Hyrax

FREE · PRINT IT

The AI PR review cheat sheet.

Ten patterns AI-generated pull requests ship, and the one check that catches each. Keep it open on your next review.

01 The auth check quietly skipped

An early return, next(), or if(true) slipped into middleware or a guard so something passes.

CHECK On any PR touching auth, grep the diff for added returns / short-circuits. Restore the guard and re-run the auth tests.

02 Green tests, broken code

The tests pass because the AI mocked out (or weakened) the exact thing it just changed.

CHECK Read the test diff first. Flag new mocks on changed paths, deleted assertions, and tests that assert the mock, not the behavior.

03 A service that does not exist

A call to an endpoint or SDK method that was invented, then mocked so it "works".

CHECK Confirm the endpoint/method in the real API docs. If it only exists in the mock, it is hallucinated.

04 A package that does not exist

An unfamiliar import or install line. Roughly 1 in 5 AI-suggested packages are not real.

CHECK Run npm view or pip index versions before install. A 404 means reject. Then check first-publish date and a real repo, not the download count.

05 5,000 lines that should be 100

A large, fluent diff for a small task, hiding the one change that matters.

CHECK Ask for the three lines that carry the change. Review those and their blast radius. If the author cannot point to them, send it back.

06 Abstraction nobody asked for

Factory, strategy, or DI patterns wrapped around a simple job "for extensibility".

CHECK For each abstraction, name the concrete second use case it serves today. None means delete it.

07 Missing input validation

User input used without a check. AI ships an OWASP Top 10 flaw in about 45% of cases.

CHECK At every input boundary, confirm validation and output escaping / parameterized queries. Assume unvalidated until shown otherwise.

08 Copy-paste instead of reuse

A block pasted in that already exists elsewhere. Code cloning rises sharply with AI.

CHECK Search the repo for the block. If it already exists, require the call, not the copy.

09 A confident wrong API

A method name or parameter that looks right but does not resolve.

CHECK Jump-to-definition on unfamiliar calls. If the symbol does not resolve, it is invented.

10 A secret hardcoded to "just work"

A literal key or token dropped into the diff to make a run succeed.

CHECK Grep the diff for sk_, AKIA, api_key, and long hex/base64 literals. Move to env and rotate.

Patterns drawn from what engineers report on r/ExperiencedDevs and r/programming, plus 2025 data on AI code security and package hallucination.

Hyrax runs every one of these on each PR.

hyrax.dev