

## Requisito 54

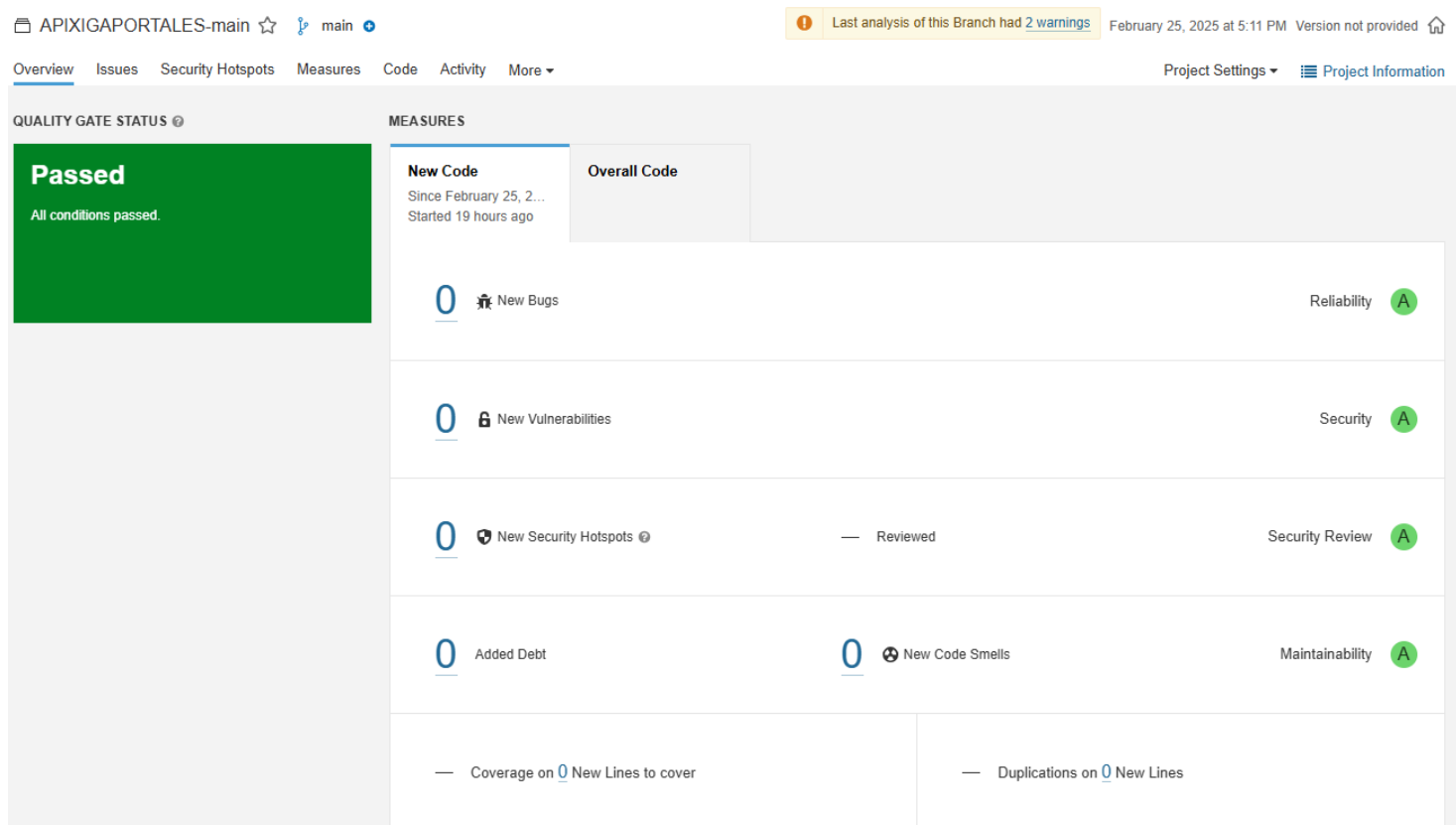
### Evidencia de Pruebas de Código Seguro mediante el escaneo con herramienta SonarQube al Portal XIGA Clientes

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.



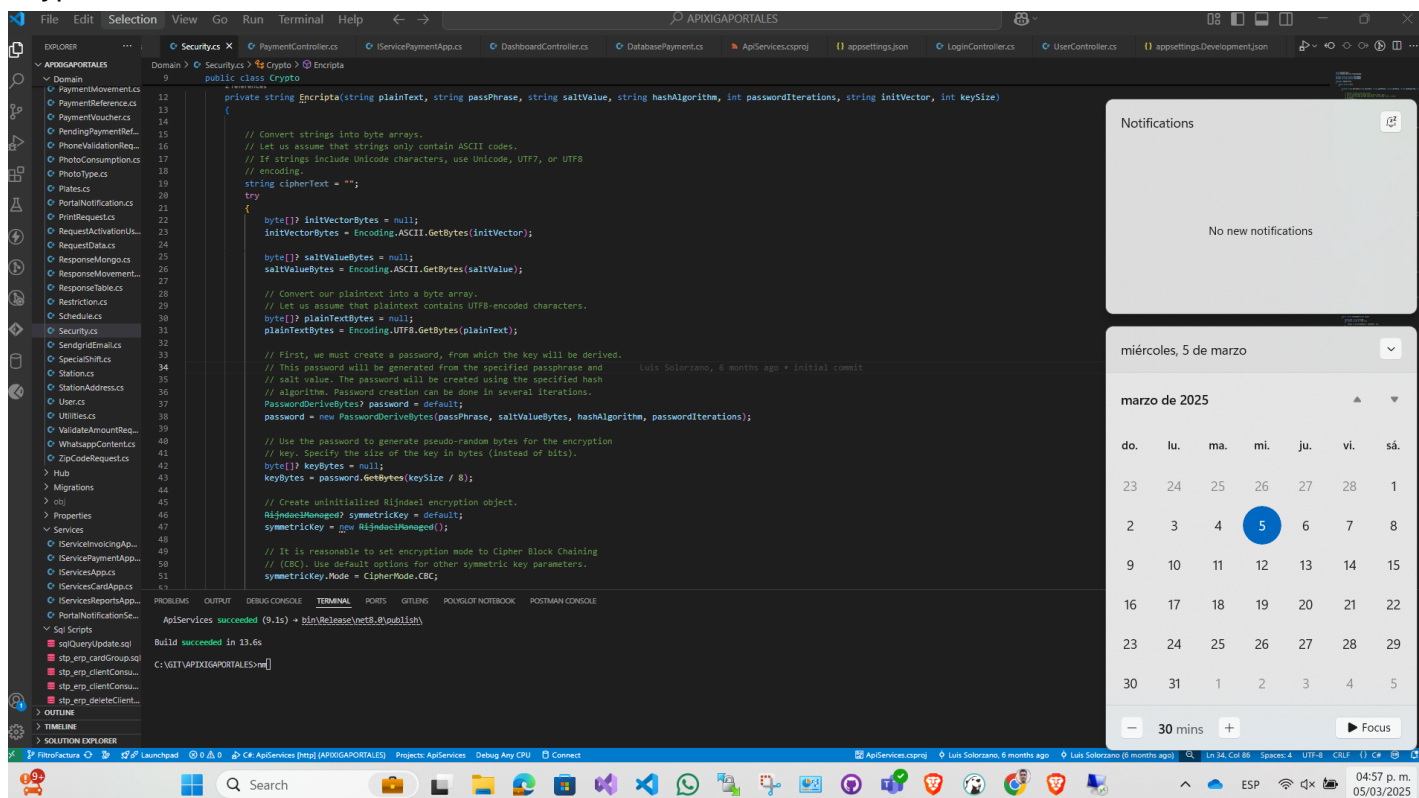


La integración con OWASP ayuda a garantizar que las aplicaciones están desarrolladas siguiendo buenas prácticas de seguridad, reduciendo así el riesgo de posibles ataques y vulnerabilidades de software.

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

DBeaver 25.0.0 - <XIGA QA> Script-301

Archivo Editar Navegar Buscar Editor SQL Base de Datos Ventana Ayuda

<XIGA> Scrip... <XIGA QA> S... <NEXUSDB-QA... <NEXUSDB> Sc... stp\_wr\_precios stp\_erp\_get... gmc\_document gmc\_movement

stp\_erp\_getSign X

gmc\_client 1

select \* from gmc\_client go where number=15

#	phase_type	A? is_check	A? status	last_purchase_date	last_payment_date	A? password	Valor
1	B	A	[NULL]	[NULL]	f3a0755d493d4abcf7cdc97cb3739177989dd482	[NULL]	16

Grilla

Record

Renovar Save Cancel Exportar datos ... 200 1 row(s) fetched - 0.215s (0.006s fetch), on 2025-03-05 at 16:...

Notifications

Herramienta Recortes

04:59 p. m.

Captura de pantalla copiada en el portapapeles  
Guardado automáticamente en la carpeta de

miércoles, 5 de marzo

marzo de 2025

do.	lu.	ma.	mi.	ju.	vi.	sá.
23	24	25	26	27	28	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

30 mins Focus

## En el código muestra líneas donde valida vigencia de contraseña

File Edit Selection View Go Run Terminal Help

APRIGAPORTALES

EXPLORER

Services > ServicesApps > ServicesApp > ValidateLogin

class ServicesApp : IServiceApp

public loginProcess ValidateLogin(string clientNumber, string password)

{

if (client == null)

{

login.Valid = false;

login.Client = null;

login.RejectedReason = RejectedReason.ClientNotFound;

login.Message = RejectedReason.ClientNotFound.ToString();

}

else

{

if (client.Password == passEncriptado)

{

#region [ Encuentro cliente activo ]

client.UserType = UserType.Administrator;

login.UserType = UserType.Administrator;

login.Client = client;

login.Valid = true;

if (client.PasswordExpired)

{

#region [ Pass Expired ]

login.PasswordExpired = true;

login.RejectedReason = RejectedReason.AdminPasswordExpired;

login.Valid = false;

#endregion

#endregion

else

{

#region [ No encuentro cliente / Busca usuario ]

ListUser> userList = \_dtb.GetClientUsers(client);

string userPassword = crypto.Enc(password, client.Number.ToString());

User user = userList.Find(x => x.Password == userPassword);

if (user == null)

{

#region [ No encuentro usuario ]

}

}

}

}

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS GITLINS POLYGLOT NOTEBOOK POSTMAN CONSOLE

ApiServices succeeded (9.1s) -> bin\Release\net8.0\publish

Build succeeded in 13.6s

stp\_viga\_portal.sql C:\GIT\APRIGAPORTALES>net

Notifications

No new notifications

miércoles, 5 de marzo

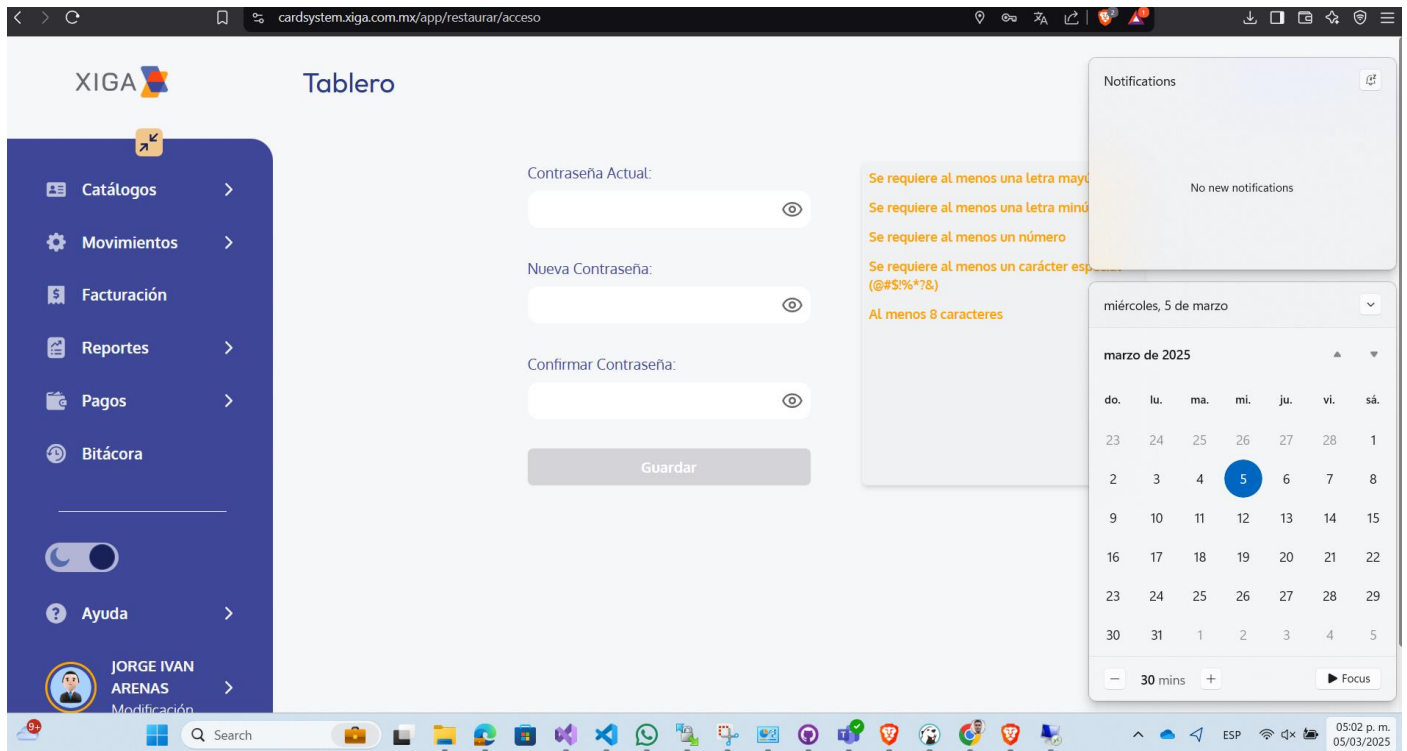
marzo de 2025

do.	lu.	ma.	mi.	ju.	vi.	sá.
23	24	25	26	27	28	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

30 mins Focus

## 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 mandatorias 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 `lf()` 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.

