What is XML external entity injection?

XXE (XML External Entity injection) is a vulnerability in how an application parses XML. XML documents can declare entities, including external ones that point at a URI. If the parser resolves those external entities on attacker-controlled input, the attacker can read local files, perform server-side request forgery against internal services, and in some configurations reach code execution or denial of service. The root cause is an XML parser configured to process document type definitions and external entities.

HOW IT WORKS

01 The abuse and payload

Shown for defensive context:

- File read: define an entity that points at a local file and reference it in the response field:

`<!DOCTYPE r [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>` then use `&xxe;` in an element the app echoes back.

- Server-side request forgery: point the entity at an internal URL such as `http://169.254.169.254/latest/meta-data/` to reach a cloud metadata service or an internal host.
- Blind / out-of-band: when the response is not reflected, host an external DTD that exfiltrates file contents to an attacker server over a second request.
- Denial of service: the classic billion-laughs entity expansion exhausts memory.

XXE frequently chains into internal-network access, which is why it is treated as high impact during application penetration testing.

HOW TO DEFEND

- Disable DTDs entirely in the XML parser wherever possible. In many libraries this is a single feature flag, for example `disallow-doctype-decl` set to true.
- If DTDs are needed, disable external entities and external DTD loading so the parser never fetches a URI.
- Prefer simpler formats; if the endpoint only needs structured data, JSON avoids the entire entity model.
- Patch and configure XML libraries centrally so every parser in the codebase inherits the safe settings, since a single default-configured parser reintroduces the flaw.

SOURCES

[1] OWASP: XML External Entity Prevention Cheat Sheet

[2] PortSwigger: XML external entity (XXE) injection

[3] MITRE ATT&CK: Exploit Public-Facing Application (T1190)

Find the parser flaw before an attacker does.

securelayer7.net/learn/web-exploitation/what-is-xxe

Open online