Informe de resultados de pruebas

Sistema de control Hotelero

Pruebas de Seguridad

#534236

Fecha de creación	23/10/2024
Analista de aseguramiento de calidad	Mario Roberto Godoy de Paz

Resumen de resultados

Casos de prueba	Cantidad
Con resultado exitoso	0
Con resultado fallido	0
No probados	0
Falsos positivos	0
Total	0

Escenarios con error	Cantidad
Críticos	2
No críticos	14

Tipo de prueba	Cantidad de errores
Robustez	0
Funcional	0
Usabilidad	0
Carga	0
Contenido	0
Configuración	0

Documentos asociados

Identificador	Nombre del documento	Versión	Revisión	Tipo de aplicación
563243	Resultados de pruebas	1.0	1	Web Service

Descripción del ambiente de pruebas

Servidores	
Componentes	**Revisión**
Api rest	1
Precondiciones generales	
SonarCloud - Vooki	

Resultados

Id. Escenario	Nombre escenario	Resultado esperado	Éxito	Crítico	No. Casos de prueba
01-01	Api rest	El mínimo de puntos graves de seguridad	SI	NO	5342
01-02	Código	Puntos vulnerables ninguno	SI	SI	6432

Detalle de las pruebas realizadas

Caso de prueba 01-01-01	Api rest	ÉXITO	NO CRÍTICO
Tipo de prueba	Configuración	Nivel del error	Seguridad
Precondiciones			
• El servidor debe estar correctamente configurado para responder a solicitudes HTTPS. • Los endpoints deben estar accesibles y funcionales durante la prueba.			
Datos de prueba			
Solicitud de Prueba: solicitudes de pruebas GET **Autenticación**: Requiere autenticación con token jwt. **Encabezados de Solicitud**: Authorization			
Detalle del resultado obtenido			
Paso 1: Realizar una solicitud HTTPS al endpoint objetivo. **Paso 2**: Verificar que la respuesta incluya el encabezado **Strict-Transport-Security** con los parámetros correctos. **Paso 3**: Validar que el encabezado tenga una directiva **max-age** configurada adecuadamente (ej. max-age=31536000). **Paso 4**: Revisar si el encabezado incluye la directiva **includeSubDomains**, si es aplicable. **Paso 5**: Si la página soporta HSTS preload, verificar que el dominio esté registrado en la lista de preload.			
Procedimiento de ejecución			
• No se detectaron errores críticos ni problemas de seguridad graves. • El servidor respondió correctamente dentro del tiempo esperado, y la política HSTS se aplicó correctamente en todos los subdominios.			

Caso de prueba 01-01-02	Código	ÉXITO	NO CRÍTICO
Tipo de prueba	Configuración	Nivel del error	Seguridad
Precondiciones			
• El código debe estar completamente disponible y sin errores de compilación. • La herramienta SonarCloud debe estar configurada correctamente para ejecutar el análisis. • Se deben aplicar las reglas de calidad y seguridad definidas previamente.			
Datos de prueba			
• Se utilizó el código fuente del servicio web, versión actual, para realizar el escaneo. • Se configuraron los siguientes parámetros para el análisis: reglas de seguridad OWASP, buenas prácticas de programación, y análisis de vulnerabilidades conocidas.			
Detalle del resultado obtenido			
El análisis estático del código fue exitoso, se detectaron vulnerabilidades críticas en este caso 1. Se identificaron algunas recomendaciones menores en cuanto a refactorización de código para mejorar la mantenibilidad, como la eliminación de código duplicado y optimización en ciertas funciones.			
Procedimiento de ejecución			
• **Paso 1**: Ejecutar SonarCloud para realizar el análisis estático del código fuente. • **Paso 2**: Verificar que el código cumpla con las mejores prácticas de programación, identificando problemas como vulnerabilidades de seguridad, bugs y código duplicado. • **Paso 3**: Revisar los resultados del análisis, enfocándose en vulnerabilidades de seguridad como inyecciones SQL, problemas de validación de entradas, y exposiciones a riesgos como Cross-Site Scripting (XSS). • **Paso 4**: Documentar todas las vulnerabilidades y problemas detectados, clasificándolos según su severidad (baja, media, alta). • **Paso 5**: Realizar recomendaciones para corregir los problemas detectados, como mejoras en el manejo de excepciones y validaciones.			

Observaciones

- **Observación para Escaneo de Código**:
  Se identificaron varios fragmentos de código que no cumplen con las mejores prácticas de seguridad, lo que podría aumentar la vulnerabilidad del sistema. Es recomendable realizar una revisión de estos fragmentos y aplicar las correcciones necesarias.

- **Observación para Flujo del API REST**:
  Se recomienda configurar el servidor web para incluir el encabezado **Strict-Transport-Security** (HSTS) con una directiva **max-age** apropiada en todas las respuestas HTTP. Una configuración comúnmente recomendada es **max-age=31536000** (un año), lo que asegura la aplicación a largo plazo de conexiones seguras.