A03-2021 Injection

It occurs when a cyberattacker inserts malicious code into a query or command, tricking the system into executing said action. This happens due to not properly validating user input. Among the types of injection are:

- **SQL Injection:** Altering SQL queries to obtain or modify data.
- **Command Injection:** Executing arbitrary commands on the system.
- **LDAP, NoSQL, and XSS Injections:** Modifying queries in different contexts.
- **XML Injection (XXE):** Exploiting vulnerabilities in XML data processing.
- **HTTP Header Injection:** Modifying HTTP headers to perform attacks such as header splitting.

Example: A form that allows an attacker to inject SQL code to obtain confidential information directly from the database.

Severity

A successful attack of this type can affect both the confidentiality, integrity, and availability of the system.

- **High impact:** It can compromise entire databases, execute arbitrary commands, or take control of the server.
- **Ease of exploitation:** Tools like SQLmap facilitate the identification and exploitation of these flaws.
- **Economic and reputational damage:** Exploitation of sensitive data can lead to illegal violations and loss of trust.

Mitigation

- **Input whitelists:** Instead of rejecting malicious characters, allow only known and safe characters.
- **Character escaping:** Escape special characters in user inputs to prevent them from being interpreted as code.
- **Least privilege execution environment:** Limit the interpreter's permissions to reduce the impact of a successful attack.
- **Web Application Firewall (WAF):** Implement a WAF to filter and block malicious requests.