open·kritt

Self-hosted Plattform zur Orchestrierung von KI-Agenten für die Suche und Validierung von Sicherheitslücken in Quellcode.

STERNE	LIZENZ	SPRACHE	VERSION	ANGELEGT	ZULETZT GEÄNDERT
2.029	AGPL-3.0	JavaScript	v1.4.1	2026-07-20	2026-08-24

Was es ist

open·kritt zerlegt die Schwachstellenanalyse in kleine, definierte Aufgaben, die parallel von KI-Agenten bearbeitet werden. Die Ergebnisse werden zusammengeführt, dedupliziert und nach Schweregrad priorisiert. Das Projekt basiert auf internen Werkzeugen, mit denen das Team über 1.500.000 US-Dollar in Bug-Bounty-Programmen verdient hat.

Was es kann

- Workflows aus verketteten Prompts als wiederverwendbare Playbooks erstellen.
- Remote- oder lokale Repositories inklusive Abhängigkeiten mit Codex oder Claude Code analysieren.
- Befunde per Post-Scripts validieren, Proof-of-Concepts erstellen und Berichte generieren.
- Scan-Ergebnisse als ZIP-Archiv mit Manifest exportieren, bei abgebrochenen Scans als partielle Exporte.
- Eigene Modelle über OpenAI, Anthropic, OpenRouter, xAI oder Codex-Login anbinden.
- Headless über Kommandozeile betreiben, ohne grafische Oberfläche.

So fängst du an

Voraussetzungen sind Git, Docker mit Docker Compose und Node.js 20 oder neuer.

```
git clone https://github.com/Kritt-ai/open-kritt
cd open-kritt
./kritt setup
./kritt start
```

Grenzen und Bedingungen

- Keine integrierte Anwendungs-Authentifizierung im Backend; der Stack muss hinter einem privaten Netzwerk laufen, da die Standardports auf 127.0.0.1 binden.
- Agenten laufen als root in wegwerfbaren Containern mit schreibbarem Repository-Zugriff und direktem Internetzugang; ein dedizierter Docker-Host oder VM ist erforderlich, besonders bei untrusted Code.
- Für private GitHub-Repositories wird ein GITHUB_TOKEN benötigt.

- Die Lizenz AGPL-3.0 verpflichtet zur Offenlegung von Änderungen bei Netzwerknutzung; kommerzielle Nutzung ohne Quellcode-Pflicht ist nicht möglich.
- 40 offene Issues im Repository (Stand 2026-08-24) deuten auf aktive, aber noch nicht abgeschlossene Entwicklung hin.

Für wen sich das lohnt

Sich lohnt für Sicherheitsforscher und entwicklerbewusste Teams, die Kontrolle über Prompts, Workflows, Modellanbieter und eigene Infrastruktur behalten wollen. Weniger geeignet für Nutzer, die eine sofort einsatzbereite Cloud-Lösung ohne eigenen Betrieb oder ohne AGPL-Verpflichtung suchen.



Zusammengestellt von **localdev.ai**
Quelle: **github.com/Kritt-ai/open-kritt** · Stand 2026-08-24

Grundlage: Lizenz: AGPL-3.0 (Badge und LICENSE in der Liesmich-Datei); Befehle: git clone, ./kritt setup, ./kritt start (Abschnitt 'Getting started'); Technische Anforderungen: Git, Docker mit Docker Compose, Node.js 20 oder neuer (Abschnitt 'Getting started'); Sicherheitsmodell: root-Container, writable copies, direct internet access, dedizierter Docker-Host oder VM (Abschnitt 'Getting started' und Verweis