

Agentic PR Risk Auditor

AI Hackathon San Francisco x Hamburg

By Acme

Date
December 2025

The Team



Maiya

Front-End Developer



Amir

Developer



Danial

Front-End Developer





Problem

Modern software teams handle **dozens to hundreds of pull requests daily**.

Some PRs introduce **hidden, high-impact risks**:

- Authentication & authorization bugs
- Database integrity issues
- Security regressions
- Broken assumptions not covered by tests

Manual review does not scale:

- Reviewers miss edge cases
- Tests are missing, weak, or outdated
- Risk assessment is subjective and inconsistent
- Running AI generated tests can introduce new risks

PR Risk Intelligence

Prioritize risk • explain why • fix first

Pull Requests

☐ High Risk only Sort Risk ↓

Fix auth bypass in login

[View Pull Request](#)

✖ 1 ⚠ 1 ✔ 2

High Risk

Risk Score: 78%

Low Confidence

Confidence: 40%

Optimize query + caching layer

[View Pull Request](#)

✖ 0 ⚠ 2 ✔ 1

Medium Risk

Risk Score: 66%

Medium Confidence

Confidence: 52%

Refactor dashboard UI components

[View Pull Request](#)

✖ 0 ⚠ 1 ✔ 2

Low Risk

Risk Score: 28%

Medium Confidence

Confidence: 66%

Fix auth bypass in login

[View Pull Request](#)

✖ 1 ⚠ 1 ✔ 2

High Risk

Risk Score: 78%

Low Confidence

Confidence: 40%

Why this PR is High Risk

- Fails critical check: "SQL Injection test" (85%)
- Touches authentication/session logic
- Interacts with data layer / query logic

Fix this first

1. ✖ SQL Injection test

Potential unsafe query detected in data access layer.

High Risk

85%

2. ⚠ Auth edge case test

Token expiry edge case not fully covered.

Medium Risk

55%

✖ Errors

✖ SQL Injection test

Potential unsafe query detected in data access layer.

High Risk

85%

⚠ Warnings

⚠ Auth edge case test

Token expiry edge case not fully covered.

Medium Risk

55%

✔ Passed Tests

✔ Login happy path

Basic login flow passed.

Generated Tests

Expired JWT validation

Reason: Auth middleware did not handle expired tokens.

Malformed payload test

Reason: Missing schema validation for login payload.

[Open PR](#) →

Try Pitch

Solution

An **Agentic PR Risk Auditor** that enforces **evidence-based validation before merge** with CodeRabbit and Daytona technology.

The system **automatically**:

- Analyzes what a PR actually changes
- Identifies its risk surface
- Generates targeted tests
- Runs the tests in an isolated Daytona sandbox
- Summarizes risk clearly for reviewers

Value



Safer merges



Faster reviews



Objective, consistent risk assessment



Security & correctness enforced ***before*** production