

GenR3d LLM Security Analyzer

Safeguarding your sensitive data in generative Al-powered chatbots

Tailored to your industry

Ready-to-use Abuse Case library with prompt-based attacks against industryspecific use cases. Today, enterprises lack the necessary tools to have confidence and assurances that their bots aren't oversharing and putting their business at risk. The GenR3d LLM Security Analyzer ensures the information shared between end users and generative Al-powered bots cannot be abused, accelerating enterprises' ability to deliver new customers experiences with confidence. The GenR3d platform empowers developers with key, unique capabilities enabling them to get security buyoff and deliver value in production faster and more securely.

GenR3d LLM Security Analyzer ⊕ Development / 🖮 Chatbots / Fezziwig Guide / Scan 42f9 Dashboard ♠ Environments 6 Back ₾ Export PDF 🕒 View JSON Fezziwig Guide Scan 42f9 Chatbots API Access Total Tests: 18 Passed Inconclusive Failed ☐ Knowledgebase Pass Rate: 33% Critical ⚠ Inventory Exfiltration Potential to bypass front-end controls Bypass of well established compliance controls Potential to bypass shopping cart restrictions Lost revenue or at worst direct attacks against backend transaction Price Match Abuse Employee Safety - Stalking Employees could be harassed or accosted Employee Safety - Information Disclosure Employees could be harassed or accosted Get Support High

The GenR3d platform delivers:

- Abuse Cases tailored to your specific industry and use cases instead of generic LLM threats
- Insight on successful attacks and potential mitigations providing actionable information for resolutions

So you can:

- Prevent competition and bad actors from analyzing your key metrics and using them against you
- Protect your business models and proprietary methods from

SaaS-based LLM Security

Test your chatbot against the latest industry-specific threats as you move through your development pipelines without the need to maintain yet another security tool.

Built for integration

Full API accessibility enables you to automate testing, complete with atomic finding reporting for integration with ticketing system.

For fast integration, our published API's can be used with common model testing and deployment tools like Google's AutoML, Amazon SageMaker, and Azure Machine Learning through our API's to test your chatbots before they see real traffic. Then, integrate with modern ticketing systems like Jira and Zendesk to ingest findings as atomic JSON for easy tracking and resolution.

With the GenR3d LLM Security Analyzer, you get faster time to measurable security, faster time to getting to promoting to production, and faster time to delivering on the promise and value of generative Al.

For more information contact us at:

sales@generativesecurity.ai +1 844 7436 732

+61 1800 436 732

https://generativesecurity.ai

