Nombre:

Lirys Nayely Zambrano Salazar

NAO ID

3127

Fecha

18/08/2024

Nombre de la trayectoria

Integridad y autenticidad de la información

Título del Reto

Protocolos de seguridad con pentesting y criptografía

Implementación del Modelo DevSecOps

El modelo **DevSecOps** se ha aplicado en el proyecto **ToCupboard**, siguiendo las mejores prácticas. A continuación, se describen los detalles de las medidas implementadas:

1. Integración Continua y Despliegue Continuo (CI/CD)

Debido a limitaciones en la infraestructura gratuita utilizada (InfinityFree), la implementación de un pipeline automatizado completo para CI/CD no ha sido posible. Sin embargo, se ha establecido una metodología de despliegue manual:

- **Verificación continua**: Cada vez que se realiza una modificación en el sitio (como actualizaciones de plugins o temas), se ejecutan pruebas de seguridad manuales y se verifican las integraciones de APIs.
- **Automatización parcial**: Se configuraron tareas manuales para la revisión de los logs y la supervisión de eventos de seguridad tras cada despliegue.
- **Copias de seguridad**: Se han configurado copias de seguridades automatizadas cada cierto tiempo para tener guarda la información del sistema.

2. Seguridad en las Integraciones de APIs

Se han integrado dos APIs:

- **PayPal API**: Se implementó una API de PayPal para procesar pagos en modo Sandbox utilizando **WooCommerce**. Esto permite simular transacciones y pruebas de pago en un entorno seguro.
- **Instagram API**: A través de un plugin, se integró la API de Instagram, utilizando un **Access Token** para mostrar el feed de la cuenta. Esta integración fue configurada siguiendo los principios de seguridad.

3. Prácticas de Seguridad Implementadas

a) Protección del Acceso

- **Autenticación de Dos Factores (2FA)**: Se ha implementado autenticación de dos factores para los administradores del sitio, asegurando que el acceso a la administración del sitio esté protegido por algo más que solo contraseñas.
- **Ocultación de la Página de Inicio de Sesión**: El plugin **WPS Hide Login** fue configurado para ocultar la URL predeterminada de acceso al administrador de WordPress, reduciendo las oportunidades de ataque a la página de inicio de sesión.

b) Protección Contra Vulnerabilidades Comunes

- **Wordfence**: Se implementó este plugin de seguridad para monitorear actividades sospechosas, escanear en busca de vulnerabilidades comunes, y bloquear ataques potenciales.

4. Monitoreo de Vulnerabilidades y Evaluaciones de Seguridad

Debido a las restricciones con el hosting gratuito, no fue posible implementar herramientas como **Cloudflare** para añadir un firewall adicional y protección DDoS. Cloudflare requiere un dominio propio, y al estar utilizando un subdominio gratuito de InfinityFree (tocupboard.infinityfreeapp.com), no se pudo realizar la integración, pero se buscaron alternativas:

- Se intentó registrar un dominio gratuito con **Freenom**, pero no fue posible debido a la disponibilidad de nombres y limitaciones de la región.
- A pesar de esto, se lograron otras configuraciones de seguridad a nivel de WordPress, como el uso de plugins para monitorear tráfico malicioso y el bloqueo de direcciones IP sospechosas.

5. Planificación de Respuesta a Incidentes

- **Logs de Seguridad**: Wordfence ha sido configurado para generar logs de actividad y posibles vulnerabilidades, lo que permite responder rápidamente a incidentes de seguridad.
- **Notificaciones Automáticas**: Cualquier actividad sospechosa o intento de acceso no autorizado genera una alerta enviada por correo electrónico al administrador.