A4-XML External Entities (XXE)

Attackers can exploit vulnerable XML processors. They can upload XML or include hostile content in an XML document, dependencies, integration or exploiting vulnerable code. Many older XML processors allow specification of an external entity. SAST also known as Source Code Analysis Tool can discover this issue by inspecting dependencies and configuration. DAST also known as Dynamic Application Security Testing require additional manual steps to detect and exploit this issue. These flaws can execute a remote request from the server. These flaws is used to extract data, scan internal systems, perform a denial of service attack and also to execute other attacks.

Medication

Developer should disable XML external entity and DTD processing in all XML. The developer should implement positive server side input validation and filtering to prevent hostile data. They should use less complex data formats such as JSON. The developers should also consider to use virtual patching, security gateways or Web Application Firewalls to detect the attacks.

Example

Numerous public XXE issues have been discovered, including attacking embedded devices. XXE occurs in a lot of unexpected places, including deeply nested dependencies. One example is when the attacker attempts to extract data from the server. Next is when an attackers probes the server’s network. Another example is when an attacker attempts a denial of service attack by including a potentially endless file.