A02-2021 Cryptographic Failures

Se refiere a problemas relacionados con la implementación incorrecta o la ausencia de medidas criptográficas necesarias para proteger datos sensibles. Dentro de las fallas pueden estar:

- Uso de algoritmos criptográficos débiles u obsoletos.
- Transmisión de datos sensibles sin cifrar.
- Almacenamiento inseguro de claves criptográficas.

Ejemplo: Almacenar contraseñas en texto plano o transmitir información confidencial sin cifrado.

Gravedad

El riesgo es alto especialmente en sistema que manejan datos sensibles, financieros o de autenticación.

- Exposición de datos sensibles: Permite a los ciberdelincuentes acceder, modificar o robar información confidencial.
- Ruptura de confidencialidad e integridad: Puede comprometer la confianza y la seguridad de los usuarios.
- Impacto en cumplimiento normativo: Violaciones de GDPR, HIPPA u otras regulaciones de protección de datos.

Mitigación

1. Cifrado de datos en tránsito y en reposo:
   - Utilizar protocolos seguros como TLS 1.2 o superior para la transmisión.
   - Almacenar que los datos sensibles almacenados estén cifrados con algoritmos modernos como AES-256.
2. Evitar algoritmos inseguros:
   - No usar algoritmos obsoletos como pueden ser MD5 o SHA-1.
   - Usar estándares actualizados como SHA-256 o superior
3. Gestión adecuada de claves criptográficas:
   - Almacenar claves en módulos seguros y no en código fuente o ubicaciones expuestas.