

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.

The screenshot shows the SonarQube Quality Gate Status page for the project 'APIXIGAPORTALES-main'. The status is 'Passed' with a green background. Key metrics listed include:

- New Code: 0 New Bugs (Reliability A)
- New Vulnerabilities: 0 (Security A)
- New Security Hotspots: 0 (Security Review A)
- Added Debt: 0 (Maintainability A)
- New Code Smells: 0
- Coverage: 0% Coverage on 0 New Lines to cover
- Duplications: 0 Duplications on 0 New Lines

At the top right, it says 'Last analysis of this Branch had 2 warnings' and the date 'February 25, 2025 at 5:11 PM Version not provided'.



En el rubro de las pruebas en apego a OWASP:

OWASP-Dependency-Check

Critical Severity Vulnerabilities	0
High Severity Vulnerabilities	0
Inherited Risk Score	0
Low Severity Vulnerabilities	0
Medium Severity Vulnerabilities	0
Total Dependencies	0
Total Vulnerabilities	0
Vulnerable Component Ratio	0.0%
Vulnerable Dependencies	0

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#

The screenshot shows a Visual Studio interface with the following details:

- Solution Explorer:** Shows the project structure for "APIXIGAPORTALES".
- Code Editor:** Displays a C# file named "Crypto.cs" containing code for encrypting strings using the Crypto library. The code includes comments explaining the conversion of strings to byte arrays and the generation of salts and keys for encryption.
- Notifications:** A floating window showing "No new notifications".
- Calendar:** A calendar view for March 2025, with the 5th highlighted in blue.
- Taskbar:** Shows various pinned icons and the system clock indicating "04:57 p.m. 05/03/2025".

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

SQL Commit Rollback Auto XIGA QA dbo@GasmartCard

stp_erp_getSign x gmc_client 1 x

select * from gmc_client gc where number=16

	hash_type	is_check	status	last_purchase_date	last_payment_date	password	passw	Valor
1	B	A	[NULL]	[NULL]	[NULL]	f3a0755d493d4abcf7cdc97cb3739177989dd482	[NULL]	16

Grilla Texto Record

Renovar Save Cancel Exportar datos ... 200 Y 1 1 row(s) fetched - 0.215s (0.006s fetch), on 2025-03-05 at 16:45:59 PST es Editable Inserción inteligente 4:1 [45]

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

04:59 p. m. 05/03/2025

En el código muestra líneas donde valida vigencia de contraseña

The screenshot shows a Visual Studio Code interface with the following details:

- File Explorer:** Shows the project structure for "APIXIGAPORTALES". The "Services" folder contains several .cs files: ServicesApp.cs, Security.cs, PaymentController.cs, IServicePaymentApp.cs, DashboardController.cs, DatabasePayment.cs, AppServices.csproj, appsettings.json, LoginController.cs, UserController.cs, and appsettings.Dev.cs.
- Code Editor:** Displays the content of ServicesApp.cs. The code handles user login validation, checking for valid clients and passwords, and handling password expiration.
- Terminal:** Shows the output of the build command: "dotnet build" followed by "dotnet run".
- Output:** Shows the result: "APIservices succeeded in 13.6s".
- Problems:** Shows no errors or warnings.
- Search:** A search bar at the bottom.
- Taskbar:** Shows icons for various applications like Filezilla, WinRAR, and Microsoft Edge.
- Right Panel:** A "Notifications" panel with the message "No new notifications". Below it is a calendar for March 2025, with March 5th highlighted.

Broken Authentication

4 de 6

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

The screenshot shows the XIGA application interface. On the left, there is a sidebar with various menu items: Catálogos, Movimientos, Facturación, Reportes, Pagos, Bitácora, Ayuda, and a user profile section for JORGE IVAN ARENAS. The main area is titled "Tablero" and contains a form for changing a password. The form fields are: "Contraseña Actual:", "Nueva Contraseña:", and "Confirmar Contraseña:". Below the form is a "Guardar" button. To the right of the form, there is a "Notifications" panel which is currently empty, displaying the message "No new notifications". Below the notifications is a calendar for March 2025, showing the days from 23 to 31. The date "miércoles, 5 de marzo" is highlighted with a blue circle. The Windows taskbar at the bottom shows various pinned icons and the system clock indicating "05:02 p.m. 05/03/2025".

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.

The screenshot shows a Microsoft Visual Studio interface. The code editor displays C# code for a class named DatabaseReports. The code includes several database queries using Entity Framework's `DbCommand` and `DbParameter` classes. A tooltip from the F12 key indicates the code is being debugged. The Solution Explorer on the left shows various project files, including Database.cs, DatabaseInvoicing.cs, DatabaseMovement.cs, DatabasePayment.cs, and DatabaseReports.cs. The Task List window on the right shows a single notification: "No new notifications". The status bar at the bottom provides system information like weather (14°C), battery level (Mayorm. soleado), and system date (07/03/2025).

```
public class DatabaseReports
{
    public List<Invoice> GetAccountStatements(int clientId, DateTime fromDate, DateTime toDate)
    {
        return invoices;
    }

    public List<Station> GetStationsByZone(int zoneId)
    {
        List<Station> stations = new List<Station>();
        string zone = zoneId.ToString();
        using (DataServer ds = new DataServer(_ctx.GasmartCard))
        {
            ds.AddParameter("method", "showStationByzone");
            if (!int.TryParse(zone, out zoneId))
            {
                return [];
            }
            else
            {
                ds.AddParameter("zoneId", zoneId);
            }
        }
    }
}
```