El incidente de las ventanas emergentes

Cuadernillo | Vol. 1

mercedev.es — 2026-04-25

El Desafío (Síntoma)

Durante una sesión de trabajo, el navegador comenzó a abrir múltiples ventanas emergentes de terceros sin control aparente. Esto generó una fuerte sensación de vulnerabilidad y la sospecha inicial de haber sufrido una inyección de código malicioso o un hackeo, coincidiendo temporalmente con un bloqueo del sistema operativo.

La Maniobra (Lógica)

Se procedió a auditar el entorno. Primero, se aisló el navegador abriéndolo desde la terminal en un modo seguro sin restaurar pestañas. Posteriormente, al revisar la configuración de privacidad del navegador, se detectó que los permisos para mostrar ventanas emergentes de sitios de terceros estaban habilitados. Se procedió a revocar dichos permisos inmediatamente.

El Aprendizaje/Deuda Técnica

En momentos de estrés tecnológico, es común establecer saltos lógicos entre síntomas visuales (pop-ups) y fallos del sistema a bajo nivel, asumiendo ataques complejos. Aunque los scripts de terceros generan saturación de recursos y una mala experiencia, no siempre implican una vulneración o "hackeo" real del equipo.

Esta experiencia refuerza, desde la empatía con el usuario final, el porqué de nuestra arquitectura en el **Merci Boilerplate**:

- La implementación de políticas **CSP (Content Security Policy)** estrictas.
- La prohibición absoluta de inyectar dependencias de terceros o scripts publicitarios que secuestren la experiencia de navegación.