A01-2021 Broken Access Control

This flaw focuses on the inability to properly restrict actions of authenticated users. This allows users to perform actions or access resources for which they are not authorized. This includes:

- Privilege escalation.
- Unauthorized access to sensitive data.
- Modification or deletion of data without proper permissions.
  Example: An attacker could modify cookies or session tokens to assume the identity of another user.

Severity

The impact can range from exposed data to compromise of the entire system, depending on the context in which it is exploited.

- Can compromise sensitive user and system data.
- Severe impacts such as loss of information, violation of privacy, and manipulation of system resources.
- Can be exploited with simple tools or manual changes to requests.

Mitigation

In order for this vulnerability to be mitigated, a continuous and updated approach is required, especially for systems that handle sensitive information or have multiple levels of users. Among the measures that can be taken are:

- Principle of least privilege (PoLP): This principle is fundamental. Each user or process should have only the permissions necessary to perform their tasks.
- Role-based access controls (RBAC): Implement RBAC to manage permissions in a centralized and efficient way.
- Input validation: Validate all user input on the server side to prevent data manipulation.
- Security by default: Deny all access by default and grant permissions explicitly.
- Implementation of access control policies: It is necessary to implement access control policies that are clear and properly documented.