ENGAGEMENT · PT-DEMO-2026-03

Informe de evaluación de seguridad

Demo Rekon SRL — RUT 000000000000

Evaluación gray-box de la plataforma SaaS de gestión de inventario: aplicación web multi-tenant, API REST y consola de administración.

ACTIVO	MODALIDAD	VENTANA	FECHA
demo.rekon.sh	Gray-box	30 días	06.03.2026
443 · 203.0.113.10	Staging	cierre 2026-04-05	v1.0 · inicial

Control del documento

TÍTULO	Informe de evaluación de seguridad — web, API y consola de administración
CLIENTE	Demo Rekon SRL — RUT 000000000000
REFERENCIA	PT-DEMO-2026-03
VERSIÓN	1.0 — inicial (2026-03-06)
CLASIFICACIÓN	CONFIDENCIAL — exclusivo del cliente
AUTOR	Rekon (placeholder de firma)
REVISOR	Rekon (placeholder de firma)
VENTANA	30 días naturales · cierre 2026-04-05T17:00Z
AUTORIZACIÓN	SOW/ROE Anexo 1 firmado 2026-03-01 · BoldSign 4f2c9a11-77de-4b02-9c8a-2ee901ab63d4
CONFIDENCIALIDAD	Acuerdo Bilateral de Confidencialidad, Montevideo, 2026-02-27
CAMBIO	v1.0 — primera emisión. Datos de demostración: este documento es un template ilustrativo y no describe un engagement real.

Distribución

DESTINATARIO	USO
Dirección / sponsor	§1 Resultado y prioridades. Residuo P0.
Ingeniería de plataforma	§2 fichas, §3 cadenas, apéndices A–B.
Administración del tenant	§4 Residuo y limpieza. Baja de ids sintéticos 204, 207 y del prefijo QA9Z.

Este documento es exclusivo de Demo Rekon SRL. Su reproducción o uso fuera de los destinatarios requiere consentimiento del cliente. El cliente puede compartirlo con auditores bajo NDA para demostrar la evaluación.

Tabla de contenidos

1 Resumen ejecutivo

1.1 Declaración de confidencialidad

Este documento es exclusivo de Demo Rekon SRL. Contiene información de su plataforma y de la evaluación autorizada PT-DEMO-2026-03. Su reproducción, redistribución o uso —completo o parcial— requiere consentimiento del cliente. El cliente puede compartirlo con auditores bajo el NDA del 2026-02-27.

1.2 Resultado

Un usuario autenticado de cualquier tenant lee y escribe los datos de todos los demás tenants de la plataforma. El token de sesión no vincula la petición a la organización que lo emitió: el servidor confía en el identificador de tenant que viaja en el cuerpo.

El generador de reportes concatena parámetros en SQL sin parametrizar, lo que expone la base completa por inyección ciega, y **un usuario estándar se asigna a sí mismo el rol de administrador con una sola llamada** a la API de perfil.

> RESIDUO QUE PIDE ACCIÓN HOY
>
> **Dos administradores sintéticos siguen activos: 204 y 207.** Ambos con contraseña conocida por la prueba (nunca copiada a esta entrega). Se recomienda darlos de baja antes de cualquier promoción del entorno a producción.
>
> El prefijo de deconflicción `QA9Z` marca todo objeto creado por esta evaluación. El SKU `QA9Z-DEMO-001` es visible en el catálogo del tenant de prueba. Inventario en §4.

La plataforma autentica correctamente las sesiones. Casi nunca verifica si este usuario puede operar sobre este objeto de este tenant. Esa ausencia de autorización a nivel de objeto y de organización explica la mayoría de los críticos y altos; varios se cierran con un cambio de patrón y no con parches puntuales.

HECHO	MEDICIÓN
Riesgo global	Aislamiento entre tenants y autorización a nivel de objeto ausentes en los componentes genéricos; la separación multi-tenant no se sostiene en la capa de datos.
Conteos	**12** confirmados (2 Critical · 4 High · 5 Medium · 1 Info sin vector). 4 cadenas. 12 PoCs.
Estado	Los 12 permanecen **Abiertos**. El cliente aún no ha remediado al cierre de este informe.
Ventana	30 días naturales. Informe 2026-03-06. Cierre de autorización 2026-04-05T17:00Z.
Activo / roles	demo.rekon.sh (443) + 203.0.113.10 + API REST. Gray-box. Staging. Cuenta de operador y clave de API entregadas.

HECHO	MEDICIÓN
RCE	**0 confirmada**. La subida sin restricción (F-06) no llegó a ejecución observable; la hipótesis de ese canal no queda refutada.

El entorno está declarado Staging y contiene una copia parcial de datos reales. Toda actuación usó objetos sintéticos y las cuentas entregadas. Las lecturas que devolvieron datos reales se registraron por forma y presencia, nunca por valor.

1.3 Prioridades

P0 — Hoy

Dar de baja los administradores sintéticos 204 y 207 y retirar el SKU `QA9Z-DEMO-001` del catálogo público. Cortar el generador de reportes vulnerable a inyección y verificar que el identificador de tenant deja de aceptarse desde el cuerpo de la petición. Impedir que la API de perfil escriba el campo de rol.

P1 — Esta iteración

Derivar el tenant siempre del token de sesión, nunca del cuerpo. Autorización a nivel de objeto en inventario, exportaciones y movimientos. Parametrizar todas las consultas del generador de reportes. Escapar y sanear las notas de SKU. Validar tipo, extensión y ruta de las subidas y servirlas fuera del origen de la aplicación.

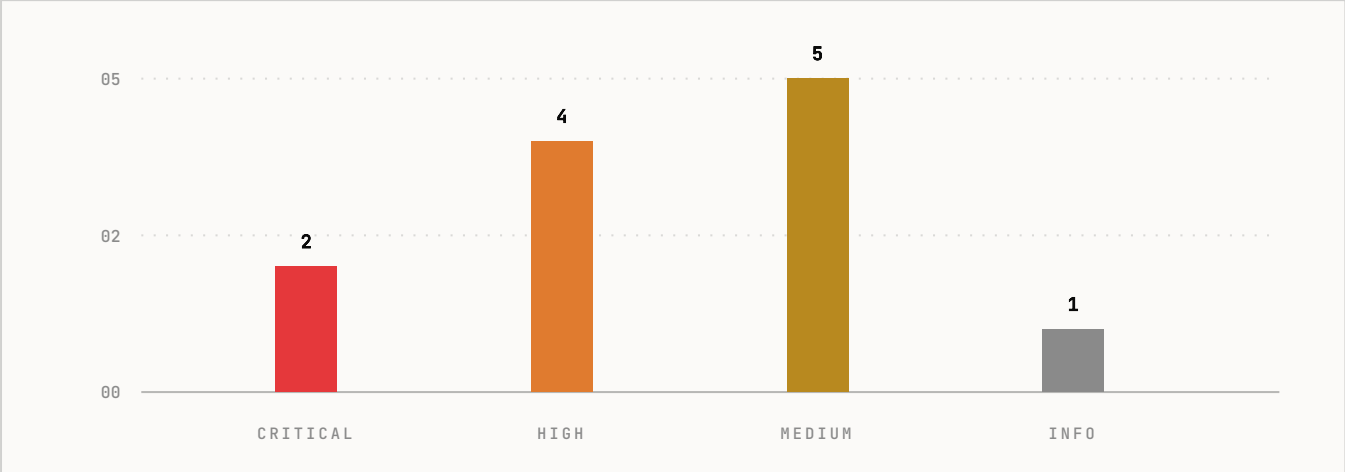
P2 — Siguiente ciclo

Token anti-CSRF en todas las escrituras sensibles. Rate limiting en OTP y en el login. Suprimir stack traces en producción. Allowlist de destinos en el retorno SSO. Cabeceras de seguridad y CSP en ambos orígenes; retirar suites TLS obsoletas.

Aplicadas P0 y P1, se ofrece retest de las rutas afectadas y constancia escrita de cierre. Este informe no es certificación ni garantía de ausencia de vulnerabilidades.

2 Hallazgos

2.1 Distribución



CRITICAL	HIGH	MEDIUM	INFORMATIVO
02	04	05	01
ABIERTOS	ABIERTOS	ABIERTOS	ABIERTOS

No hay cerrados al 2026-03-06: las barras no se apilan. Total 2+4+5+1 = 12. El resultado negativo de RCE por subida (F-06) se documenta en su ficha, no en esta distribución.

- **Critical.** Confusión de tenant en el token (AUTH-JWT-TENANT-CONFUSION) e inyección SQL en el generador de reportes (SQLI-REPORT-BUILDER).
- **High.** Lectura de inventario ajeno (BOLA), XSS almacenado en notas de SKU, autopromoción de rol y subida de archivos sin restricción.
- **Medium.** CSRF en rotación de clave, OTP sin límite de intentos, export CSV sin propiedad, stack traces expuestos y redirección abierta en el retorno SSO.
- **Informativo.** Suites TLS obsoletas (TLS-LEGACY-CIPHERS), sin vector directo a propósito.

2.2 Tabla maestra

Una fila por hallazgo confirmado. Orden: puntaje descendente, idéntico al índice de fichas. Estado único en todo el informe: Abierto.

#	ID	TÍTULO	ESTADO	CVSS 4.0	BANDA
01	AUTH-JWT-TENANT-CONFUSION	El token de sesión no vincula la petición a su tenant: acceso cruzado total	ABIERTO	9.4	CRITICAL
02	SQLI-REPORT-BUILDER	Inyección SQL ciega en el generador de reportes: lectura de toda la base	ABIERTO	9.1	CRITICAL
03	IDOR-INVENTORY-READ	Un usuario lee el inventario de cualquier otro tenant por id	ABIERTO	8.6	HIGH
04	STORED-XSS-SKU-NOTES	Las notas de SKU ejecutan código en la consola del administrador	ABIERTO	8.2	HIGH
05	PRIVESC-ROLE-SELF	Un usuario se asigna a sí mismo el rol de administrador vía API de perfil	ABIERTO	8.1	HIGH
06	FILE-UPLOAD-UNRESTRICTED	La subida de adjuntos no valida tipo ni ruta y se sirve desde el origen	ABIERTO	7.7	HIGH
07	CSRF-API-KEY-ROTATE	La rotación de la clave de API no valida token anti-CSRF	ABIERTO	6.8	MEDIUM
08	OTP-NO-RATE-LIMIT	El OTP del segundo factor no limita la tasa de intentos	ABIERTO	6.5	MEDIUM
09	IDOR-EXPORT-CSV	La exportación CSV de movimientos responde por id sin verificar propiedad	ABIERTO	6.3	MEDIUM
10	VERBOSE-STACKTRACE	Las respuestas 500 devuelven la traza de pila completa	ABIERTO	5.4	MEDIUM
11	OPEN-REDIRECT-SSO	El retorno del flujo SSO redirige a un destino arbitrario	ABIERTO	5.1	MEDIUM
12	TLS-LEGACY-CIPHERS	El endpoint acepta suites TLS obsoletas	ABIERTO	n/d	INFORMATIVO

Datos de demostración. Los vectores CVSS son ilustrativos y coherentes con la banda, no producto de una medición real.

2.3 Fichas detalladas

Campos en este orden: identificadores, componente, metadatos, descripción, impacto de negocio, cómo se explota, evidencia, remediación, control negativo, criterio de retest, cadenas.

2.3.1 AUTH-JWT-TENANT-CONFUSION ■ CRITICAL ABIERTO

El token de sesión no vincula la petición a su tenant: acceso cruzado total

IDENTIFICADO EL 2 DE MARZO DE 2026

COMPONENTE	`GET /api/v2/{tenant}/inventory` · el segmento **tenant** se toma del path y no se contrasta contra el **org_id** del token · rol requerido: cualquier usuario autenticado.
CVSS 4.0	9.4 · CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

La plataforma es multi-tenant: cada organización debería ver solo sus datos. El token de sesión incluye un `org_id`, pero las rutas de la API v2 resuelven el tenant a partir del segmento de path (o del header `X-Tenant-Id`) sin compararlo con el del token. Cambiar ese valor por el de otra organización devuelve sus datos con un 200.

El defecto es transversal: afecta inventario, movimientos, usuarios y facturación bajo el mismo prefijo `/api/v2/`. No requiere escalar privilegios ni interacción de la víctima.

IMPACTO DE NEGOCIO

Cualquier cliente de la plataforma lee y modifica los datos de todos los demás: stock, precios de coste, proveedores y movimientos. El aislamiento comercial entre clientes competidores no existe en la capa de datos.

CÓMO SE EXPLOTA

01 Autenticarse con una cuenta de tenant propio y capturar el token de sesión.

02 Emitir `GET /api/v2/{otro_tenant}/inventory` reutilizando el mismo token.

03 Observar 200 con el inventario de la otra organización; repetir con `X-Tenant-Id` para confirmar la segunda vía.

EVIDENCIA · AUTH-JWT-TENANT-CONFUSION FIG 01

```
GET /api/v2/demo-b/inventory   (token org_id=demo-a)
200 OK · 1.284 filas · org ajena · precios de coste incluidos
X-Tenant-Id: demo-b  → misma respuesta por la segunda vía
```

Figura 1 — el segmento de tenant se honra por encima del token. Custodia: `evidence/raw/wave-01/TENANT/`.

REMEDIACIÓN

Primario: derivar el tenant exclusivamente del token de sesión firmado; ignorar el segmento de path y el header como fuente de autorización. Añadir un predicado `org_id = token.org_id` en cada consulta.

Compensatorio: WAF que rechace peticiones donde el tenant del path difiera del de la sesión; alertar accesos cruzados en logs.

CONTROL NEGATIVO · No se modificó ningún objeto de un tenant real; las lecturas cruzadas se registraron por conteo y forma, nunca por valor.

CRITERIO DE RETEST · El mismo request con un tenant ajeno responde 403 y ninguna vía alternativa (path o header) altera el aislamiento.

CADENAS · CH-01

> VARIANTE / ALCANCE EXTRA · AUTH-JWT-ADD-1
>
> El mismo salto de tenant funciona sobre `/api/v2/{tenant}/users`: expone correos y hashes de la organización ajena. No se enumeró más allá de la primera página de prueba.

2.3.2 SQLI-REPORT-BUILDER ■ CRITICAL ABIERTO

Inyección SQL ciega en el generador de reportes: lectura de toda la base

IDENTIFICADO EL 3 DE MARZO DE 2026

COMPONENTE	`POST /api/v2/reports/build` · parámetro `sort_by` (y `group_by`) concatenados en la cláusula `ORDER BY` · rol requerido: usuario autenticado con acceso a reportes.
CVSS 4.0	9.1 · `CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:L/SI:L/SA:N`
CVSS 3.1	n/d

DESCRIPCIÓN

El constructor de reportes acepta un nombre de columna de ordenamiento y lo concatena directamente en la consulta. Los campos de filtro sí están parametrizados; el de ordenamiento no. Una expresión condicional en `sort_by` altera el orden de las filas de forma observable, lo que habilita inyección ciega basada en booleanos.

IMPACTO DE NEGOCIO

Lectura de toda la base de datos, incluidos hashes de contraseña, claves de integración y datos de todos los tenants, a ritmo de un bit por petición. La inyección corre con el usuario de aplicación, que tiene acceso de lectura amplio.

CÓMO SE EXPLOTA

01 Enviar `POST /api/v2/reports/build` con un `sort_by` benigno y registrar el orden base.

02 Sustituir por una expresión `CASE WHEN (...) THEN col_a ELSE col_b END` que invierta el orden según un predicado.

03 Automatizar la extracción bit a bit observando el cambio de orden en la respuesta.

EVIDENCIA · SQLI-REPORT-BUILDER FIG 02

```
POST /api/v2/reports/build
{ "sort_by": "(CASE WHEN (SUBSTRING(@@version,1,1)='8') THEN name ELSE id END)" }
200 OK · orden observablemente distinto → predicado verdadero
```

Figura 2 — el orden de las filas filtra un bit por petición. Custodia: `evidence/raw/wave-01/SQLI/`.

REMEDIACIÓN

Primario: allowlist estricta de columnas de ordenamiento (mapa nombre-lógico → columna física); rechazar cualquier valor fuera de la lista. Nunca concatenar identificadores desde entrada del usuario.

Compensatorio: usuario de base con privilegios mínimos por tenant; monitorizar `ORDER BY` anómalos.

CONTROL NEGATIVO · La extracción se detuvo tras confirmar el canal booleano sobre una tabla de prueba; no se volcaron datos reales.

CRITERIO DE RETEST · Cualquier `sort_by` fuera de la allowlist responde 400 y el orden no cambia ante expresiones condicionales.

CADENAS · CH-02

2.3.3 IDOR-INVENTORY-READ HIGH ABIERTO

Un usuario lee el inventario de cualquier otro tenant por id

IDENTIFICADO EL 3 DE MARZO DE 2026

COMPONENTE	`GET /api/v2/items/{item_id}` · el handler resuelve el objeto por id y no verifica propiedad · rol requerido: usuario autenticado.
CVSS 4.0	8.6 · CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

El detalle de artículo se sirve por identificador numérico secuencial. El handler no comprueba que el artículo pertenezca al tenant del llamador. Incrementar o decrementar el id devuelve artículos de otras organizaciones con su coste, proveedor y niveles de stock.

IMPACTO DE NEGOCIO

Enumeración del catálogo completo de la plataforma por un solo cliente, incluyendo información comercialmente sensible de competidores.

CÓMO SE EXPLOTA

01 Autenticarse y solicitar un artículo propio para conocer el formato de id.

02 Solicitar `GET /api/v2/items/{id±n}` con ids fuera del propio tenant.

03 Observar 200 con datos de artículos ajenos.

EVIDENCIA · IDOR-INVENTORY-READ FIG 03

```
GET /api/v2/items/48213     (usuario tenant demo-a)
200 OK · item de tenant "demo-b" · cost=..., supplier=..., stock=...
```

Figura 3 — id secuencial sin predicado de propiedad. Custodia: `evidence/raw/wave-02/IDOR-ITEM/`.

REMEDIACIÓN

Primario: filtrar por `tenant_id` del token en toda lectura por id; responder 404 (no 403) ante objetos ajenos para no revelar existencia.

Compensatorio: identificadores opacos (UUID) en lugar de secuenciales; rate limiting por patrón de enumeración.

CONTROL NEGATIVO · Solo se leyeron tres ids ajenos, registrados por forma; no hubo enumeración masiva.

CRITERIO DE RETEST · Un id de otro tenant responde 404 y no filtra ningún campo.

CADENAS · CH-01

2.3.4 STORED-XSS-SKU-NOTES HIGH ABIERTO

Las notas de SKU ejecutan código en la consola del administrador

IDENTIFICADO EL 4 DE MARZO DE 2026

COMPONENTE	`POST /api/v2/items/{id}/notes` · campo `body` renderizado sin escapar en la vista de detalle del panel · rol requerido: usuario con permiso de edición de catálogo.
CVSS 4.0	8.2 · CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:N/SC:L/SI:L/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

Las notas internas de un artículo se guardan tal cual y se insertan en el DOM del panel de administración sin escapar. Un operador de bajo privilegio deja una nota con marcado activo; cuando un administrador abre el artículo, el código corre en el origen del panel.

IMPACTO DE NEGOCIO

Robo de sesión del administrador y ejecución de acciones privilegiadas en su nombre. Punto de entrada para escalar del catálogo al control del panel (CH-03).

CÓMO SE EXPLOTA

01 Con una cuenta de edición de catálogo, crear una nota en un artículo con una carga inerte de prueba.

02 Esperar a que un administrador abra el detalle del artículo.

03 Confirmar la ejecución mediante el marcador inerte registrado.

EVIDENCIA · STORED-XSS-SKU-NOTES FIG 04

```
POST /api/v2/items/48090/notes
{ "body": "<img src=x onerror=REKON_MARK()>" }
→ el panel ejecuta REKON_MARK() al renderizar la nota
```

Figura 4 — carga inerte, sin exfiltración real. Custodia: `evidence/raw/wave-02/XSS-NOTE/`.

REMEDIACIÓN

Primario: escapar en salida toda nota de SKU; renderizar como texto plano. Añadir CSP con `script-src` restrictivo en el origen del panel.

Compensatorio: sanear en entrada con allowlist de etiquetas; cookies de sesión `HttpOnly` y `SameSite`.

CONTROL NEGATIVO · Solo se usó un marcador inerte propio; no se capturó ninguna sesión real.

CRITERIO DE RETEST · La misma carga se muestra como texto y no ejecuta.

CADENAS · CH-03

2.3.5 PRIVESC-ROLE-SELF HIGH ABIERTO

Un usuario se asigna a sí mismo el rol de administrador vía API de perfil

IDENTIFICADO EL 4 DE MARZO DE 2026

COMPONENTE	PATCH /api/v2/me · acepta el campo role en el cuerpo · rol requerido: cualquier usuario autenticado.
CVSS 4.0	8.1 · CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

El endpoint de auto-edición de perfil aplica un binding de modelo masivo. Además de nombre y avatar, acepta el campo `role`. El servidor no filtra campos privilegiados, de modo que el usuario reescribe su propio rol a administrador del tenant.

IMPACTO DE NEGOCIO

Cualquier usuario estándar obtiene control administrativo de su organización: gestión de usuarios, claves de API y facturación.

CÓMO SE EXPLOTA

01 Autenticarse como usuario estándar.

02 Enviar `PATCH /api/v2/me` con `{"role":"admin"}`.

03 Recargar y comprobar el acceso a las vistas de administración.

EVIDENCIA · PRIVESC-ROLE-SELF FIG 05

```
PATCH /api/v2/me   { "display_name": "qa", "role": "admin" }
200 OK · perfil actualizado · role=admin persistido
```

Figura 5 — mass assignment sobre un campo privilegiado. Custodia: `evidence/raw/wave-02/PRIVESC/`.

REMEDIACIÓN

Primario: allowlist de campos editables en el endpoint de perfil; el rol solo se cambia por un flujo administrativo con verificación del llamador.

Compensatorio: alertar cambios de rol fuera del panel de administración de usuarios; invalidar sesiones al elevar privilegios.

CONTROL NEGATIVO · La elevación se probó sobre una cuenta sintética y se revirtió; ninguna cuenta real fue promovida.

CRITERIO DE RETEST · El campo `role` se ignora en `/api/v2/me` y su envío responde 400.

CADENAS · CH-03

2.3.6 FILE-UPLOAD-UNRESTRICTED ■ HIGH ABIERTO

La subida de adjuntos no valida tipo ni ruta y se sirve desde el origen

IDENTIFICADO EL 6 DE MARZO DE 2026

COMPONENTE	`POST /api/v2/attachments` · sin validación de MIME/extensión · servido en `/uploads/` del mismo origen · rol requerido: usuario autenticado.
CVSS 4.0	7.7 · CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:L/SC:N/SI:L/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

El endpoint de adjuntos acepta cualquier tipo de archivo y conserva el nombre y la extensión provistos, sin normalizar la ruta. Un archivo HTML o SVG con marcado activo queda accesible en `/uploads/`, en el mismo origen que la aplicación, y ejecuta en el contexto de quien lo abra.

IMPACTO DE NEGOCIO

XSS almacenado servido desde el propio dominio y superficie de phishing con URL legítima. No se confirmó ejecución del lado servidor: el intérprete no fue observable en staging.

CÓMO SE EXPLOTA

01 Subir `qa9z-probe.svg` con un script inerte vía `POST /api/v2/attachments`.

02 Recuperar la URL devuelta bajo `/uploads/`.

03 Abrirla y confirmar la ejecución en el origen de la aplicación.

EVIDENCIA · FILE-UPLOAD-UNRESTRICTED — FIG 06

```
POST /api/v2/attachments  (multipart, qa9z-probe.svg)
201 · url=/uploads/qa9z-probe.svg  · Content-Type: image/svg+xml
GET /uploads/qa9z-probe.svg → script inerte ejecuta en el origen
```

Figura 6 — sin validación de tipo; ejecución del lado servidor no establecida. Custodia: `evidence/raw/wave-03/UPLOAD/`.

REMEDIACIÓN

Primario: allowlist de tipos, renombrado a identificador aleatorio, y servir los adjuntos desde un origen sin cookies con `Content-Disposition: attachment`.

Compensatorio: `X-Content-Type-Options: nosniff`; análisis antimalware en la ingesta.

CONTROL NEGATIVO · No se intentó ejecución del lado servidor; el archivo de prueba lleva el prefijo QA9Z y queda en el inventario de residuo.

CRITERIO DE RETEST · Los tipos ejecutables se rechazan y los adjuntos se sirven fuera del origen de la app.

CADENAS · CH-04

2.3.7 CSRF-API-KEY-ROTATE MEDIUM ABIERTO

La rotación de la clave de API no valida token anti-CSRF

IDENTIFICADO EL 6 DE MARZO DE 2026

COMPONENTE	`POST /settings/api-keys/rotate` · escritura con cookie de sesión y sin token anti-CSRF · rol requerido: administrador del tenant (víctima).
CVSS 4.0	6.8 · CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

La acción de rotación de clave de API se valida solo con la cookie de sesión. No exige token anti-CSRF ni cabecera de origen. Un sitio de terceros puede forzar la rotación con la sesión activa del administrador, invalidando la clave en uso.

IMPACTO DE NEGOCIO

Denegación de servicio sobre las integraciones del cliente: los sistemas que usan la clave dejan de autenticar hasta que se reconfiguran.

CÓMO SE EXPLOTA

01 Alojar un formulario auto-enviado que apunte al endpoint de rotación.

02 Inducir a un administrador con sesión activa a visitar la página.

03 Comprobar que la clave anterior deja de autenticar.

EVIDENCIA · CSRF-API-KEY-ROTATE FIG 07

```
POST /settings/api-keys/rotate   (sin token CSRF, cookie de sesión)
200 OK · nueva clave emitida · la anterior queda invalidada
```

Figura 7 — escritura sensible sin protección CSRF. Custodia: `evidence/raw/wave-03/CSRF/`.

REMEDIACIÓN

Primario: token anti-CSRF por sesión en todas las escrituras y verificación de `Origin` / `Referer`.

Compensatorio: cookies `SameSite=Strict`; confirmar la rotación con reautenticación.

CONTROL NEGATIVO · La rotación se ejecutó sobre una clave sintética y se documentó; ninguna integración real fue interrumpida.

CRITERIO DE RETEST · La rotación sin token válido responde 403.

CADENAS · CH-03

2.3.8 OTP-NO-RATE-LIMIT MEDIUM ABIERTO

El OTP del segundo factor no limita la tasa de intentos

IDENTIFICADO EL 4 DE MARZO DE 2026

COMPONENTE	`POST /auth/2fa/verify` · el código de 6 dígitos no tiene tope de intentos ni expiración corta · rol requerido: ninguno (paso intermedio de login).
CVSS 4.0	6.5 · CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

Tras la primera etapa de login, el segundo factor se verifica en un endpoint que no cuenta ni bloquea los intentos fallidos. El espacio de 10^6 códigos es forzable en minutos con concurrencia moderada.

IMPACTO DE NEGOCIO

El segundo factor deja de ser una barrera efectiva frente a un atacante que ya conoce la contraseña.

CÓMO SE EXPLOTA

01 Completar la primera etapa con credenciales válidas hasta llegar al paso de OTP.

02 Iterar códigos contra `/auth/2fa/verify` sin recibir bloqueo.

03 Registrar el número de intentos permitidos (sin completar el bypass real).

EVIDENCIA · OTP-NO-RATE-LIMIT — FIG 08

```
POST /auth/2fa/verify  × 500 intentos
sin 429, sin lockout, sin captcha · latencia estable
```

Figura 8 — medido a 500 intentos; no se completó fuerza bruta real. Custodia: `evidence/raw/wave-02/OTP/`.

REMEDIACIÓN

Primario: límite de intentos por sesión y por cuenta, expiración de 30–60 s y bloqueo tras fallos consecutivos.

Compensatorio: captcha tras el primer fallo; alertar ráfagas de verificación.

CONTROL NEGATIVO · No se completó ninguna adivinación; solo se midió la ausencia de límite.

CRITERIO DE RETEST · El endpoint responde 429 y bloquea tras N fallos.

CADENAS · —

2.3.9 IDOR-EXPORT-CSV MEDIUM ABIERTO

La exportación CSV de movimientos responde por id sin verificar propiedad

IDENTIFICADO EL 6 DE MARZO DE 2026

COMPONENTE	`GET /exports/movements/{export_id}.csv` · responde por id sin sesión ni propiedad · rol requerido: ninguno.
CVSS 4.0	6.3 · CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

Los CSV de movimientos generados quedan accesibles por un id incremental sin autenticación. Adivinar o iterar el id descarga exportaciones de otros tenants con sus movimientos de stock y precios.

IMPACTO DE NEGOCIO

Fuga de datos operativos de cualquier cliente a un actor sin cuenta, siempre que exista una exportación generada.

CÓMO SE EXPLOTA

01 Generar una exportación propia y observar el formato del id.

02 Solicitar `GET /exports/movements/{id-1}.csv` sin cookie.

03 Confirmar la descarga de una exportación ajena.

EVIDENCIA · IDOR-EXPORT-CSV FIG 09

```
GET /exports/movements/10442.csv   (sin cookie)
200 OK · text/csv · movimientos de un tenant ajeno
```

Figura 9 — mismos bytes que vería el dueño. Custodia: `evidence/raw/wave-03/EXPORT/`.

REMEDIACIÓN

Primario: exigir sesión y verificar propiedad del export; ids opacos y de un solo uso con expiración.

Compensatorio: URLs firmadas de vida corta.

CONTROL NEGATIVO · Solo se descargó una exportación ajena, registrada por forma; sin enumeración masiva.

CRITERIO DE RETEST · El endpoint exige sesión y responde 404 ante exports ajenos.

CADENAS · CH-01

2.3.10 VERBOSE-STACKTRACE MEDIUM ABIERTO

Las respuestas 500 devuelven la traza de pila completa

IDENTIFICADO EL 3 DE MARZO DE 2026

COMPONENTE	Varios endpoints `/api/v2/*` ante entrada malformada · modo debug activo en staging · rol requerido: ninguno.
CVSS 4.0	5.4 · CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

Ante ciertas entradas malformadas la API responde 500 con la traza de pila completa: framework y versión, rutas de archivos del servidor y fragmentos de consulta SQL. Esa información acelera el resto de los ataques.

IMPACTO DE NEGOCIO

Divulgación de detalles internos que reducen el coste de explotación de otros hallazgos, en especial la inyección SQL.

CÓMO SE EXPLOTA

01 Enviar un cuerpo JSON malformado a un endpoint de la API.

02 Leer la respuesta 500 con la traza completa.

EVIDENCIA · VERBOSE-STACKTRACE FIG 10

```
POST /api/v2/reports/build   { "filters": [ }   (JSON roto)
500 · stack trace · framework 4.x · /srv/app/... · fragmento SQL
```

Figura 10 — divulgación de entorno en el error. Custodia: `evidence/raw/wave-01/ERRORS/`.

REMEDIACIÓN

Primario: desactivar el modo debug en entornos accesibles; página de error genérica con identificador de correlación.

Compensatorio: registrar el detalle solo del lado servidor.

CONTROL NEGATIVO · No se explotó ningún dato revelado; solo se documentó la divulgación.

CRITERIO DE RETEST · Los errores 500 devuelven un cuerpo genérico sin traza.

CADENAS · CH-02

2.3.11 OPEN-REDIRECT-SSO MEDIUM ABIERTO

El retorno del flujo SSO redirige a un destino arbitrario

IDENTIFICADO EL 6 DE MARZO DE 2026

COMPONENTE	`GET /auth/sso/return?next=` · el parámetro `next` se sigue sin validar contra una allowlist · rol requerido: ninguno.
CVSS 4.0	5.1 · CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	n/d

DESCRIPCIÓN

El retorno del inicio de sesión federado toma un parámetro `next` y redirige a él sin comprobar el dominio. Un enlace que empieza en el origen legítimo termina en un sitio del atacante, lo que da credibilidad a campañas de phishing.

IMPACTO DE NEGOCIO

Phishing con URL de arranque confiable; puede encadenarse con robo de tokens de retorno.

CÓMO SE EXPLOTA

01 Construir `/auth/sso/return?next=https://evil.example/`.

02 Enviar el enlace desde el dominio legítimo.

03 Comprobar la redirección al destino externo.

EVIDENCIA · OPEN-REDIRECT-SSO FIG 11

```
GET /auth/sso/return?next=https://qa9z.example/probe
302 · Location: https://qa9z.example/probe
```

Figura 11 — destino de retorno sin allowlist. Custodia: `evidence/raw/wave-03/REDIRECT/`.

REMEDIACIÓN

Primario: allowlist de rutas de retorno relativas al propio origen; rechazar URLs absolutas externas.

Compensatorio: página intersticial de salida para destinos no reconocidos.

CONTROL NEGATIVO · El destino usado es un host de prueba QA9Z; no se dirigió a ningún usuario real.

CRITERIO DE RETEST · Un `next` externo se ignora o rechaza.

CADENAS · CH-04

2.3.12 TLS-LEGACY-CIPHERS ■ INFORMATIVO ABIERTO

El endpoint acepta suites TLS obsoletas

IDENTIFICADO EL 2 DE MARZO DE 2026

COMPONENTE	TLS · 443 · negociación de suites y versiones obsoletas · sin vector directo demostrado.
CVSS 4.0	n/d · informativo, publicado sin vector a propósito.
CVSS 3.1	n/d

DESCRIPCIÓN

El servicio negocia TLS 1.1 y suites con CBC y RSA de intercambio de clave, además de TLS 1.2/1.3 modernas. No se demostró un ataque concreto; se reporta como higiene de configuración.

IMPACTO DE NEGOCIO

Superficie criptográfica innecesaria y posibles observaciones de auditoría de cumplimiento; sin explotación demostrada en este trabajo.

CÓMO SE EXPLOTA

01 Enumerar suites y versiones aceptadas en el puerto 443.

02 Registrar las obsoletas ofrecidas por el servidor.

EVIDENCIA · TLS-LEGACY-CIPHERS FIG 12

```
TLS handshake · aceptadas: TLSv1.1, TLS_RSA_WITH_AES_128_CBC_SHA
(coexisten con TLSv1.3 modernas)
```

Figura 12 — inventario de suites, sin ataque. Custodia: `evidence/raw/wave-01/TLS/`.

REMEDIACIÓN

Primario: deshabilitar TLS 1.1 y las suites CBC/RSA; dejar solo TLS 1.2+ con AEAD y forward secrecy.

Compensatorio: HSTS con `max-age` largo.

CONTROL NEGATIVO · No se intentó descifrado ni downgrade activo.

CRITERIO DE RETEST · El servidor rechaza TLS 1.1 y las suites obsoletas.

CADENAS · —

3 Cadenas de ataque

Las cadenas no llevan puntaje propio. Muestran cómo se componen los hallazgos. Ninguna afirma nada sobre detección: no se revisó ninguna fuente de logs en esta campaña.

CH-01 Cruce total de tenants sin escalar privilegios

Hallazgos: AUTH-JWT-TENANT-CONFUSION, IDOR-INVENTORY-READ, IDOR-EXPORT-CSV.

CADENA · CH-01	FLOW
usuario de cualquier tenant → cambia el tenant del path/header → /inventory y /items/{id} de otros → /exports/*.csv sin cookie → datos de toda la plataforma	

Entrada. Una cuenta estándar de cualquier organización. **Pivote.** El servidor confía en el tenant del cliente y en ids secuenciales. **Resultado.** Lectura del catálogo, stock y precios de todos los clientes. **Qué la corta.** Derivar el tenant del token y añadir predicado de propiedad por objeto; cerrar solo la confusión de tenant deja en pie los BOLA por id.

CH-02 De la inyección a las credenciales de administración

Hallazgos: SQLI-REPORT-BUILDER, VERBOSE-STACKTRACE.

CADENA · CH-02	FLOW
usuario con reportes → 500 revela framework y SQL → sort_by inyecta → lectura bit a bit → hashes y claves de integración	

Entrada. Usuario con acceso a reportes. **Pivote.** El error verboso orienta la inyección ciega. **Resultado.** Volcado de credenciales de toda la base. **Qué la corta.** Parametrizar el ordenamiento con allowlist y suprimir las trazas en entornos accesibles.

CH-03 Del SKU al secuestro del panel de administración

Hallazgos: STORED-XSS-SKU-NOTES, PRIVESC-ROLE-SELF, CSRF-API-KEY-ROTATE.

CADENA · CH-03	FLOW
operador de catálogo → nota de SKU con marcado activo → el admin abre el artículo → código en el panel → PATCH /me role=admin | rotación de clave por CSRF	

Entrada. Cuenta de edición de catálogo, el privilegio más bajo con escritura. **Pivote.** La nota corre en el origen del panel cuando la abre un administrador. **Resultado.** Control administrativo del tenant y de sus integraciones. **Qué la corta.** Escapar las notas, CSP en el panel, allowlist de campos en el perfil y token

CSRF en las escrituras.

La mitad delantera se midió con un marcador inerte; la promoción de rol se probó sobre una cuenta sintética y se revirtió.

CH-04 Subida y redirección como cebo de phishing

Hallazgos: FILE-UPLOAD-UNRESTRICTED, OPEN-REDIRECT-SSO.

CADENA · CH-04 FLOW

```
usuario → sube SVG activo a /uploads/ (mismo origen) → enlace de SSO ?next= arranca en el dominio legítimo → destino controlado
```

Entrada. Una cuenta autenticada cualquiera. **Pivote.** Contenido activo servido desde el propio dominio, más un salto de redirección con URL de arranque confiable. **Resultado.** Phishing y XSS con la reputación del dominio del cliente. **Qué la corta.** Servir adjuntos fuera del origen y aplicar allowlist al destino del retorno SSO.

Ejecución del lado servidor no establecida: el resultado se limita al contexto de navegador.

4 Residuo y limpieza

Acción hoy

Administradores sintéticos activos: 204 y 207. Darlos de baja desde el panel. Si alguno no lleva el marcador QA9Z, detenerse y consultar antes de tocarlo.

SKU `QA9Z-DEMO-001` visible en el catálogo del tenant de prueba. Despublicar y verificar como visitante anónimo.

El delete de la aplicación es lógico, no físico. Un 200 OK no significa que la fila desapareció. Las bajas dejan `deleted=1` y la fila se sigue leyendo por consulta directa. Tras cada baja, leer de vuelta para confirmar.

Inventario de residuo

ID / OBJETO	TIPO	ESTADO	ACCIÓN
204, 207	Admin sintético	Activo · credencial conocida por la prueba	Baja hoy
QA9Z-DEMO-001	SKU / artículo	Visible en catálogo	Despublicar + verificar anónimo
5521	Usuario sintético	Rol admin (autopromoción de prueba)	Baja; no es restauración
qa9z-probe.svg	Adjunto en /uploads/	Inerte · accesible por URL	Borrar del almacén de adjuntos
export 10442	CSV de movimientos	Generado durante la prueba	Purgar del almacén de exportaciones

Ningún objeto de un cliente real fue creado, modificado ni borrado. Datos de demostración: los ids son ilustrativos. Tras cada baja, leer de vuelta: un 200 no prueba desaparición.

Ap. A Alcance y metodología

ACTIVO	demo.rekon.sh (443), IP 203.0.113.10, API REST del mismo host
FUERA	Dominios corporativos del cliente distintos del activo; infraestructura de correo; sistemas de terceros integrados por API.
MODALIDAD	Gray-box. Cuenta de operador y clave de API entregadas. Entorno declarado Staging con copia parcial de datos reales.
VENTANA	30 días naturales, 24-7, cierre 2026-04-05T17:00Z. SOW/ROE Anexo 1 firmado 2026-03-01.
MÉTODO	Pruebas manuales guiadas por OWASP WSTG y ASVS. Deconflicción por prefijo `QA9Z` en todo objeto creado. Sin escaneo destructivo ni denegación de servicio.

Este informe no es certificación, auditoría de cumplimiento ni garantía de ausencia de vulnerabilidades. Lo que no se probó está declarado como tal en cada ficha. Es un documento de demostración con datos ficticios.

Ap. B Glosario

TÉRMINO	EN ESTE TRABAJO
Multi-tenant	Una sola instancia sirve a muchas organizaciones (tenants). El aislamiento entre ellas debe sostenerse en cada capa, sobre todo en la de datos.
BOLA / IDOR	El handler resuelve un objeto por id y no pregunta si el llamador es su dueño. Inventario, export y movimientos.
Confusión de tenant	El servidor deriva la organización de un valor controlado por el cliente (path o header) en lugar del token firmado.
Mass assignment	El binding de modelo acepta campos privilegiados no previstos, como `role`, desde el cuerpo de la petición.
SQLi ciega (booleana)	La inyección no devuelve datos directamente; se infiere bit a bit por una diferencia observable, aquí el orden de las filas.
QA9Z	Prefijo de deconflicción de todo objeto de esta evaluación. Si aparece en un log o en la base, es de esta prueba.
CVSS 4.0	Métrica primaria. En este template los vectores son ilustrativos y coherentes con la banda, no fruto de una medición real.
Marcador inerte	Carga de prueba que solo señala ejecución (p. ej. una función testigo), sin exfiltrar ni dañar.