

Enkrypt AI Launches RAYDER: A Game Changer for Chatbot Security Testing

BOSTON, MA, UNITED STATES, July 23, 2025 /EINPresswire.com/ -- Designed for security teams, [AI developers](#), and operations professionals, [RAYDER](#) brings real-world testing directly into the browser. There is no need for APIs, backend access, or complex setup.

What Makes RAYDER Different

- Zero Setup: Start testing within seconds, no engineering effort required
- Real-World Testing: Audit chatbot interfaces, filters, and moderation behavior as end users experience them
- AI-Powered Automation: Automatically generates adversarial prompts and detailed risk reports

Key Features

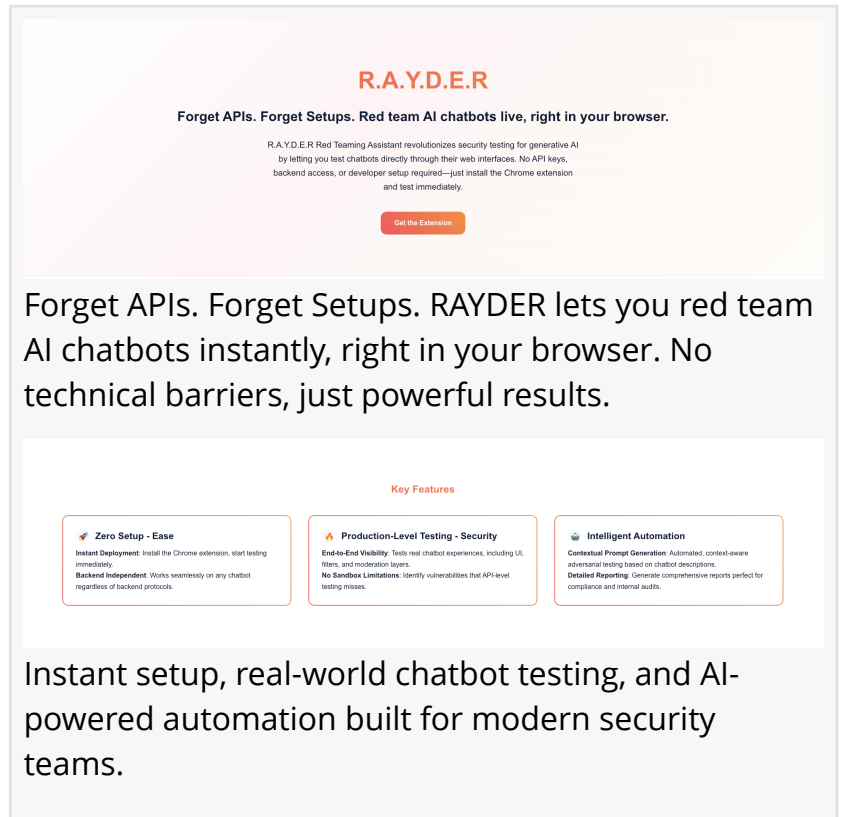


RAYDER enables real-time, in-browser security and compliance testing for Generative AI systems. It is fast, intuitive, and built for the way AI is used today, in production."

Sahil Agarwal, CEO and Co-Founder of Enkrypt AI

- Browser-Based Testing: Works seamlessly with any chatbot via the front-end interface
- Context-Aware Prompt Generation: Uses AI to adapt tests to specific model behavior
- Actionable Reporting: Generates structured output for security, compliance, and audit teams

RAYDER is built on a simple but powerful vision: ****[AI safety](#) should be testable by anyone, not just insiders.**** With nothing more than a browser, anyone; researchers, red teamers, or concerned citizens, can now probe AI systems



The screenshot displays the RAYDER web interface. At the top, the logo 'R.A.Y.D.E.R' is shown in orange. Below it, the tagline 'Forget APIs. Forget Setups. Red team AI chatbots live, right in your browser.' is presented. A brief description follows: 'RAYDER Red Teaming Assistant revolutionizes security testing for generative AI by letting you test chatbots directly through their web interfaces. No API keys, backend access, or developer setup required—just install the Chrome extension and test immediately.' A prominent orange button labeled 'Get the Extension' is visible. The 'Key Features' section is organized into three columns: 'Zero Setup - Ease' (highlighting instant deployment and backend independence), 'Production-Level Testing - Security' (emphasizing end-to-end visibility and no sandbox limitations), and 'Intelligent Automation' (describing contextual prompt generation and detailed reporting). At the bottom, a summary states: 'Instant setup, real-world chatbot testing, and AI-powered automation built for modern security teams.'

in real-world conditions. It's the first step toward a more transparent, accountable AI ecosystem, where community-driven testing becomes a cornerstone of responsible deployment. With RAYDER, Enkrypt AI is democratizing red teaming and accelerating secure AI adoption across industries.

Learn more at
[\[https://www.enkryptai.com/rayder\]](https://www.enkryptai.com/rayder)

About Enkrypt AI

Enkrypt AI is an AI security and compliance platform that safeguards enterprises against generative AI risks by automatically detecting, removing, and monitoring threats. The company's unified platform combines red teaming, security guardrails, and compliance automation to help enterprises move faster without sacrificing control. Fortune 500 companies are using Enkrypt AI to safely productionize their agents and chatbots. As adoption of generative AI accelerates, organizations face critical risks such as data leakage, jailbreaks, hallucinations, and compliance gaps. Enkrypt AI addresses these risks through end to end protection across the entire AI lifecycle.

The company has tested a wide range of language models, launched the first public AI Safety Leaderboard, and developed defenses against real world threats including prompt injection, bias, and misuse. Its solutions are gaining traction across finance, healthcare, and insurance industries, where security and compliance are non negotiable. Founded by Yale PhD experts in 2022, Enkrypt AI is backed by Boldcap, Berkeley SkyDeck, ARKA, Kubera, and other investors. Enkrypt AI is committed to making the world a safer place by promoting the responsible and secure use of AI technology, ensuring that its benefits can be harnessed for the greater good.

Sheetal Janala
Enkrypt AI
sheetal@enkryptai.com
Visit us on social media:
[LinkedIn](#)
[YouTube](#)
[X](#)

RAYDER vs Traditional Tools

Traditional web security tools like Burp Suite were game-changers—but they can't meet the complexity of today's generative AI. **RAYDER** does what no existing tool can: deliver comprehensive, real-time security testing of live, user-facing AI interactions, seamlessly in your browser.

No Waiting

Real-time vulnerability discovery

No Complexity

Simplified interface, powerful outcomes

Full Transparency

Detailed, actionable vulnerability reports

Feature	Burp Suite	RAYDER
UI-based chatbot testing	❌ No	✅ Fully supported
Bypasses rate-limited APIs	🚫 Often blocked	✅ Works through UI
Contextual prompt generation	🖱️ Manual	✅ AI-driven
End-to-end prod testing	🔗 APIs only	✅ Actual user-facing chatbot
Setup required	⚙️ Moderate-high	🚀 Minimal
Safety reporting	📄 Generic	📊 Detailed analysis
Designed for LLM security	❌ No	✅ Purpose-built

RAYDER vs Traditional Tools: RAYDER outperforms legacy solutions with UI-based chatbot testing, AI-powered automation, and built-in safety reporting purpose-built for LLM security.

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.