PENTESTING WEB/API

Informe de pentest de ejemplo: API multi-tenant

Informe completamente sintético con alcance, hallazgos, evidencia, remediación y retest. No contiene datos ni resultados de clientes.

REKON — SEGURIDAD OFENSIVA HÍBRIDA · 2026-09-18

Ejemplo sintético · DEMO-2026-01

Todos los nombres, datos, versiones, resultados y fechas de prueba siguientes son ficticios. Este documento ilustra un entregable; no demuestra un trabajo contratado ni certifica un sistema. Organización: Demo, aplicación: portal.example y api.example. Revisión editorial: 18 de septiembre de 2026.

Resumen ejecutivo

Escenario simulado: evaluación de lectura y exportación de documentos en una API multi-tenant, versión demo-1.0. Se ilustran dos hallazgos: acceso cruzado a documentos (alto) y acceso de miembro a una exportación administrativa (medio). El riesgo principal es la exposición de información de otra organización. Prioridad: centralizar autorización en el servidor y verificarla en cada operación. Las severidades son cualitativas y dependen del contexto ficticio; no se presenta un CVSS calculado.

Alcance y limitaciones

Activos: portal.example y api.example en laboratorio. Identidades: miembro A, administrador A y miembro B. Operaciones: lectura de documentos y exportación de miembros. Ventana ficticia: 14–15 de septiembre de 2026. Exclusiones: infraestructura, proveedores externos, carga, phishing y pagos. Evidencia mínima con datos sintéticos; sin extracción masiva. No se revisó código fuente ni se probaron roles distintos de los listados.

F-01 · Lectura entre tenants · Alta

Precondición: sesión de miembro A; documento doc-b-01 pertenece a B. **Reproducción sintética:** solicitar GET https://api.example/v1/documents/doc-b-01 con la sesión de A. **Esperado:** 403 o 404 sin contenido. **Observado ficticio:** 200 con document=doc-b-01, tenant=B, title=Documento de prueba. Control positivo: miembro B puede leer su documento. Control de sesión: sin autenticar responde 401. **Impacto:** un usuario autenticado podría leer documentos ajenos si conoce un identificador. No se demuestra enumeración masiva. **Remediación:** resolver el objeto dentro del tenant autorizado y comprobar permisos en el servidor; agregar pruebas cruzadas entre tenants. Referencia: OWASP API1:2023.

F-02 · Exportación administrativa · Media

Precondición: miembro A sin permiso de gestión. **Reproducción sintética:** GET https://api.example/v1/admin/members/export con sesión de miembro A. **Esperado:** 403. **Observado ficticio:** 200 con dos miembros sintéticos del tenant A. No se observó acceso al tenant B por esta ruta. **Impacto:** exposición del directorio interno a un rol no autorizado. **Remediación:** validar permiso de exportación en el servidor y mantener el filtro por tenant. Un botón oculto no aplica autorización. Referencia: OWASP API5:2023.

Retest simulado y estado final

Versión demo-1.1, fecha ficticia 17 de septiembre de 2026. **F-01: corregido en los casos probados**: miembro A y administrador A reciben 404 para doc-b-01; miembro B conserva acceso 200; sin sesión, 401. **F-02: persiste**: miembro A sigue recibiendo 200 y el directorio. La remediación visual no corrigió el permiso del servidor. Riesgo residual: F-02 abierto y cobertura limitada a operaciones y roles listados. El retest no declara segura toda la aplicación.

Cómo usar este ejemplo

Compará si tu informe permite reconstruir identidad, activo, versión, evidencia, impacto y estado de corrección. Los dominios .example están reservados para documentación y no son objetivos de prueba. Prepará el alcance o solicitá una propuesta. Descargar informe PDF en español.