21-4-2025

Servicio Web en Producción

Unidad de trabajo 6

Francisco Javier Otero Herrero
Grupo ATU

Servicio Web en Producción

Servicio Web en Producción

Como administradores que somos de un portal web de difusión de noticias generalistas, tenemos que realizar el mantenimiento de nuestro portal. Para el mismo decidimos en su día montarlo con el ***CMS WordPress.*** *Responde a las siguientes cuestiones:*

PREGUNTAS/ACTIVIDADES A REALIZAR

I. *¿Qué operaciones debes tener definidas en los manuales de procedimiento para el mantenimiento del portal?*

✓ *Copias de Seguridad (Backups)*

- Procedimiento de Backup Completo:
  - Documentar cómo realizar copias de seguridad tanto de los archivos del sitio web como de la base de datos.
  - Especificar la frecuencia de los backups (diario, semanal, mensual, etc.).
  - Indicar dónde se almacenan los backups (servidor, nube, almacenamiento externo).
  - Definir un sistema de rotación de backups (cuántos backups se guardan y durante cuánto tiempo).
  - Probar periódicamente la restauración de los backups para asegurar que funcionan correctamente.

  - Procedimiento de Backup Incremental:
    - Si se utiliza, documentar cómo realizar backups incrementales (solo los cambios desde el último backup).

  - Procedimiento de Restauración:
    - Documentar los pasos para restaurar el sitio web desde un backup, incluyendo la restauración de archivos y la base de datos.

✓ *Actualizaciones*

- Procedimiento de Actualización de WordPress:
  - Explicar cómo actualizar el núcleo de WordPress a la última versión.
  - Recomendar la creación de un entorno de staging (copia del sitio web) para probar las actualizaciones antes de aplicarlas al sitio en producción.
  - Especificar los pasos para realizar un backup antes de la actualización.

- Documentar cómo resolver posibles problemas de compatibilidad.
- Procedimiento de Actualización de Plugins y Temas:
    - Explicar cómo actualizar los plugins y temas instalados.
    - Recomendar la verificación de la compatibilidad de los plugins y temas con la versión de WordPress.
    - Especificar los pasos para realizar un backup antes de la actualización.
    - Documentar cómo revertir a versiones anteriores si hay problemas.

✓ *Seguridad*

- Procedimiento de Análisis de Seguridad:

    - Documentar cómo realizar análisis de seguridad periódicos del sitio web.
    - Especificar las herramientas de seguridad utilizadas (plugins, escáneres externos, etc.).
    - Definir los pasos para identificar y corregir vulnerabilidades de seguridad.

    - Procedimiento de Gestión de Usuarios:
        - Explicar cómo crear, modificar y eliminar cuentas de usuario.
        - Definir las políticas de contraseñas (complejidad, caducidad, etc.).
        - Documentar cómo revocar accesos de usuarios en caso de necesidad.

    - Procedimiento de Monitorización de Seguridad:
        - Documentar cómo monitorizar los registros de actividad del sitio web.
        - Especificar las alertas de seguridad que se deben configurar.
        - Definir los pasos para responder a incidentes de seguridad.

Servicio Web en Producción

✓ *Rendimiento*

- Procedimiento de Optimización de la Base de Datos:

  – Explicar cómo optimizar la base de datos de WordPress (por ejemplo, eliminar revisiones de publicaciones, optimizar tablas).
  – Especificar las herramientas o plugins utilizados para la optimización.
  – Procedimiento de Optimización de la Velocidad del Sitio:
    - Documentar las técnicas para mejorar la velocidad de carga del sitio web (por ejemplo, almacenamiento en caché, compresión de imágenes, minificación de CSS y JavaScript).
    - Especificar las herramientas o plugins utilizados para la optimización de la velocidad.

  – Procedimiento de Monitorización del Rendimiento:
    - Documentar cómo monitorizar el rendimiento del sitio web (tiempo de carga, uso de recursos del servidor, etc.).
    - Especificar las herramientas utilizadas para la monitorización.

✓ *Gestión de Contenido*

- Procedimiento de Publicación de Contenido:

  – Aunque WordPress es un CMS, es útil tener pautas sobre el flujo de trabajo de publicación de noticias, incluyendo la revisión y edición.
  – Procedimiento de Mantenimiento de Contenido:
    - Explicar cómo revisar y actualizar el contenido existente.
    - Definir la frecuencia de las revisiones de contenido.
    - Documentar cómo gestionar los comentarios y la interacción con los usuarios.

Servicio Web en Producción

✓ *Mantenimiento del Servidor*

- Procedimiento de Monitorización del Servidor:
  - Documentar cómo monitorizar el estado del servidor donde está alojado WordPress (uso de CPU, memoria, espacio en disco, etc.).
  - Especificar las alertas que se deben configurar.
  - Procedimiento de Actualización del Software del Servidor:
    - Explicar cómo actualizar el sistema operativo, el servidor web (Apache, Nginx), PHP y MySQL/MariaDB.
    - Recomendar la creación de un entorno de staging para probar las actualizaciones del servidor.

- Estructura de los Manuales de Procedimiento
  - Para cada una de las operaciones anteriores, los manuales de procedimiento deben incluir:
    - ***Objetivo:*** Una breve descripción del propósito de la operación.
    - ***Frecuencia:*** La frecuencia con la que se debe realizar la operación.
    - ***Responsable:*** La persona o el equipo responsable de realizar la operación.
    - ***Pasos Detallados:*** Una descripción paso a paso de cómo realizar la operación, incluyendo comandos, capturas de pantalla y ejemplos.
    - ***Herramientas y Recursos:*** Una lista de las herramientas, plugins, software o recursos necesarios para realizar la operación.
    - ***Solución de Problemas:*** Una guía básica para solucionar los problemas más comunes que puedan surgir durante la operación.
    - ***Documentación:*** Dónde se deben registrar los resultados de la operación (por ejemplo, registros, informes).

Al tener manuales de procedimiento claros y detallados, puedes garantizar que el mantenimiento del portal web se realice de manera eficiente, consistente y segura.

II. ¿Cómo medirías el rendimiento y disponibilidad del servicio además de la calidad del servicio?

Para medir el rendimiento, la disponibilidad y la calidad del servicio de un portal web, se pueden utilizar diversas métricas y herramientas. Aquí se presentan algunas de las más importantes:

➢ *Medición del Rendimiento*

El rendimiento se refiere a la velocidad y eficiencia con la que el portal web responde a las solicitudes de los usuarios. Algunas métricas clave son:

- ***Tiempo de carga de la página:*** Mide cuánto tiempo tarda en cargarse completamente una página web en el navegador del usuario. Se puede medir utilizando herramientas como Google PageSpeed Insights, GTmetrix o WebPageTest.
- ***Tiempo de respuesta del servidor:*** Mide cuánto tiempo tarda el servidor en responder a una solicitud del navegador. Se puede medir utilizando herramientas de monitorización del servidor o mediante pruebas de rendimiento.
- ***Tasa de transferencia:*** Mide la cantidad de datos que se transfieren desde el servidor al navegador en un período de tiempo determinado.
- ***Uso de recursos del servidor:*** Mide el uso de CPU, memoria y ancho de banda del servidor.

➢ *2. Medición de la Disponibilidad*

La disponibilidad se refiere a la capacidad del portal web para estar accesible y operativo para los usuarios. Algunas métricas clave son:

- ***Tiempo de actividad (Uptime):*** Mide el porcentaje de tiempo que el portal web está disponible para los usuarios. Se puede medir utilizando herramientas de monitorización de la disponibilidad que realizan comprobaciones periódicas del sitio web.
- ***Tiempo de inactividad (Downtime):*** Mide el porcentaje de tiempo que el portal web no está disponible para los usuarios.
- ***Tasa de errores:*** Mide el número de errores que experimentan los usuarios al acceder al portal web (por ejemplo, errores 404, errores 500).

➢ *3. Medición de la Calidad del Servicio*

La calidad del servicio (QoS) se refiere a la experiencia general del usuario al interactuar con el portal web. Es un concepto más subjetivo que el rendimiento y la disponibilidad, pero se puede medir mediante:

- ***Satisfacción del usuario:*** Se puede medir mediante encuestas, formularios de comentarios o análisis de sentimientos en las redes sociales.
- ***Tasa de rebote:*** Mide el porcentaje de usuarios que abandonan el portal web después de ver solo una página. Una alta tasa de rebote puede indicar una mala experiencia del usuario.
- ***Tiempo de permanencia:*** Mide cuánto tiempo pasan los usuarios en el portal web. Un tiempo de permanencia bajo puede indicar que el contenido no es relevante o que la navegación es difícil.
- ***Tasa de conversión:*** Mide el porcentaje de usuarios que realizan una acción deseada en el portal web (por ejemplo, suscribirse a un boletín, realizar una compra).
- ***Accesibilidad:*** Se asegura que el portal web cumple con las pautas de accesibilidad web (WCAG) para que sea utilizable por personas con discapacidades.
- ***Usabilidad:*** Se evalúa la facilidad con la que los usuarios pueden navegar e interactuar con el portal web.

➢ *Herramientas y Técnicas*

Para llevar a cabo estas mediciones, se pueden utilizar diversas herramientas y técnicas:

- ***Herramientas de monitorización del rendimiento:*** *Google Analytics, New Relic, Pingdom, etc.*
- ***Herramientas de pruebas de carga:*** *Apache JMeter, LoadView, etc.*
- ***Herramientas de análisis de registros del servidor:*** *Para identificar errores y patrones de tráfico.*
- ***Encuestas y formularios de comentarios:*** *Para recopilar la opinión de los usuarios.*
- *Pruebas de usabilidad: Para evaluar la facilidad de uso del portal web.*

Es importante definir claramente los objetivos de rendimiento, disponibilidad y calidad del servicio, y establecer métricas específicas para medir el progreso hacia esos objetivos.

III. *Si nos encontráramos con el problema de que con una inyección de código nos hayan destruido la base de datos del CMS, ¿cómo actuarías?*

- *Identificación y Contención*

Detener el ataque: Lo primero es detener cualquier actividad maliciosa en curso. Esto puede implicar desconectar el sitio web del acceso público, cerrar sesiones activas y revisar los registros del servidor y la base de datos para identificar la fuente y el método de la inyección.

Evaluar el daño: Determinar la extensión del daño a la base de datos. Esto implica revisar las tablas, los datos y la estructura de la base de datos para ver qué se ha modificado, eliminado o corrompido.

Aislar el entorno: Si es posible, aislar el servidor o la aplicación comprometida para evitar que el ataque se propague a otras partes del sistema.

- *Recuperación de la Base de Datos*

Restaurar desde una copia de seguridad: La forma más rápida y efectiva de recuperar la base de datos es restaurarla desde una copia de seguridad limpia y reciente. Es crucial tener un sistema de copias de seguridad robusto y probar las copias de seguridad periódicamente para asegurarse de que funcionan.

Recuperación manual (si no hay copia de seguridad): Si no hay una copia de seguridad disponible, la recuperación se vuelve mucho más difícil y puede que no sea posible recuperar toda la información. Se pueden intentar técnicas como la recuperación de datos de los registros de la base de datos o la reconstrucción de la base de datos a partir de archivos en caché, pero estos métodos son complejos y requieren conocimientos especializados.

- *Análisis Forense*

Investigar la causa raíz: Es fundamental determinar cómo ocurrió la inyección de código. Esto implica analizar los registros del servidor, el código de la aplicación y cualquier otra información relevante para identificar la vulnerabilidad que permitió el ataque.

Identificar al atacante (si es posible): En algunos casos, puede ser posible identificar al atacante a través de los registros o las direcciones IP. Esto puede ser útil para fines legales o para mejorar la seguridad en el futuro.

➢ *Corrección de la Vulnerabilidad*

Parchear la vulnerabilidad: Una vez que se ha identificado la causa raíz, es crucial corregir la vulnerabilidad que permitió el ataque. Esto puede implicar actualizar el CMS, los plugins o las bibliotecas, modificar el código de la aplicación o cambiar la configuración del servidor.

Implementar medidas de seguridad adicionales: Además de corregir la vulnerabilidad específica, es recomendable implementar medidas de seguridad adicionales para proteger el sistema contra futuros ataques. Esto puede incluir la instalación de un firewall de aplicaciones web (WAF), la implementación de la validación de entradas y la adopción de prácticas de desarrollo seguro.

➢ *Restauración del Servicio*

Restaurar la aplicación: Una vez que se ha recuperado la base de datos y se ha corregido la vulnerabilidad, se puede restaurar la aplicación y volver a ponerla en línea.

Monitorizar el sistema: Después de la restauración, es importante monitorizar cuidadosamente el sistema para asegurarse de que funciona correctamente y de que no hay signos de actividad maliciosa.

➢ *Mejora Continua*

Revisar los procedimientos de seguridad: El incidente debe utilizarse como una oportunidad para revisar y mejorar los procedimientos de seguridad existentes. Esto puede incluir la implementación de pruebas de penetración periódicas, la formación de los desarrolladores en seguridad y la adopción de un enfoque de seguridad en profundidad.

Implementar un plan de respuesta a incidentes: Es fundamental tener un plan de respuesta a incidentes bien definido para poder responder de manera rápida y efectiva a futuros incidentes de seguridad.

En resumen, la respuesta a una inyección de código que destruye la base de datos de un CMS debe ser un proceso multifacético que incluya la contención del ataque, la recuperación de la base de datos, el análisis forense, la corrección de la vulnerabilidad, la restauración del servicio y la mejora continua de la seguridad.