Carlos Andres

Informe donde se describirá el paso a paso para realizar las pruebas de seguridad en sonarqube y owasp

Informe de Seguridad

1906630

Tabla de contenido

[INTRODUCCION 2](#_Toc89602219)

[OWASP 3](#_Toc89602220)

[DEFINICION 3](#_Toc89602221)

[INSTALACION 3](#_Toc89602222)

[PASO1 3](#_Toc89602223)

[PASO2 3](#_Toc89602224)

[PASO3 4](#_Toc89602225)

[SONARQUBE 5](#_Toc89602226)

[DEFINICION 5](#_Toc89602227)

[INSTALACION 5](#_Toc89602228)

[PASO1 5](#_Toc89602229)

[PASO2 5](#_Toc89602230)

[PASO3 6](#_Toc89602231)

[CONCLUSIONES 7](#_Toc89602232)

[RESULTADOS DE LAS PRUEBAS 7](#_Toc89602233)

[SONARQUBE 7](#_Toc89602234)

[OWASP 8](#_Toc89602235)

# INTRODUCCION

Este informe pretende mostrar los resultados de las pruebas de seguridad realizadas a la página de CoolStyle donde se evidenciarán si la página cumple con los estándares mínimos de seguridad requeridos, las pruebas o escaneos se desarrollarán en el ambiente de OWASP y Sonarqube donde se mostrará el proceso de cómo se realizaron están pruebas y si el lector de este informe desea repetir las pruebas.

# OWASP

## DEFINICION

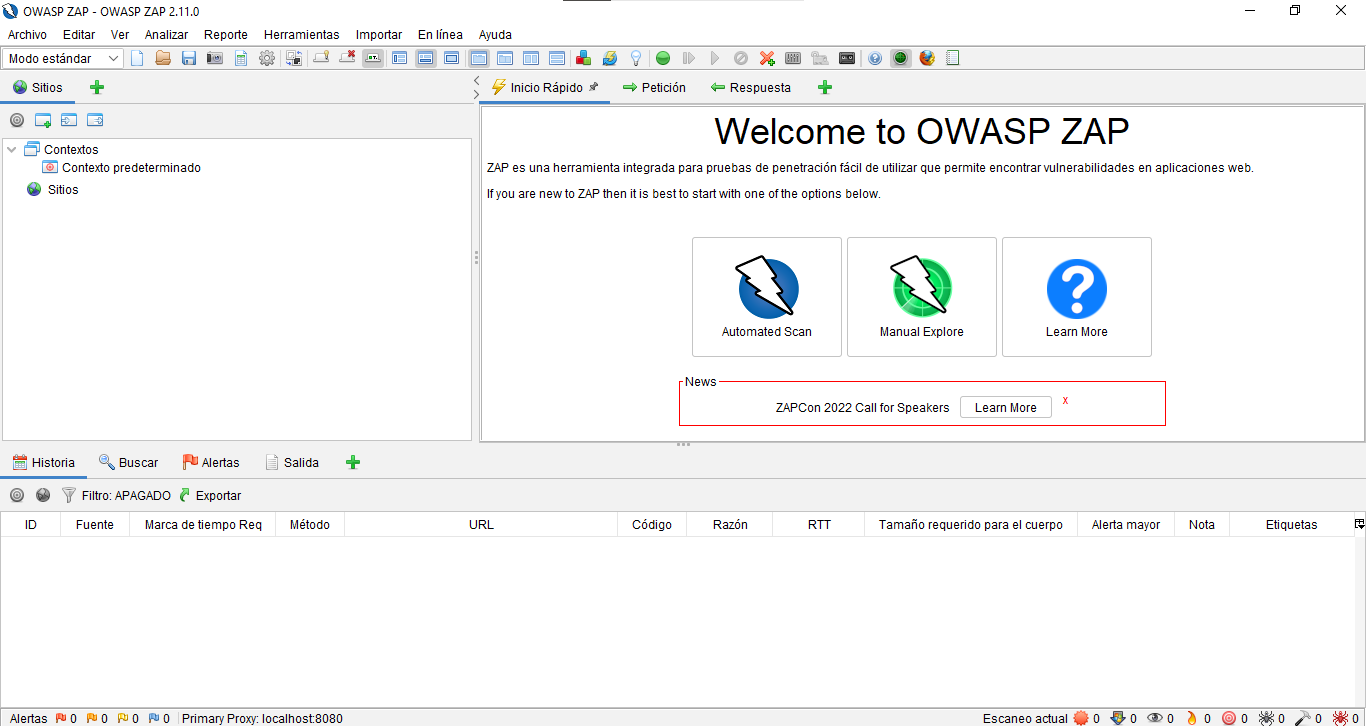
OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP.

## INSTALACION

Primero tenemos que instalar la aplicación que estaría en esta url: https://www.zaproxy.org/download/, escogemos en que sistema operativo está desarrollando la actividad y culmina la instalación

### PASO1

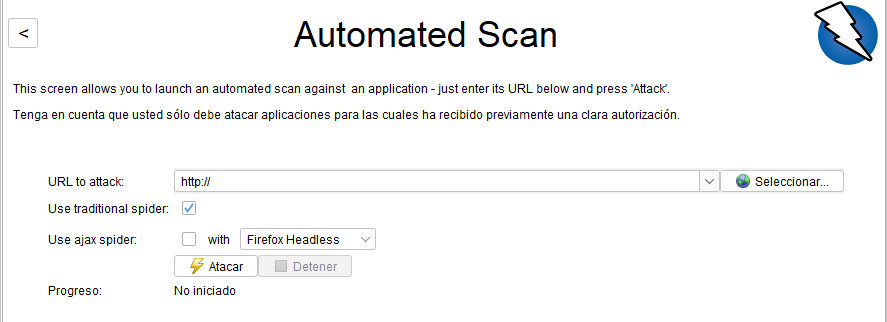
Una vez instalada entramos a la aplicación, nos aparecerá una ventana como esta:



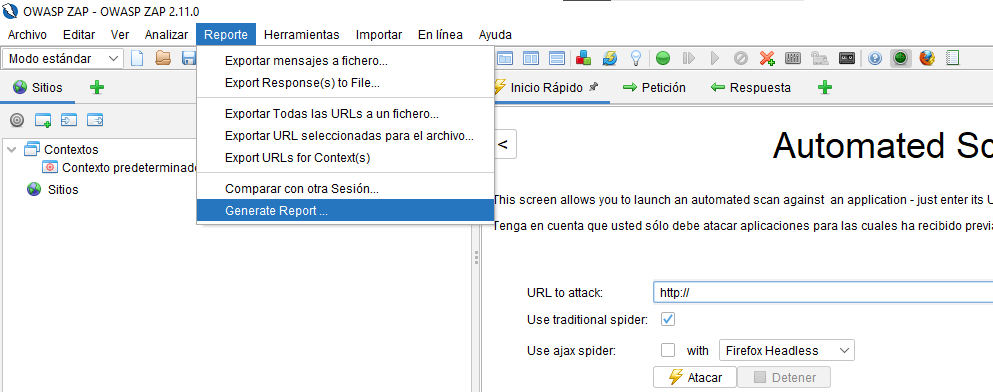
Clicamos en la opción Automation Scan

### PASO2

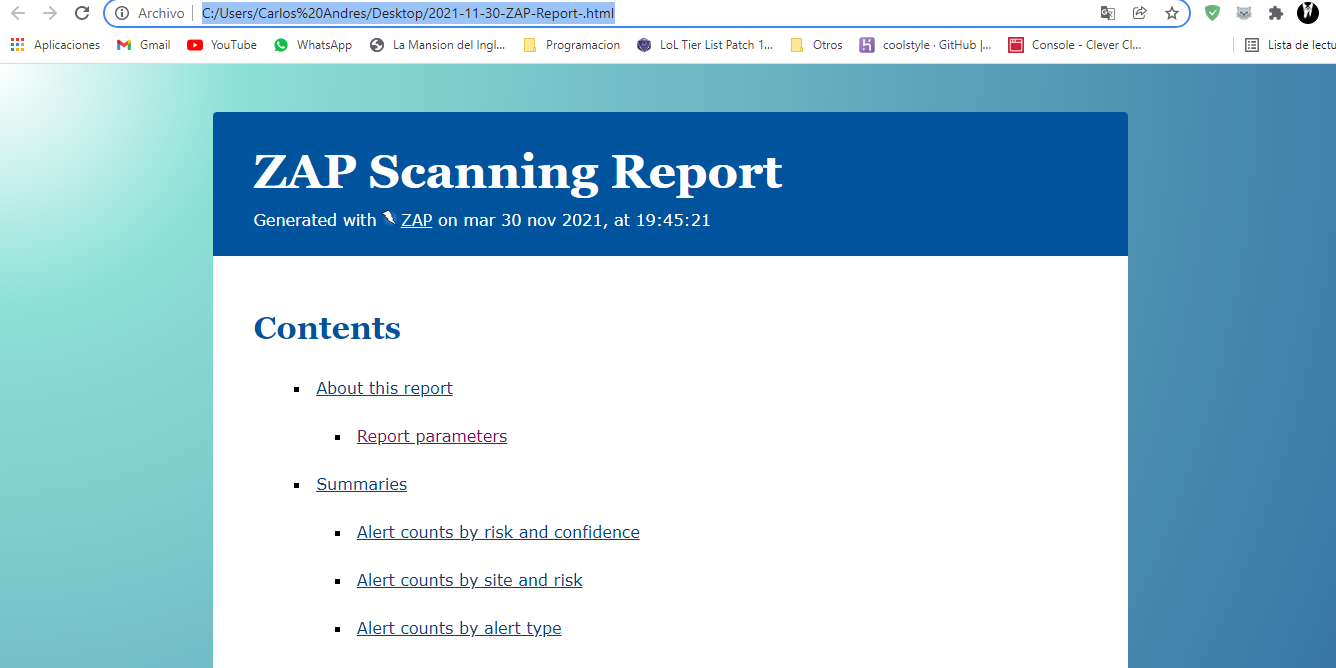
Colocamos la URL de sitio web que deseamos evaluar y después en atacar



### PASO3



Después de que termine la prueba generamos el informe y lo guardamos donde queremos y después lo abrimos, se mostrara de la siguiente manera:



Ya habremos culminado la prueba de vulnerabilidades en owasp, desde allí se desglosarán todas las vulnerabilidades del sitio catalogadas en bajo medio y alto.

# SONARQUBE

## DEFINICION

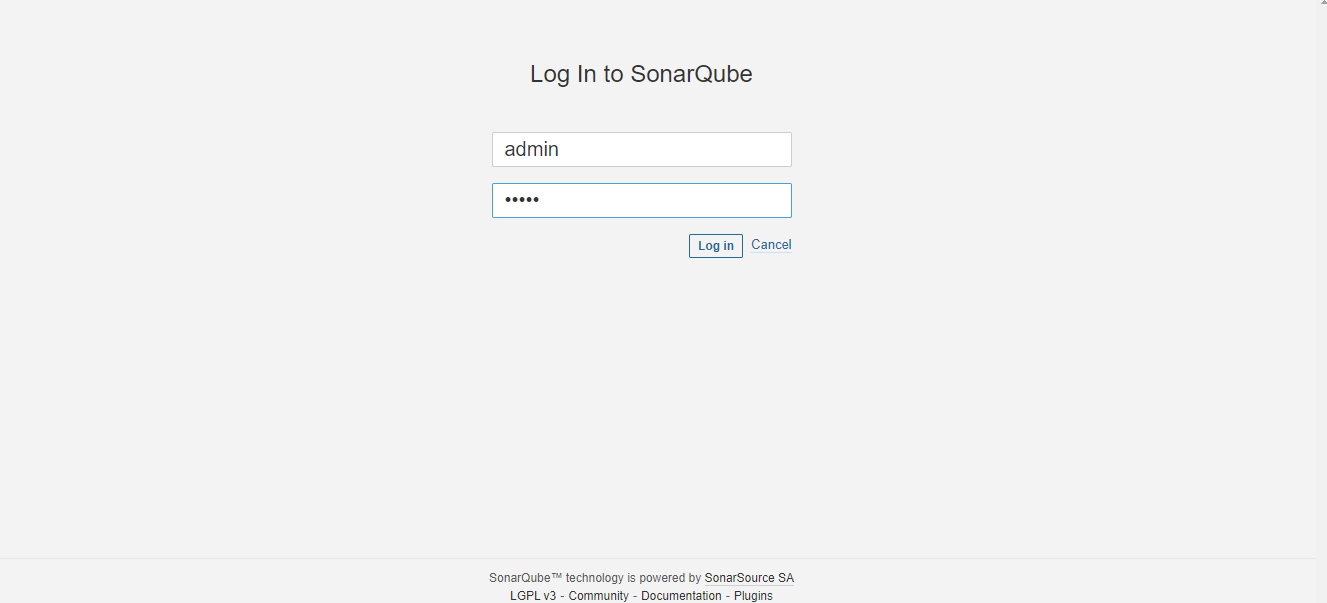
SonarQube es una plataforma para evaluar código fuente. Es software libre y usa diversas herramientas de análisis estático de código fuente como Checkstyle, PMD o FindBugs para obtener métricas que pueden ayudar a mejorar la calidad del código de un programa. ​

## INSTALACION

La prueba con sonarqube es un poco más difícil, requisitos para esta prueba es tener instalado y configurado Docker y crear el contenedor de sonarqube por medio de un pipeline que está en el proyecto titulado “docker-compose”.

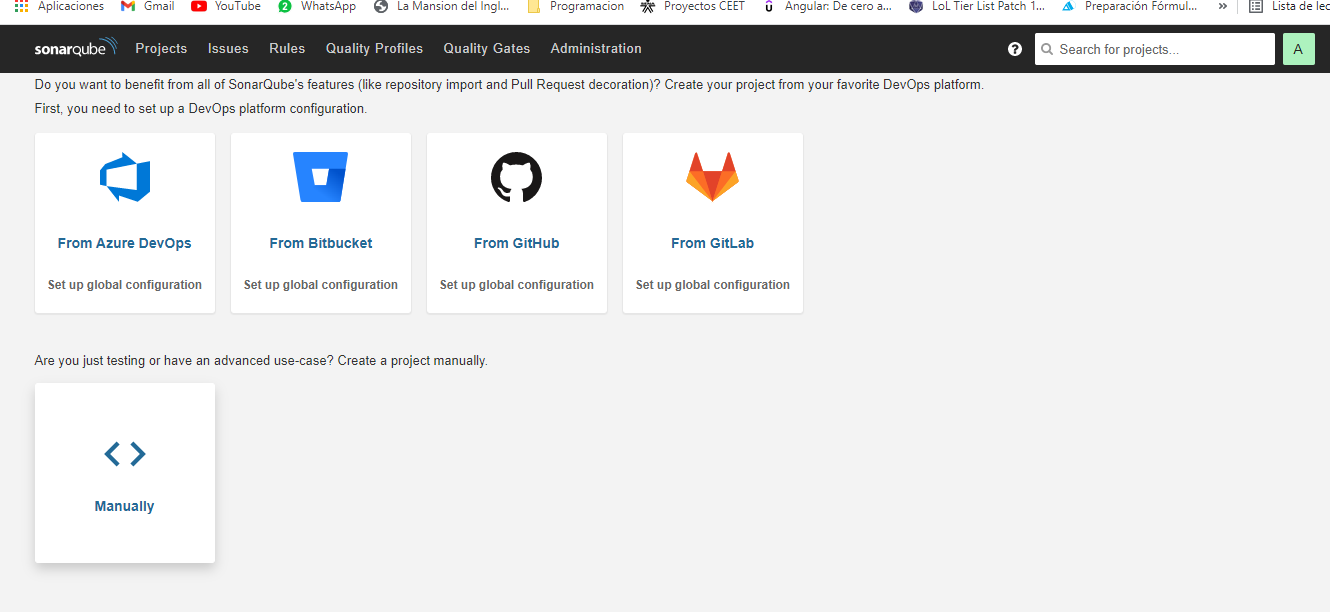
### PASO1

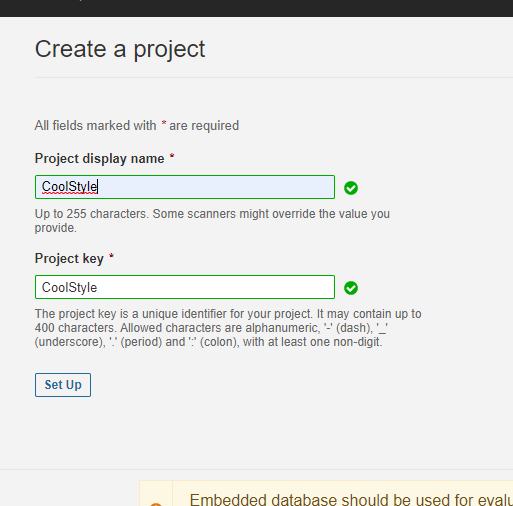
Entramos a sonarqube por primera vez como admin: admin



### PASO2

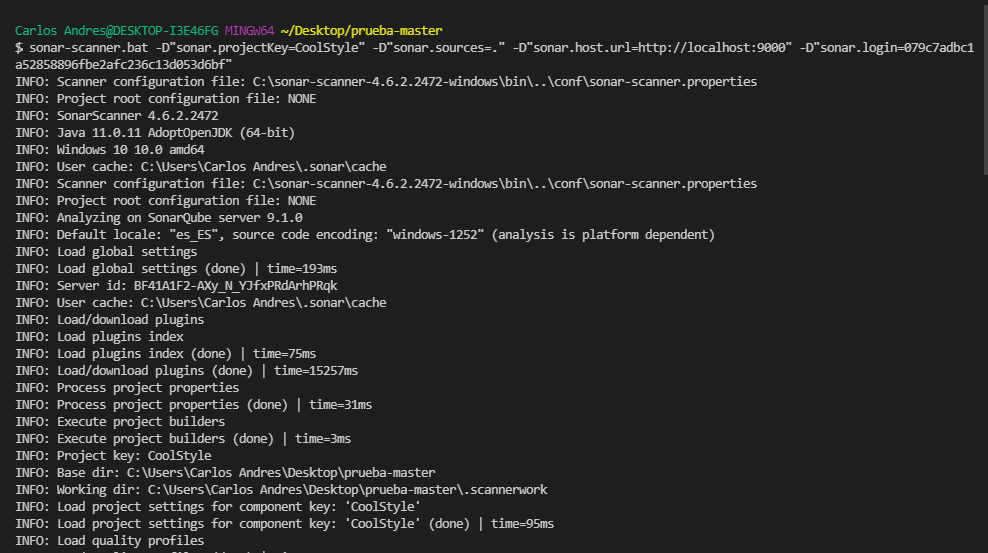
Configuramos lo siguiente





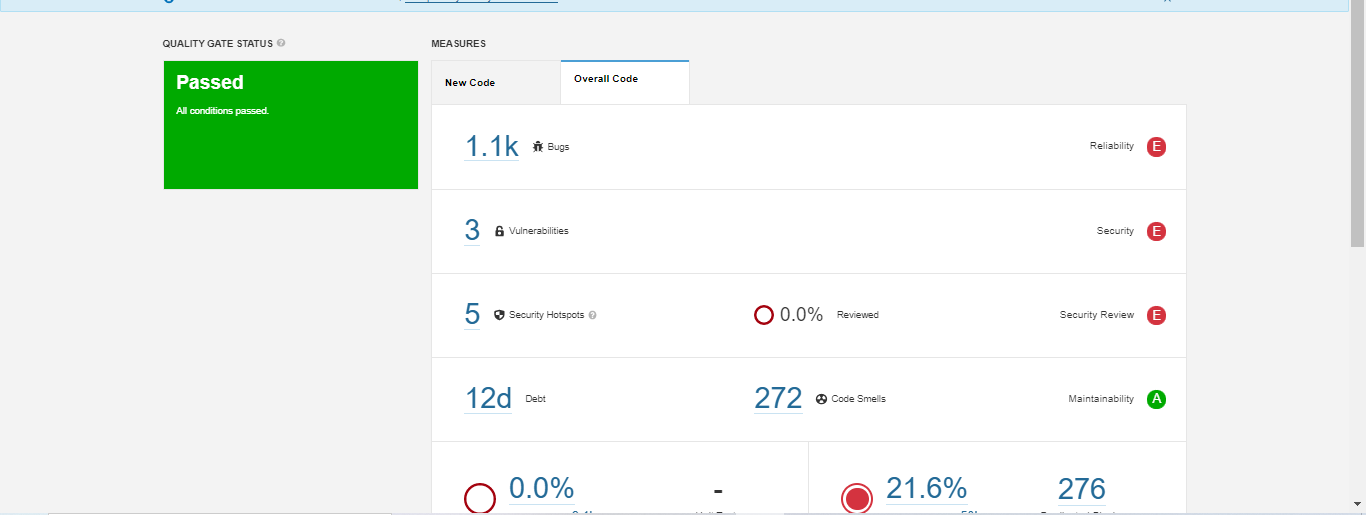
Lo que hicimos fue crear el repositorio ahora solo falta ejecutar el escáner, desde el código fuente abrimos una terminal y ejecutamos lo siguiente

### PASO3



PASO4

Después de que termine ya tendremos los resultados de esta manera:



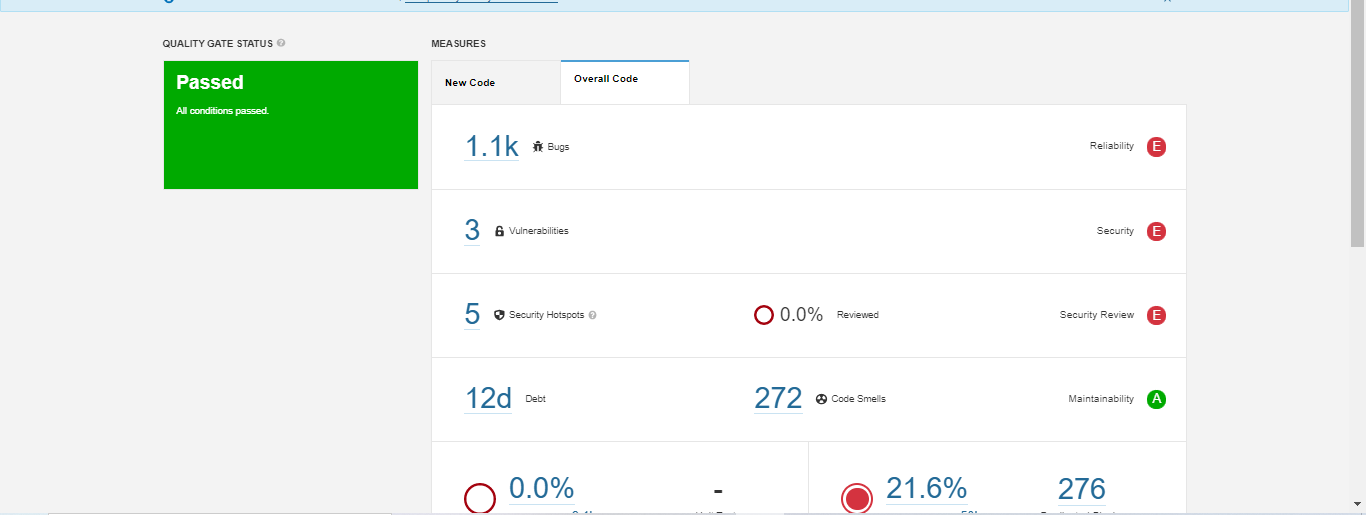
# CONCLUSIONES

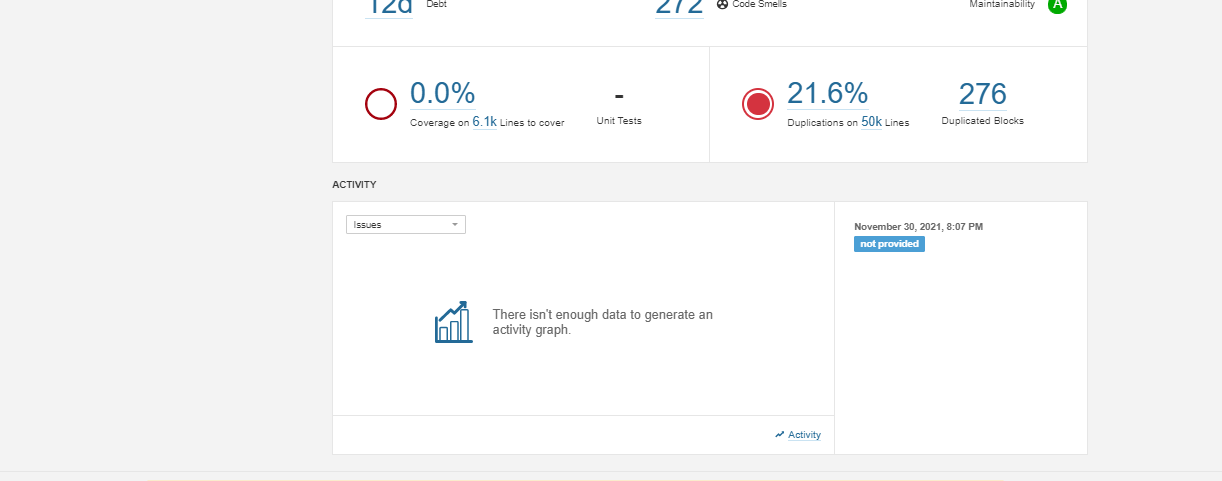
Como vimos anteriormente se ejecutaron las dos pruebas y las métricas nos indican que fueron suficientemente aceptables para que la pagina sea desplegada sin presentar algún inconveniente

# RESULTADOS DE LAS PRUEBAS

Los resultados estarán como anexos en el repositorio del proyecto en la carpeta de Documentos > Modelo de calidad. Por si desea ir a verlos con más detalle

## SONARQUBE





## OWASP

