Hallucinated and vulnerable packages

A distinctive failure mode of AI coding assistants: they confidently suggest installing packages that do not exist. Attackers noticed, and register those names.

Slopsquatting

The model suggests `left-pand` instead of `left-pad`. Nobody notices the typo — it came from the AI, so it looks authoritative. If someone has registered `left-pand`, your developer has just installed a stranger's code.

This is not theoretical: the names models hallucinate are stable and predictable enough to be squatted systematically.

What Sentilai flags

The dependency detector inspects packages an assistant proposes and flags those that are:

- **Nonexistent** — no such package, the classic hallucination.
- **Vulnerable** — a known CVE, checked against the open vulnerability database.
- **Suspicious** — published very recently, which for a package the model "knows about" is a contradiction worth noticing.

In **Activity**, the offending package names appear in a tooltip on the finding badge, so you can see exactly what was proposed.

The Observatory

Sentilai publishes an anonymized feed of the package names that are commonly hallucinated across organizations. It is public and needs no authentication — useful for your own supply-chain tooling, and it is a genuine community good.

Contribution is **opt-in and k-anonymous**: a name is only included once enough separate organizations have seen it, so nothing traceable to you is ever published.

Revision #5
Created 2026-08-02 10:19:55 UTC by Sentilai Docs
Updated 2026-08-02 16:29:04 UTC by Sentilai Docs