Requisito 54

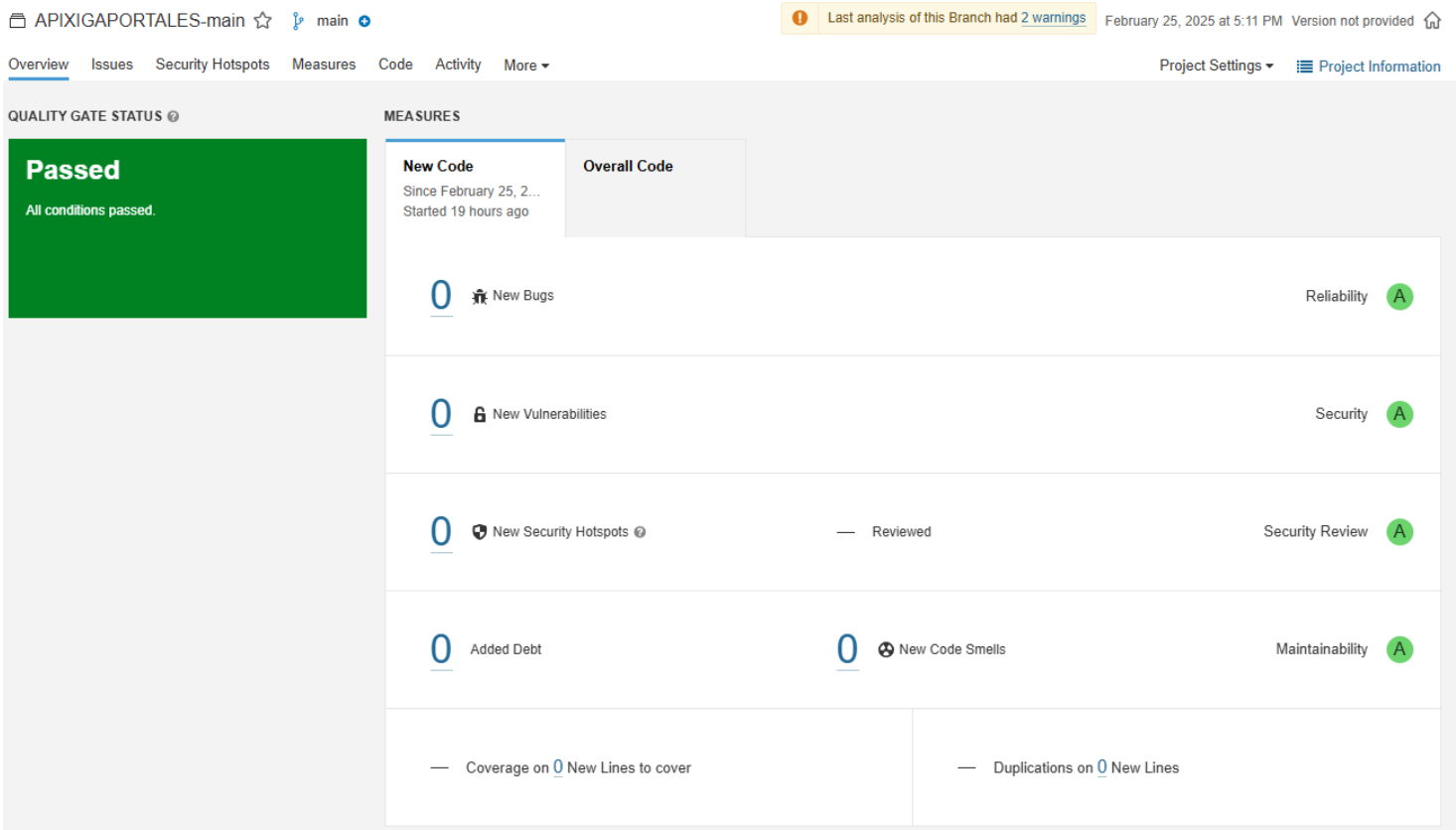
Evidencia de Pruebas de Código Seguro mediante el escaneo con herramienta SonarQube al Portal XIGA Clientes

SonarQube es una plataforma de código abierto diseñada para evaluar y mejorar la calidad del código de proyectos de software. Funciona como una herramienta de análisis estático que examina el código fuente en busca de problemas de seguridad, errores, vulnerabilidades, y malas prácticas de codificación. Además de proporcionar una evaluación detallada de la calidad del código SonarQube, ofrece métricas y estadísticas útiles para medir la salud general del proyecto.

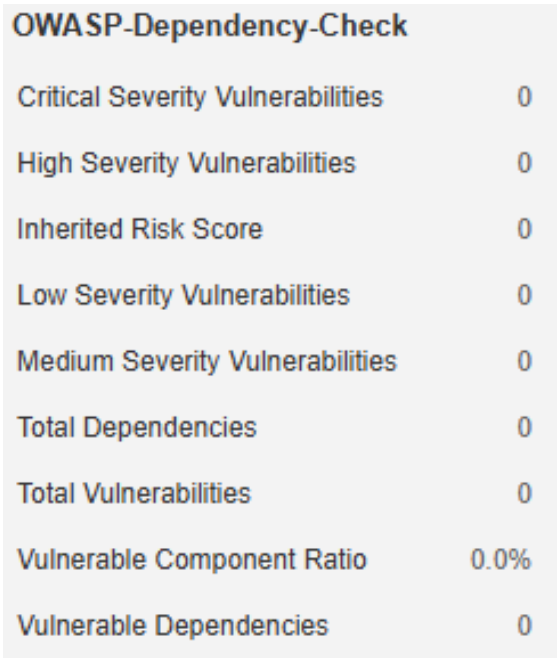
En el siguiente resumen muestra los principales **indicadores de calidad del código** después del análisis con la herramienta SonarQube. Se identificaron:

- ✓ 0 bugs,
- ✓ 0 vulnerabilidades y
- ✓ 0 code smells,

Aprobando con clasificación “A” en todos los rubros.



En el rubro de las pruebas en apego a OWASP:



SonarQube y OWASP

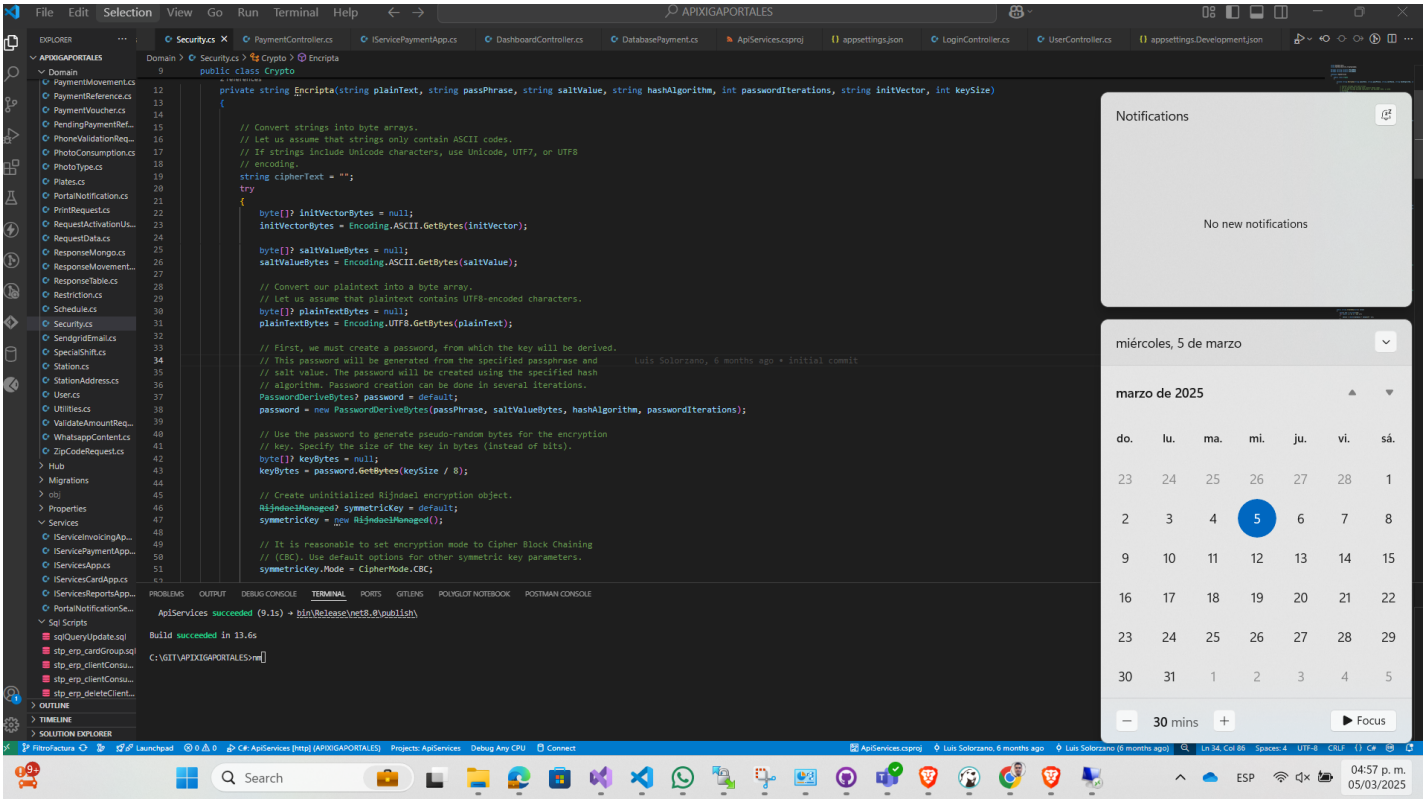
SonarQube es plataforma de análisis estático de código que también puede implementar la revisión con las pautas y recomendaciones de seguridad de OWASP. Esto permite identificar y abordar posibles vulnerabilidades y problemas de seguridad en el código fuente de las aplicaciones web.

La integración con OWASP ayuda a garantizar que las aplicaciones están desarrolladas siguiendo buenas prácticas de seguridad, reduciendo así el riesgo de posibles ataques y vulnerabilidades de software.

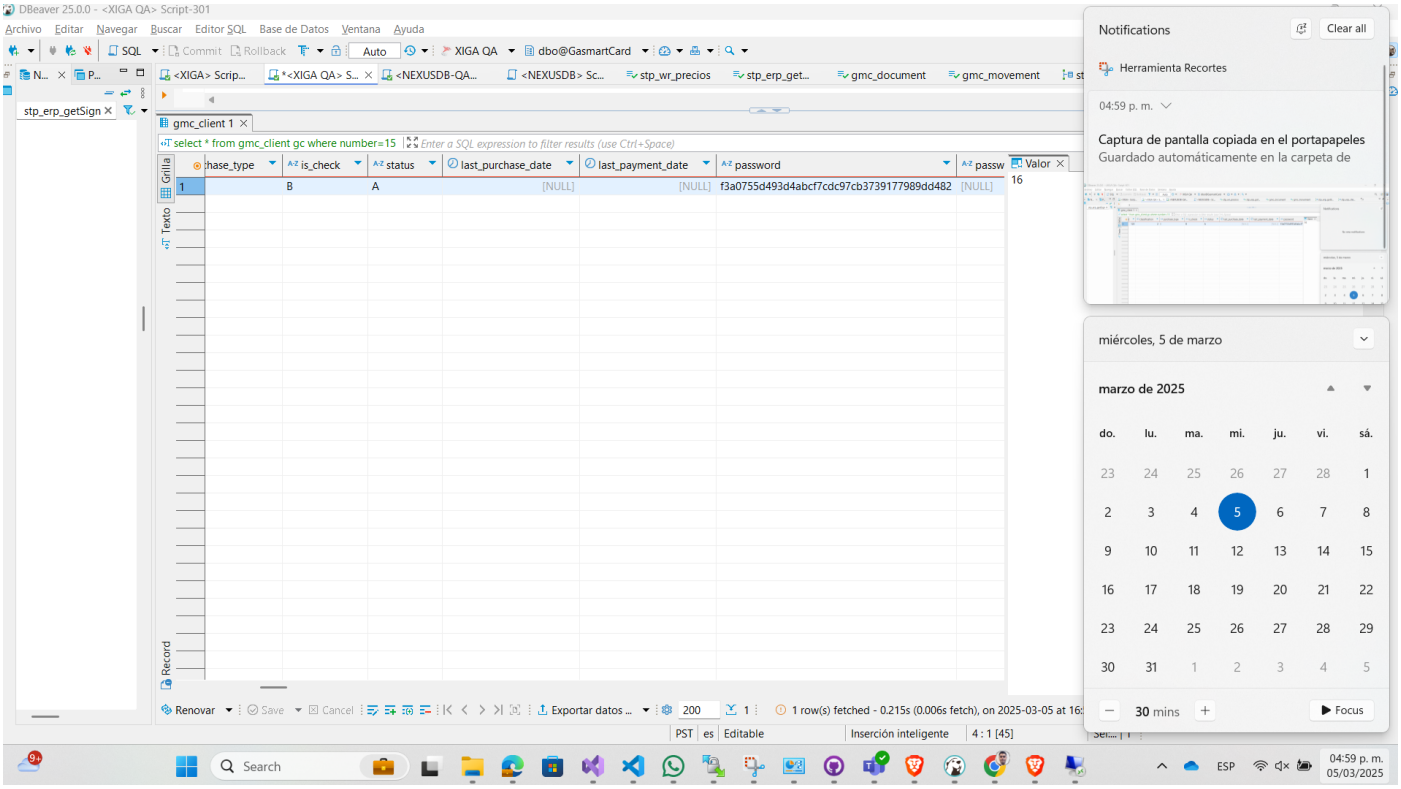
Las categorías aprobadas aplicantes al Proyecto:

Cryptographic Failures

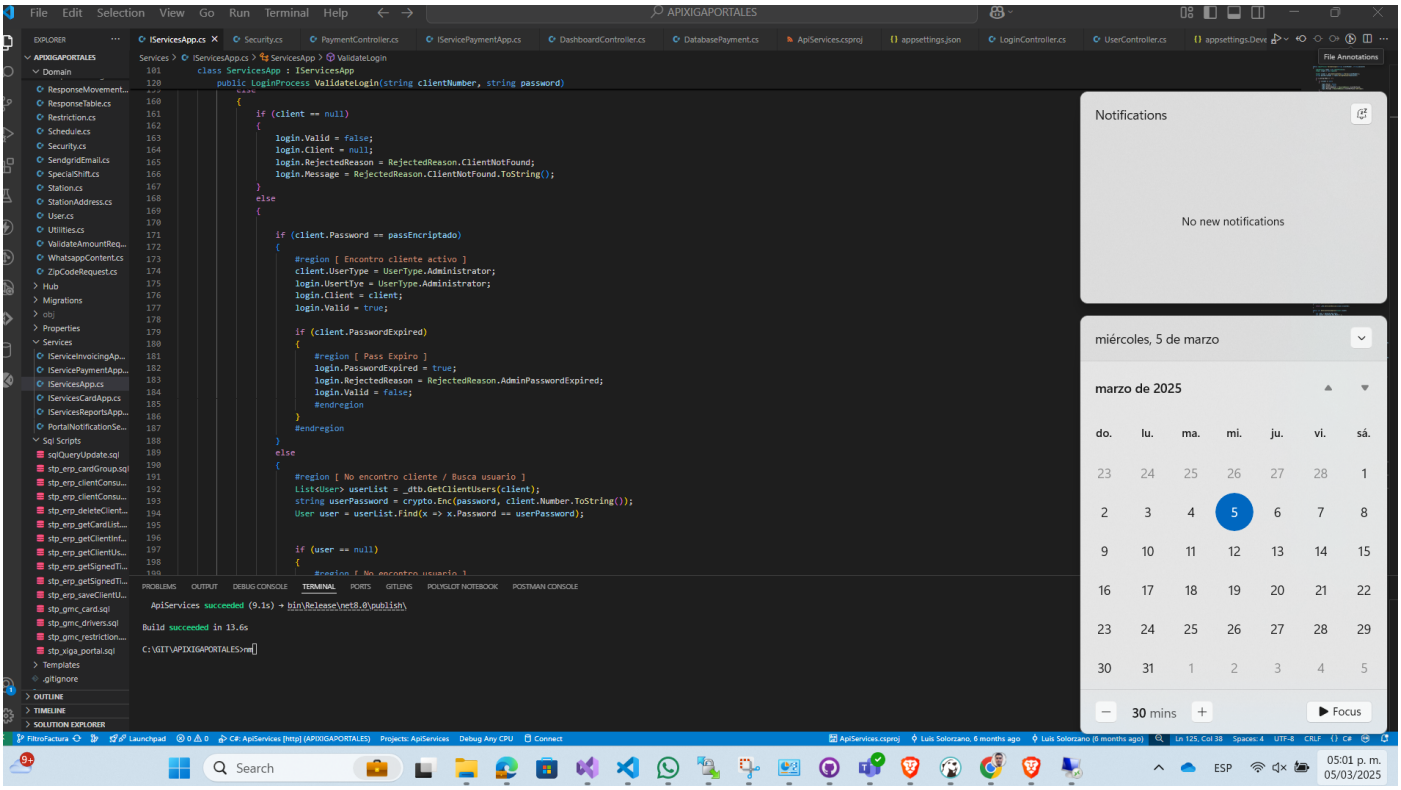
La exposición de datos confidenciales se asegura al guardar el password del usuario administrador y/ usuarios secundarios, se encripta antes de almacenarse en la base de datos, mediante la librería Crypto de C#



La contraseña encriptada en base de datos

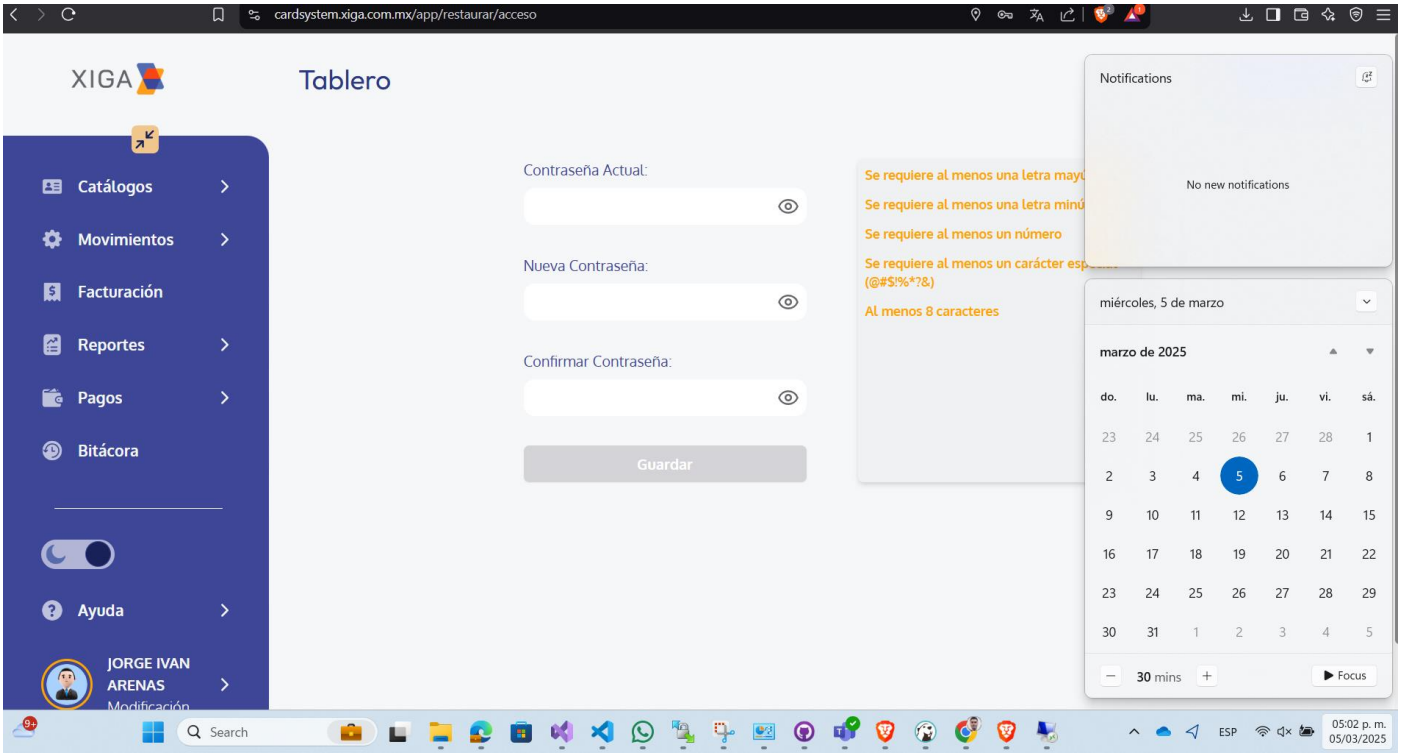


En el código muestra líneas donde valida vigencia de contraseña



Broken Authentication

Protección contra ataques donde se le concede a un usuario no autenticado privilegios de acceso una o más cuentas. Vencimiento de contraseña, cuando va a cambiar contraseña, pide que cumpla con las especificaciones de seguridad mandatorios para contraseña segura



Injection

Protección contra ataques de inyección de código en consultas con manejadores de base de datos. Se parametriza la inserción de datos con If() y su método de revisión del parámetro, para garantizar que los datos proporcionados por el usuario corresponden únicamente a los datos a capturar en el repositorio de base de datos.