

Venture money piles into a few names as AI-found vulnerabilities spread past PHP

VC Tech Radar

2026-10-23

Venture money piles into a few names as AI-found vulnerabilities spread past PHP

By VC Tech Radar • October 23, 2026

Modal's raise and the 20VC/SaaStr debate show how concentrated venture capital has become. OpenAI says finding and fixing bugs one at a time won't scale, while new incidents and investor appetite for security, AI-for-science and frontier companies all grow.

Capital is going to fewer companies

The 20VC x SaaStr discussion described an unusually narrow market. Harry Stebbings met a profitable company with \$20M ARR, growing 600–700% and with a strong team, and no VC responded [1]. Rory O'Driscoll says space data centers and quantum are still getting money. The squeeze is on vertical software, where investors quietly fear AI erases the category [1]. Jason Lemkin's tactical advice: founders with top-decile numbers outside hot categories should plan to meet 100 VCs [1].

The panel also went through the math of funding at each stage: - **Large funds:** \$5B+ funds need billion-dollar positions, which makes a \$2B outcome hard to use without majority ownership [1]. - **Seed:** entry prices of \$50–100M and multi-stage firms crowding allocations leave seed investors with stakes too small to matter [1]. - **The counterview:** Rory cites history: 10–20 decacorns per decade, against a market behaving as if 90 will appear this year [1].

Inference vs. neoclouds. Modal raised a \$750M Series D led by Accel at \$15.75B post-money and says it crossed \$1B in annualized run rate. Its May Series C valued it at \$4.65B [1]. The CEO says sandboxes, which run AI-generated code, now make up about a third of revenue. Demand came from vibe-coding companies, background agents and RL work at new labs [2]. Rory's argument: if quality is similar, cost-sensitive buyers like Replit will move tokens

from a 70%-gross-margin lab to a 30%-margin inference host [1]. Replit did switch its default model to OpenAI, which Lemkin attributes to prices 30–40% lower for similar quality [1].

CoreWeave shows the other side. It fell 15.5% on October 14, some of its bonds yielded above 15%, and credit-default-swap spreads passed 1,000bp [1].

Anthropic. Anthropic reportedly told prospective investors Q3 revenue was \$16.8B, up from \$11.6B in Q2. IPO talk reportedly centered on about \$1.5T, below the ~\$2T investors expected [1].

Late-stage multiples. An Anduril employee tender implied about \$90B on \$2.2B of trailing revenue [1]. Rory calls private multiples “almost certainly disconnected” [1].

Security: OpenAI says bug-by-bug fixing won’t scale

Greg Brockman published OpenAI’s account of PHP2Shell. The bug sat in PHP for 14 years. Calif researchers found a version using GPT-5.6 Sol in August, and OpenAI found a fuller version independently in September [3]. He also mentions a Node.js RCE disclosed the same day. He calls the fixing process “slow and manual” and says it won’t scale [3]. He floats authorized defenders, such as government, scanning for vulnerable hosts and in extreme cases patching them remotely [3]. Brockman says OpenAI moved 25% of its production engineers to model-driven hunting for holes in its own systems [4].

The fallout widened this period: - **Quest Diagnostics** was reported hacked, with patient data exposed. Quest serves roughly half of US hospitals and physicians [5]. - **Replit** says it patched its infrastructure and blocked exploits after vulnerabilities in widely used third-party software [6]. - **Jason Clinton** (Anthropic) told security leaders to ask their boards for funding for the basics, not AI, and to “hold on for ~18 months” [7]. - **Nick Dobos** claims, without sourcing, that 3% of all recorded “critical” bugs were found in the past month [8].

CrowdStrike’s view. George Kurtz says attacker breakout time now averages 29 minutes and can be as fast as 27 seconds [9]. He says much of the attacking runs on open-weight models, because frontier models refuse cyber requests [9]. He claims a general remediation task costs about \$0.03 on CrowdStrike’s post-trained model versus about \$10 on a top frontier cyber model [9]. One bank CIO told him open-weight models a few months behind the frontier are “plenty” for most work [9].

On the startup side, Cogent Security (CEO Vineet Edupuganti, formerly at Abnormal) has raised \$53M, with Greylock and Bain Capital among its backers [10].

Agents in bank accounts. Axios reports major US banks are finding third-party AI agents inside customer accounts and can’t reliably tell humans from agents [11]. David Sacks says most of this is customers handing their credentials

to agents. He argues banks should support user-directed agents, with read-only access as an interim step [12]. The open question is how to identify and permission agents.

Frontier bets and new funds

- **a16z Frontier:** a16z renamed a16z Crypto to a16z Frontier and widened its mandate to companies building markets that may take years to develop [13]. Named interests include AI-native uses, autonomous machines, bio, full-stack startups, and networks of agents that transact with each other [13]. Chris Dixon leads it with Marc Andreessen, Ben Horowitz, Eddy Lazzarin and Guy Wuollet [13]. Andreessen predicts startup formation will “skyrocket” because individuals are adopting AI faster than institutions [14].
- **Warp Sciences:** raised a \$215M Series A led by Lightspeed to apply AI and robotics to drug development. Co-founders are Kevin Weil, DJ Patil, FAIR co-founder Manohar Paluri and Sol Reisberg [15]. The pitch is a US robotics-first CRO, a contract lab that runs experiments for biotech. Its founders say US CROs cost 4–5x more than offshore ones, but offshore labs carry IP and geopolitical risk [16].
- **AMI Labs:** a moderator restated details of Yann LeCun’s company, a world-models bet against LLM scaling. It raised \$1.03B in March at a \$3.5B pre-money, described as Europe’s largest pre-launch AI round [17].
- **Tractian (YC W21):** raised a \$130M Series D at \$1.4B. It sells sensors plus AI for predicting industrial machine failures, has passed \$100M ARR and is growing 90% a year [18].
- **Robotics caution:** Jason Shuman says robotics venture funding is up over 400% in two years while installations grew less than 25% year over year [19].

How AI is changing incumbents

Podium says it crossed \$150M in AI ARR in 2.5 years. Its first \$150M business took eight years, and it had well over \$100M in revenue when it chose to start over [20]. It reports 20,000 agents working for customers, and says it is profitable and free-cash-flow positive [20]. Paul Graham called it “founder mode”: a hired CEO couldn’t have abandoned the existing revenue [21].

Anthropic says its merged code changes went from about 2,500 a day in May to over 30,000 in September. It now sees source control, builds and CI as the bottleneck [22]. It built a closed-source source-control system (Scion) and a code-review tool (Antique) to replace Git and GitHub [22]. Together with the panel’s view that making AI-written code production-ready is software’s most important category [1], this points to developer infrastructure as an area to invest in.

Getty Images filed for Chapter 11, and public shareholders get nothing [23].

Its active annual subscribers fell 25.2% to 240K, while editorial revenue grew 9.2% [23]. That is one data point on generative AI eroding stock content while news coverage holds up.

Briefly

- **Carbon-X:** Hugging Face’s 14.8B open DNA-and-text model averages 66.7% on five DNA benchmarks, versus 67.5% for GPT-6.1 Sol. It fits on one 80GB GPU and is not clinically validated [24].
 - **OCRia-1:** LlamaIndex’s document-parsing model claims top scores on ParseBench and three third-party benchmarks [25].
 - **Whop:** reportedly raised \$200M at \$5.1B, led by Sequoia, as it moves into payments [26].
-

Sources

1. 20VC x SaaStr: \$20M ARR and Unfundable, Anthropic’s \$16.8B Quarter, and Modal at \$15.75B
2. Why AI Compute Comes in Rectangles — Erik Bernhardsson, Modal CEO
3. X article by @gdb
4. X post by @a16z
5. X post by @AndrewCurran__
6. X post by @Replit
7. X post by @JasonDCClinton
8. X post by @NickADobos
9. The New Apex Predator: CrowdStrike CEO George Kurtz on Adversaries Armed With AI Agents
10. Vineet Edupuganti (Cogent Security) - First Principles in the AI Era [Entire Talk]
11. X post by @MadisonMills22
12. X post by @DavidSacks
13. X article by @cdixon
14. X post by @a16z
15. X post by @kevinweil
16. Science Is Limited by How Many Experiments Humans Can Run | Weil and Reisberg, Warp Sciences
17. Yann LeCun, AI legend, Co-Founder of AMI Labs, NYU Professor [AI Founders Masterclass Session 5]
18. X post by @ycombinator
19. X post by @JasonrShuman
20. X post by @ericwilliamrea
21. X post by @paulg
22. The Pulse: Anthropic builds its own source control system
23. Getty Images Files for Chapter 11 at a ~\$910M Run-Rate: 27% EBITDA Margins, 25% Fewer Subscribers, and \$0 for Public Shareholders

- 24. r/MachineLearning post by u/jatingargiitk
- 25. X post by @jerryjliu0
- 26. r/SaaS post by u/Putrid_Meal_3231