What is pull request injection?

Pull request injection is opening a malicious pull request whose code or CI configuration runs in the target's pipeline when the PR is built. On misconfigured pipelines that build untrusted PRs with access to secrets, the attacker's PR reads runner credentials or reaches internal systems, without the PR ever being merged. Defend by never exposing secrets to untrusted-PR builds and requiring approval to run them.

HOW IT WORKS

01 How it works and example

The attacker opens a pull request that changes a workflow or adds code that runs during the build, then the pipeline executes it with whatever access the runner has, dumping environment secrets or reaching internal services. This pwn-request pattern often hinges on triggers that expose secrets to untrusted PRs. A 2026 intrusion opened a malicious PR precisely to trigger credential probing in the runner.

SOURCES

[1] OWASP Top 10 CI/CD Security Risks

[2] HuggingFace, Agent intrusion technical timeline

[3] OWASP Top 10 CI/CD Security Risks

Find the CI/CD and supply-chain risks before an attacker does.

securelayer7.net/learn/ci-cd-security/pull-request-injection

Open online