2020

Memoria Técnica Escaneo de código Fortify Jenkins plugin

1017 - Servicios para Fortify Procesar RFP - ES

Fecha de publicación:
21/06/2021

Última revisión:
29/06/2021

AVATTAR CONSULTING

Índice

Introducción.

Información General del Proyecto.

Implementación de la solución tecnológica de herramientas de Micro Focus Fortify Static Code Analyzer y Software Security center, que tienen como objeto mitigar con un enfoque preventivo, las vulnerabilidades de seguridad en el código de las aplicaciones desarrolladas por Procesar.

Introducción de la Herramienta.

La Solución Tecnológica basada en MF Fortify Static Code Analyzer (SCA), producto para el análisis de código estático automatizado, esto permite a los desarrolladores eliminar las vulnerabilidades en el código y crear software seguro, encontrando e indicando defectos de seguridad en tiempo real durante el proceso de codificación con integraciones con IDEs soportados.
Compartiendo los resultados a MF Fortify Software Security Center (SSC), encargada de centralizar los resultados de los escaneos para su visualización y seguimiento de las vulnerabilidades encontradas dentro del mismo, gestionando el riesgo de seguridad del software por medio de colaboración, evaluación de error y resolución visualizándolo por medio de paneles de control e informes centralizados.

Propósito del Documento

El propósito del diseño físico del proyecto Servicios para Fortify Procesar RFP ES es, documentar e identificar los pasos para la instalación de Jenkins y su uso con Fortify para poder realizar escaneos.

Escaneo de código – Jenkins – Fortify SSC.

1.- Como primer paso es necesario iniciar sesión en el aplicativo, posteriormente se muestra el dashboard principal, en la parte superior izquierda se muestra las opciones que son capaces de generar, para crear una validación de código, es necesario crear un nuevo item, por lo que se comienza seleccionando la opción de "New Item".

Figura 1.- Dashboard principal.

2.- Para generar un nuevo job es necesario colocar el nombre y seleccionar la opción de "Freestyle Project" posteriormente seleccionar OK para crearlo.
Como recomendación, crear el nombre sin espacios y con "_" en las separaciones, y que este tenga el mismo nombre de la aplicación a escanear.

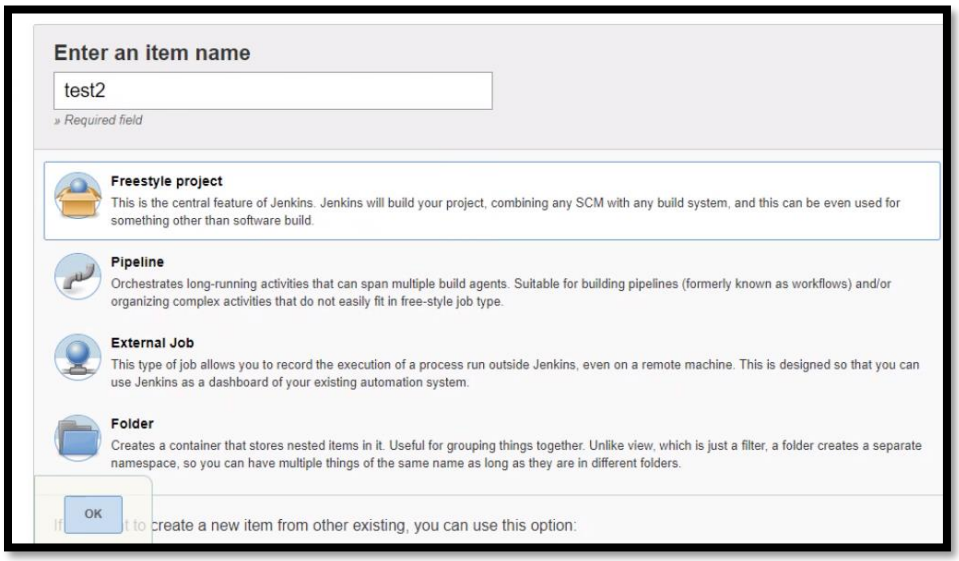

Figura 2.- Crear nuevo item.

3.- Una vez que se genera el nuevo item, se muestran las configuraciones para este job, la primera configuración a realizar es en “Source Code Management”, una vez en esta opción se selección “Subversion” esto le da entrada a la configuración de este.
Para poder descargar el código de SVN, es necesario tener el repositorio de SVN y seleccionar las credenciales de ujenkins, con eso es suficiente para que se configure la descarga de código.

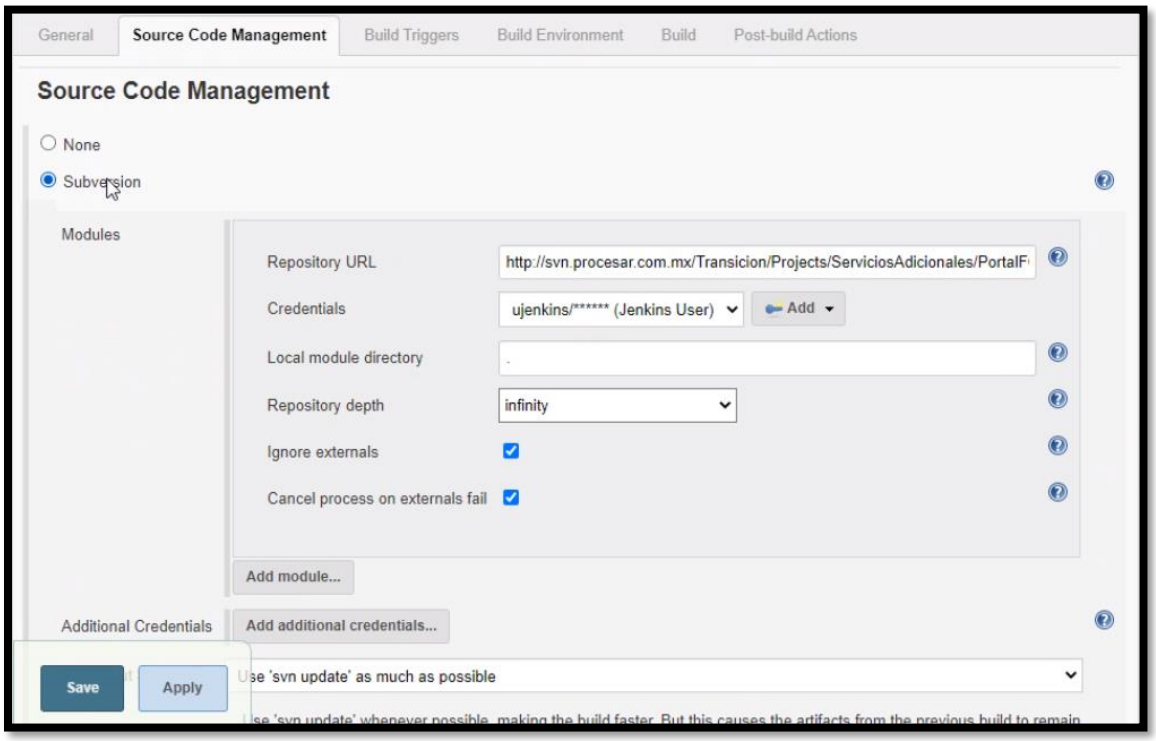

Figura 3.- Configuración de SVN.

4.- Una vez guardada la configuración de Fortify assessment, se mostrará el dashboard del job, en este se selecciona “build now” para comenzar la ejecución del item.

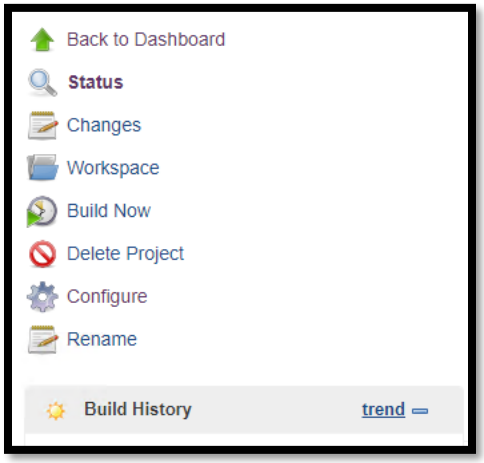

Figura 4.- Build now.

5.- Si la configuración se realizo correctamente, se mostrará un build successful en el cual el código de SVN indicado se descargo correctamente y se podrá validar en el workspace, el cual muestra el contenido descargado.

Figura 5.- Console output SVN.

6.- Para configurar la ejecución de los escaneos de Fortify, es necesario dirigirse a "Build environment" y seleccionar una opción llamada "Add post build action" este se va a desplegar y se debe seleccionar la opción de "Fortify Assessment" esto desplegará la configuración de Fortify.

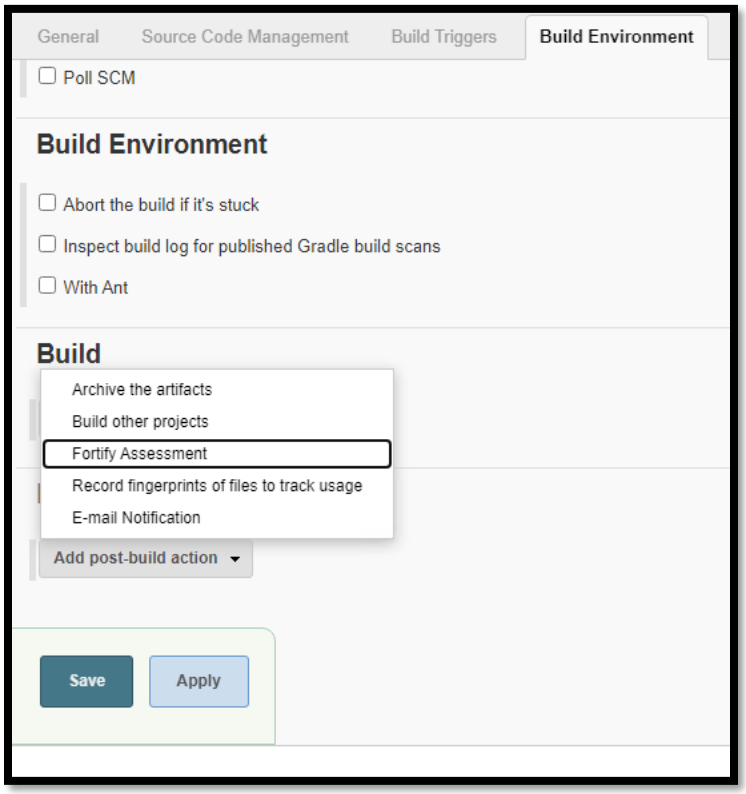

Figura 6.- Fortify Assessment.

7.- Una vez desplegado el Fortify Assessment, esto indica que realizara un escaneo, se mostraran 3 opciones, es necesario seleccionar la última, **“local translation & local scan”**, se mostraran opciones en la parte inferior, de estas es necesario colocar

- Colocar el build ID del escaneo (Mismo nombre de item en jenkins).
- El nombre de resultados que tendrá el archivo fpr (Mismo nombre de item en Jenkins + “.fpr” al final).
- De igual manera es necesario seleccionar el tipo de aplicación que se va a escanear, siendo esta “Java”
- En la sección de “source files” se debe colocar el path donde se encuentra el código, siempre será estructurado de la siguiente manera: **“C:\Users\fortify\.jenkins\workspace\NOMBREJOB”**, esto ya que no detecta la variable Workspace de Jenkins, por lo que es necesario indicar el path completo.
- En la sección de Exclude list, se va a seleccionar el path de las carpetas de test, un ejemplo es el siguiente:
  "C:\Users\fortify\.jenkins\workspace\prueba_subversion\portalFct-persistencia\src\test"
  "C:\Users\fortify\.jenkins\workspace\prueba_subversion\portalFct-presentacion\src\test"
  "C:\Users\fortify\.jenkins\workspace\prueba_subversion\portalFct-servicios\src\test"
  Donde se sigue la estructura del path y posteriormente la carpeta donde se encuentra ubicada la carpeta test, así al hacer el escaneo se excluye esta carpeta.

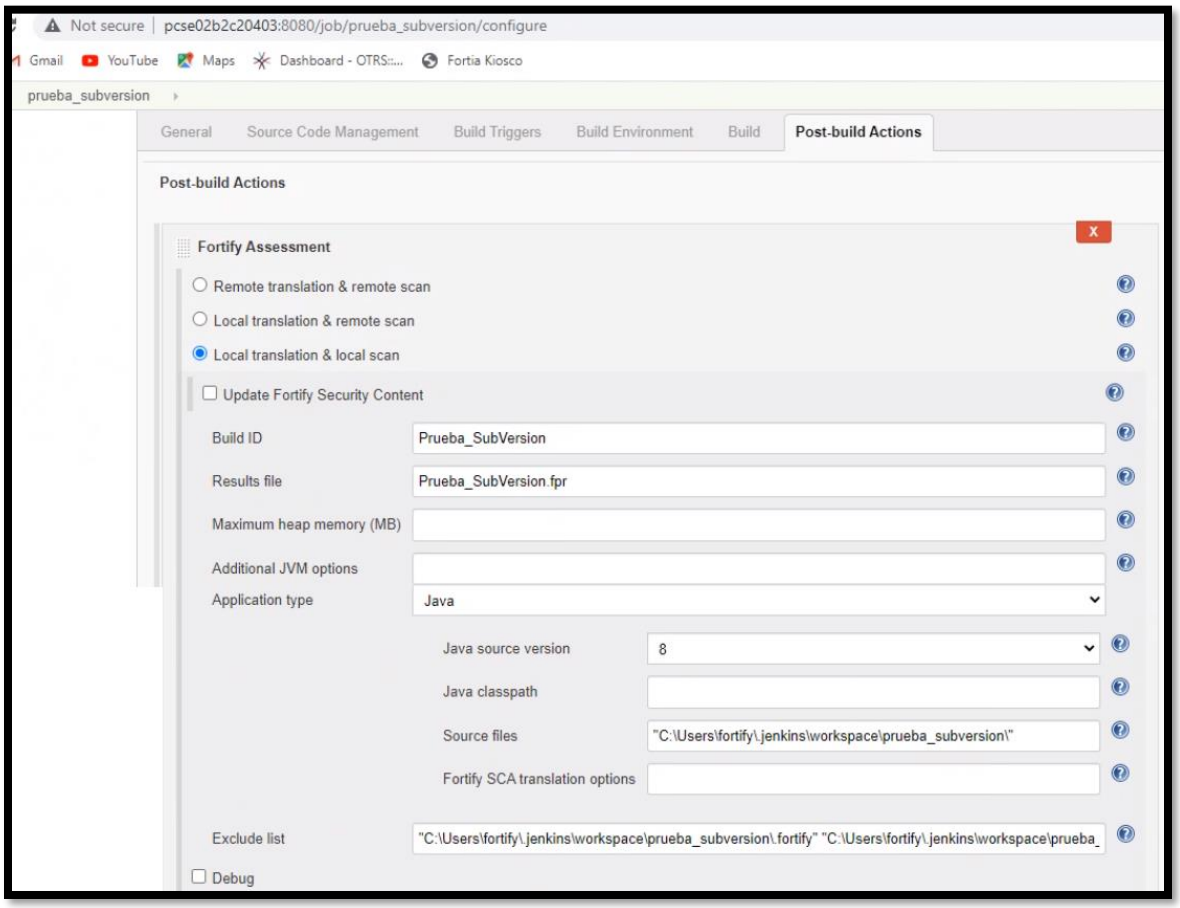

Figura 7.- Fortify Assessment Local translation.

8.- En la parte inferior es necesario colocar la opción de “Run Fortify SCA Scan” para que realice el escaneo.
Y la opción de “Upload Fortify SCA scan results to SSC”, aquí se mostrarán las aplicaciones disponibles en el SSC y las versiones asociadas a este.
Se puede indicar una aplicación nueva escribiendo el nombre y la versión, una vez colocada la información se guarda el job y se ejecuta.

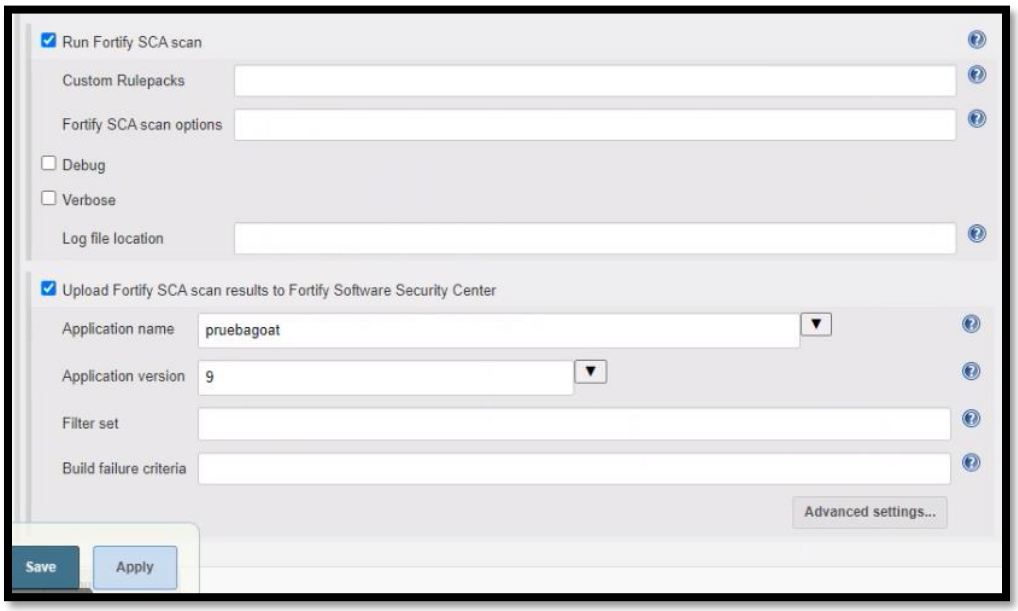

Figura 8.- Escaneo y compartir resultados.

9.- Una vez guardada la configuración de Fortify assessment, se mostrará el dashboard del job, en este se selecciona “build now” para comenzar con el escaneo.

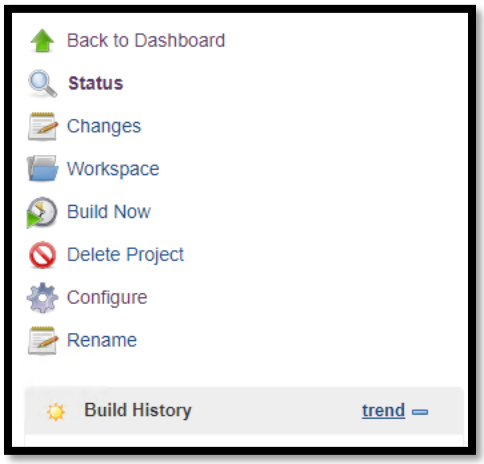

Figura 9.- Build now.

10.- Al comenzar con la ejecución del escaneo, lo primero que se muestra es que detecta la versión del Fortify, posteriormente ejecuta los comandos necesarios para realizar el escaneo, siendo esto lo que se configuro previamente, incluyendo carpetas a excluir, al finalizar el proceso menciona que se crea el archivo fpr, el cual contiene las vulnerabilidades del escaneo realizado.

Figura 10.- Escaneo realizado - FPR.

11.- En el mismo build, al finalizar el escaneo, se genera el proceso de subir el fpr hacia el Fortify SSC, menciona el archivo fpr que está utilizando, así como su locación en el equipo, posteriormente el template que estará utilizando, así como de las estadísticas que extraer del SSC, siendo estas las vulnerabilidades que encontró por categoría.

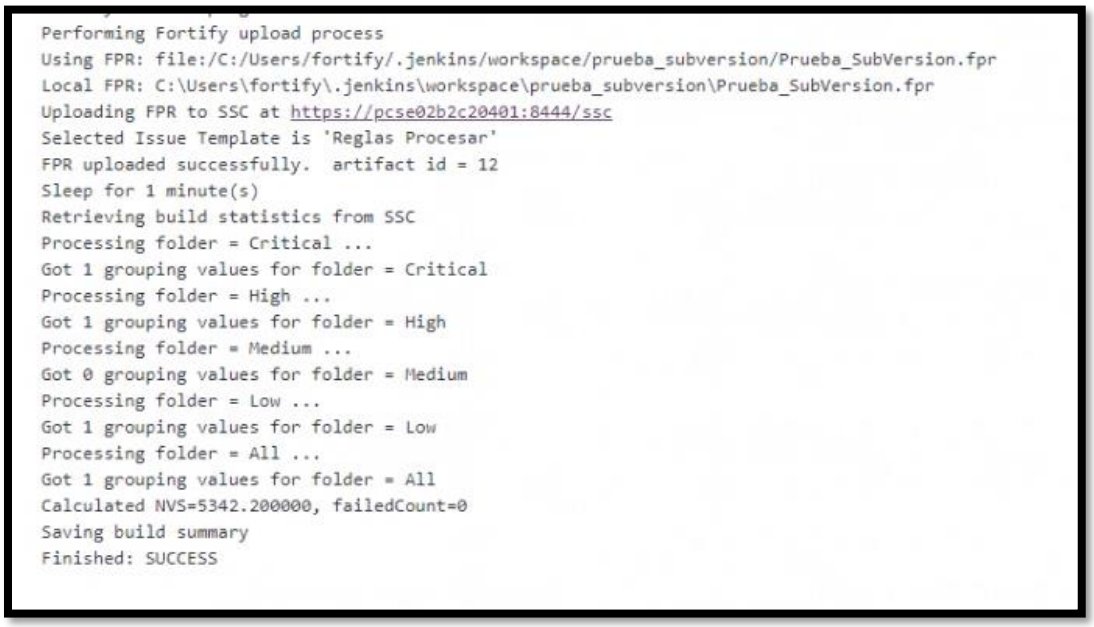

Figura 11.- Compartir resultados a SSC.

12.- Al finalizar del build, el resultado se mostrará en el Jenkins de la siguiente manera, mostrando una nueva pestaña llamada “Fortify Assessment”, en la cual se muestran los resultados de las vulnerabilidades que fueron encontradas al realizar el escaneo.

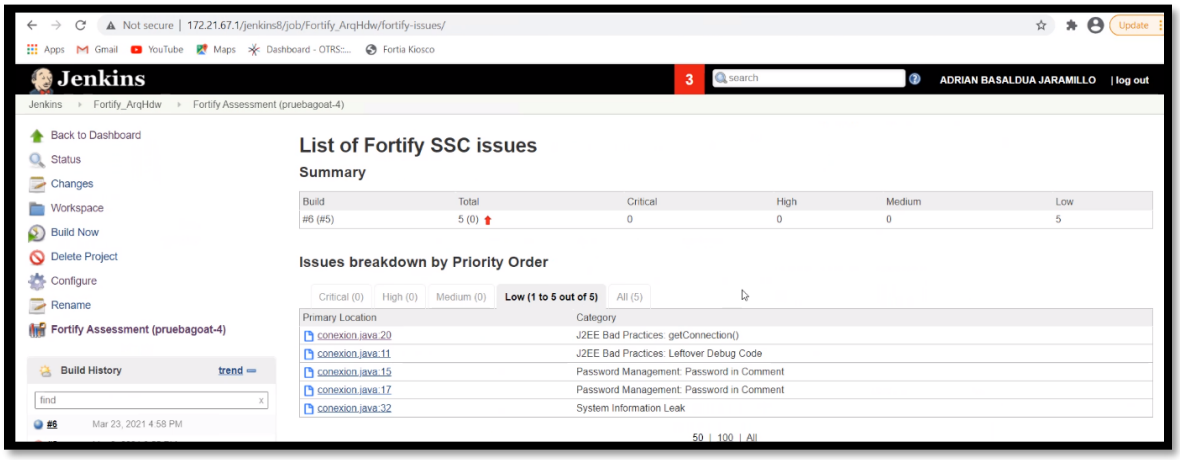

Figura 12.- Lisa de vulnerabilidades.

13.- Al seleccionar una vulnerabilidad en el Jenkins, nos desplazará hacia el Fortify SSC, mostrando esta vulnerabilidad en la sección de Audit, finalizando el proceso de generar un escaneo de código a partir de Jenkins y visualizar los resultados en Fortify SSC.

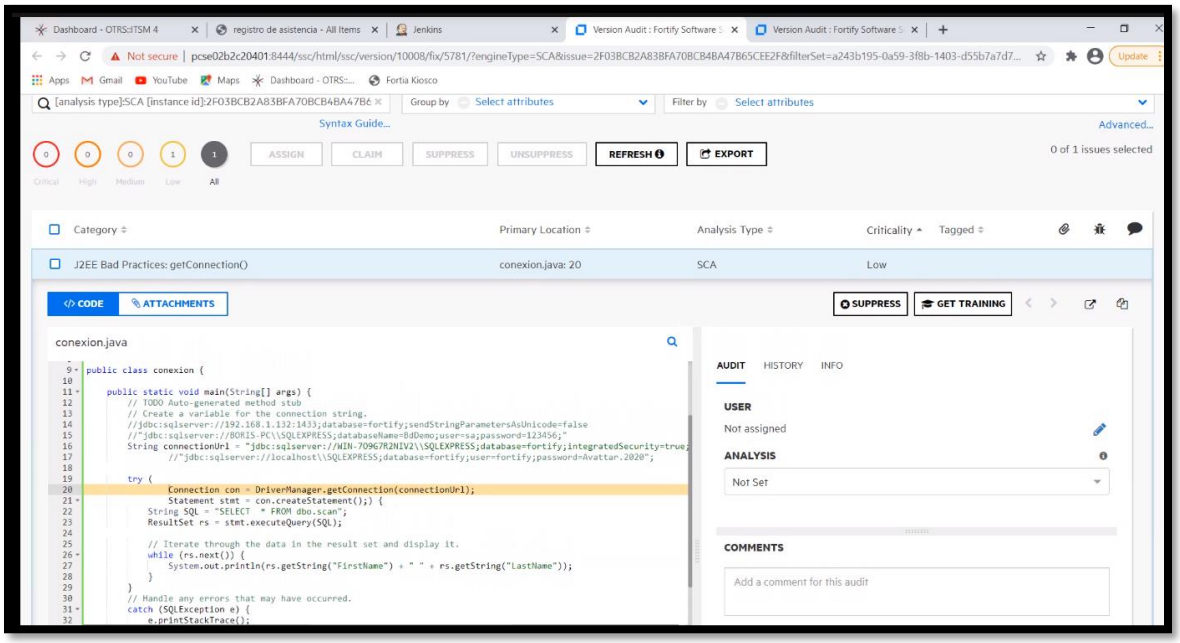

Figura 13.- Resultados de escaneo.

Cierre del Documento

Firmas de Aceptación.

Francisco Corzo Crail
Project Manager