What is OS command injection?

OS command injection occurs when an application passes user-controlled input into a system shell as part of a command. Because the shell treats certain characters as separators and operators, an attacker can break out of the intended command and run their own, executing with the privileges of the web process. Impact ranges from reading files to full server takeover. The root cause is invoking a shell and building the command string from untrusted input.

HOW IT WORKS

01 The abuse and payload

Shown for defensive context:

- Confirm with a separator: in a hostname field, submit `127.0.0.1; id` or `127.0.0.1 | whoami-`. Output containing user or uid confirms execution.
- Command substitution: `$(id)` or `` `id` `` embeds the result of one command inside another.
- Blind injection: when output is not returned, prove execution by timing, `; sleep 10`, or by triggering an out-of-band DNS or HTTP callback the tester controls.
- Escalate to a shell: a reverse shell one-liner in the injected command gives interactive access.

Because the payoff is immediate code execution, command injection is among the first things checked against any input that reaches a system utility during application security testing.

HOW TO DEFEND

- Do not call a shell. Use language APIs that execute a program directly with an argument array, so arguments are passed as data and never parsed by a shell, for example `execFile(cmd, [arg1, arg2])` rather than `exec("cmd " + input)`.
- Avoid shelling out at all when a native library can do the job.
- If a value must reach a command, allowlist it, validate strictly against an expected format rather than trying to block bad characters.
- Run the process with least privilege so a successful injection yields the smallest possible foothold.

SOURCES

[1] OWASP: OS Command Injection Defense Cheat Sheet

[2] PortSwigger: OS command injection

[3] MITRE ATT&CK: Command and Scripting Interpreter (T1059)

Find the injection before an attacker does.

securelayer7.net/learn/web-exploitation/what-is-os-command-injection

Open online