What is server-side template injection?

Server-Side Template Injection (SSTI) happens when an application places untrusted input into a server-side template that is then rendered, so the input is evaluated as template syntax rather than plain data. Depending on the engine, Jinja2, Twig, Freemarker, Velocity, or others, this leads to information disclosure and very often full remote code execution. It is usually introduced when developers concatenate user input into a template string instead of passing it as a bound variable.

HOW IT WORKS

01 Detection and the abuse

Testers first confirm evaluation with a math probe, then identify the engine, then reach the OS. Shown for defensive context:

- Detect: submit `${7*7}`, `{{7*7}}`, or `<%= 7*7 %>`. A response containing 49 confirms server-side evaluation.
- Fingerprint the engine: engine-specific payloads behave differently, for example `{{7*'7'}}` returns `7777777` in Jinja2 but 49 in Twig.
- Reach code execution (Jinja2 example): `{{ config.__class__.__init__.__globals__['os'].popen('id').read() }}` walks the object model to the `os` module and runs a command.
- Twig example: `{{ ['id']|filter('system') }}` invokes a PHP callback.

Because SSTI so reliably becomes command execution, it is one of the highest-severity findings surfaced during web application penetration testing.

HOW TO DEFEND

- Never concatenate user input into a template string. Always pass it as a bound variable or context value.
- Prefer logic-less templates (for example Mustache) where the engine cannot evaluate arbitrary expressions.
- Sandbox the engine if dynamic templates are unavoidable, and keep the sandbox patched, since many sandbox escapes are known.
- Validate and constrain input that must appear in a template context, and encode output for its destination.

SOURCES

[1] PortSwigger: Server-side template injection

[2] OWASP Testing Guide: Server-Side Template Injection

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

Find the injection before an attacker does.

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

Open online