Validación de Defensas DevSecOps con Chaos Monkey y merciaudit.py

Estantería: DevSecOps e Infraestructura

Subtema: Gobernanza

mercedev.es — 2026-05-12 | Epic 2 - Fase 4

El Desafío (Síntoma)

Se detectó que las defensas DevSecOps del proyecto no eran suficientemente robustas contra ataques impulsados por IA. Específicamente, el linter merciaudit.py no lograba detener vulnerabilidades como estilos en línea o scripts XSS inyectadas por un Chaos Monkey.

La Maniobra (Lógica)

Se implementó una solución arquitectónica que incluye: 1. El uso de `git restore` dentro de un bloque `try...finally` para garantizar que el código no quede envenenado en caso de interrupciones manuales (Ctrl+C). 2. La mejora de las Regex del auditor merciaudit.py para cazar etiquetas script maliciosas sin generar falsos positivos con datos estructurados JSON-LD.

El Aprendizaje / Deuda Técnica

Se aprendió que el mecanismo de Rollback debe estar siempre dentro de un bloque `try...finally` para evitar dejar el código envenenado. Además, las Regex del auditor deben ser lo suficientemente robustas para distinguir entre etiquetas script maliciosas y datos estructurados JSON-LD. Esta solución es la óptima porque garantiza la integridad del código y reduce los falsos positivos, pero se ha asumido una deuda técnica en el futuro debido a la necesidad de mantener y mejorar continuamente estas soluciones.