aikido

aikido.dev

AI Pentest Vulnerability Benchmarking

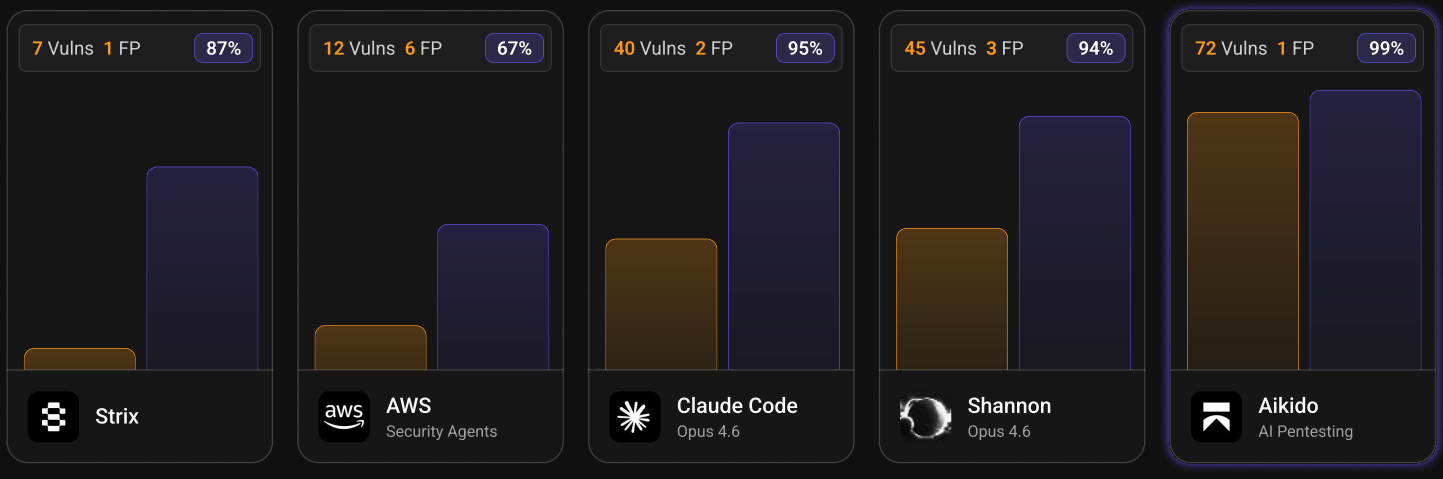
This one-pager outlines the performance of the Aikido AI Pentest agent against key competitors in finding vulnerabilities and minimizing false positives on a standardized application. The test application contained a total of 87 known vulnerabilities across various categories. The benchmarking test assessed how many vulnerabilities each agent could successfully identify out of a maximum of 87 and the number of reported false positives.

The application's vulnerabilities were categorized as:

Access Control | Authentication | CSRF | Cross-Site Scripting | Cyptographic Failure | File Upload | Information Disclosure | Injection | Insecure Design | Path Traversal | Race Condition | Redirect | Security Misconfiguration | Server-Side Request Forgery | Session Management | Server-Side Request Forgery

Comparative Analysis

Vulnerability detection *(more the better)* and false positive rates *(fewer the better)*.



FP=False Positive

Aikido's Competitive Advantage

The Aikido AI Pentest agent significantly outperforms its competitors, identifying 72 out of 87 total vulnerabilities, demonstrating superior detection capability. Furthermore, Aikido maintains the lowest false positive rate alongside Claude, ensuring actionable and efficient security reports.

We are committed to continuous security testing beyond a single pentest. In addition to the AI Pentest, we offer Aikido Infinite, a proactive solution for continuously pentesting every new software release, ensuring that security is a consistent and integrated part of the development lifecycle.

Learn more about what Aikido has to offer

Start AI Pentest | About Aikido Infinite