

Vibe-Coded and Vulnerable

A Benchmark Study of Agentic Security Tooling on AI-Generated Applications

Zauth, Inc. | May 2026 | zauth.inc

The Problem

AI-assisted development platforms including Lovable, Replit, Bolt, and Base44 have collectively amassed over 80 million users and generate 100,000 new applications every day. They handle real users, real data, and in many cases real financial assets. The developers building them are not security engineers. They are founders, designers, and students, regular people who now have the ability to build and ship anything. The result is predictable: 62% of AI-generated code contains security vulnerabilities, at 2.74x the rate of human-written software.

In March 2026, Lovable became the first major vibe-coding platform to integrate native security scanning, partnering with Aikido Security, a unicorn-backed agentic pentesting platform, at \$100 per assessment. The question was whether a tool designed for enterprise security teams could actually protect the developers who need it most. This paper answers that question.

Methodology

Vector is zauth's autonomous black-box security scanner. It operates without source code access, using browser automation and dynamic analysis to find vulnerabilities the way a real attacker would. Ten production-grade Lovable applications were assessed concurrently by Vector and Aikido Security. Both tools ran against identical targets with no prior knowledge or configuration advantages. All findings were scored using CVSS v3.1 and normalized by root cause. Aikido had full visibility into every line of application code. Vector had none.

Results

Metric	Vector	Aikido Security
Total normalized findings	98	71
Critical findings	16	8
Unique critical findings	9	1
Critical detection rate	94%	47%
Unique findings	70	43
Total cost (10 scans)	\$143.12	\$1,000.00
Cost per finding	\$1.46	\$14.08
Average scan time	34.7 min	69.7 min

Aikido Security pricing reflects the Lovable-specific integration rate (\$100/scan). Standard Aikido pricing begins at \$1,000 to \$4,000 per engagement, making the real-world cost gap substantially larger than this study reflects.

Key Findings

Vector detected 94% of critical vulnerabilities to Aikido's 47%, at roughly 14% of the cost and in less than half the time. A tool with no source code access, running for under \$15 and 35 minutes, outperformed a unicorn-backed platform with full code visibility on the vulnerabilities that matter most.

The findings Vector uniquely identified were not subtle. They included Solana private keys readable by any unauthenticated user on a live cryptocurrency platform, an unauthenticated admin panel returning full platform data to any browser, and a four-step exploit chain on a live NFT platform demonstrating financial manipulation of royalty distributions. Aikido had the source code for every one of these applications and did not find them.

Where Aikido did surface unique findings, they concentrated in two narrow areas: business logic flaws requiring deep knowledge of intended application behavior, and infrastructure configuration details. Outside those categories, Vector found everything, including 9 of the 10 most severe vulnerabilities in the dataset, without a single line of source code.

Scale

The attack surface documented here is not unique to Lovable. Bolt, Replit, and Base44 generate materially identical architectures by default. Vector has been deployed across hundreds of additional applications on these platforms and finds critical vulnerabilities consistently across all of them. The ten applications in this study are a documented subset of a pattern that exists across the entire vibe-coding ecosystem.

Conclusion

One hundred thousand applications ship on vibe-coding platforms every day, built by people with no security background and no security tooling priced for how they work. The platforms driving this wave are beginning to take security seriously. But integrating a tool that misses 53% of critical vulnerabilities while operating with full source code access does not solve the problem.

For a platform with eight million users building applications that handle real data and real financial assets, a 53% critical detection gap is not a rounding error. Those are real wallets, real health records, and real businesses left exposed.

The vibe-coding security problem will be solved by infrastructure that operates at the speed, price, and accuracy of the platforms generating it. At \$14.31 per scan, 34.7 minutes per assessment, and 94% critical detection without source code access, Vector already does. The data says so.