REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN DE APLICACIÓN

ÍNDICE

1. Introducción

La información reflejada en el presente documento es propiedad exclusiva de Pegasus Control. Cualquier tipo de modificación que se realice sobre el mismo deberá de ser supervisada por personal autorizado. Si en algún momento esta norma no se cumpliese, el contenido del documento sería considerado nulo y carecería de total validez.

La información contenida se divide en una serie de apartados como son:

- Introducción: información explicativa de la distribución de la información contenida en el informe.
- Objetivo: información explicativa del objetivo del documento.
- Confidencialidad: en este apartado se detallan un conjunto de consideraciones relativas a la distribución y confidencialidad del documento.
- Marco de referencia: apartado en donde se enlistan los dispositivos dentro del alcance y su fecha de revisión.
- Metodología: aquí se agrupan un conjunto de recomendaciones de uso para el presente informe.
- Vulnerabilidades detectadas: presenta un listado de vulnerabilidades identificadas en lugares concretos. El concepto de ocurrencia se asocia a un problema de seguridad en una ubicación específica.

2. Objetivo

El presente documento tiene como finalidad, presentar y describir el resultado del escaneo de vulnerabilidades realizado al entorno de controles volumétricos.

3. Confidencialidad

La información contenida en este documento es propiedad intelectual de Pegasus Control en el contexto de análisis de vulnerabilidades. No está permitida su distribución a terceros ni darle un uso diferente al anteriormente citado. Cualquier modificación de su contenido deberá de ser autorizada expresamente y supervisada por personal autorizado de Pegasus Control.

Se entiende que esta norma es previa y de obligado cumplimiento para todas aquellas personas que puedan tener acceso a este documento, se obligan a garantizar la seguridad, integridad y confidencialidad de la información intercambiada entre ellas.

Asimismo, se acuerda que tendrá la consideración de información confidencial, toda información susceptible de ser revelada de palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, intercambiada como consecuencia de la presente oferta o, llegado el caso, del proyecto futuro que pudiera desarrollarse.

Pegasus Control adoptará las medidas oportunas para:

- Garantizar el correcto uso y destino de la información que se considere confidencial.
- Permitir el acceso a esta información tan sólo a aquellas personas físicas o jurídicas que la necesiten para el desarrollo de tareas para las que su uso sea estrictamente necesario.
- A este respecto, la parte receptora de la información advertirá a dichas personas de sus obligaciones respecto a la confidencialidad, velando por el cumplimiento de estas.
- No develar ni revelar información de una de las partes a terceras personas salvo autorización previa y escrita de dicha parte.
- Mantener vigente este compromiso de confidencialidad durante la vigencia de la oferta, y en su caso durante la vigencia del proyecto/contrato que se genere, como consecuencia de la aceptación de la presente oferta.

Las consideraciones anteriores no aplicarán a ninguna información sobre la que cualquiera de las partes pudiera demostrar que fuera del dominio público en el momento de haberle sido revelada, que tuviera consentimiento escrito previo de la otra parte para ello o que exista obligación legal de o que haya sido solicitada por una autoridad administrativas o judiciales competente.

3. Responsabilidades

Actividades	Responsable
Ejecutar escaneo de vulnerabilidades. Identificar y clasificar los hallazgos para presentarlos.	Sysadmin
Tomar los requerimientos, planificar las actividades y tiempo para contener o resolver los hallazgos encontrados.	Sysadmin
Ejecutar las acciones correctivas dentro del área de aplicativo.	Gerente de producto

Figura 1. Tabla de Responsabilidades

4. Marco de referencia

- Para la detección de vulnerabilidades de la aplicación se usan los criterios establecidos por las organizaciones de seguridad informática líderes y vigentes que son:
    - **OWASP Top 10:** Listado de los 10 riesgos de seguridad más importantes.
    - **SANS TOP 25:** Describe los errores de software más peligrosos.
    - **CWE:** Sistema de categorías que describe las debilidades y vulnerabilidades del software

4.1 Alcance

El presente reporte detalla las vulnerabilidades detectadas en los sistemas de software involucrados en el entorno de controles volumétricos listados a continuación:

Nombre
SGC Planta
SGC Estacion

El análisis de vulnerabilidades se realizó durante la siguiente ventana temporal:

Fecha de Inicio	10-09-2021
Fecha de Fin	10-09-2021

4.2 Vulnerabilidades de software

Las vulnerabilidades de software identifican brechas de seguridad en el software que puede permitir a terceros atacantes obtener acceso no autorizado a la información, el borrado de la información o la sustitución de la información afectando la integridad y confiabilidad de la información

4.3 Escaneo de vulnerabilidades

Un escaneo de vulnerabilidades, es una actividad que se ejecuta por un experto en seguridad informática, que permite detectar ya sea manual, o con la ayuda de sistemas especializados, las vulnerabilidades más comunes y las vulnerabilidades documentadas en diccionarios de vulnerabilidades.

Los escaneos de vulnerabilidades pueden realizarse de manera manual y pueden realizarse con ayuda de software de seguridad específicos, que permiten automatizar y realizar un escaneo en un tiempo mucho menor del que una persona puede realizarlo.

4.4 Tipos de Escáner

A continuación describiremos una serie de escáneres de vulnerabilidades que pueden ser

utilizados por las empresas para encontrar los puntos débiles y así mitigar los riesgos:

Escáner de red: Escáner de uso general usado para encontrar vulnerabilidades potenciales en la red de la empresa. (también se podría incluir a los escáneres de redes VoIP)
Escáner de Puerto: Software diseñado para buscar en una red los puertos abiertos que podrían ser usados por los atacantes como puntos de entrada.
Escáner para la Seguridad de aplicaciones web: Permite a los negocios realizar evaluaciones de riesgo para identificar las vulnerabilidades en aplicaciones web y así evitar ataques. Este tipo de escáneres deberían ser utilizados también por el departamento de desarrollo (programación) de una aplicación web, ayudando así a encontrar todos los bugs que puedan generarse durante la creación de la aplicación, antes de poner la aplicación a un entorno de producción.
Escaner de Base de datos: Permite encontrar puntos débiles en bases de datos, protegiendo así el activo más importante de una empresa.

4.5 Herramientas para hacer escaneo de vulnerabilidades

La herramienta seleccionada y autorizada para realizar el escaneo de vulnerabilidades de software es la siguiente:

- **SonarQube:** SonarQube es una herramienta de análisis continuo de seguridad y calidad de código, SonarQube se basa en **OWASP Top 10, SANS TOP 25 y CWE** como definiciones para el escaneo de seguridad de la información.

4.6 Criterio de Clasificación

Las vulnerabilidades identificadas han sido clasificadas de la siguiente forma:

SEVERIDAD	DESCRIPCIÓN
MENOR	Son consideradas satisfactorias durante una revisión, sin embargo, se propone corregir estas vulnerabilidades para minimizar la probabilidad de riesgo al mínimo.

MAYOR	Son vulnerabilidades que deben ser corregidas para obtener un estado CONFORME en la seguridad de la aplicación pero su riesgo o probabilidad de ocurrencia no es tan alto.
CRÍTICA	Son vulnerabilidades que deben ser corregidas para obtener un estado CONFORME en la seguridad de la aplicación, son vulnerabilidades que requieren ser solucionadas inmediatamente de ser detectadas.

5. Metodología:

1. El personal interno designado debe realizar el escaneo una vez cada doce meses a las aplicaciones.
2. El escaneo debe de ser notificado al SysAdmin, Gerente de producto y Líder de producto para contemplar en su plan de actividades.
3. Realizado el escaneo de vulnerabilidades, el personal interno debe de presentar los reportes (Ejemplo: Evidencia escaneo de vulnerabilidades) al Sysadmin para que pueda clasificar las vulnerabilidades y ver la importancia del impacto
4. Realizada la clasificación de vulnerabilidades a los activos, el personal interno debe de llenar el documento **DOC-033-TI BITÁCORA ESCANEO VULNERABILIDADES** el punto anterior.
5. Con la bitácora completa correctamente, se presentará al Líder de producto y Gerente de producto para poder presentar los hallazgos y planificar las acciones correctivas de acuerdo al documento **PRT-034-TI SEGUIMIENTO A HALLAZGOS EN PRUEBAS DE VULNERABILIDAD DE SOFTWARE**

6. Descripción detallada de las actividades realizadas

1) El usuario Sysadmin se conecta al equipo 192.168.9.126 en el cual se encuentra la aplicación de escaneo de vulnerabilidades Sonarqube
2) Se actualizan las aplicaciones a la última versión en el equipo.
3) Se ejecutan los análisis de vulnerabilidades desde la terminal para los proyectos SGC Planta y SGC Ventas
4) Se ingresa a la plataforma web de SonarQube 192.168.9.126:9000 se ingresa a cada proyecto y dentro de Overview se selecciona la opción Vulnerabilidades
5) Se guarda impresión del reporte y se documentan los hallazgos en este reporte.

7. Vulnerabilidades identificadas

La siguiente tabla muestra el resumen de vulnerabilidades detectadas:

Criticidad	Baja	Media	Alta
Total	**0**	**0**	**27**

Figura 1: Resumen de vulnerabilidades detectadas

SGC Planta

Archivo	Línea	VULNERABILIDAD	Regla	Criticidad
ModuleInstall/PackageManager/PackageManagerDownloader.php	30	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/nusoap/class.soap_transport_http.php	205	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/nusoap/class.soap_transport_http.php	206	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/nusoap/nusoap.php	2204	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/nusoap/nu	2205	Enable server certificate	cwe	Alta

soap.php		validation on this SSL/TLS connection	owasp-a3 owasp-a6	
include/phpmailer/class.smtp.php	194	Change this code to use a stronger protocol.	cwe owasp-a3 owasp-a6	Alta
modules/SchedulersJobs/SchedulersJob.php	183	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
modules/SchedulersJobs/SchedulersJob.php	184	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
modules/.../LDAPAuthenticate/LDAPAuthenticateUser.php	307	Provide username and password to authenticate the connection	cwe owasp-a2	Alta
service/example/Rest_Proxy.php	26	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta

SGC Estacion

Archivo	Línea	VULNERABILIDAD	Regla	Criticidad
ModuleInstall/PackageManager/PackageManagerDownloader.php	64	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/nusoap/class.soap_transport_http.php	205	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/nusoap/class.soap_transport_http.php	206	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/nusoap/nusoap.php	2204	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/nusoap/nusoap.php	2205	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
include/phpmailer/	194	Change this code to use a	cwe	Alta

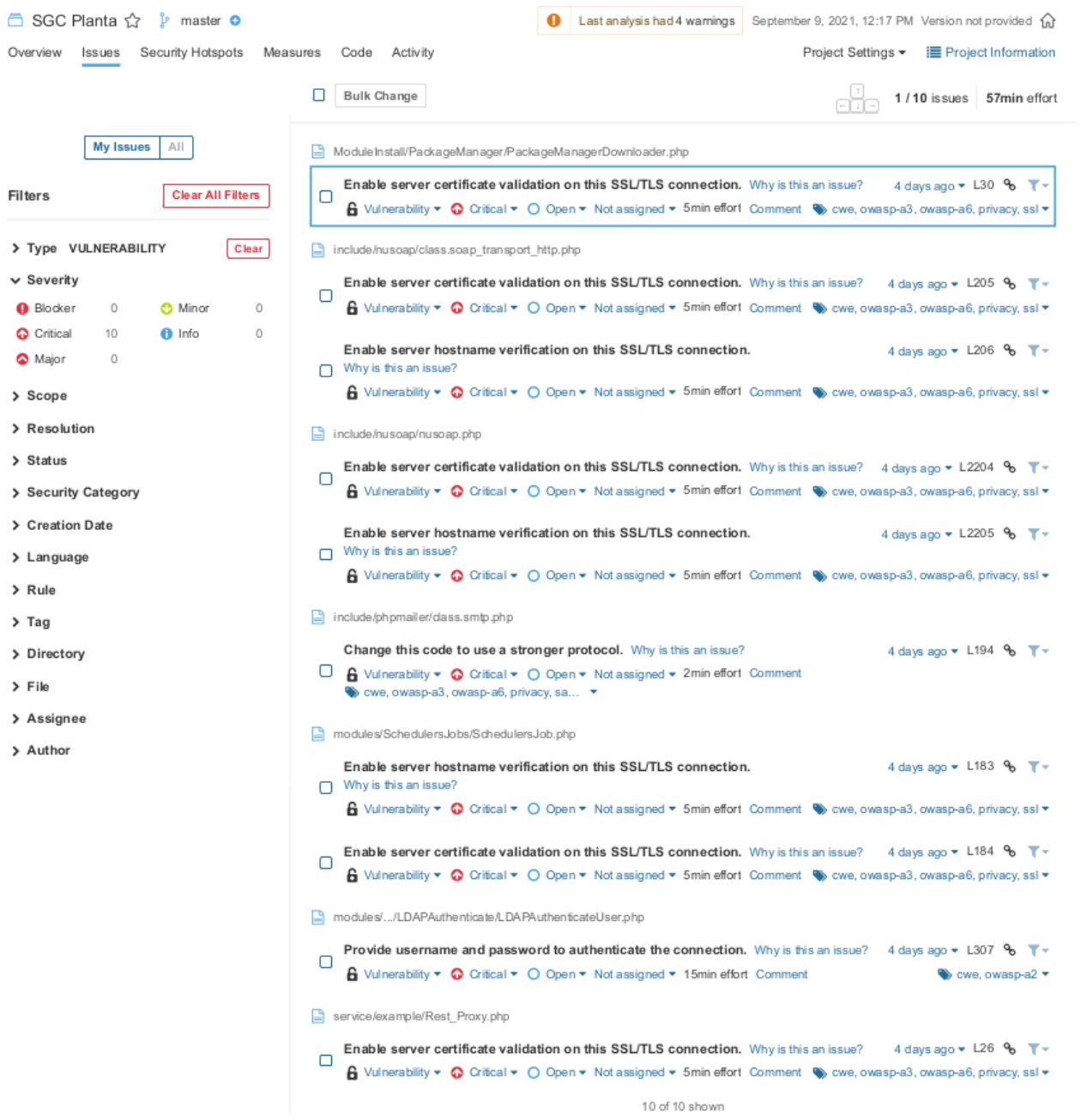
class.smtp.php		stronger protocol.	owasp-a3 owasp-a6	
modules/SchedulersJobs/SchedulersJob.php	216	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
modules/SchedulersJobs/SchedulersJob.php	217	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
modules/.../LDAPAuthenticate/LDAPAuthenticateUser.php	340	Provide username and password to authenticate the connection	cwe owasp-a2	Alta
modules/.../library/Zend/Mail/Protocol/Imap.php	113	Change this code to use a stronger protocol	cwe owasp-a3 owasp-a6	Alta
modules/.../library/Zend/Mail/Protocol/Pop3.php	124	Change this code to use a stronger protocol	cwe owasp-a3 owasp-a6	Alta
modules/.../library/Zend/Mail/Protocol/Smtp.php	210	Change this code to use a stronger protocol	cwe owasp-a3 owasp-a6	Alta
modules/.../conexionInternet.php	12	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
modules/.../envioArchivos.php	141	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
modules/isies_importacion/saldosCreditosIcontrol.php	88	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
service/example/Rest_Proxy.php	59	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta
ws/1070/example/Rest_Proxy.php	59	Enable server certificate validation on this SSL/TLS connection	cwe owasp-a3 owasp-a6	Alta

8. Plan de seguimiento a los hallazgos encontrados

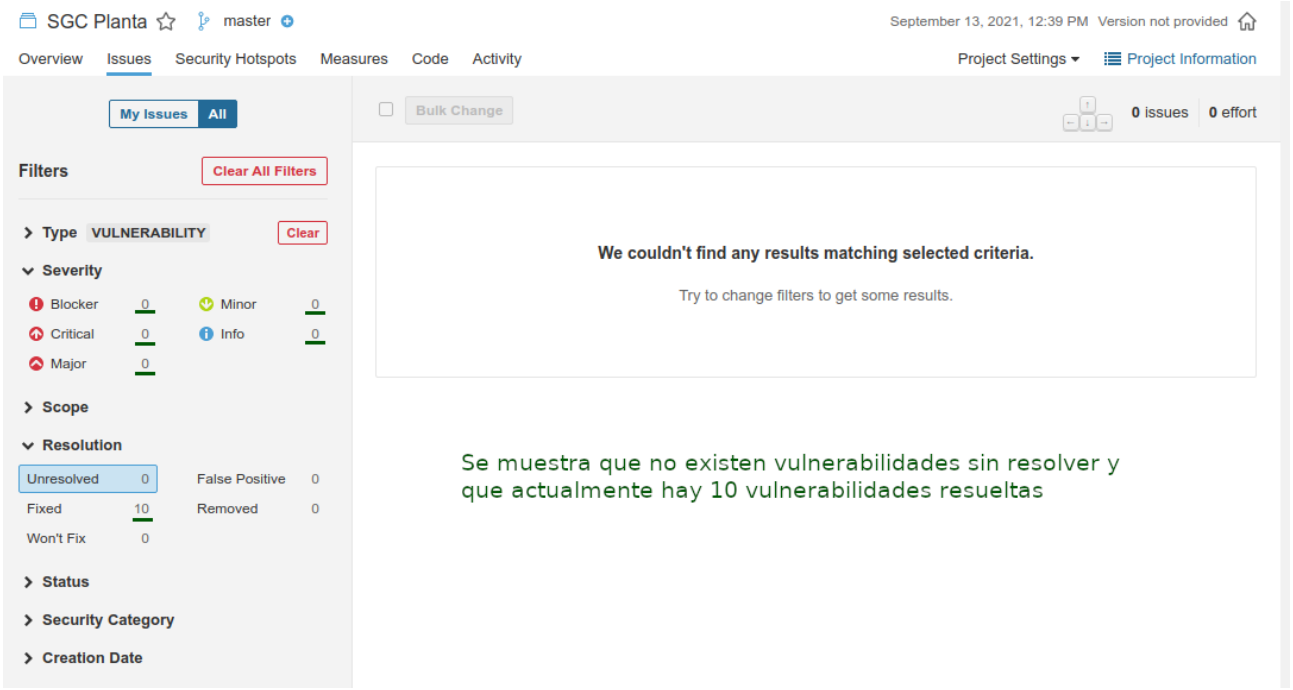
Todos los hallazgos con prioridad Alta deben ser corregidos en máximo 30 días y se deberá adjuntar la prueba de corrección de los mismos con un nuevo escaneo de los productos, visualizando que ya no se encuentren las vulnerabilidades detectadas.

Evidencia ejecuciones planificadas y completadas

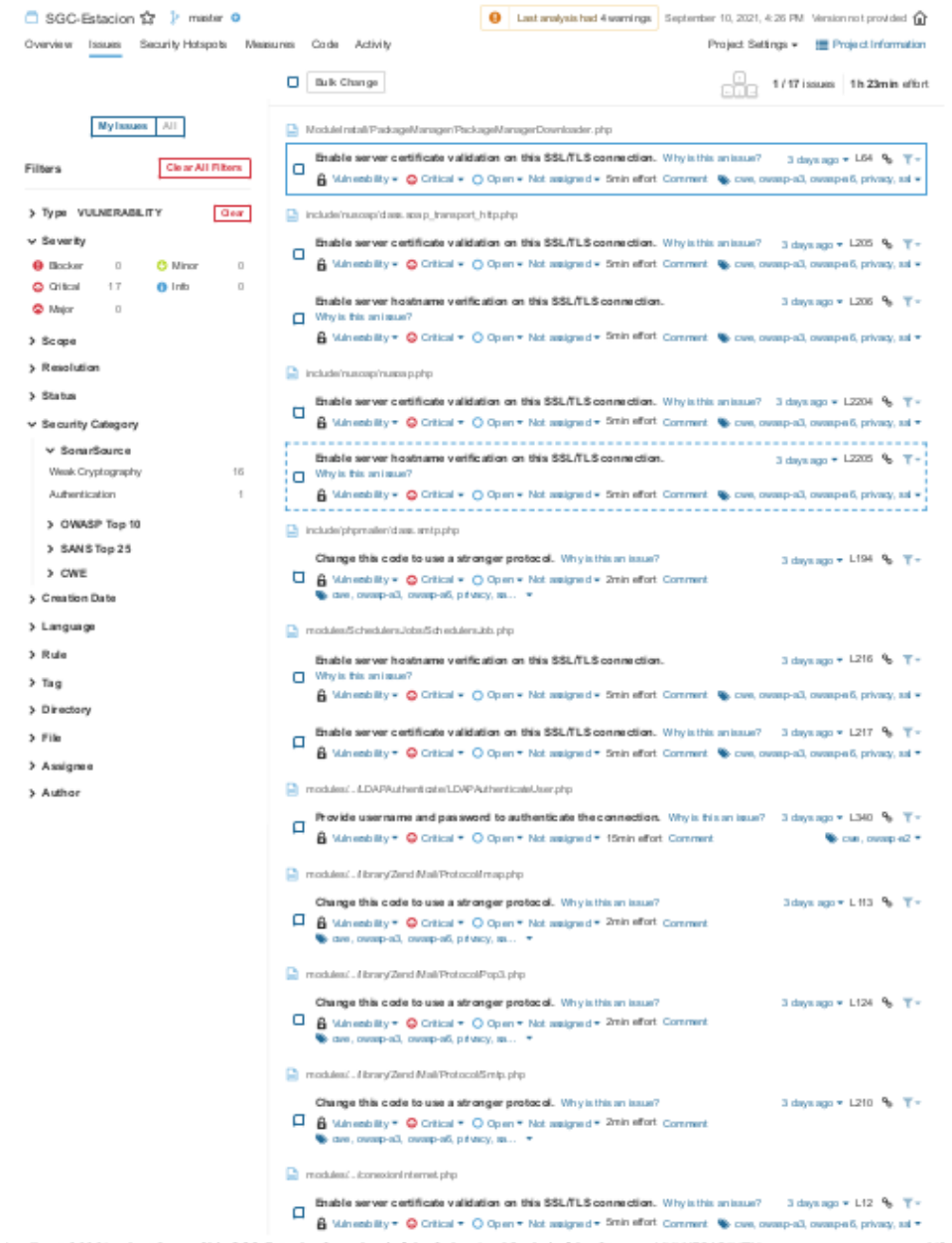
Evidencia Escaneo SGC Planta

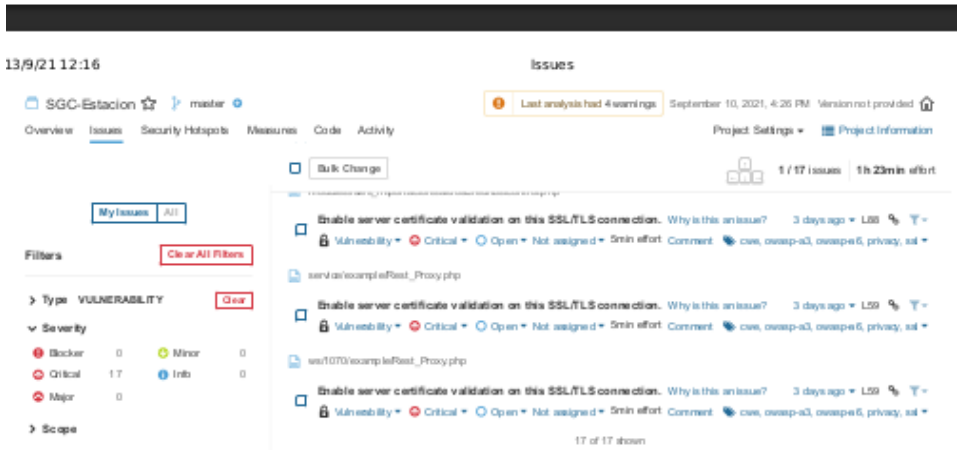


Evidencia Escaneo SGC Planta vulnerabilidades resueltas

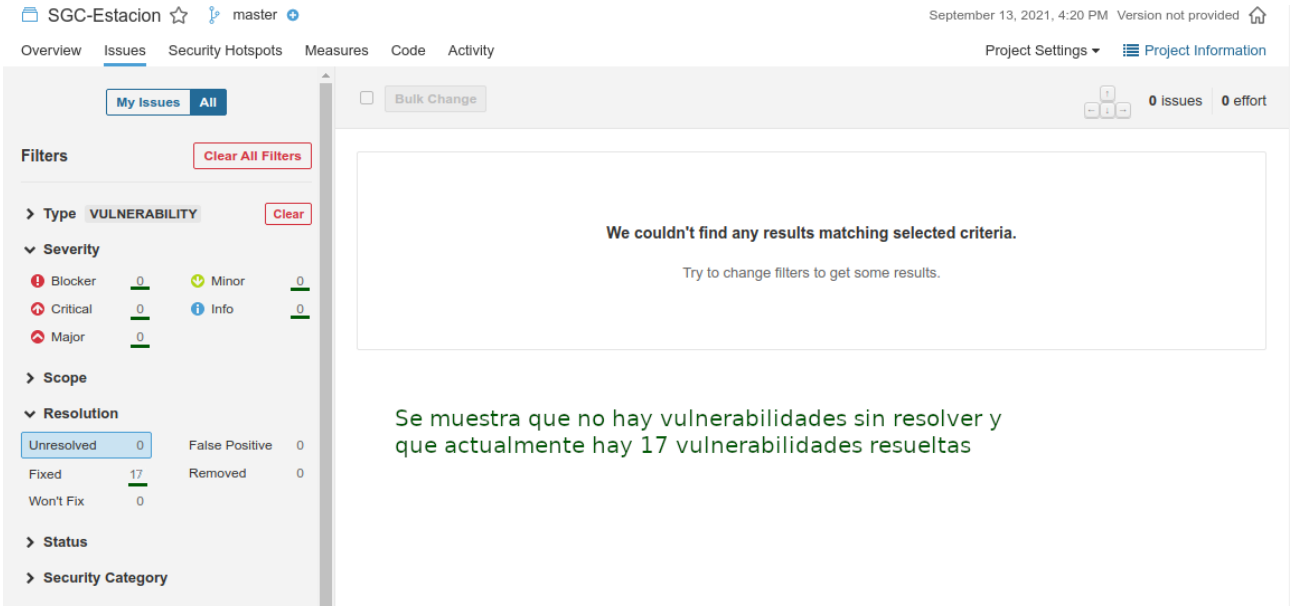


Evidencia Escaneo SGC Estación





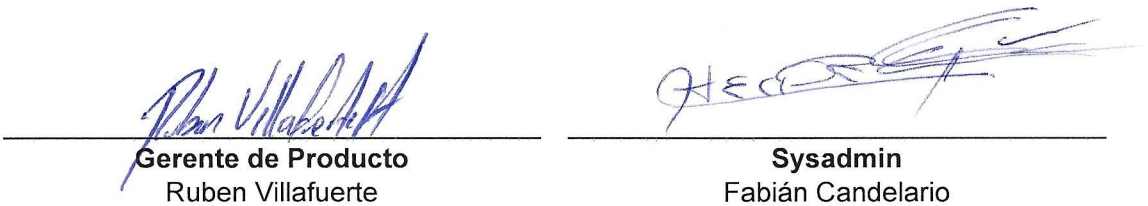
Evidencia Escaneo SGC Estacion vulnerabilidades resueltas



9. Historial de Revisiones

Versión	Fecha	Cambios	Elaboró	Revisó	Aprobó
1.0	13/09/2021	Creación de documento	Silvestre Garcia	Rubén Villafuerte	Rubén Villafuerte
1.1	06/12/2022	Revisión de documentación	Omar Aguilar	Rubén Villafuerte	Rubén Villafuerte

10. Firmas de Revisión



Gerente de Producto
Ruben Villafuerte

Sysadmin
Fabián Candelario