A10-2021 Server-Side Request Forgery (SSRF)

It occurs when a web application allows an attacker to manipulate and send requests to internal or external servers on behalf of the vulnerable server. This typically happens due to insufficient validation of user-provided inputs, allowing the attacker to:

- Access internal network resources.
- Execute additional attacks, such as data extraction or internal port scanning.
- Make malicious requests to external servers.

Example: An attacker could use SSRF to access internal databases, administration servers, or internal APIs.

Severity

- Scope of impact: It can be used to access internal networks, potentially exposing sensitive information or unprotected internal services.
- Ease of exploitation: Many applications rely on user inputs to generate requests without proper validation.
- Base for secondary attacks: It can enable attacks such as remote code execution, cloud metadata extraction, or compromise of internal systems.

Mitigation

- URL whitelists: Allow only requests to specific URLs or domains.
- Disable redirects: Avoid using functions that allow redirects without validation.
- Network isolation: Isolate internal servers from the external network to limit the impact of an SSRF attack.
- Request security policy: It is very important that companies have request security policies, so that those responsible for the systems can have a correct handling of this type of problems.