POWERED BY MOZILLA

ODIN Vulnerability Scanner DATASHEET

Continuous Security Intelligence for GenAI Models

Monitor, measure, and mitigate GenAI model vulnerabilities with real-time analytics, probe automation, and researcher-driven insights all from a centralized scanning platform built for scale.

WHY 0DIN VULNERABILITY SCANNER?

Built for AI Security at Scale

The 0DIN Vulnerability Scanner is an enterprise-grade application engineered to analyze security risks across AI models. It integrates directly with ODIN's probe network and bug bounty program to convert findings into real-time, structured intelligence.

What You Get:

- Centralized dashboard with metrics and taxonomies
- Model-specific vulnerability tracking
- Configurable probe execution and scan scheduling
- Custom reporting and data export tools
- Researcher recognition and provenance logs

Continuous Security Lifecycle

1. Probe Ingestion
Submissions from ODIN's bounty program are validated, classified, and converted into executable probes.

2. Scan Configuration
Admins define model targets, choose relevant probes, and schedule scans (hourly, daily, weekly).

3. Automated Execution
The engine runs tests using NVIDIA Garak and updates the dashboard in real time with structured outcomes.

4. Impact Analysis
All findings are scored for severity, categorized by taxonomy, and displayed with model responses and metadata.

5. Reporting & Export
Reports are available in PDF, CSV, and image formats for internal security reviews or compliance audits.

Platform Features

- Landing Dashboard: Key metrics, top vulnerabilities, taxonomy, and heatmaps
- Scan Reports: Full vulnerability timelines and model-specific security profiles
- Taxonomy Web: Dynamic mapping of jailbreak and prompt injection classifications
- Probe Browser: Detailed views of each test, including impact score and prompt samples

KEY BENEFITS

Automate Vulnerability Discovery: Continuously scan GenAI systems using validated probes derived from ODIN's bug bounty program. Detect one-shot and multi-step jailbreaks with precision.

Track Trends Across Models: Visualize vulnerability patterns across models, providers, and timeframes. Map weaknesses using interactive dashboards and taxonomy webs.

Benchmark GenAI Security: Compare security posture across different model types, versions, and deployments. Identify which classes of attacks each model resists—or fails.

Empower Threat-Informed Remediation: Turn raw findings into actionable intelligence with structured reports, impact scoring, and exportable data for fine-tuning and compliance.

Support Compliance and Auditability: Demonstrate continuous assessment and secure operations with historical scan records, TLP-classified reports, and audit-ready logs.

As GenAI deployments expand, new vulnerabilities emerge faster than traditional security teams can respond. Static assessments and point-in-time audits fall short in the face of evolving, model-specific threats.

0DIN Vulnerability Scanner delivers continuous, probe-driven visibility—empowering your organization to track, analyze, and respond to AI vulnerabilities in real time. Stay ahead of adversaries by knowing exactly where your models are exposed—and how to harden them before attackers strike.

0DIN: Securing Tomorrows AI.

Learn More: https://www.0din.ai
Email: 0din@mozilla.com