A03-2021 Injection

Ocurre cuando un ciberatacante inserta código malicioso en una consulta o comando, engañando al sistema para que ejecute dicha acción. Esto sucede por no validar adecuadamente la entrada del usuario. Dentro de los tipos de inyección están:

- SQL Injection: Alterar consultas AQL para obtener o modificar datos.
- Command Injection: Ejecutar comandos arbitrarios en el sistema.
- LDAP, NoSQL y XSS Injections: Modifica consultas en diferentes contextos.
- Inyección de XML (XXE): Explotación de vulnerabilidades en el procesamiento de datos XML.
- Inyección de cabeceras HTTP: Modificación de cabeceras HTTP para realizar ataques como la división de cabeceras.

Ejemplo: Un formulario que permite a un atacante inyectar código SQL para obtener información confidencial directamente desde la base de datos.

Gravedad

Un ataque exitoso de este tipo puede afectar tanto la confidencialidad como la integridad y disponibilidad del sistema.

- Alto impacto: Puede comprometer bases de datos completas, ejecutar comandos arbitrarios o tomar control del servidor.
- Facilidad de explotación: Herramientas como SQLmap facilitan la identificación y explotación de estas fallas.
- Daño económico y reputacional: La explotación de datos sensibles puede provocar violaciones ilegales y pérdida de confianza.

Mitigación

- Listas blancas de entrada: En lugar de rechazar caracteres maliciosos, permitir solo caracteres conocidos y seguros.
- Entorno de ejecución con privilegios mínimos: Limitar los permisos del intérprete para reducir el impacto de un ataque exitoso.
- Análisis estático de código: Utilizar herramientas de análisis estático para identificar posibles vulnerabilidades de inyección en el código fuente.