OWASP A02:2025 – Configuración de Seguridad Incorrecta

Vulnerabilidades de infraestructura y endurecimiento de sistemas

Anatomía del Riesgo

No es un fallo de programación, es un fallo operativo. Muchas veces ocurre por priorizar la rapidez del despliegue sobre la seguridad.

Configuraciones por defecto: Uso de credenciales de fábrica (`admin/password`).

Servicios innecesarios: Puertos abiertos que no se usan (FTP, Telnet) o páginas de muestra/demo activas.

Mensajes de error detallados: Revelar rutas internas o versiones de software (Stack Traces).

Almacenamiento mal protegido: Almacenamiento en la nube (S3, Azure Blobs) con acceso público.

Parches de seguridad no instalados.

Exposición de Datos en la Nube

Este es el método más común hoy en día. Los atacantes no 'hackean', simplemente 'entran' por configuraciones olvidadas.

Escaneo: Un atacante usa bots para buscar directorios `.git` o archivos `.env` expuestos.

Acceso: Encuentra un servidor con el "Listado de directorios" activo.

Extracción: Descarga un archivo de configuración que contiene las claves de acceso a la base de datos de producción.

Impacto: Robo total de información sensible sin romper ni una sola línea de código.

¿Cómo protegernos? (Hardening)

La seguridad debe ser parte del proceso de despliegue, no algo que se revisa al final.

Automatización: Usar plantillas de Infraestructura como Código (Terraform/Ansible) para que todos los servidores nazcan seguros.

Principio de Mínimo Privilegio: Desactivar funciones y puertos que no sean estrictamente necesarios.

Auditoría de Seguridad: Escaneos periódicos de vulnerabilidades y revisión de cabeceras HTTP.

Manejo de Errores: Configurar la app para mostrar mensajes genéricos y guardar el error real solo en logs internos seguros.