Top 10 OWASP

A01: Control de Acceso Roto

Sucede cuando un usuario puede acceder a recuros o realizar acciones para las que no tiene autorización, incluyendo IDOR, escalación de privilegios y ahora también SSRF.

A02: Error de Configuración de Seguridad

Errores de configuración en apliacaciones, servidores, contenedores, APIs o servicios en la nube que exponen el sistema de ataques.

A03: Fallo en la Cadena de Suministro de Software

Amplía el concepto de componentes vulnerables. Incluye riesgos en dependencias, bibliotecas externas, repositorios, pipelines CI/CD y procesos de distribución de software.

A04: Fallo Criptográfico

Se centra en fallos relacionados con falta de criptografía, una criptografía insuficiente, la filtración de claves criptográficas y errores relacionados.

A05: Inyección

Ocurre cuando una aplicación pasa entrada no confiable a un intérprete sin la validación o escape adecuados, permitiendo a los atacantes ejecutar comandos no previstos.

A06: Diseño Inseguro

Fallas de seguridad originadas en la arquitectura o diseño de la aplicación, incluso si el código está bien implementado.

A07: Fallo en la Autenticación

Caundo un atacante es capaz de engañar a un sistema para que reconozca como legítimo a un usuario no válido o incorrecto.

A08: Fallo de Integridad de Software o Datos

Se produce cuando no se verifica correctamente que el software o los datos provienen de fuentes confiables y no han sido alterados.

A09: Fallo en el Registro y Alertas de Seguridad

Sin alertas adicionales vinculadas a fuentes de logs, las brechas pasan desapercibidas mientras la evidencia permanece almacenada.

A10: Mal Manejo de Condiciones Excepcionales

Enfocada en errores relacionados con situaciones inesperadas, fallas, sobrecargas, agotamiento de recursos y manejo incorrecto de excepciones.