

PR #46373 完整报告

vllm-project/vllm

[docs] link security docs from AGENTS

合并时间: 2026-06-22 21:28

原文链接: <http://prhub.com.cn/vllm-project/vllm/pull/46373>

执行摘要

- 一句话: AGENTS.md 添加安全文档引导
- 推荐动作: 此 PR 仅作文档补充, 无需精读代码。但作为安全治理的基础设施优化, 值得维护者确认链接正确性后合并。

功能与动机

帮助 AI 代理或安全审查者在接触代码时快速找到安全相关的权威文档, 确保安全策略被正确引用和遵循。PR body 明确说明了添加的是指向三个安全文档的 routing sentence。

实现拆解

1. 在 AGENTS.md 的安全审查相关区域 (第 135 行附近) 新增一段 Markdown 链接文本。
2. 文本中依次引用 SECURITY.md、docs/usage/security.md 和 docs/contributing/vulnerability_management.md, 并用中文说明这些文档分别涵盖项目安全策略、威胁模型与部署假设、漏洞处理流程。
3. 变更仅 6 行新增, 无删除, 无其他文件改动。

关键文件:

- AGENTS.md (模块 代理指南; 类别 docs; 类型 documentation): 唯一变更文件, 新增安全文档引导段落, 是 PR 的全部内容。

关键符号: 未识别

评论区精华

无 review 讨论。仅有一条 mergify bot 的文档预览链接评论。

- 暂无高价值评论线程

风险与影响

- 风险: 无技术风险。变更仅为文档内文本增加, 不影响任何代码逻辑、配置或构建流程。若链接路径错误可能导致 404, 但路径均与仓库现有文档结构一致, 风险极低。
- 影响: 影响范围极小: 仅影响 AGENTS.md 的读者 (AI 代理或安全审查者)。帮助其更高效地定位安全文档, 提升安全审查的一致性和完整性。无其他系统影响。

- 风险标记：暂无

关联脉络

- 暂无明显关联 PR