USE CASE

Every payment API in your code, ranked by risk

Aribot lists every endpoint in your code, ranks the risky ones and maps the fixes to PCI DSS, so security review keeps pace with releases.

THE PROBLEM

For a fintech, the APIs are the product and the attack surface. The security team is small and sits inside engineering, existing scanners are noisy, and nobody can produce a complete list of the endpoints that touch card data.

HOW ARIBOT HANDLES IT

1. **Scan the code**
   Review each repository and pipeline; every finding points to the line that caused it.
2. **Discover the endpoints**
   Build the inventory of every API your code exposes and every AI model it calls.
3. **Map to PCI DSS**
   Tie each fix to the PCI DSS requirement it supports.
4. **Gate the build**
   Call the same checks from CI and fail the build only on what matters.

WHAT YOU SEE IN THE DEMO

- Code Review: findings on the exact lines
- Unified Workbench: endpoints feeding the threat model
- MCP Platform: checks called from a pipeline or an assistant

WHO IT IS FOR

Head of Security · Staff Security Engineer · CTO

WHAT YOU GET

- An API inventory you can defend
- Findings developers trust, each tied to a line and a fix
- PCI DSS evidence from work already done
- Security checks inside the pipeline, not after it

15%

of organisations are strongly confident in their API inventory; 99% had API security issues in the past year

Source: Salt Security, State of API Security 2025

PCI DSS 4.0.1 · 31 Mar 2025
Future-dated requirements became mandatory, including authenticated internal scanning.

See it: ayurak.com/demos/code-review

€50 per review · €40 per pipeline scan · €40 per discovery run