A04-2021 Insecure Design

Se centra en las deficiencias a nivel de arquitectura y diseño, es decir, antes de la implementación del código. Esto implica que la seguridad debe ser una consideración primordial desde el inicio del ciclo de vida del desarrollo de software. A diferencia de otras categorías que se enfocan en errores de implementación específicos, el diseño inseguro es un problema sistémico que puede dar lugar a múltiples vulnerabilidades.

Ejemplo: No separar las redes internas y externas, lo que permite que un ataque a una red afecte a otras.

Gravedad

- Causa problemas estructurales: Las fallas en el diseño afectan todo el sistema y suelen ser difíciles de corregir sin una reestructuración significativa.
- Habilita otras vulnerabilidades: Un diseño inseguro puede facilitar la explotación de problemas como inyección, control de acceso débil, etc.
- Riesgo a largo plazo: Los sistemas mal diseñados son más propensos a fallar frente a amenazas futuras.

Mitigación

- Modelado de amenazas: Realizar análisis de amenazas para identificar posibles vectores de ataque y diseñar controles de seguridad para mitigarlos.
- Arquitectura de referencia segura: Utilizar arquitecturas de referencia seguras y patrones de diseño probados.
- Revisiones de diseño de seguridad: Realizar revisiones de diseño de seguridad periódicas para identificar y corregir posibles vulnerabilidades.
- Desarrollo basado en riesgos: Priorizar las actividades de seguridad en función del riesgo que representan las diferentes funcionalidades y componentes del sistema.