
En función de su ubicación

Según el tipo de fallo



Más externo es más particular

Vista de fallos concretos



Vista fallo detallado

Explicación

< See all issues | PIVAA com.htbridge.pivaa · 1.0 · Analysed November 15, 2022 3:01 PM

High • Android manifest attribute `android:debuggable="true"` is set

The attribute `android:debuggable` is set to `true` in the app's manifest. This means that your app can be debugged using Java Wired Debugging Protocol. Using JWP, it is possible to gain full access to the Java process and execute arbitrary code in the context of a debuggable app.

Releasing an app with this flag set can lead to leakage of sensitive information and leaves the app vulnerable to debugging.

Note that setting `android:debuggable` to `false` is necessary to prevent debugging, but is not sufficient. An adversary can still connect a debugger and use it to reverse-engineer or tamper with the app's behaviour.

MSG-CODE-2

1 Finding

AndroidManifest.xml

Localización del fallo

```
<? AndroidManifest.xml

[...]  
  <uses-permission android:name="android.permission.CALL_PHONE"/>  
  <uses-permission android:name="android.permission.CAMERA"/>  
  <uses-permission android:name="android.permission.RECORD_AUDIO"/>  
  <application android:protectionLevel="dangerous" android:debuggable="true" android:allowBackup="true"  
    <activity android:name="com.htbridge.pivaa.MainActivity" android:protectionLevel="dangerous" a  
      <intent-filter>  
        <action android:name="android.intent.action.MAIN"/>  
      </intent-filter>  
    </activity>  
  </application>  
[...]
```

Solución

Recommendations








Ensure that the flag `android:debuggable` is set to `false` in your AndroidManifest.xml when building for release.

Ventajas de la Herramienta

- Herramienta intuitiva
- Testeo del software
- Recomendaciones prácticas ante los errores
- Integración de aspectos de la seguridad
- Retroalimentación completa y temprana

Tarea

- Analizar vuestros proyectos de gasolineras.
- Estudiar los problemas de seguridad detectados.
- Arreglar al menos 3 problemas.

REPOSTAPP	
	CEPSA CARRETERA 6316 KM. 10,5 Gasolina: 1,79 € Diésel: 1,89 € Distancia: 24,29 km
	REPSOL CR N-629 79,7 Gasolina: 1,77 € Diésel: 1,87 € Distancia: 37,79 km
	PETRONOR CARRETERA N-611 KM. 163,2 Gasolina: 1,74 € Diésel: 1,82 € Distancia: 33,00 km
	CAMPSA CARRETERA ARGOÑOS SOMO KM. 28,7 Gasolina: 1,75 € Diésel: 1,82 € Distancia: 24,48 km
	E.S. CARBURANTES DE ARNUERO S.L. CARRETERA CASTILLO SIETEVEILLAS KM. S/N Gasolina: 1,76 € Diésel: 1,85 € Distancia: 25,44 km
	G2 CALLE BOQ, 52 Gasolina: 1,74 € Diésel: 1,84 € Distancia: 3,93 km
	AREA DE SERVICIO LA PALMERA CALLE PROSPERIDAD, 61 Gasolina: 1,74 € Diésel: 1,84 € Distancia: 3,93 km