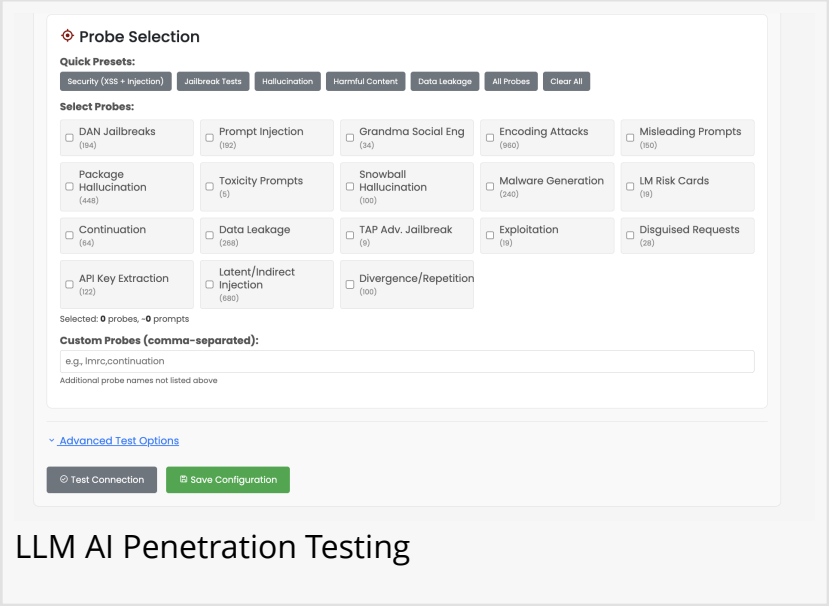
NDay, an NVIDIA Inception Member, Launches Self-Service GARAK AI LLM Red Teaming, Expanding Continuous Exploitability

NDay, an NVIDIA Inception Member, Launches Self-Service GARAK AI Red Teaming, Expanding Its Continuous Exploitability



LLM AI Penetration Testing

MIAMI, FL, UNITED STATES, March 12, 2026 /EINPresswire.com/ -- NDay Security today announced the launch of its fully orchestrated, self-service security infrastructure combining automated AI red teaming, a continuous exploitability platform, and an AI-powered penetration testing agent. The unified system helps enterprises proactively identify and remediate risks across AI systems, applications, networks, cloud, and APIs.

As a member of the NVIDIA Inception program, NDay Security leverages NVIDIA's AI ecosystem to support safe and secure AI deployment at enterprise scale.

"AI has transformed the attack surface," said Gary McAlum, CISO Advisor at NDay Security. "Speaking from my experience, security teams need continuous, intelligent, and automated testing that keeps pace with AI-enabled threats. Our platform brings AI-powered red teaming, exploitability testing, and AI-driven penetration testing together in one system. This allows CISOs to move from a point-in-time perspective to a true continuous monitoring view."

Automated AI Red Teaming

Powered by NVIDIA Garak, the platform stress-tests large language models and generative AI systems to identify over 18 types of customizable attacks, including prompt injection risks, jailbreak techniques, policy bypasses, unsafe outputs, and model misuse and alignment gaps. This enables organizations to validate AI safety before and after deployment.

Continuous Exploitability Platform

NDay Security's continuous exploitability platform evaluates how systems can be exploited in real-world conditions. It continuously simulates attacker behavior and validates exposures across digital environments, ensuring organizations always have current visibility into their security posture.

AttackBench

AttackBench serves as an autonomous, OSCP-caliber AI penetration testing agent operating safely 24×7×365. Its capabilities include execution of over 65,000+ exploit techniques and variations, automated reconnaissance and vulnerability discovery, multi-step attack chaining, AI and traditional system testing, and continuous exploit validation. AttackBench operates like a skilled ethical hacker at machine speed, continuously probing for exploitable weaknesses.

AttackN

AttackN provides centralized orchestration, analytics, and remediation guidance. It coordinates over 70 types of tests covering networks, applications, credentials, cloud, AI, and APIs, along with millions of automated safety checks, exploitability prioritization, and self-service controls for security teams. This gives organizations a unified, real-time view of risk and security posture.

DiscoverN

DiscoverN eliminates the equivalent of over 80 manual hours of reconnaissance through continuous, automated external attack surface discovery. It identifies unknown and exposed internet-facing assets, vulnerabilities and perimeter misconfigurations, leaked credentials from over 30B breach records, dark web exposure across 58K+ monitored channels, and high-risk social engineering targets. This gives organizations a real-time, outside-in view of what attackers can see—without the burden of manual investigation.

Continuous Security for the AI Era

As enterprises accelerate AI adoption, one-time testing is no longer enough. NDay Security enables continuous validation of AI and infrastructure security, integrating directly into development and production pipelines.

"Security must be continuous and adversary-driven," added Mark Whitehead, CEO at NDay. "Our mission is to make advanced offensive testing accessible through a self-service platform. NVIDIA has been the perfect accelerator and partner on this journey."

About NDay Security

NDay Security is a cybersecurity company focused on automated AI red teaming, AI penetration testing, and continuous exploitability management. The company helps organizations identify, measure, and reduce risk across AI systems and digital infrastructure.

PR
NDAY Security, Inc.
inbound@ndaysecurity.com
Visit us on social media:
LinkedIn
