

TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN

INGENERIA EN DESARROLLO Y GESTION DE SOFTWARE

SEGURIDAD EN EL DESARROLLO DE APLICACIONES

Escaneo de Código SonarQube

Integrantes:

Alba Nájera Susana

Castillo Sanchez Jose Guadalupe

Flores Montoya Ricardo Daniel

Limon De La Cruz Luz Elena

Carlos Iván Mercado Marín

Salas Flores Miguel Angel

Talamantes Castañeda Angela María

Grado y grupo: IDGS-8-A-11

Catedrático: Miguel Antonio Araujo Gonzales

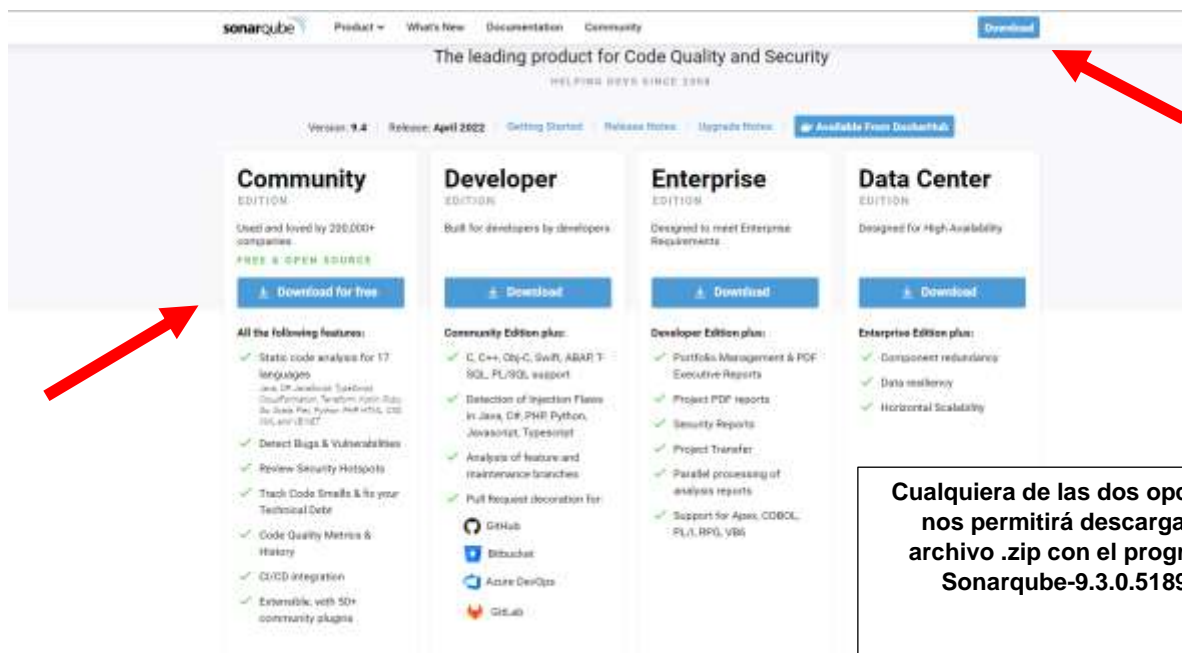
Fecha de entrega: 04-04-2022

Evaluación/Escaneo de código Fuente con Sonarqube

Para realizar las respectivas pruebas del sitio utilizaremos la herramienta de evaluación de código fuente Sonarqube, Es software libre y usa diversas herramientas de análisis estático de código fuente como Checkstyle, PMD o FindBugs para obtener métricas que pueden ayudar a mejorar la calidad del código de nuestro programa.

Proceso de instalación y configuración Sonarqube

Como primer paso del proceso de instalación debemos dirigirnos al sitio web de sonarqube en el cual descargaremos el archivo.zip el cual contiene nuestro programa



The screenshot shows the Sonarqube website with a navigation bar at the top. A red arrow points to the 'Download' button in the top right corner. Below the navigation bar, the main heading reads 'The leading product for Code Quality and Security'. A second red arrow points to the 'Download for free' button under the 'Community EDITION' section. The website lists four editions: Community, Developer, Enterprise, and Data Center. Each edition has a list of features and a 'Download' button. The Community Edition is highlighted as 'FREE & OPEN SOURCE'.

Community EDITION
Used and loved by 200,000+ companies
FREE & OPEN SOURCE
[Download for free](#)

Developer EDITION
Built for developers by developers
[Download](#)

Enterprise EDITION
Designed to meet Enterprise Requirements
[Download](#)

Data Center EDITION
Designed for High Availability
[Download](#)

All the following features:

- ✓ Static code analysis for 17 languages
Java, C#, JavaScript, TypeScript, C/C++, PHP, Python, Kotlin, Swift, Go, Ruby, Perl, R, Rust, C#, C++
- ✓ Detect Bugs & Vulnerabilities
- ✓ Review Security Hotspots
- ✓ Track Code Smells & fix your Technical Debt
- ✓ Code Quality Metrics & History
- ✓ CI/CD integration
- ✓ Extensible, with 50+ community plugins

Community Edition plus:

- ✓ C, C++, Obj-C, Swift, ABAP, T-SQL, PL/SQL, esport
- ✓ Detection of Injection Flaws in Java, C#, PHP, Python, JavaScript, TypeScript
- ✓ Analysis of feature and maintenance branches
- ✓ Pull Request decoration for GitHub, Bitbucket, Azure DevOps, GitLab

Developer Edition plus:

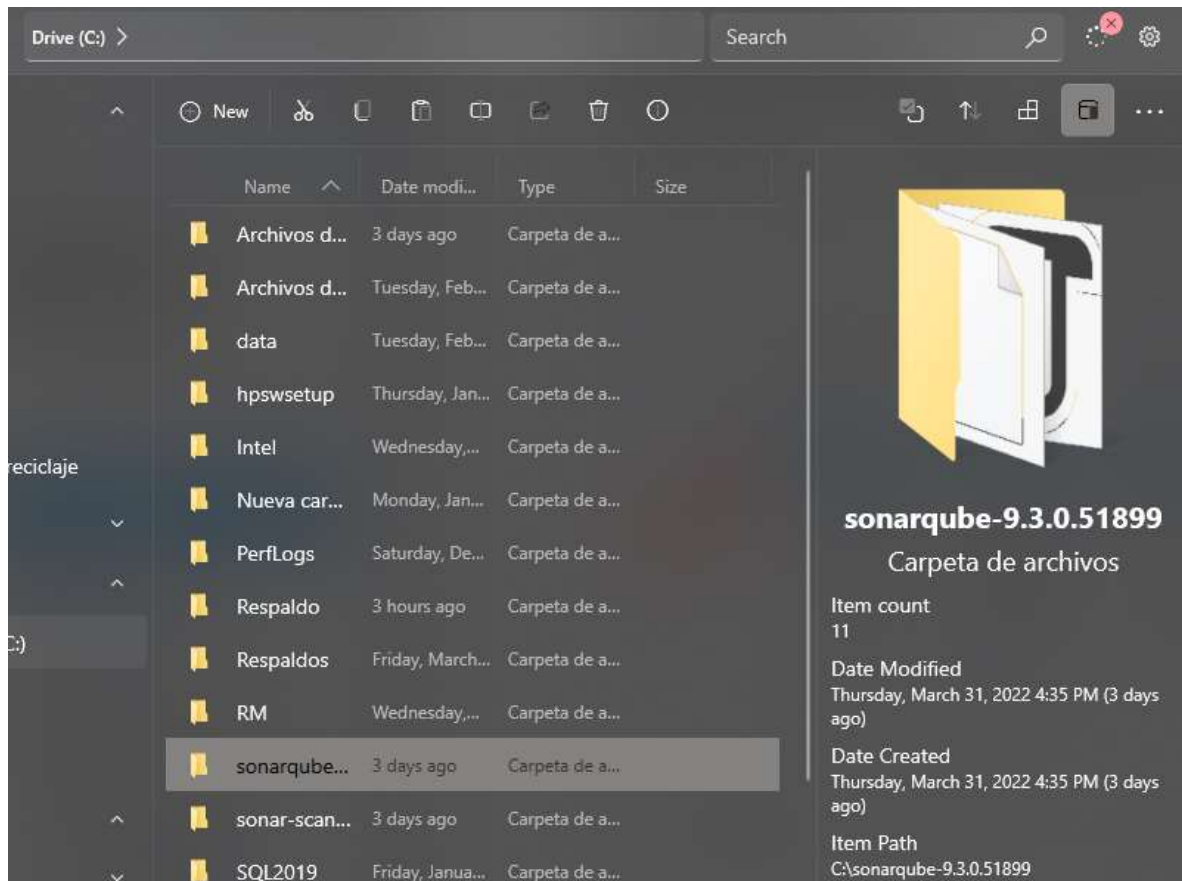
- ✓ Portfolio Management & PDF Executive Reports
- ✓ Project PDF reports
- ✓ Security Reports
- ✓ Project Transfer
- ✓ Parallel processing of analysis reports
- ✓ Support for Apex, COBOL, PL/SQL, RPG, VB6

Enterprise Edition plus:

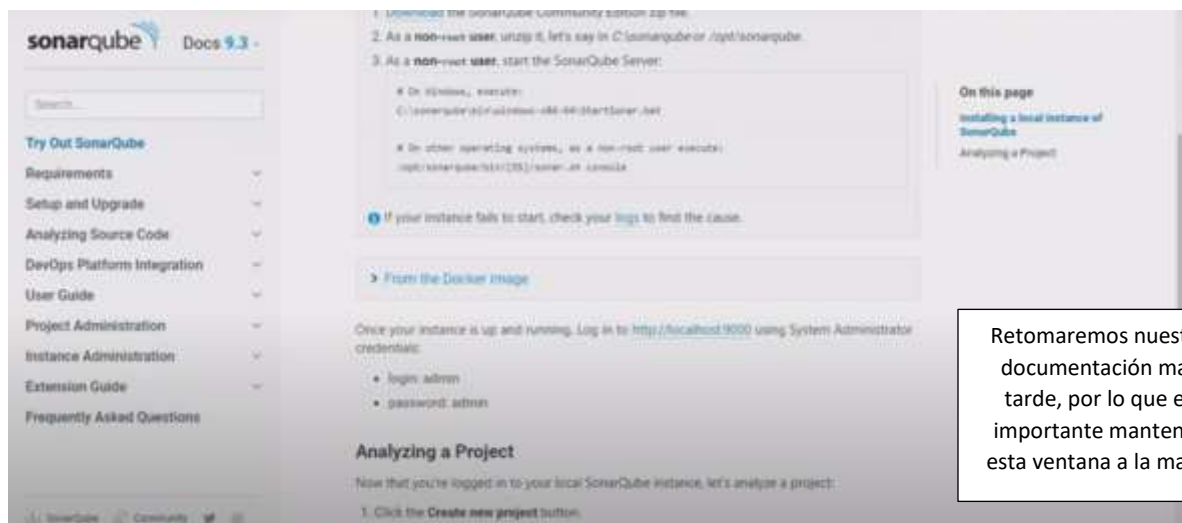
- ✓ Component redundancy
- ✓ Data resiliency
- ✓ Horizontal Scalability

Cualquiera de las dos opciones nos permitirá descargar el archivo .zip con el programa Sonarqube-9.3.0.51899

Una vez instalado lo extraeremos y copiamos el archivo en una unidad de disco



Después de copiar el archivo nos dirigiremos a la documentación de sonarqube



La documentación nos pedirá ejecutar un archivo llamado StartSonar.bat, para ello viajaremos por las carpetas hasta llegar a ese archivo .bat, es importante elegir la opción de acuerdo a nuestro sistema operativo, pues de ello depende el correcto funcionamiento de este proceso.

```
Microsoft Windows [Versión 10.0.19044.1500]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Jose Castillo>CD ..

C:\Users>CD ..

C:\>cd sonarqube-9.3.0.51899

C:\sonarqube-9.3.0.51899>cd bin

C:\sonarqube-9.3.0.51899\bin>dir/w
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 42DE-978A

Directorio de C:\sonarqube-9.3.0.51899\bin

[.]          [..]          [jsw-license]          [linux-x86-64]          [macosx-universal-64]
[windows-x86-64]
            0 archivos            0 bytes
            6 dirs 11,905,536,000 bytes libres

C:\sonarqube-9.3.0.51899\bin>cd windows-x86-64

C:\sonarqube-9.3.0.51899\bin\windows-x86-64>dir/w
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 42DE-978A

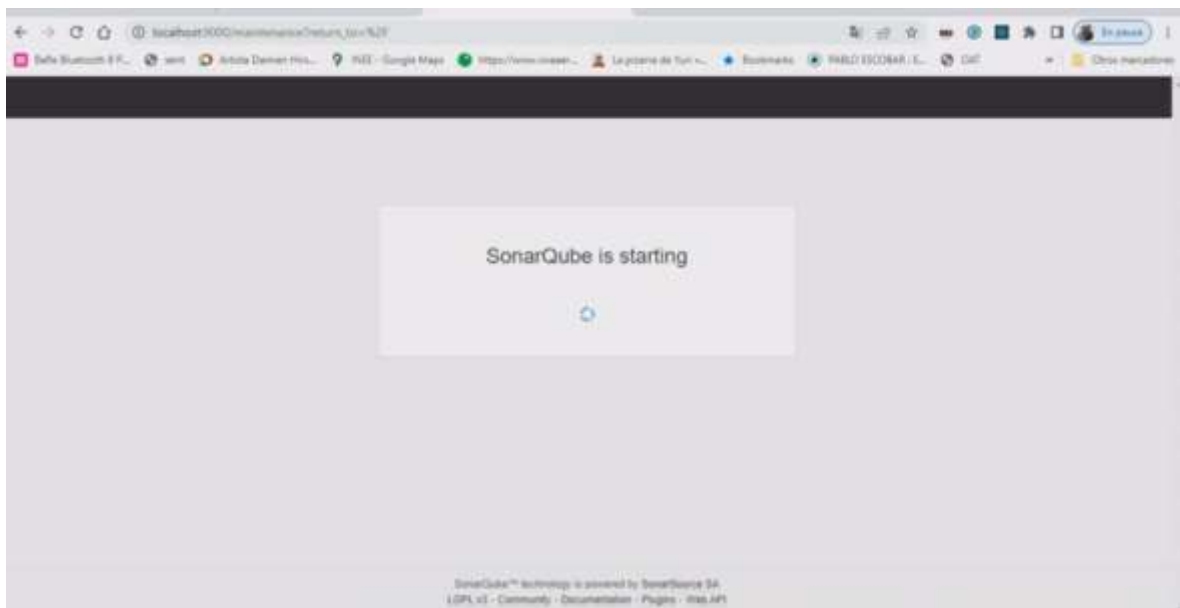
Directorio de C:\sonarqube-9.3.0.51899\bin\windows-x86-64

[.]          [..]          [lib]          StartNTService.bat  StartSonar.bat
stopNTService.bat  wrapper.exe
            4 archivos            224,469 bytes
            3 dirs 11,904,712,704 bytes libres
```

Una vez que nos encontramos dentro de la carpeta Windows-x86-64 ejecutaremos el StartSonar.bat para levantar los respectivos servicios

```
C:\sonarqube-9.3.0.51899\bin\windows-x86-64>StartSonar.bat
wrapper --> Wrapper Started as Console
wrapper Launching a JVM...
jvm 1 Wrapper (Version 3.2.3) http://wrapper.tanukisoftware.org
jvm 1 Copyright 1999-2006 Tanuki Software, Inc. All Rights Reserved.
jvm 1
jvm 1 2022.04.04 12:47:40 INFO app[[o.s.a.AppFileSystem] Cleaning or creating temp directory C:\sonarqube-9.3.0.51899\temp
jvm 1 2022.04.04 12:47:40 INFO app[[o.s.a.es.EsSettings] Elasticsearch listening on [HTTP: 127.0.0.1:9001, TCP: 127.0.0.1:54175]
jvm 1 2022.04.04 12:47:40 INFO app[[o.s.a.ProcessLauncherImpl] Launch process[[key='es', ipcIndex=1, logFileNa
mePrefix=es]] from [C:\sonarqube-9.3.0.51899\elasticsearch: D:\Program Files\Java\jdk-11.0.13\bin\java -XX:+UseG1GC
-Djava.io.tmpdir=C:\sonarqube-9.3.0.51899\temp -XX:ErrorFile=../logs/es_hs_err_pid%p.log -Des.networkaddress.cache.ttl
1=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=true -Dfile.encoding=U
TF-8 -Djna.nosys=true -Djna.tmpdir=C:\sonarqube-9.3.0.51899\temp -XX:-OmitStackTraceInFastThrow -Dio.netty.noUnsafe=tr
ue -Dio.netty.noKeySetOptimization=true -Dio.netty.recycler.maxCapacityPerThread=0 -Dio.netty allocator.numDirectAren
as=0 -Dlog4j.shutdownHookEnabled=false -Dlog4j2.disable.jmx=true -Dlog4j2.formatMsgNoLookups=true -Djava.locale.provi
ders=COMPAT -Dcom.redhat.fips=false -Xmx512m -Xms128m -XX:MaxDirectMemorySize=256m -XX:+HeapDumpOnOutOfMemoryError -D
elasticsearch -Des.path.home=C:\sonarqube-9.3.0.51899\elasticsearch -Des.path.conf=C:\sonarqube-9.3.0.51899\temp\conf
\es -cp lib/* org.elasticsearch.bootstrap.Elasticsearch
jvm 1 2022.04.04 12:47:40 INFO app[[o.s.a.SchedulerImpl] Waiting for Elasticsearch to be up and running
jvm 1 2022.04.04 12:47:52 INFO app[[o.s.a.SchedulerImpl] Process[es] is up
jvm 1 2022.04.04 12:47:52 INFO app[[o.s.a.ProcessLauncherImpl] Launch process[[key='web', ipcIndex=2, logFileNa
mePrefix=web]] from [C:\sonarqube-9.3.0.51899]: D:\Program Files\Java\jdk-11.0.13\bin\java -Dfile.encoding=UTF-8 -Djava.io.tmpdir=C:\sonarqube-9.3.0.51899\temp -XX:-OmitStackTraceInFastThrow --add-opens=java.
base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --ad
d-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED --add-exports=java.base/jdk.internal.ref=ALL-UNNAMED --add-opens=java.
base/java.nio=ALL-UNNAMED --add-opens=java.base/sun.nio.ch=ALL-UNNAMED --add-opens=java.management/sun.management=ALL
-UNNAMED --add-opens=jdk.management/com.sun.management.internal=ALL-UNNAMED -Dcom.redhat.fips=false -Xmx512m -Xms128m
-XX:+HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localhost[127.*][:11] -cp ./lib/sonar-application-9.3.0.51899.j
ar;C:\sonarqube-9.3.0.51899\lib\jdbc\h2-1.4.199.jar org.sonar.server.app.WebServer C:\sonarqube-9.3.0.51899\temp\s
q-process17137023718909930166properties
jvm 1 2022.04.04 12:48:01 INFO app[[o.s.a.SchedulerImpl] Process[web] is up
jvm 1 2022.04.04 12:48:01 INFO app[[o.s.a.ProcessLauncherImpl] Launch process[[key='ce', ipcIndex=3, logFileNa
mePrefix=ce]] from [C:\sonarqube-9.3.0.51899]: D:\Program Files\Java\jdk-11.0.13\bin\java -Djava.awt.headless=true -D
file.encoding=UTF-8 -Djava.io.tmpdir=C:\sonarqube-9.3.0.51899\temp -XX:-OmitStackTraceInFastThrow --add-opens=java.ba
se/java.util=ALL-UNNAMED --add-exports=java.base/jdk.internal.ref=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNN
AMED --add-opens=java.base/java.nio=ALL-UNNAMED --add-opens=java.base/sun.nio.ch=ALL-UNNAMED --add-opens=java.managem
ent/sun.management=ALL-UNNAMED --add-opens=jdk.management/com.sun.management.internal=ALL-UNNAMED -Dcom.redhat.fips=f
alse -Xmx512m -Xms128m -XX:+HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localhost[127.*][:11] -cp ./lib/sonar-app
lication-9.3.0.51899.jar;C:\sonarqube-9.3.0.51899\lib\jdbc\h2-1.4.199.jar org.sonar.ce.app.CeServer C:\sonarqube-9
.3.0.51899\temp\sq-process18161810719765018838properties
jvm 1 2022.04.04 12:48:05 INFO app[[o.s.a.SchedulerImpl] Process[ce] is up
jvm 1 2022.04.04 12:48:05 INFO app[[o.s.a.SchedulerImpl] SonarQube is up
```

en nuestro explorador colocaremos "localhost:9000", esto en el puerto 9000, pues sonarqube por defecto esta a la escucha a través de este puerto



Agregaremos las credenciales, por defecto Sonarqube nos proporciona admin y admin en cada campo



Podemos cambiar las credenciales por seguridad

Update your password

This account should not use the default password.

Enter a new password

All fields marked with * are required

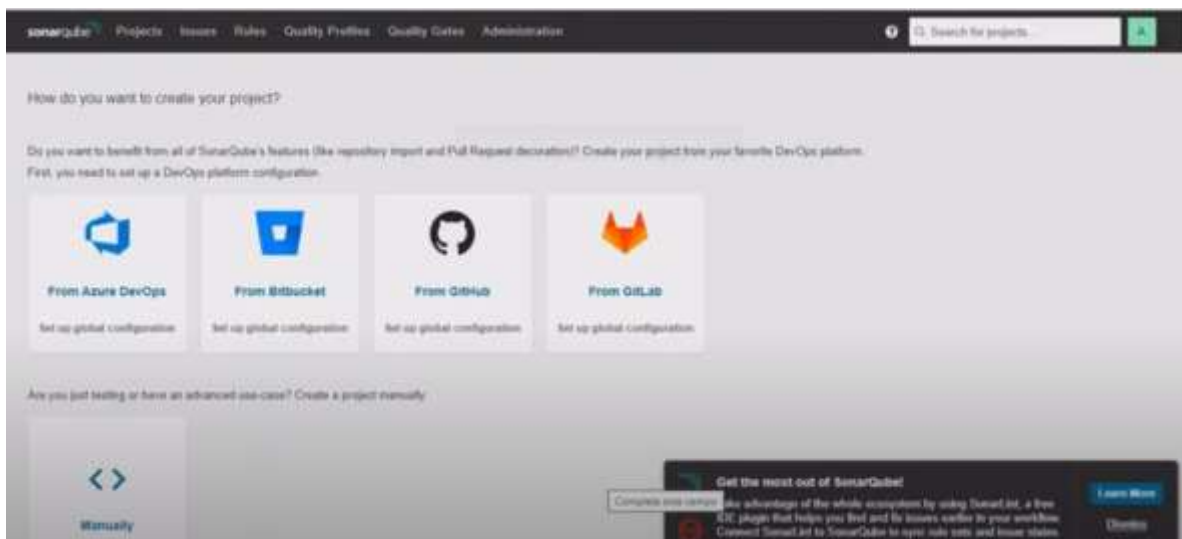
Old Password *

New Password *

Confirm Password *

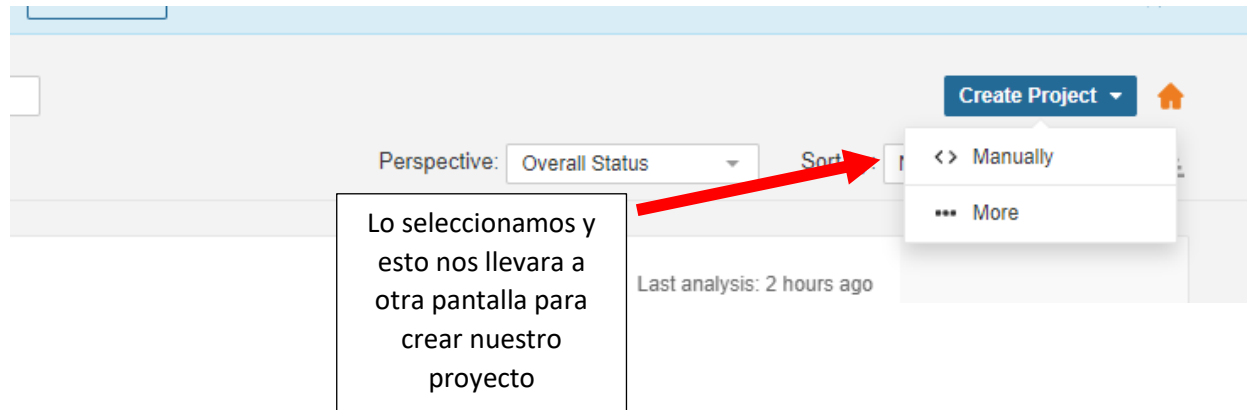
Update

Y aquí tenemos la aplicación de sonarqube y con ello estaremos listos para empezar a escanear el código fuente de nuestro sistema

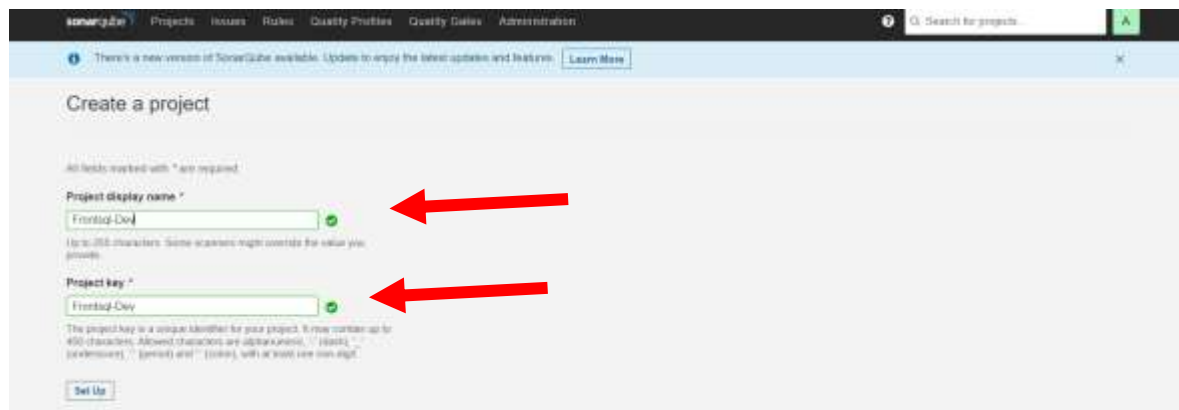


Creacion de proyecto Sonarqube

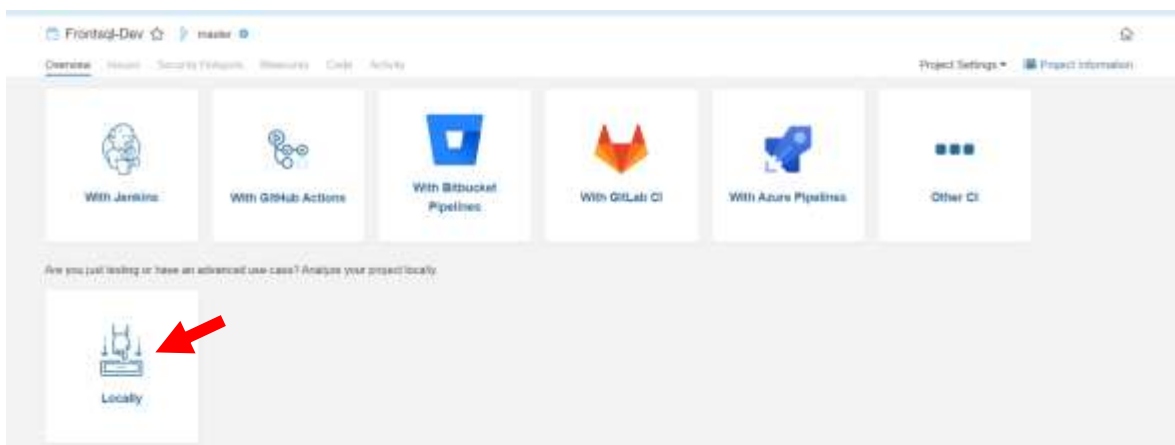
Damos click en “create project” y seleccionamos “Manually”



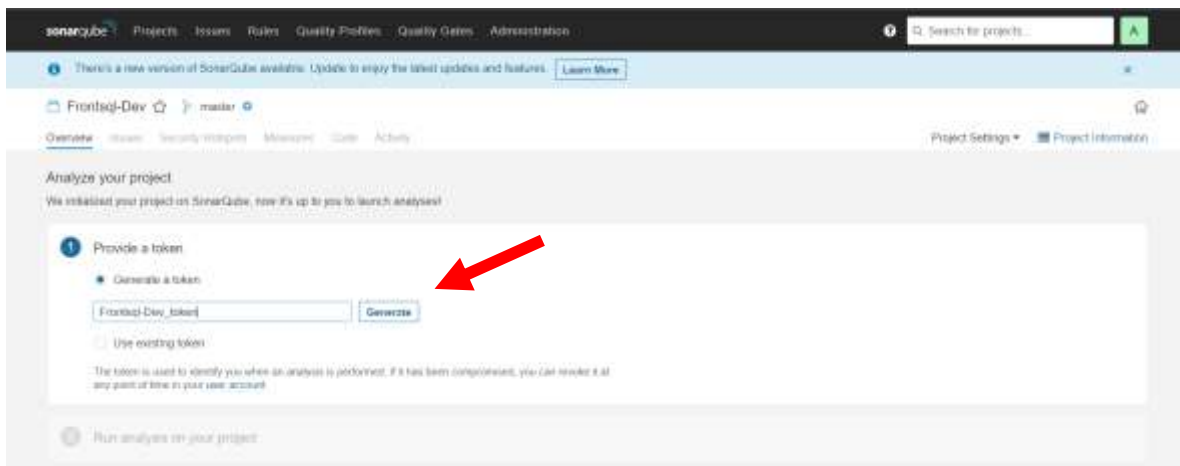
Ingresaremos en nombre que llevará nuestro proyecto, el cual nos deberá de quedar como lo muestra la imagen



Y daremos click en Set Up. En la siguiente pantalla que nos muestra sonarqube elegiremos la opción Localy



En esta pantalla generaremos el token de nuestro proyecto, ingresaremos el nombre que llevara el token y daremos click en Generate.



Damos click en continuar

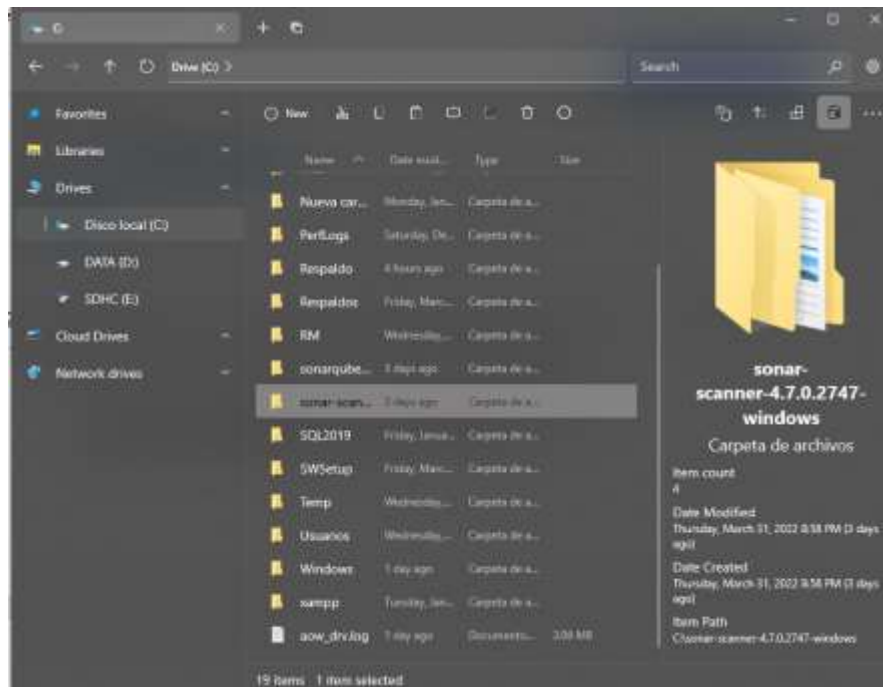


En el siguiente paso seleccionares el tipo de código del proyecto a analizar y también nuestro respectivo sistema operativo



Regresamos a la documentación de sonarqube y descargamos el paquete de Windows 64-bit, y haremos lo mismo, lo copiaremos a la misma unidad de disco

Nota: es importante agregar en el path la dirección de la carpeta bin de sonarqube-9.3.0.51899 y sonar-scanner-4.7.0.2747-windows



Copiaremos las líneas de código las cuales nos permitirán el escaneo de los archivos donde se encuentra nuestro código

Configuring your project

Create a configuration file in your project's root directory called `sonar-project.properties`

```
# must be unique in a given SonarQube instance
sonar.projectKey=my:project

# --- optional properties ---

# defaults to project key
sonar.projectName=my project
# defaults to "not provided"
sonar.projectVersion=1.0

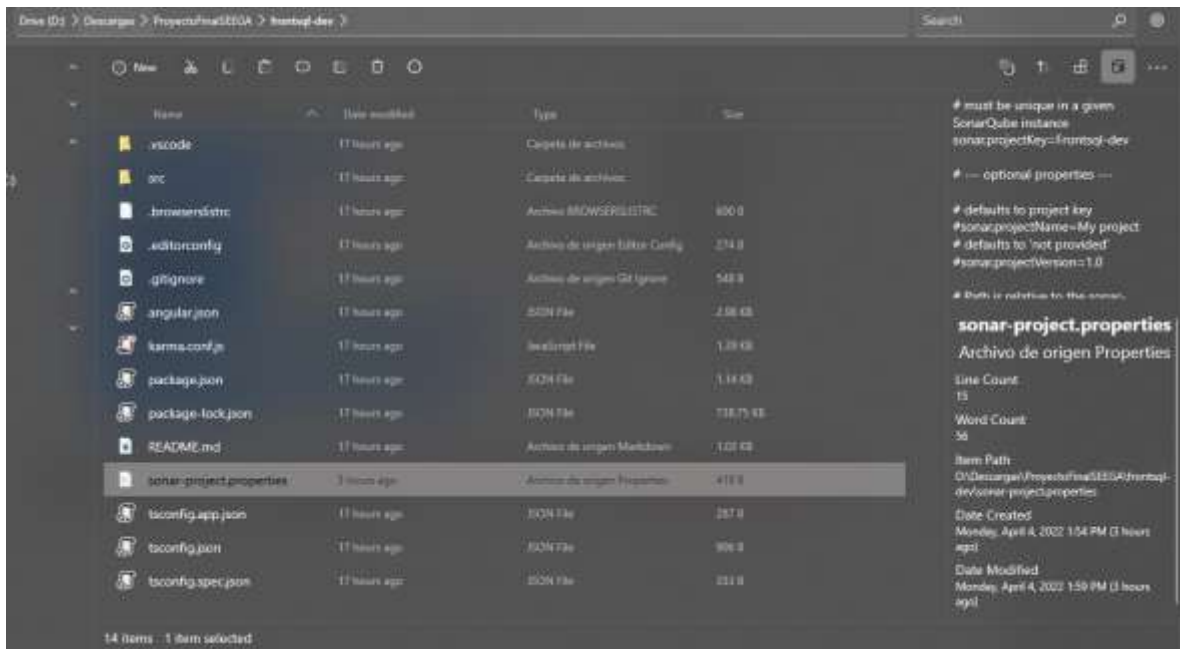
# Path is relative to the sonar-project.properties file. Defaults to .
sonar.sources=.

# Encoding of the source code. Default is default system encoding
sonar.sourceEncoding=UTF-8
```

On this page

- [Configuring your project](#)
- [Running SonarScanner from the zip file](#)
- [Running SonarScanner from the Docker image](#)
- [Scanning C, C++, or ObjectiveC Projects](#)
- [Sample Projects](#)
- [Alternatives to sonar-project.properties](#)
- [Alternate Analysis Directory](#)
- [Advanced Docker Configuration](#)
- [Troubleshooting](#)

Crearemos dicho archivo y lo guardaremos con el nombre `sonar-project.properties`, todo esto en la carpeta que se quiera escanear, nos quedara algo así:



Abriremos con un editor y pegamos el contenido, agregamos el nombre de nuestro proyecto

```

1 # must be unique in a given SonarQube instance
2 sonar.projectKey=Frontsql-Dev
3
4 # --- optional properties ---
5
6 # defaults to project key
7 #sonar.projectName=My project
8 # defaults to 'not provided'
9 #sonar.projectVersion=1.0
10
11 # Path is relative to the sonar-project.properties file. Defaults to .
12 #sonar.sources=.
13
14 # Encoding of the source code. Default is default system encoding
15 #sonar.sourceEncoding=UTF-8

```

Regresamos a sonarqube y copiamos la instrucción de como analizar el proyecto



Abrimos una terminal, mediante la cual nos posicionaremos en la carpeta a analizar

```
D:\Descargas>cd ProyectoFinalSEGA

D:\Descargas\ProyectoFinalSEGA>dir/w
El volumen de la unidad D es DATA
El número de serie del volumen es: 0A68-002F

Directorio de D:\Descargas\ProyectoFinalSEGA

[.]                [..]                [backsql-master] [frontsql-dev]
0 archivos          0 bytes
4 dirs  201,067,134,976 bytes libres

D:\Descargas\ProyectoFinalSEGA>cd frontsql-dev

D:\Descargas\ProyectoFinalSEGA\frontsql-dev>dir/w
El volumen de la unidad D es DATA
El número de serie del volumen es: 0A68-002F

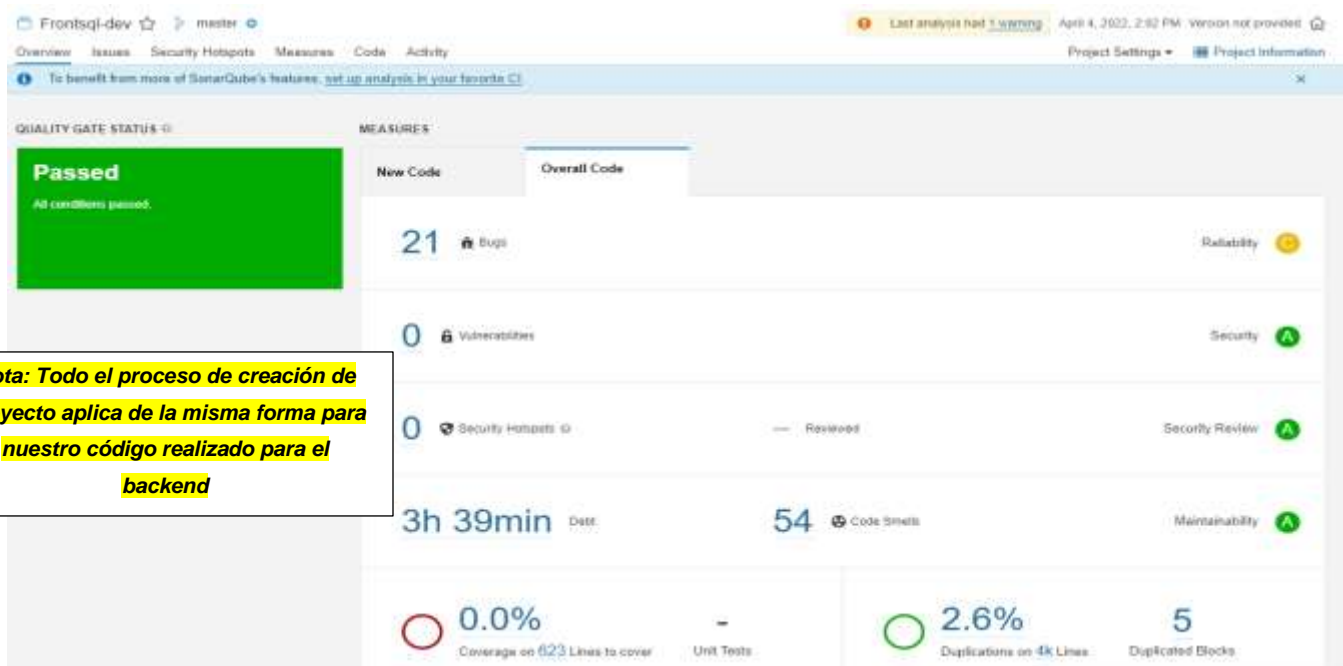
Directorio de D:\Descargas\ProyectoFinalSEGA\frontsql-dev

[.]                [..]                .editorconfig
.gitignore          [.vscode]                karma.conf.js
package-lock.json  package.json              README.md
[src]               tsconfig.app.json          tsconfig.json
12 archivos        760,541 bytes
4 dirs  201,067,134,976 bytes libres
```

Una vez dentro de ella pegaremos la instrucción que nos proporciona sonarquebe, damos ENTER y el escaneo inicia

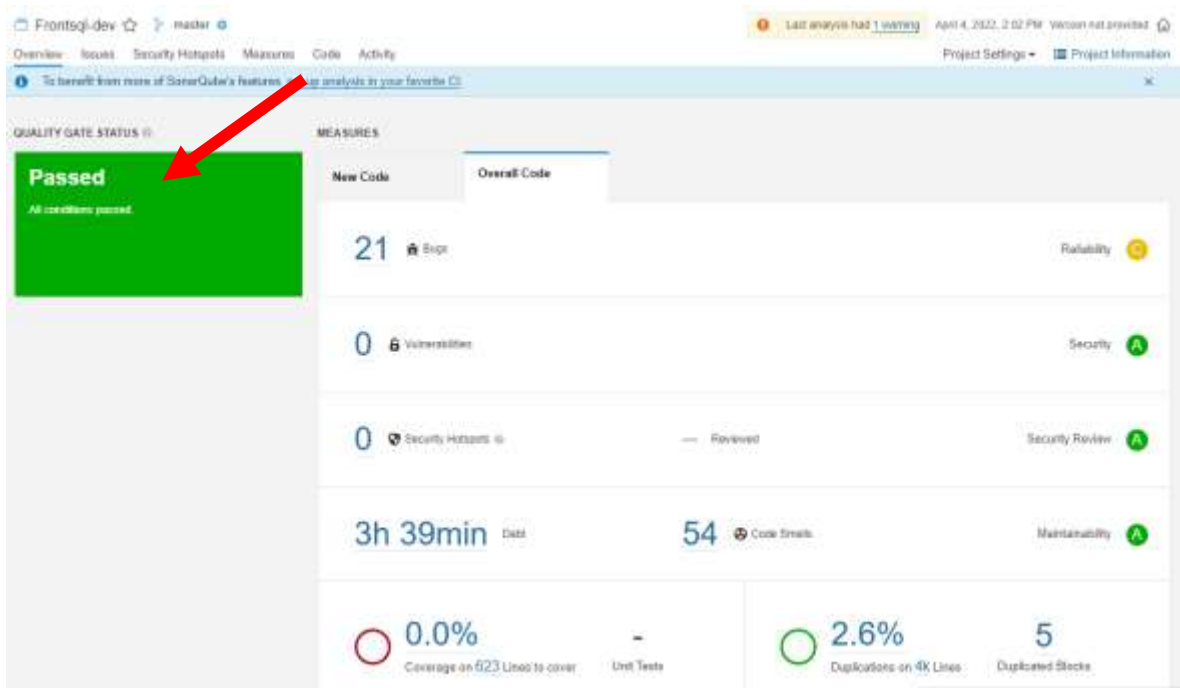
[illegible]

Una vez terminado el escaneo nos saltara una pestaña con los resultados del análisis de nuestro código.



Resultado de Análisis de código

Sonarqube nos muestra el apartado de Quality Gate la cual tiene dos valores, los cuales son: passed y failed, si nos muestra el primer valor es porque nuestro código paso todas las condiciones del análisis



Issues

Nos muestran un problema cada vez que un fragmento de código no cumple con una regla de codificación antes definida, estas reglas se definen a través de los quality gate,

En ella encontramos 3 tipos de problemas

- bugs
- vulnerability
- code smell

Encontraremos la gravedad del problema la cual se divide en 5 tipos de severidades, las cuales son:

- Blocker

- Critical
- Major
- Minor
- Info

Frontsql-dev master

Overview Issues Security Hotspots Measures Code Activity

My Issues All Bulk Changes

1 / 75 Issues 5h

Filters

Type

- Bug 21
- Vulnerability 0
- Code Smell 54

Severity

- Blocker 0
- Critical 3
- Major 29
- Minor 43
- Info 0

Scope

Resolution

Status

Security Category

Creation Date

Language

Rule

Tag

Directory

File

Assignee

src/app/component.css

Unexpected empty source. Why is this an issue? 4 hours ago

Code Smell Major Open Not assigned 1min effort Comment

src/app/module.ts

"@angular/forms" import is duplicated. Why is this an issue? 4 hours ago

Code Smell Minor Open Not assigned 1min effort Comment

src/app/auth/login/login.component.ts

Remove this unused import of 'FormControl'. Why is this an issue? 4 hours ago

Code Smell Minor Open Not assigned 2min effort Comment

Remove this unused import of 'Validators'. Why is this an issue? 4 hours ago

Code Smell Minor Open Not assigned 2min effort Comment

Remove this unused import of 'FormGroup'. Why is this an issue? 4 hours ago

Code Smell Minor Open Not assigned 2min effort Comment

Unexpected empty method 'ngOnInit'. Why is this an issue? 4 hours ago

Code Smell Critical Open Not assigned 3min effort Comment

src/app/components/header/header.component.css

Unexpected empty source. Why is this an issue? 4 hours ago

Code Smell Major Open Not assigned 1min effort Comment

src/app/components/home/dashboard/dashboard.component.css

Resultados Front-end

A continuación, se muestran los resultados del análisis de código realizado en el apartado Front-end de nuestro sistema

Bugs

Numero de bugs:21

Este apartado se pueden mejorar los resultados corrigiendo los bugs encontrados para una mejor experiencia en nuestro sistema

```
30     </div>
31     <div *ngIf="divmostras == 1">
32         <div>
33             <h3 class="border border-danger p-3" style="color: red">
34                 Sin Tareas En Este Proyecto
35             </h3>
36         </div>
37     </div>
38     <div *ngIf="divmostras == 2">
39         <table class="table table-dark table-striped">
40
41         <thead>
42             <tr>
43                 <th scope="col">Tareas</th>
44                 <th scope="col">Descripcion</th>
45                 <th scope="col">Fecha de entrega</th>
46                 <th scope="col">Estado Actual</th>
47                 <th scope="col">Nuevo Estado</th>
48             </tr>
49         </thead>
50         <tbody *ngFor="let tarea of listatareas; count as C">
```

Add a description to this table. Why is this an issue? 4 hours ago • L39

Bug • Minor • Open • Not assigned • 5min effort Comment access@itfy.wcag2-a

Vulnerability

Numero de vulnerabilidades: 0

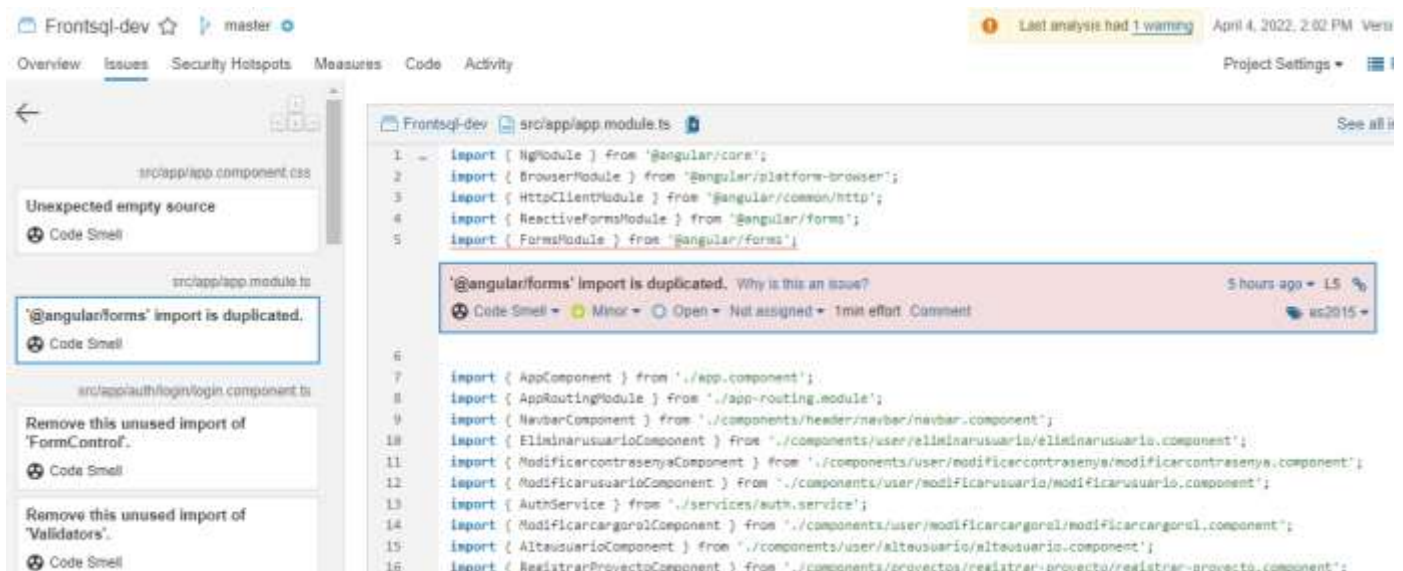
En este apartado de vulnerabilidades es en el que mas estamos orgullosos, pues en el estas son nulas.



Code Smell

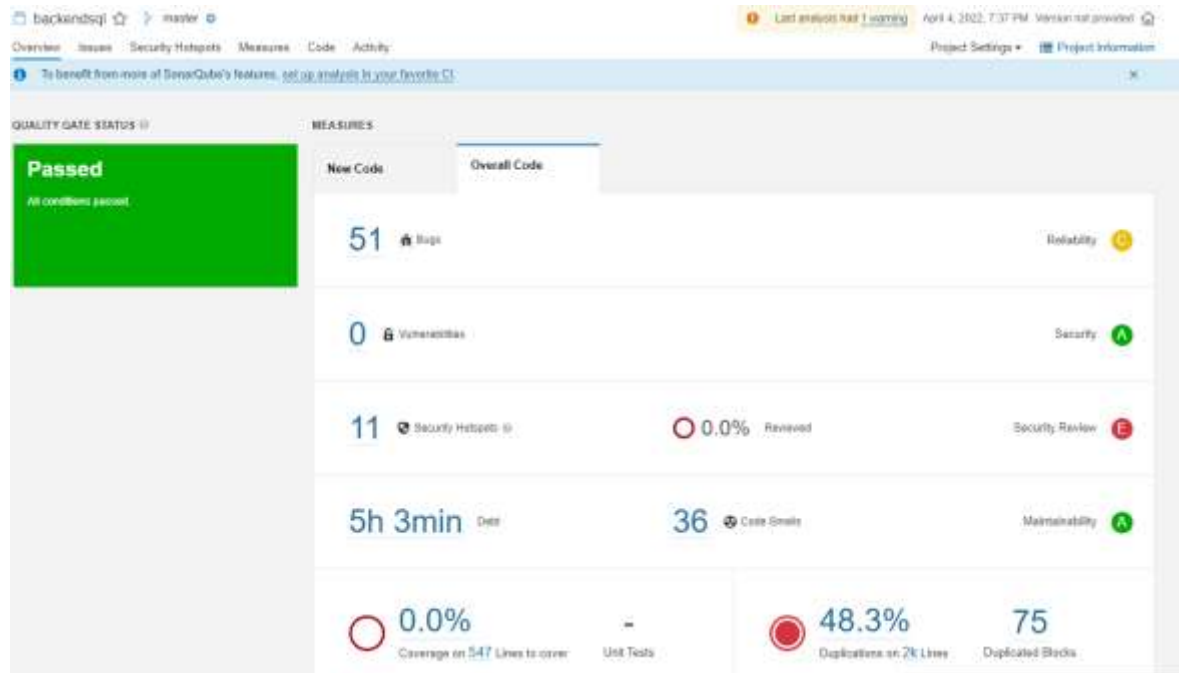
Numero de Code Smells: 54

Si bien los olores de código no son algo de que preocuparse tanto, el corregirlos y/o eliminarlos nos ayuda a que los demás desarrolladores entiendan nuestro código pues al corregirlo, eliminamos aspectos como variables duplicadas, valores innecesarios., etc y esto por consecuente nos ayuda a llevar una excelente mantenibilidad del código.



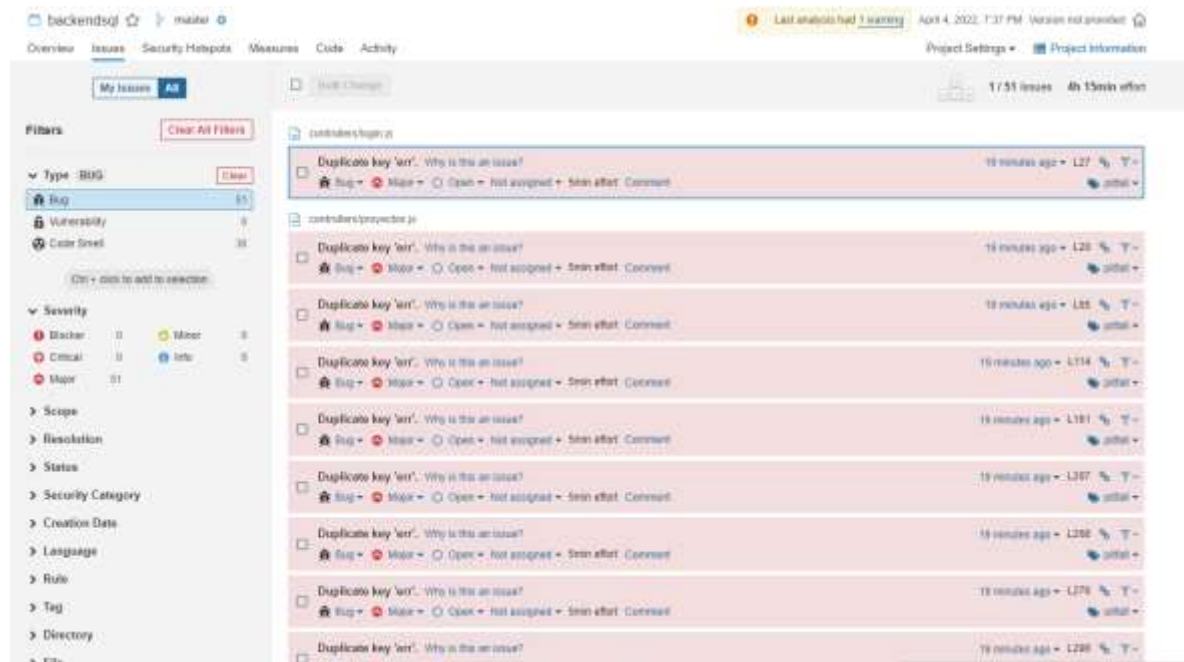
Resultados Back-end

A continuación, se muestran los resultados del análisis de código realizado en el apartado Back-end de nuestro sistema



Bugs

Numero de Bugs:51



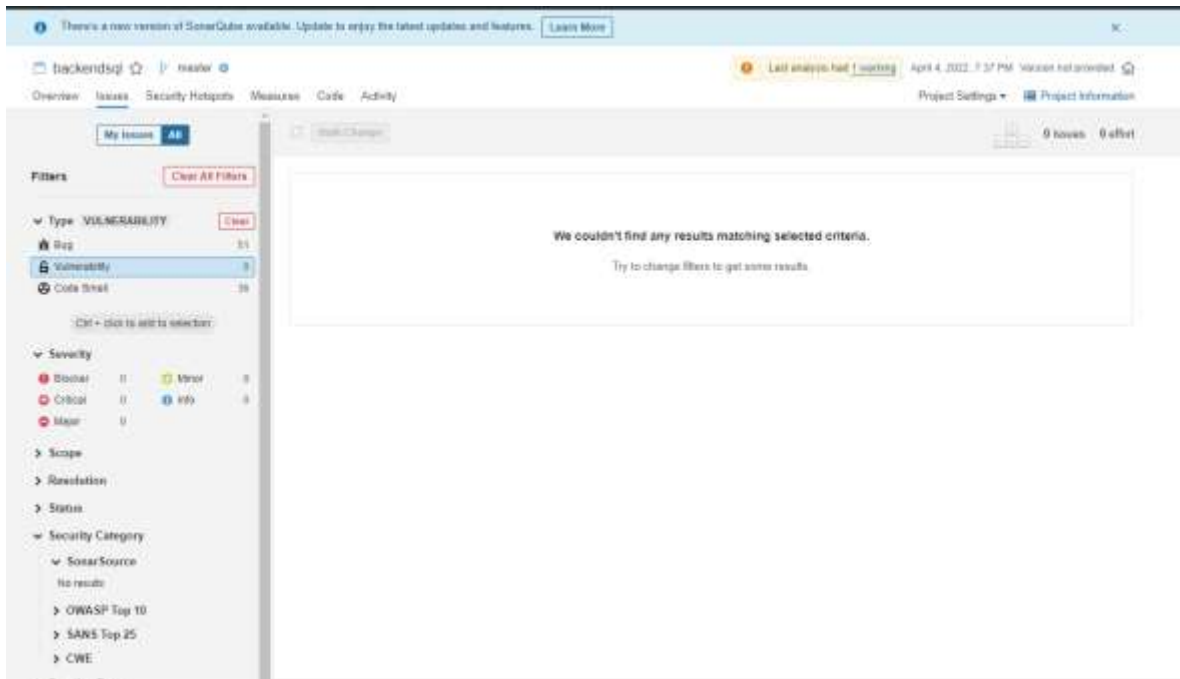
Aquí se tiene como prioridad inmediata el corregir los bugs, que surgieron durante el desarrollo del sistema para entregar un sistema de calidad y sin fallas.



Vulnerability

Numero de vulnerabilidades:0

Una vez mas encontramos un buen trabajo en el apartado de seguridad



Code Smell

Numero de code smells:36

como se comento anteriormente es recomendable corregir los olores de código, pues con ello evitaremos los problemas de legibilidad y entendimiento de código, además de que esto nos ayudara a mejorar como desarrolladores

