BACKLOG

Tablas de registro

Listas de requerimientos	
Historias de usuarios	Requerimientos
Jean quiere una Presentación Ejecutiva que describa el modelo DevSecOps para mejorará la seguridad de los productos de la empresa ToCupboard.	-Descripción de cómo la seguridad se incorpora en cada fase del ciclo de desarrollo (desarrollo, integración, despliegue, mantenimiento).
Jean gerente de TI, quiero que todo el equipo de desarrollo reciba capacitación regular en seguridad, para que comprendan mejor las amenazas y puedan escribir código más seguro.	-Los desarrolladores completan la capacitación y pasan un examen de certificación.
Jean desarrollador web, quiero implementar autenticación segura utilizando mecanismos como OAuth o JWT, para que los usuarios puedan acceder a sus cuentas de forma segura y proteger la integridad de la sesión.	-Se implementa un sistema de autenticación que utiliza tokens seguros (OAuth o JWT). -Se realiza una revisión de seguridad para asegurar que el sistema de autenticación es resistente a ataques comunes.
Jean desarrollador web, quiero asegurar que mi sitio web utilice HTTPS y políticas de seguridad de contenido (CSP) adecuadas, para que los datos del usuario estén cifrados y se reduzca el riesgo de ataques como XSS y MITM.	-El sitio web utiliza certificados SSL/TLS válidos para asegurar las comunicaciones HTTPS. -Se configura y aplica una política de seguridad de contenido (CSP) estricta. -Se verifica que todas las conexiones al sitio se realicen a través de HTTPS.
Jean Como administrador de seguridad, quiero generar reportes sobre los incidentes de seguridad detectados en el sitio web, para que pueda realizar un seguimiento detallado y analizar patrones para mejorar la seguridad.	-Los incidentes críticos se destacan y se proporcionan recomendaciones para prevenir futuros incidentes.

Lista priorizada			
Requerimientos	Etapas	tiempo	Entregable
Descripción de cómo la seguridad se incorpora en cada fase del ciclo de desarrollo (desarrollo, integración, despliegue, mantenimiento).	1	24hrs	13de septiembre
El sitio web utiliza certificados SSL/TLS válidos para asegurar las comunicaciones HTTPS. -Se configura y aplica una política de seguridad de contenido (CSP) estricta. -Se verifica que todas las conexiones al sitio se realicen a través de HTTPS.	2	24hrs	16 de septiembre
Jean Como administrador de seguridad, quiero generar reportes sobre los incidentes de seguridad detectados en el sitio web,	3	24hrs	16 de septiembre

para que pueda realizar un seguimiento detallado y analizar patrones para mejorar la seguridad.			

ROADMAP

Página web en WordPress

Objetivo General: Implementar un modelo DevSecOps, asegurando la protección de los recursos de la nube y el cumplimiento de las mejores prácticas de seguridad en el desarrollo y despliegue de una página web en WordPress con pasarela de pago.

Objetivos Específicos:

- Aplicar Mejores Prácticas de Seguridad en la Nube para el Modelo DevSecOps.
- Desplegar y Configurar una Página Web en WordPress con Pasarela de Pago.
- Realizar una Evaluación de Seguridad Inicial.
- Documentar y Reportar la Configuración de Seguridad.

Entregables: en proceso

Fechas de entrega:

Sprint 1: viernes 13 de septiembre

Sprint 2: Domingo15 de septiembre

Sprint 3: lunes 16 de septiembre

Procesos Involucrados:

- **Desarrollo e Implementación del Modelo DevSecOps:** Integrar prácticas de seguridad en el ciclo de vida del desarrollo de software, desde la codificación hasta el despliegue.
- **Configuración de la Página Web en WordPress:** Desplegar y asegurar una instalación de WordPress, incluyendo la integración de una pasarela de pago segura.
- **Evaluación y Documentación de Seguridad:** Realizar una evaluación de seguridad para identificar y mitigar riesgos, y documentar las configuraciones y prácticas de seguridad implementadas.

Entregables	Actividades	Plazo de entrega
Sprint1	Modelo devsecops	Viernes 13
Sprint2	Desarrollar una página web en WordPress.	Lunes16
Sprint 3	Reporte de seguridad	lunes16

Digital_NAO

Consultor de Ciberseguridad

RETO 2: Protocolos de seguridad con pentesting y criptografía

Nombre completo:

Jean Carlos Delgado Montes

NAO ID:

3163

16/09/24

Índice

Reporte de Evaluación de Riesgos y Seguridad

Nombre del Proyecto: Evaluación de Seguridad de la Tienda Online (Expansión impecable)

1.Introducción

El propósito de este reporte es documentar los hallazgos derivados de la evaluación de riesgos y seguridad realizada en el sitio web de una tienda online. El objetivo principal es identificar vulnerabilidades potenciales y proponer soluciones adecuadas para garantizar la integridad, confidencialidad y disponibilidad de los datos y servicios ofrecidos por el sitio.

1.1. Metodología

La evaluación de riesgos y seguridad se llevó a cabo utilizando un enfoque sistemático que incluye las siguientes etapas:

1. **Revisión Documental**: Análisis de la documentación existente relacionada con la seguridad del sitio web y la pasarela de pagos.
2. **Escaneo de Vulnerabilidades**: Uso de herramientas automatizadas para identificar vulnerabilidades comunes en el sitio web y la pasarela de pagos.
3. **Revisión de Configuración**: Inspección de la configuración del servidor web, bases de datos y pasarela de pagos para asegurar prácticas seguras.

Evaluación de Seguridad del Sitio Web

2.1. Descripción del Sitio Web

El sitio web evaluado es una tienda online que ofrece productos de cuidado a la piel y permite a los usuarios realizar compras en línea. El sitio está basado en la plataforma WordPress https://expansion.free.nf .

3.2. Análisis de Vulnerabilidades

- **Wpscan: es una herramienta poderosa para administradores de WordPress y profesionales de seguridad que buscan asegurar sus instalaciones de WordPress contra vulnerabilidades conocidas**.

3.3. Evaluación de Seguridad de la Infraestructura

- **Configuración del Servidor**: el servidor está configurado correctamente y seguro
- **Certificados SSL**: se utiliza HTTPS, el certificado SSL está configurado con las últimas prácticas de seguridad.

Evaluación de Seguridad de la Pasarela de Pagos

4.1. Descripción de la Pasarela de Pagos

La pasarela de pagos utilizada en el sitio web es PayPal. Esta pasarela gestiona las transacciones financieras y se integra con el sitio web.

4.2. Análisis de Vulnerabilidades

- **Protección de Datos de Tarjeta**: Se identificó que los datos de la tarjeta de crédito están cifrados adecuadamente en el lado.
- **Validación de Transacciones**: La pasarela implementa medidas robustas para validar transacciones sospechosas.

4.3. Evaluación de la Integridad y Protección de Datos

- **Seguridad en el Tránsito**: se monitora con wpscan y me informa si hay alerta por medio de mi correo personal.
- **Almacenamiento de Datos Sensibles**: Los datos sensibles se almacenan en una base de datos con las medidas adecuadas de cifrado y protección.

. Hallazgos y Análisis

5.1. Hallazgos en la Evaluación del Sitio Web

- **Inyección SQL**: No se identificaron vulnerabilidades de inyección SQL durante el análisis automatizado y las pruebas manuales. Sin embargo, se recomienda mantener prácticas de codificación seguras para evitar futuros problemas.
- **Cross-Site Scripting (XSS)**: No se encontraron vulnerabilidades de XSS en el análisis realizado con wpscan. El sitio está adecuadamente configurado para evitar la ejecución de scripts maliciosos.

- **Configuración del Servidor**: La configuración del servidor ha sido revisada y está alineada con las mejores prácticas de seguridad. No se encontraron configuraciones inseguras.
- **Certificados SSL**: El certificado SSL está correctamente configurado con las últimas prácticas de seguridad, como TLS 1.2/1.3 y Perfect Forward Secrecy (PFS). No se identificaron problemas relacionados con la configuración de SSL.

5.2. Hallazgos en la Evaluación de la Pasarela de Pagos

- **Protección de Datos de Tarjeta**: Los datos de tarjeta de crédito están cifrados adecuadamente durante el tránsito y el almacenamiento, cumpliendo con los estándares PCI-DSS.
- **Validación de Transacciones**: La pasarela de pagos implementa medidas robustas para validar transacciones sospechosas y detectar fraudes, garantizando la seguridad de las transacciones.
- **Seguridad en el Tránsito**: La pasarela de pagos se monitorea regularmente utilizando WPScan y se notifica cualquier alerta relevante al correo personal del administrador, asegurando una respuesta rápida ante posibles amenazas.
- **Almacenamiento de Datos Sensibles**: Los datos sensibles se almacenan en una base de datos cifrada y protegida, siguiendo las mejores prácticas de seguridad.

Recomendaciones

1. **Monitoreo Continuo**: Implementar un sistema de monitoreo continuo para detectar vulnerabilidades emergentes y ataques en tiempo real. Aunque no se encontraron problemas graves, el monitoreo continuo ayudará a identificar nuevas amenazas rápidamente.
2. **Actualización de Plugins y Temas:** Mantener todos los plugins y temas del sitio web actualizados a sus versiones más recientes. Las actualizaciones regulares aseguran que las vulnerabilidades conocidas se resuelvan y se mantenga la seguridad del sitio.
3. **Pruebas de Penetración Regulares**: Realizar pruebas de penetración periódicas para evaluar la seguridad del sitio web y la pasarela de pagos. Las pruebas de penetración ayudan a identificar vulnerabilidades que no se detectan con escáneres automáticos.
4. **Revisión de Políticas de Seguridad**: Revisar y actualizar las políticas de seguridad y procedimientos de respuesta a incidentes. Tener políticas claras y actualizadas asegura una respuesta efectiva en caso de un incidente de seguridad.

Conclusión:

La evaluación de seguridad del sitio web de la tienda online y su pasarela de pagos ha demostrado que el sistema está bien configurado y protegido en las áreas revisadas. No hay vulnerabilidades críticas en el sitio web ni en la pasarela de pagos. La implementación de las recomendaciones proporcionadas ayudará a fortalecer aún más la seguridad del sitio y a garantizar que se mantenga protegido frente a nuevas amenazas.

El compromiso con la seguridad proactiva y la mejora continua es fundamental para proteger los datos de los usuarios y asegurar la integridad de las transacciones en línea.