Informe de prueba de seguridad

Resumen

Empresa Ejemplo S.A.

Tienda en línea. 5 días de prueba, con autorización firmada del dueño.



10 fallas encontradas. La crítica y las dos altas permiten ver o cambiar datos de otros clientes y se corrigen primero.

Falla 2 de 10

Un cliente puede ver pedidos ajenos

Gravedad alta

Al cambiar el número del pedido en la dirección, la tienda muestra el pedido de otra persona, con nombre, domicilio y teléfono.

Evidencia

- Cuenta de prueba A abre el pedido 1042: correcto.
- La misma cuenta abre el pedido 1043: la tienda responde con datos de la cuenta B.

Corrección

Comprobar en el servidor que el pedido pertenece a la cuenta que lo pide.

Plan de corrección

Esta semana
Control de acceso a pedidos

Este mes
Doble factor en el panel

Este trimestre
Respaldos probados

Trabajo alineado a OWASP Top 10 y ASVS. No emito certificaciones: eso lo hace un auditor acreditado.