



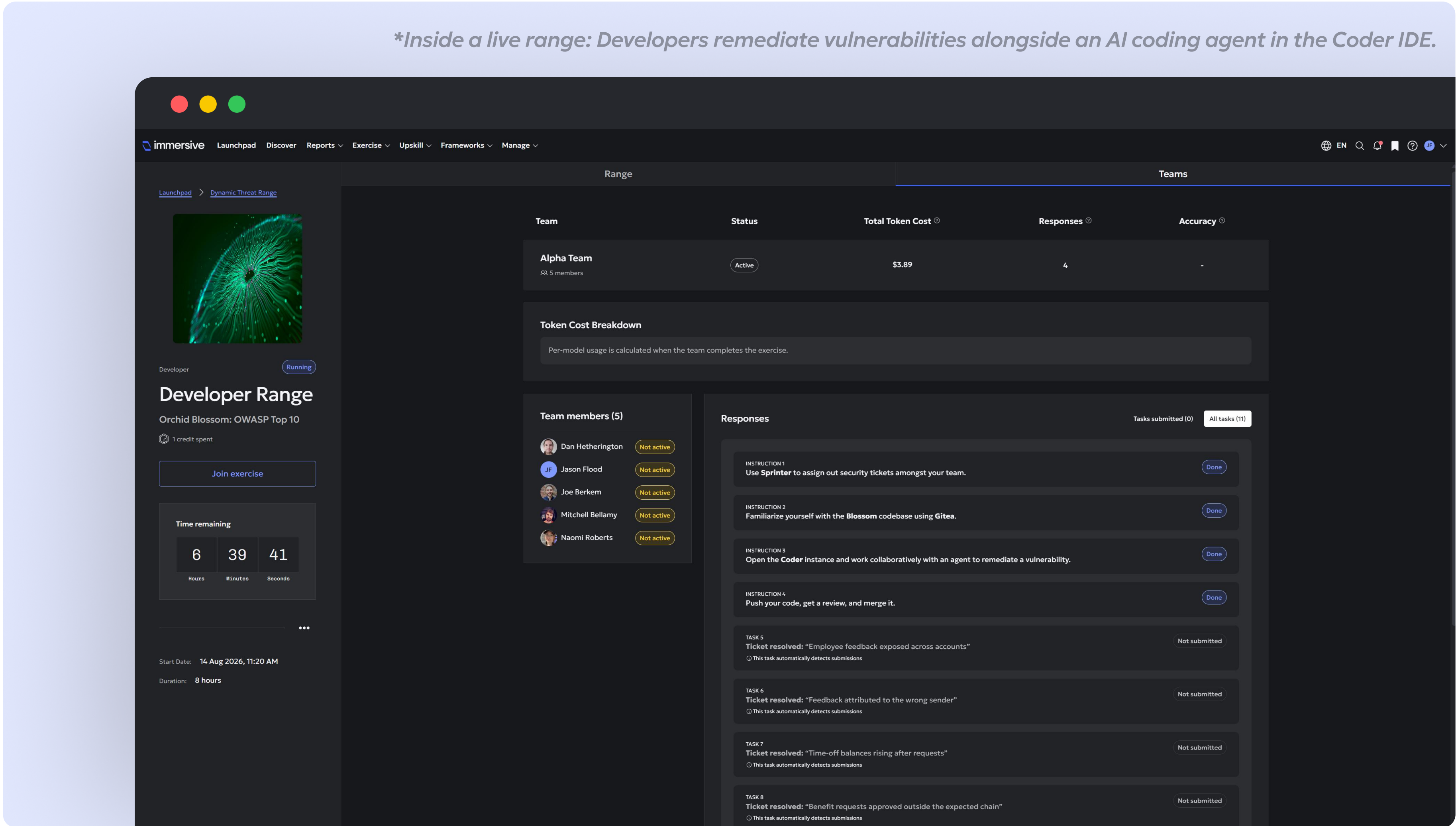
Developer AI ranges

Ground-truth verdicts reveal exactly what developers caught—and missed.

Developer AI ranges

Prove developers can build securely with AI

Ground-truth verdicts reveal exactly what developers caught—and missed.



Your proving ground for AI-generated code

AI is writing more code than security teams can review, and legacy tools can’t catch what’s new. Test every pull request against real, AI-native threats to uncover capability gaps.

Immersive One offers:

- Realistic SDLC sandbox
 - Live CI/CD feedback
 - Multi-language pull requests
- AI-native threats
 - OWASP threat mapped
 - Ground-truth verdicts

CATCH VULNERABLE
CODE EARLY

Baseline how well your developers spot flawed, AI-generated code.

Then, stress-test them against live pull requests carrying real AI-native vulnerabilities.

INNOVATE AT
MACHINE SPEED

Exercises keep pace with AI-assisted development.

Your team can build quickly and securely, confident knowing when AI misses the mark.

MAKE SECURE
DEVELOPMENT STICK

Validate custom AI guardrails directly in live code.

You can turn security policy into a habit developers actually retain.

UNDER THE HOOD

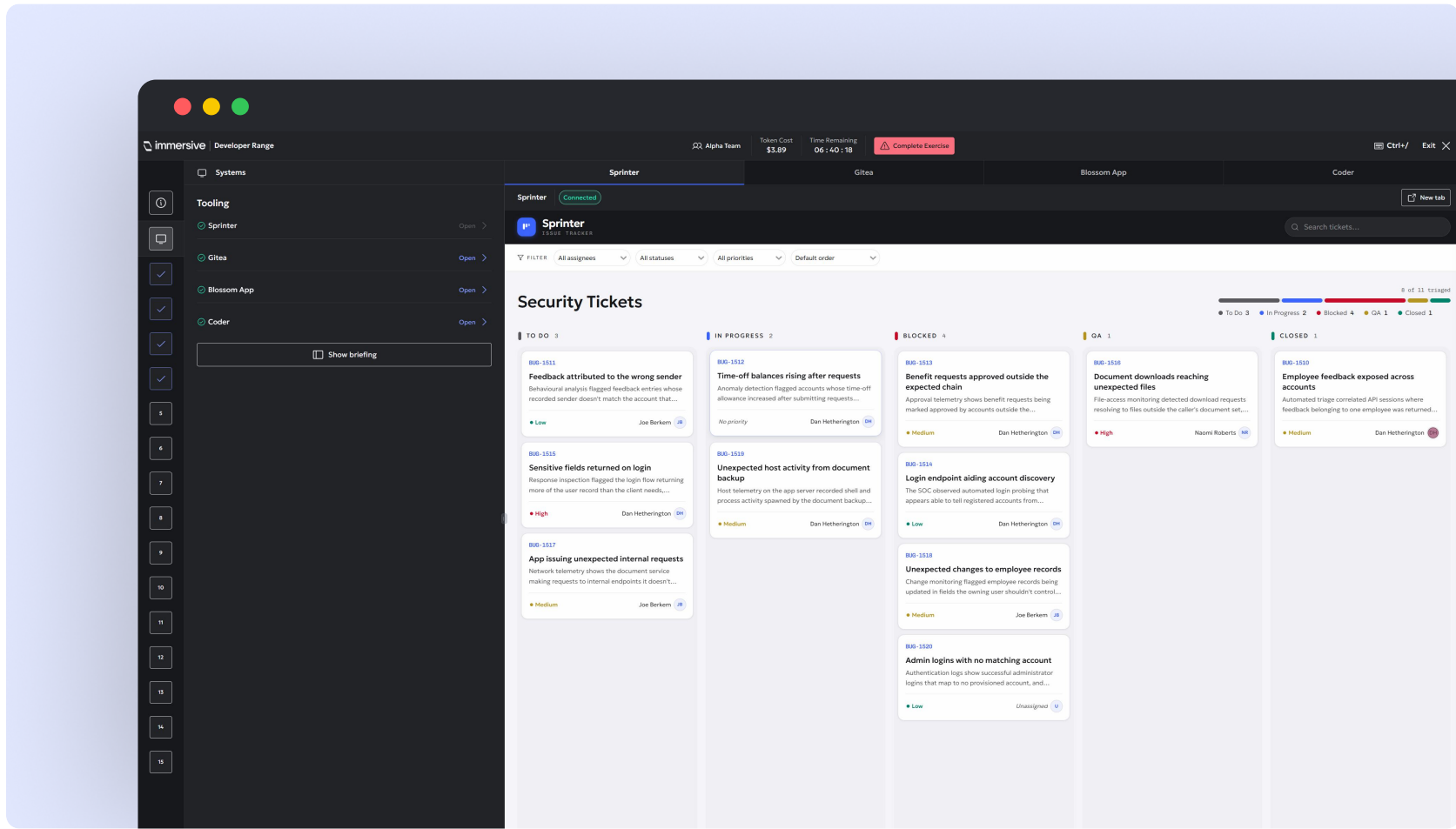
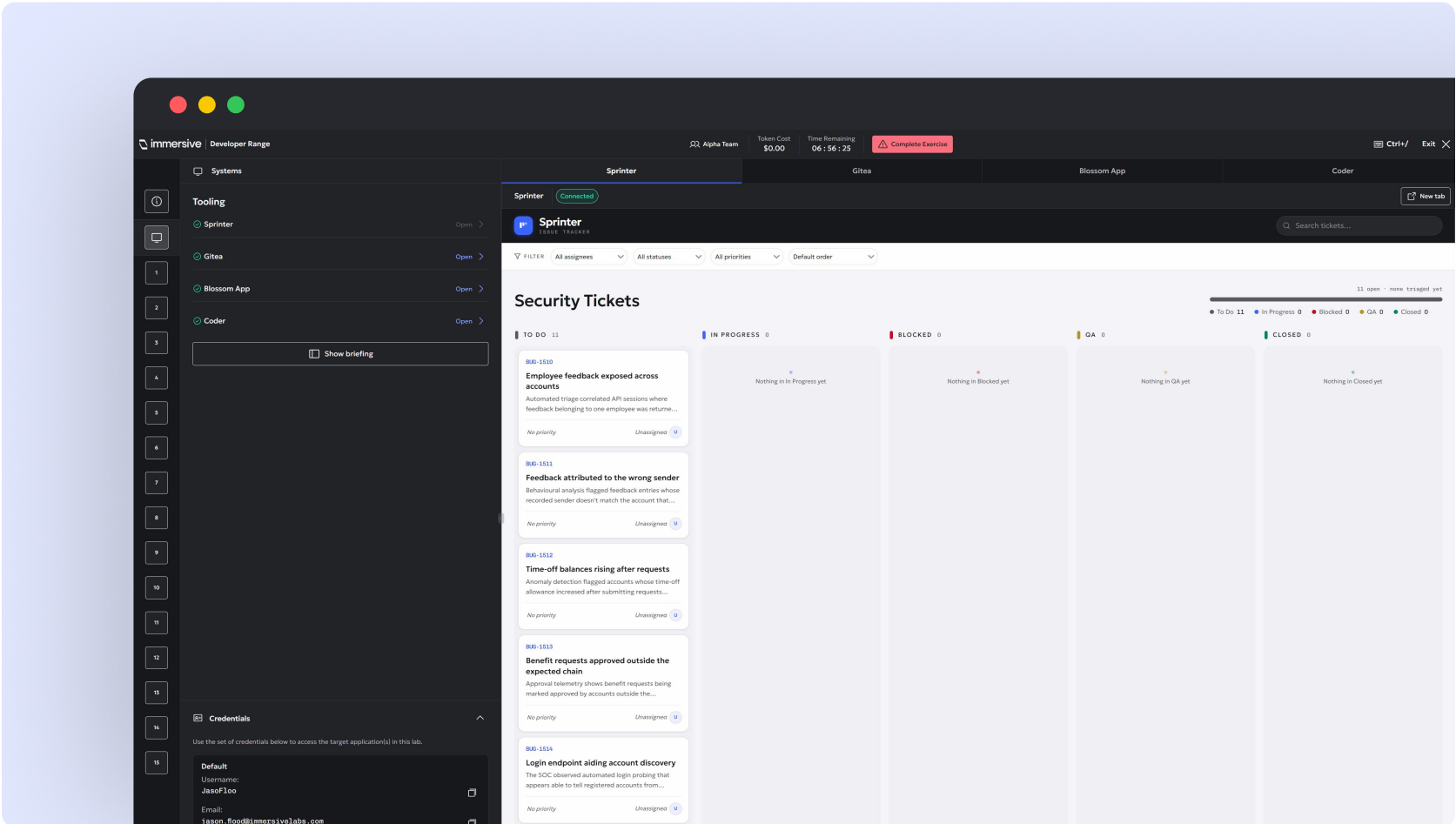
Use Case: Fix an application (Blossom HR range)

Working alongside an AI coding agent, developers find and fix injected AI-native vulnerabilities, then ship the fix as a pull request.

01

TRIAGE THE SECURITY BACKLOG

The range opens on a live-issue tracker of security tickets, including broken access control, command injection, SSRF, and data exposure. Each is tied to a real route in the target application. Developers choose what to tackle. (Image: Sprinter, security backlog)



02

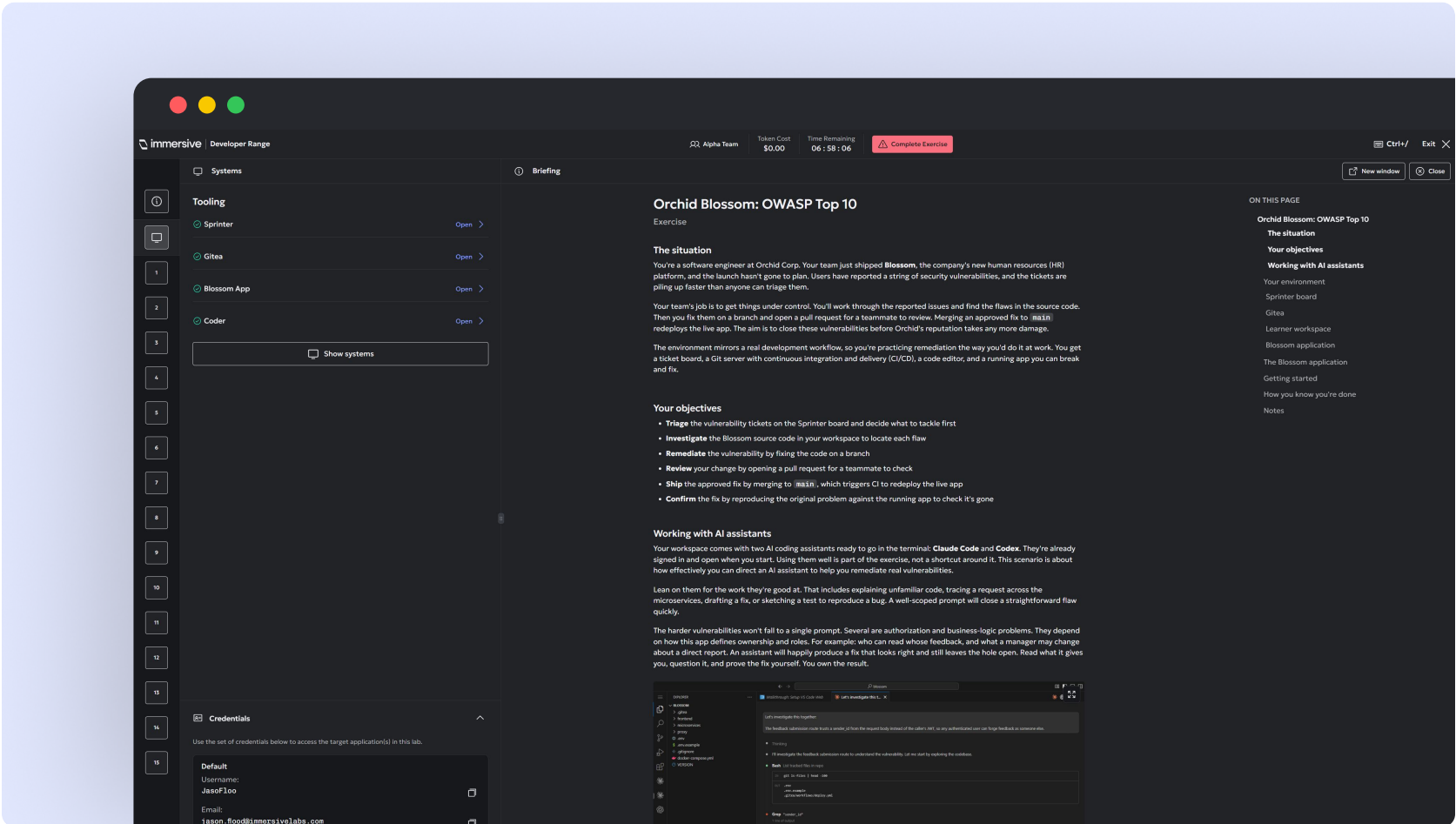
EXPLORE THE APP AND ITS CODEBASE

Developers get hands-on with the running Blossom HR application, browsing its multi-service codebase (frontend, microservices, proxy) to understand how the target actually behaves. (Image: Blossom App, target application)

03

WORK WITH AN AI CODING AGENT

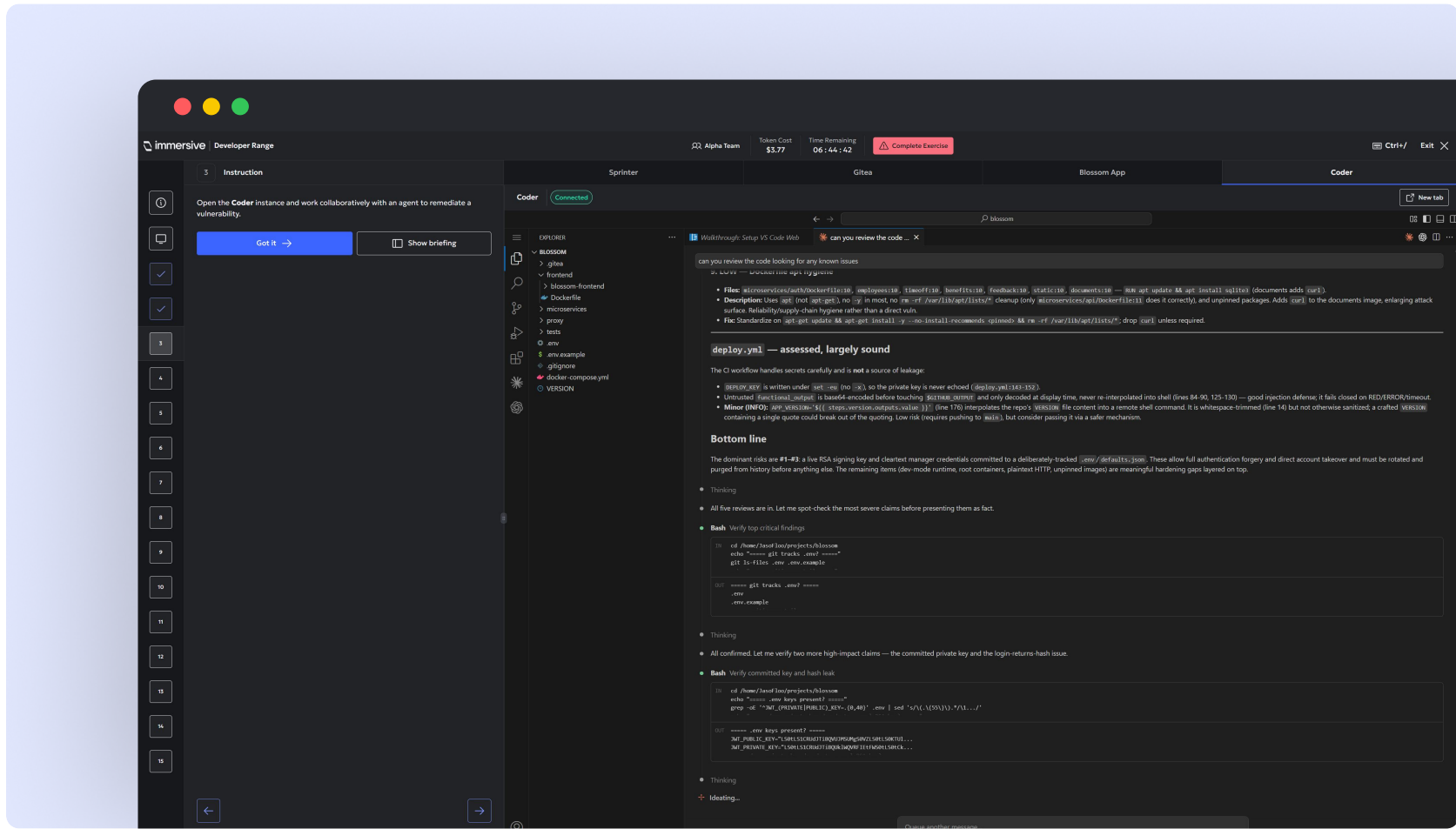
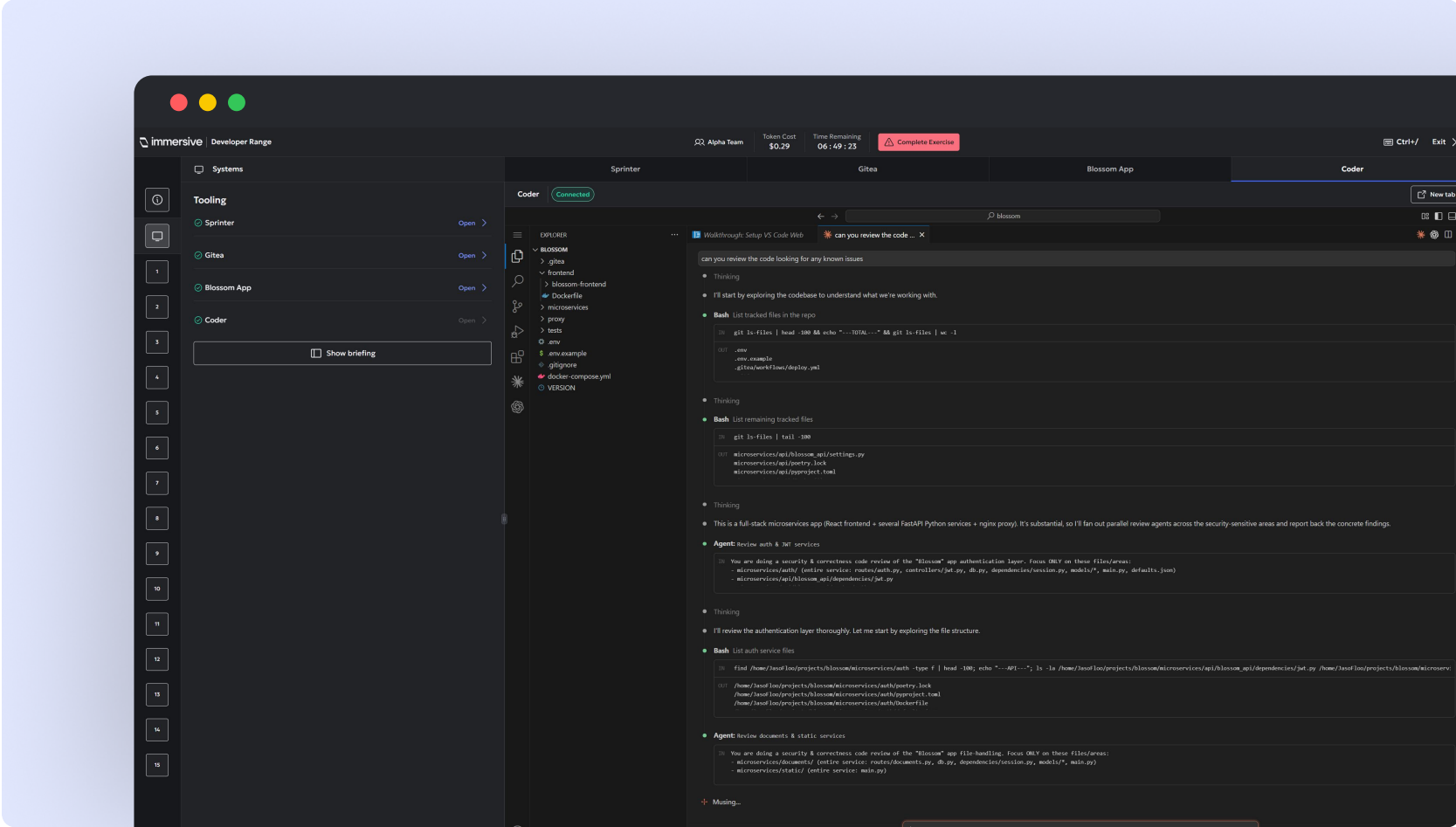
Developers task an AI agent to identify a vulnerability, approving each tool call as it explores the routes and reasons about the flaw, exactly how AI-assisted development happens on the job. (Image: Coder working with AI agent)



04

REMEDiate THE VULNERABILITY

The agent proposes a fix as reviewable diffs, for example, deriving identity from the authenticated JWT instead of trusting a client-supplied ID, and the developer decides what to accept. (Image: Coder remediation differences)



05

SHIP THE FIX, GET THE VERDICT

A pull request is merged and the change ships. The range records merges, ticket movement, and fixes alongside token spend, accuracy, and time, then returns a verdict on exactly what was caught, and what was missed. (Image: Coder pull request & verdict)

Contact your account manager to explore how organizations are proving their AI agents can find and fix vulnerabilities before code ever reaches production.

The cyber proving ground for the AI enterprise

Turn real-world performance into measurable proof of cyber resilience.

#1 In The Forrester Wave™ 2026

Trusted By 30%+ Of The Fortune 100

Trusted by the world's largest organizations:





Prove your business can move securely at AI speed.

Immersive is the cyber proving ground for the AI enterprise. We help organizations prove their people, AI agents, and leadership decisions are ready for a world where AI is used inside the business and against it.