

acme/tienda-online

Repositorio GitHub · main · 25/10/2026, 03:35:36

🕒 Ya analizamos este código antes

Es el escaneo #3 de este proyecto. El código cambió desde la última revisión. Comparado con el escaneo anterior (19/10/2026):

Postura 0 → 0 0 pts	Resueltos 5 ya no aparecen	Nuevos 1 aparecieron ahora	Persisten 9 siguen abiertos
---------------------------	----------------------------------	----------------------------------	-----------------------------------

RESUELTOS

- ✓ RCE vía deserialización insegura
- ✓ Token de admin hardcodeado
- ✓ next@12.1.0 — CVE con SSRF

NUEVOS

- ▲ Open redirect en /login

● VEREDICTO DE LANZAMIENTO

No publicar todavía

Hay 3 hallazgos críticos que un atacante puede aprovechar hoy. Resuélvelos antes de abrir al público.



F

postura de seguridad

RESUMEN EJECUTIVO

3 Crítico	2 Alto	4 Medio	1 Bajo	0 Info
--------------	-----------	------------	-----------	-----------

10

Hallazgos totales

8

Validados por prueba

142

Archivos analizados

340

Dependencias

QUÉ REVISAMOS

 Secretos expuestos Clave de Stripe expuesta al cliente.	 Control de acceso (IDOR / multi-tenant) IDOR en pedidos a revisar.
 Inyección (SQL/NoSQL/OS/SSTI) SQLi confirmada por explotación.	 XSS XSS confirmado en navegador.
 SSRF No se detectaron pedidos a URLs controladas por el usuario.	 Autenticación y sesión Sin debilidades evidentes de auth.
 Dependencias vulnerables lodash con CVE crítico conocido.	 Calidad / arquitectura (CI, tests) Faltan CI, tests y lockfile.
 SAST avanzado (Semgrep) Análisis ejecutado con el ruleset Semgrep de VibeScan.	 Explotación dinámica (DAST) App atacada en vivo; hallazgos confirmados con PoC.

PLAN DE CORRECCIÓN PRIORIZADO

P0

3

Resolver antes de abrir al público.

P1

2

Resolver en los próximos días.

P2

5

Resolver antes de escalar el tráfico.

Empezá por los **3 ítems P0**: bloquean el lanzamiento. Muchos tienen un comando de arreglo listo para copiar.

HALLAZGOS (10)

Crítico

Stripe Live Secret Key expuesto al navegador

P0 · SEC-001 · A05:2021 Security · CVSS 9.1 · [fix listo](#)

✓ **Probado**



Crítico

Inyección SQL confirmada (error-based)

P0 · DAST-001 · A03:2021 Injection · CVSS 9.3

✓ **Probado**



Crítico

lodash@4.17.11 — CVE-2021-23337

P0 · DEP-001 · A06:2021 Vulnerable · CVSS 9.1 · [fix listo](#)

✓ **Probado**



Alto**XSS confirmado (ejecución en el navegador)****P1** · DAST-002 · A03:2021 Injection · CVSS 7.6**✓ Probado****Alto****IDOR: pedido accedido por id sin chequeo de pertenencia****P1** · SG-001 · A01:2021 Broken · CVSS 7.6**Firme****Medio****Faltan headers de seguridad (4)****P2** · DAST-003 · A05:2021 Security · CVSS 5.4**✓ Probado****Medio****Open redirect****P2** · DAST-004 · A01:2021 Broken · CVSS 5.4**✓ Probado****Medio****Sin CI: nada impide publicar algo roto****P2** · QA-001 · Quality &**✓ Probado****Medio****Sin tests automatizados detectados****P2** · QA-002 · Quality &**Firme****Bajo****Sin lockfile de dependencias****P2** · QA-003 · A08:2021 Software · **fix listo****✓ Probado**

Auditoría generada por VibeScan. Los hallazgos marcados "No confirmado" provienen de análisis estático y requieren validación dinámica (Fase 2) antes de afirmarse como explotables. Sólo se analizó código autorizado por el solicitante.