What is XXE injection?

XXE (XML External Entity injection) is a vulnerability where an application parses attacker-supplied XML with external entities enabled, letting the attacker define an entity that points at a local file or internal URL. The parser fetches it, so the attacker reads server files (like `/etc/passwd`), performs SSRF against internal services, or exfiltrates data out-of-band. It is caused by XML parsers that resolve external entities by default, and the fix is simply to disable external entity and DTD processing.

HOW IT WORKS

01 How it works and example

The attacker submits XML with a malicious external entity:

- Read a local file:

`<!DOCTYPE r [<!ENTITY x SYSTEM "file:///etc/passwd">]> <r>&x;</r>` returns the file in the response.

- SSRF to internal services: point the entity at `http://169.254.169.254/...` (cloud metadata) or an internal host.

- Blind/out-of-band XXE exfiltrates data to an attacker server using parameter entities and an external DTD when responses are not reflected.

XXE often appears in file uploads (SVG, DOCX, SAML) and any endpoint that accepts XML. Examples shown for defensive context.

> ONE SETTING FIXES IT
>
> *XXE is almost always fixed by disabling external entities and DTDs in the XML parser configuration. There is rarely a legitimate need for them in application input.*

HOW TO DEFEND

- Disable external entity resolution and DTD processing in every XML parser (the exact flags vary by library; OWASP documents them per platform).
- Prefer simpler formats like JSON where XML is not required.
- Patch and update XML libraries, since older defaults are unsafe.
- Validate file uploads that contain XML under the hood (SVG, Office documents, SAML).
- Test every XML-accepting endpoint for entity resolution.

SOURCES

[1] OWASP: XML External Entity Prevention

[2] MITRE CWE-611: Improper Restriction of XML External Entity Reference

[3] OWASP Top 10

Test your application for XXE and 30+ other classes.

securelayer7.net/learn/application-security/xxe-injection

Open online