DOCUMENTO DE MUESTRA

MM

TEST DE INTRUSIÓN · APLICACIÓN WEB Y API

Informe de test de intrusión

Aplicación web y API de cliente · Evaluación técnica de seguridad

Cliente Ejemplo, S.L.

Referencia: MM-2026-PT-0142 · **Versión:** 1.0 · **Fecha:** 12 de mayo de 2026
Alcance: app.ejemplo-cliente.es (entorno de preproducción, datos sintéticos)
Estándares: OWASP WSTG 4.2 · PTES · **Clasificación:** Confidencial
Autor: Martín Martín · mmartin.me

AVISO

Confidencialidad y naturaleza del documento

Documento de muestra

Este informe es un **ejemplo demostrativo**. No corresponde a ningún cliente ni sistema real. La organización (Cliente Ejemplo, S.L.), el dominio (`ejemplo-cliente.es`), los datos y las capturas son ficticios, y las direcciones IP utilizadas pertenecen a los rangos reservados para documentación por la RFC 5737 (`203.0.113.0/24`). Su único fin es mostrar el formato, el nivel de detalle y el rigor de un informe de test de intrusión.

Los informes reales entregados a clientes se rigen por un acuerdo de confidencialidad (NDA) y no se comparten. Este documento sustituye a esa muestra sin comprometer a ningún cliente.

Cláusula de confidencialidad

La información contenida en un informe de este tipo describe debilidades de seguridad concretas y explotables. Su distribución se limita a las personas de la organización con responsabilidad directa sobre la corrección de los hallazgos y sobre la relación con el auditor de certificación. La reproducción total o parcial fuera de ese círculo requiere autorización expresa.

Índice

1 Introducción

1.1 Contexto y objetivos

Cliente Ejemplo, S.L. encarga una evaluación técnica de seguridad de su aplicación web de cliente y de la API que la sustenta, en el marco de su preparación para la certificación ISO/IEC 27001 y su adecuación al Esquema Nacional de Seguridad (ENS).

El objetivo es doble. Primero, identificar y demostrar vulnerabilidades reales que un atacante podría aprovechar contra la aplicación y sus usuarios. Segundo, aportar evidencia técnica que el auditor de certificación pueda aceptar como prueba de que la organización somete sus sistemas a pruebas de seguridad periódicas, con hallazgos, priorización y verificación de la corrección.

Un escáner automático no cubre este segundo objetivo. Detecta configuraciones débiles conocidas, pero no razona sobre la lógica de negocio ni sobre los límites de acceso entre clientes. El hallazgo principal de esta evaluación (HALL-01) es exactamente de ese tipo: ninguna herramienta automática lo habría encontrado.

1.2 Alcance acordado

Activo principal	`https://app.ejemplo-cliente.es (aplicación web + API REST /api/v1)`
Entorno	Preproducción, réplica funcional de producción, con datos sintéticos. No se ejecutó ninguna prueba contra el entorno productivo.
Tipo de prueba	Caja gris. Se facilitaron dos cuentas de cliente de distinta organización y una cuenta de usuario estándar, sin credenciales de administración.
Perspectivas	No autenticada y autenticada (cliente estándar).
Ventana de pruebas	Del 5 al 9 de mayo de 2026, en horario acordado.
Fuera de alcance	Infraestructura de red subyacente, ataques de denegación de servicio, ingeniería social y phishing, sistemas de terceros (pasarela de pago, correo).

Cualquier prueba sobre el entorno de producción se realiza únicamente bajo un contrato específico que define ventana, salvaguardas, datos afectados y responsabilidades. Por defecto se trabaja sobre preproducción con datos sintéticos.

1.3 Metodología y estándares

Las pruebas siguen la **OWASP Web Security Testing Guide (WSTG 4.2)** y el marco **PTES** (Penetration Testing Execution Standard), combinando revisión manual con apoyo de herramientas. El trabajo se organiza en reconocimiento, mapeo de la superficie, pruebas de autenticación y autorización, pruebas de lógica de negocio, y validación y encadenamiento de hallazgos.

Cada hallazgo se relaciona con los controles del **Anexo A de ISO/IEC 27001:2022** y con las medidas del **ENS (Real Decreto 311/2022)** a las que aporta evidencia. Esta correspondencia figura en la tabla de la sección 3 y en cada hallazgo. No pretende ser exhaustiva respecto a todos los controles del sistema de gestión, sino señalar los controles que esta prueba ayuda a evidenciar.

1.4 Escala de severidad

La severidad de cada hallazgo se expresa mediante una categoría cualitativa (Crítica, Alta, Media, Baja, Informativa), respaldada por una puntuación **CVSS 3.1** con su vector completo. La categoría es la que orienta la decisión de negocio; el vector aporta la trazabilidad técnica que el auditor puede revisar.

Severidad	CVSS 3.1	Interpretación
CRÍTICA	9.0 – 10.0	Compromiso directo de datos o del sistema. Corrección inmediata.
ALTA	7.0 – 8.9	Impacto grave y explotación viable. Corrección prioritaria.
MEDIA	4.0 – 6.9	Impacto apreciable o explotación condicionada. Corrección planificada.
BAJA	0.1 – 3.9	Impacto limitado. Refuerzo de defensa en profundidad.
INFORMATIVA	0.0	Observación sin impacto directo de seguridad.

2 Resumen ejecutivo

La aplicación presenta un problema grave de aislamiento entre clientes que permite a un usuario autenticado acceder a los datos de facturación de otras organizaciones. Es el hallazgo que decide esta evaluación y requiere corrección inmediata.

La evaluación identificó **seis hallazgos**: uno crítico, dos altos, dos medios y uno bajo. La mayoría se concentra en el control de acceso, es decir, en quién puede hacer qué dentro de la aplicación. Este patrón es habitual en aplicaciones que han crecido rápido: las funciones se construyen confiando en que la capa anterior ya comprobó la autorización, y nadie la comprueba.

1	2	2	1	6
CRÍTICA	ALTA	MEDIA	BAJA	TOTAL

Riesgo para el negocio

El hallazgo crítico (HALL-01) expone datos personales y económicos de clientes de la plataforma a cualquier usuario registrado. En una aplicación multicliente, esto es la peor consecuencia posible en materia de confidencialidad: rompe la frontera que separa a un cliente de otro. Además del daño reputacional, supone una brecha de datos personales con implicaciones regulatorias (RGPD).

Los dos hallazgos altos permiten, respectivamente, que un usuario normal se convierta en administrador (HALL-02) y que un cliente ejecute código en el navegador del personal de administración (HALL-03). Cualquiera de los dos convierte una cuenta de bajo privilegio en control efectivo de la plataforma.

Prioridad de corrección

- **Inmediata:** HALL-01 (aislamiento entre clientes) y HALL-02 (escalada de privilegios).
- **A corto plazo:** HALL-03 (XSS almacenado) y HALL-04 (crédito por cantidad negativa).
- **Planificada:** HALL-05 (enumeración y rate limiting) y HALL-06 (cabeceras y cookies).

Ninguno de los hallazgos exige rediseñar la aplicación. Todos se corrigen aplicando validación y comprobaciones de autorización del lado del servidor, tal y como se detalla en cada apartado. Se incluye una verificación (retest) para confirmar las correcciones antes de la auditoría.

3 Resumen de hallazgos

La siguiente tabla resume los hallazgos, su severidad y los controles a los que cada uno aporta evidencia. La columna «Estado» refleja la situación en el momento de emitir este informe.

ID	Título	Severidad	CVSS	Estado	ISO 27001:2022	ENS
HALL-01	Acceso a facturas de otros clientes (IDOR)	CRÍTICA	9.1	Abierto	A.5.15 · A.8.3	op.acc.4 · mp.info
HALL-02	Escalada de privilegios a administrador	ALTA	8.1	Abierto	A.5.15 · A.8.2	op.acc.4 · op.acc.5
HALL-03	XSS almacenado en la consola de administración	ALTA	7.6	Abierto	A.8.28 · A.8.26	mp.sw.1 · mp.s.2
HALL-04	Crédito arbitrario por cantidad negativa	MEDIA	6.5	Abierto	A.8.26 · A.8.29	mp.sw.2 · op.exp.2
HALL-05	Enumeración de cuentas y ausencia de rate limiting	MEDIA	5.3	Abierto	A.8.5	op.acc.6 · mp.s.2
HALL-06	Cabeceras de seguridad y atributos de cookie	BAJA	3.1	Abierto	A.8.9	op.exp.3 · mp.s.2

Correspondencia de controles: A.5.15 Control de acceso · A.8.2 Derechos de acceso privilegiados · A.8.3 Restricción del acceso a la información · A.8.5 Autenticación segura · A.8.9 Gestión de la configuración · A.8.26 Requisitos de seguridad de las aplicaciones · A.8.28 Codificación segura · A.8.29 Pruebas de seguridad en desarrollo y aceptación. Medidas ENS según el Real Decreto 311/2022.

4 Hallazgos detallados

HALL-01

Acceso a facturas de otros clientes (IDOR)

CRÍTICA

CVSS 3.1: 9.1
AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

RESUMEN

El endpoint `GET /api/v1/facturas/{id}` devuelve una factura a partir de su identificador numérico sin comprobar que la factura pertenece a la organización del usuario autenticado. Cualquier cliente registrado (el alta es libre) puede recorrer los identificadores y leer las facturas de las demás organizaciones de la plataforma.

IMPACTO

Ruptura del aislamiento entre clientes en una aplicación multicliente. Un usuario cualquiera accede a datos de facturación de terceros: razón social, NIF, importes, conceptos y dirección fiscal. Es una brecha de datos personales (RGPD) y la peor consecuencia posible en confidencialidad para este tipo de plataforma. La enumeración secuencial de identificadores permite extraer la base de facturación completa de forma sistemática.

PRUEBA DE CONCEPTO

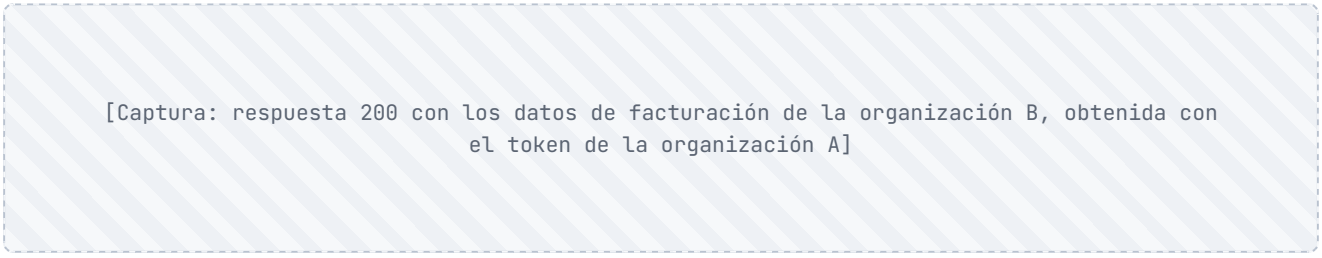
Autenticado como usuario de la organización A (cuenta de prueba `demo-a`), se solicita una factura propia y, a continuación, una factura contigua que pertenece a la organización B:

```
# Factura propia (organizacion A): esperado
GET /api/v1/facturas/1042 HTTP/1.1
Host: app.ejemplo-cliente.es
Authorization: Bearer <token-demo-a>

HTTP/1.1 200 OK
{"id":1042,"organizacion":"A","nif":"B00000001","total":1210.00, ...}

# Factura de otra organizacion: NO deberia ser accesible
GET /api/v1/facturas/1043 HTTP/1.1
Host: app.ejemplo-cliente.es
Authorization: Bearer <token-demo-a>

HTTP/1.1 200 OK
{"id":1043,"organizacion":"B","nif":"B00000002","total":3480.50,
 "cliente":"Otra Empresa, S.L.","direccion":"Calle Ejemplo 1, Madrid", ...}
```



El mismo patrón se reproduce recorriendo el rango de identificadores. La respuesta no varía según la organización propietaria: el servidor solo comprueba que el token es válido, no que el recurso pertenece a quien lo pide.

REMEDIACIÓN

Aplicar la comprobación de propiedad en el servidor, en la capa de acceso a datos, no en la interfaz. La consulta debe filtrar por la organización del token, no solo por el identificador:

```
// En lugar de: buscar por id
SELECT * FROM facturas WHERE id = :id;

// Filtrar siempre por la organización del usuario autenticado
SELECT * FROM facturas WHERE id = :id AND organizacion_id = :org_del_token;
```

- Derivar la organización del token de sesión en el servidor, nunca de un parámetro del cliente.
- Devolver 404 (no 403) ante un recurso de otra organización, para no confirmar su existencia.
- Aplicar el mismo filtro de propiedad a todos los endpoints que reciben un identificador de recurso, no solo a facturas.
- Añadir pruebas automáticas de autorización entre organizaciones al conjunto de pruebas de integración.

HALL-02

Escalada de privilegios a administrador

ALTA

CVSS 3.1: 8.1
AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

RESUMEN

El endpoint de actualización de perfil `PUT /api/v1/perfil` acepta un campo `rol` enviado por el cliente y lo aplica sin validación. Un usuario estándar puede asignarse el rol de administrador y obtener acceso a la consola de administración.

IMPACTO

Un usuario de bajo privilegio obtiene control total de la plataforma: gestión de usuarios, acceso a la configuración y a los datos de todas las organizaciones. Combinado con el alta libre de cuentas, cualquier persona en internet puede convertirse en administrador.

PRUEBA DE CONCEPTO

```
# El campo "rol" viaja en el cuerpo de la petición y se acepta tal cual
PUT /api/v1/perfil HTTP/1.1
Host: app.ejemplo-cliente.es
Authorization: Bearer <token-usuario-estandar>
Content-Type: application/json

{"nombre":"Demo","rol":"admin"}

HTTP/1.1 200 OK
{"nombre":"Demo","rol":"admin"}

# A partir de aquí, la consola de administración es accesible
GET /admin HTTP/1.1  ->  HTTP/1.1 200 OK
```

[Captura: consola de administración accesible tras modificar el rol desde una cuenta estándar]

REMEDIACIÓN

- No aceptar nunca el rol ni ningún atributo de autorización desde el cliente. El rol se asigna y se modifica solo en el servidor, mediante un flujo administrativo controlado.
- Descartar de forma explícita los campos no esperados en el cuerpo de la petición (lista de permitidos), en lugar de asignar todo el objeto recibido.
- Comprobar el rol efectivo del usuario en cada acceso a funciones de administración, del lado del servidor.

HALL-03

XSS almacenado en la consola de administración

ALTA

CVSS 3.1: 7.6
AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N

RESUMEN

El asunto de los tickets de soporte se almacena sin neutralizar y se muestra sin escapar en la cola de tickets de la consola de administración. Un cliente puede introducir código en el asunto que se ejecuta en el navegador del personal de administración cuando abre la cola.

IMPACTO

El código se ejecuta en el origen de la aplicación y en la sesión de un administrador, que es un privilegio superior al del atacante. Permite robar la sesión, actuar en nombre del administrador o encadenar con HALL-02. Al cruzar la frontera de privilegio (cliente a administrador), el alcance es «cambiado» (S:C) en el vector CVSS.

PRUEBA DE CONCEPTO

```
# Un cliente crea un ticket con código en el asunto
POST /api/v1/tickets HTTP/1.1
Host: app.ejemplo-cliente.es
Content-Type: application/json

{"asunto":"<img src=x onerror=alert(document.domain)>",
 "mensaje":"Consulta de prueba"}

# Al abrir la cola de tickets, el navegador del administrador ejecuta el código
```

[Captura: ejecución de alert(document.domain) en la consola de administración al listar los tickets]

REMEDIACIÓN

- Escapar la salida según el contexto en el momento de renderizar (codificación HTML del asunto y de cualquier dato aportado por el usuario). Es la corrección principal.
- Validar la entrada en el servidor como refuerzo, no como única defensa.
- Aplicar una política de seguridad de contenido (CSP) que limite la ejecución de scripts en línea en la consola de administración.

HALL-04

Crédito arbitrario por cantidad negativa

MEDIA

CVSS 3.1: 6.5
AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

RESUMEN

El proceso de compra acepta una cantidad negativa en una línea del carrito. El total resultante es negativo y la diferencia se aplica como crédito a la cuenta. El servidor confía en el total calculado en el cliente en lugar de recalcularlo.

IMPACTO

Fraude económico directo. Un usuario puede generarse crédito arbitrario y reducir el importe a pagar por debajo de su valor real. No compromete la confidencialidad, pero sí la integridad de los datos económicos de la plataforma.

PRUEBA DE CONCEPTO

```
# Una línea con cantidad negativa reduce el total por debajo de cero
POST /api/v1/carrito/linea HTTP/1.1
Host: app.ejemplo-cliente.es
Content-Type: application/json

{"producto":123,"cantidad":-5}

HTTP/1.1 200 OK
{"total":-245.00,"credito_aplicado":245.00}
```

[Captura: resumen del carrito con total negativo y crédito aplicado a la cuenta]

REMEDIACIÓN

- Validar en el servidor que la cantidad es un entero mayor que cero antes de procesar la línea.
- Recalcular siempre el total en el servidor a partir de precios de confianza. No aceptar totales ni importes calculados por el cliente.
- Definir invariantes de negocio (el total nunca es negativo) y registrar cualquier intento de vulnerarlas para su seguimiento.

HALL-05

MEDIA

Enumeración de cuentas y ausencia de rate limiting

CVSS 3.1: 5.3
AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

RESUMEN

El endpoint de restablecimiento de contraseña `POST /api/v1/recuperar-clave` responde de forma distinta según el correo exista o no, lo que permite enumerar cuentas válidas. Además no aplica ninguna limitación de frecuencia, por lo que la enumeración y los intentos de fuerza bruta no encuentran freno.

IMPACTO

Un atacante puede confirmar qué direcciones de correo tienen cuenta en la plataforma y usar esa lista para ataques dirigidos. Sin rate limiting, la enumeración es masiva y, si el token de restablecimiento fuera débil, facilitaría la toma de cuentas.

PRUEBA DE CONCEPTO

```
# Correo con cuenta
POST /api/v1/recuperar-clave  {"email":"existe@ejemplo.es"}
HTTP/1.1 200 OK  {"mensaje":"Te hemos enviado un correo"}

# Correo sin cuenta: la respuesta delata que no existe
POST /api/v1/recuperar-clave  {"email":"noexiste@ejemplo.es"}
HTTP/1.1 404 Not Found  {"error":"No existe una cuenta con ese correo"}

# Sin límite de frecuencia: cientos de peticiones sin bloqueo
```

REMEDIACIÓN

- Responder siempre igual, exista o no la cuenta («si el correo tiene cuenta, recibirás un mensaje»).
- Aplicar limitación de frecuencia por IP y por cuenta, y un desafío (CAPTCHA) a partir de un umbral.
- Emitir tokens de restablecimiento de alta entropía, de un solo uso y con caducidad corta.

HALL-06

BAJA

Cabeceras de seguridad y atributos de cookie

CVSS 3.1: 3.1
AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N

RESUMEN

Las respuestas de la aplicación no incluyen la cabecera `Strict-Transport-Security` ni una política de seguridad de contenido, y la cookie de sesión se emite sin el atributo `SameSite` y, en una de las rutas, sin `Secure`. Son debilidades de defensa en profundidad, sin explotación directa por sí solas.

IMPACTO

Reducen los márgenes de seguridad frente a ataques de degradación de protocolo y de falsificación de petición en escenarios concretos. No comprometen la aplicación de forma aislada, pero conviene corregirlas por higiene y porque son revisadas en las auditorías.

PRUEBA DE CONCEPTO

```
# Respuesta sin HSTS ni CSP; cookie sin SameSite
HTTP/1.1 200 OK
Set-Cookie: sesion=...; Path=/; HttpOnly
# faltan: Strict-Transport-Security, Content-Security-Policy,
#         y el atributo SameSite en la cookie de sesión
```

REMEDIACIÓN

- Añadir `Strict-Transport-Security` con una duración razonable y, valorada, la inclusión en la lista de precarga.
- Definir una política de seguridad de contenido (CSP) ajustada a la aplicación.
- Emitir la cookie de sesión con `SameSite=Lax` (o `Strict`), `Secure` y `HttpOnly` en todas las rutas.

5 Pruebas realizadas

Esta sección resume las categorías de prueba ejecutadas sobre el alcance, siguiendo la OWASP Web Security Testing Guide. Deja constancia de la cobertura: qué se revisó, con independencia de que se identificaran o no hallazgos.

Categoría (OWASP WSTG)	Estado	Resultado
Recopilación de información	Probado	Sin hallazgos
Configuración y despliegue	Probado	HALL-06
Gestión de identidades y registro	Probado	HALL-02
Autenticación	Probado	HALL-05
Autorización y control de acceso	Probado	HALL-01, HALL-02
Gestión de sesiones	Probado	HALL-06 (atributos de cookie)
Validación de entrada y salida	Probado	HALL-03
Lógica de negocio	Probado	HALL-04
Criptografía en tránsito (TLS)	Probado	Sin hallazgos
Manejo de errores	Probado	Sin hallazgos
Seguridad de la API REST	Probado	HALL-01, HALL-02, HALL-05
Cliente (client-side)	Probado	HALL-03

«Sin hallazgos» indica que la categoría se revisó y no se identificaron debilidades reportables, no que el riesgo sea nulo.

6 Observaciones positivas

No todo lo revisado presenta debilidades. Esta sección recoge los controles que se comportaron correctamente, para ofrecer una imagen equilibrada del estado de seguridad y señalar qué prácticas conviene mantener.

- **Almacenamiento de contraseñas.** Las contraseñas se guardan con una función de hash robusta y con sal. No se identificaron contraseñas en claro ni algoritmos obsoletos.
- **Cifrado en tránsito.** El servicio fuerza HTTPS con TLS 1.2 o superior y una suite de cifrado adecuada. No se detectaron protocolos ni cifrados obsoletos.
- **Ausencia de inyección SQL.** Las consultas revisadas usan sentencias parametrizadas. No se identificó inyección SQL en ningún punto del alcance.
- **Gestión de sesión en el cierre.** El cierre de sesión invalida el token en el servidor, no solo en el cliente.
- **Protección frente a CSRF.** Los formularios que modifican estado incluyen un token anti-CSRF válido y verificado en el servidor.
- **Control de los mensajes de error.** Los errores no revelan trazas internas, rutas de fichero ni versiones de componentes.

A Verificación (retest)

La corrección de los hallazgos se confirma con una verificación posterior, incluida en el alcance del trabajo. Su objetivo es que la organización llegue a la auditoría con evidencia de que las debilidades identificadas se han cerrado.

Cómo funciona

- La organización comunica los hallazgos que ha corregido y aporta acceso al mismo entorno de preproducción.
- Se reprueba cada hallazgo con el mismo procedimiento con el que se identificó, no solo la corrección declarada.
- Cada hallazgo pasa a uno de tres estados: **Corregido**, **Corregido parcialmente** (con el detalle de lo que falta) o **No corregido**.
- Se emite un anexo de verificación con la tabla de estados actualizada, que acompaña al informe original como evidencia para el auditor.

Alcance y plazos

Incluye	Reprueba de todos los hallazgos del informe, en el mismo entorno.
Plazo de entrega	3 días laborables desde el acceso al entorno corregido.
Resultado	Anexo de verificación con estados y, si procede, indicaciones sobre las correcciones incompletas.

¿Preparando una certificación ISO 27001, ENS o SOC 2?

Este es un informe de muestra. Un test sobre tu alcance real sigue esta misma estructura: hallazgos accionables, mapeo a controles y evidencia de reprueba lista para el auditor, en 10 días laborables.

Martín Martín · Seguridad ofensiva
mmartin.me · hi@mmartin.me

Reserva una llamada de scoping de 30 min →

Fin del informe de muestra. Documento demostrativo de Martín Martín (mmartin.me). Ni la organización ni los datos son reales.