AZACUS.IO
CYBERSECURITY

APLICACION WEB Y API

Informe de pentesting de ejemplo

Evidencias claras. Correcciones prácticas.

Organización de ejemplo
Northstar Workspace: plataforma B2B ficticia

Referencia del documento
AZ-SAMPLE-2026 / Versión 1.0 / 6 de noviembre de 2026

Demostración ilustrativa de la estructura y profundidad técnica de un informe. Todos los sistemas, cuentas, peticiones, hallazgos y resultados son ficticios. No corresponde a un cliente, no acredita la seguridad de ningún sistema ni demuestra una vulnerabilidad real.

01 / Resumen ejecutivo

La evaluación ficticia examinó si las cuentas de un cliente podían acceder a registros de otra empresa, si se aplicaban los roles y si la revocación del acceso detenía una sesión existente. Las pruebas se centraron en la aplicación web y su API.

Impacto de negocio

Se describen dos debilidades ilustrativas. La falta de una comprobación de autorización a nivel de empresa permite a un usuario estándar autenticado obtener la factura de otro cliente. Además, eliminar un usuario no revoca inmediatamente su token de acceso y deja una ventana limitada de acceso continuado.

Prioridades

Alta: acceso a facturas de otra empresa
Corregir la autorización en servidor antes de publicar el flujo afectado. Revisar otros endpoints de facturas y documentos por si repiten el patrón.

Media: el acceso persiste tras la baja
Aplicar la revocación a sesiones y tokens existentes. Verificar el comportamiento en navegadores, clientes móviles y llamadas API en segundo plano.

Decisión para el responsable del sistema

Priorizar la autorización de facturas y después implementar y validar la revocación. Ambas correcciones necesitan pruebas dirigidas: cerrar una tarea o revisar código no demuestra por sí solo que se impida el acceso.

Qué no demuestra este informe

El ejemplo no representa todas las funciones ni vías de ataque. Una evaluación real tiene límites de tiempo y alcance; la ausencia de hallazgos no demuestra ausencia de vulnerabilidades. Estos hallazgos ficticios no representan una intrusión real.

02 / Alcance y enfoque

Destinos ficticios
app.northstar.example y api.northstar.example. El dominio .example está reservado para documentación.

Modelo de acceso
Dos empresas cliente aisladas, con un administrador y un usuario estándar cada una, y una sesión sin autenticar. Todas las cuentas y registros son ficticios.

Incluido
Inicio y gestión de sesiones; límites entre roles y empresas; lectura de facturas; baja de usuarios y peticiones API relacionadas. Manipulación manual y pruebas de concepto controladas.

Excluido
Denegación de servicio, ingeniería social, servicios de terceros, revisión de código, administración cloud y datos reales de clientes. Un alcance real debe identificar los destinos autorizados y sus restricciones.

Enfoque de prueba

Establecer el comportamiento normal por rol. Repetir peticiones con una cuenta o identificador de otra empresa. Comparar decisiones de autorización, datos devueltos y efectos. Validar con el mínimo de registros ficticios y conservar evidencias suficientes para reproducir el resultado.

Criterio de gravedad

El ejemplo utiliza gravedad Alta y Media según el acceso demostrado, privilegios necesarios, sensibilidad y límites prácticos. No se asigna CVSS porque el alcance ficticio no permite establecer todas sus hipótesis. Una evaluación real debe explicar el contexto y la incertidumbre.

03 / Resumen de hallazgos

AZ-001 | Alta | Abierto (ilustrativo)
Acceso a facturas de otra empresa. Un usuario estándar obtiene una factura de otro cliente. Afecta a GET /v1/invoices/{id}. Categoría: autorización incorrecta a nivel de objeto.

AZ-002 | Media | Abierto (ilustrativo)
Los usuarios eliminados mantienen el acceso hasta caducar el token. Los tokens previos siguen aceptándose tras la baja. Afecta a endpoints autenticados. Categoría: revocación de sesiones y acceso.

Orden recomendado

Primero: corregir la autorización de facturas y revisar endpoints similares.
Después: revocar tokens activos tras la baja.
Por último: verificar ambas correcciones con controles positivos y negativos y registrar los límites restantes.

Interpretación de las evidencias

Todas las peticiones y respuestas son ficticias. Un informe real debe identificar rol, destino, fecha, resultado esperado y observado. Se ocultan tokens y datos personales manteniendo la evidencia mínima necesaria para reproducir el problema.

Estados de verificación

Abierto: pendiente de corregir.
Resuelto: la vía documentada ya no funciona en las condiciones verificadas.
Parcialmente resuelto: quedan vías relacionadas.
No verificado: no hay conclusión de comprobación.

04 / AZ-001

Acceso a facturas de otra empresa | Alta

Requisitos: cuenta estándar válida de A e identificador de una factura de B. Conocer un identificador basta para este ejemplo; no se demuestra enumeración masiva.

Observado: la API autentica al usuario pero devuelve la factura de otra empresa sin comprobar su propietario. La respuesta expone información de facturación ficticia.

```
GET /v1/invoices/inv_B_1042 HTTP/1.1
Host: api.northstar.example
Authorization: Bearer [ORG_A_STANDARD_USER_TOKEN]

HTTP/1.1 200 OK
Content-Type: application/json

{"id":"inv_B_1042","organisation":"org_B",
 "billing_contact":"finance@customer-b.example",
 "total":2400,"currency":"GBP"}
```

Esperado: no devolver datos; respuesta 403 o 404 coherente con la política de divulgación de recursos.

Reproducción

1. Crear una factura ficticia en B y registrar su identificador.
2. Iniciar sesión como usuario estándar de A.
3. Solicitar la factura de B con el token de A.
4. Confirmar que los datos pertenecen a B. Repetir con una factura de A como control positivo.

Impacto: divulgación no autorizada de datos de facturación de otro cliente. No se demuestra modificación, acceso completo a la base de datos ni acceso sin autenticar.

05 / Corrección de AZ-001

Corregir la decisión de autorización

Obtener el contexto de usuario y empresa de una sesión validada en servidor. Buscar la factura dentro de esa empresa y aplicar la política de rol u objeto. No confiar en un identificador de empresa facilitado por el solicitante como prueba de acceso.

```
# Logica ilustrativa del servidor
actor = require_authenticated_user(request)
invoice = find_invoice(
    id=request.path.invoice_id,
    organisation_id=actor.organisation_id
)
if invoice is None or not may_read(actor, invoice):
    deny_access()
return permitted_invoice_fields(invoice)
```

Revisar vías relacionadas

Revisar exportaciones, adjuntos, búsqueda, APIs masivas y tareas en segundo plano. Los identificadores opacos reducen las conjeturas, pero no sustituyen la autorización. Revisar registros de acceso; el hallazgo no demuestra por sí solo abuso histórico.

Criterios de aceptación

Un usuario válido de A no puede leer facturas de B por el endpoint ni por rutas equivalentes de descarga o exportación. Sí puede leer las autorizadas de A. Las peticiones sin autenticar fallan. Los administradores conservan solo el alcance permitido.

Responsable sugerido
Ingeniería de aplicación/API con el responsable de seguridad de producto.

Resultado de verificación
No realizada: informe ilustrativo. En un caso real se registran versión, fecha, cuentas, rutas y limitaciones.

06 / AZ-002

El acceso persiste tras la baja | Media

Requisitos: token sin caducar emitido antes de la baja. En este escenario ficticio, le quedan hasta 15 minutos de validez.

Observado: el administrador elimina al usuario, pero sus tokens siguen leyendo datos hasta caducar. Se bloquean nuevos inicios de sesión. El acceso conserva los permisos anteriores; no se demuestra elevación de privilegios.

```
10:00  Inicio de sesion; token caduca a las 10:15.
10:02  Administrador elimina al usuario.
10:03  Usuario solicita GET /v1/projects.
       API devuelve 200 con datos de proyectos.
10:16  Token rechazado tras caducar.
```

Impacto: la baja no surte efecto inmediato en sesiones activas. Importa ante cuentas comprometidas o personal sin autorización. La gravedad refleja la duración limitada y la necesidad de un token válido previo.

Corrección

Invalidar sesiones y tokens de renovación al eliminar la pertenencia. Las peticiones protegidas deben comprobar la pertenencia actual o una versión de revocación/sesión controlada por servidor. Reducir la vida del token limita la exposición, pero no revoca inmediatamente.

Criterios de verificación

Capturar un token válido, eliminar al usuario y repetir peticiones inmediatamente y durante la antigua ventana de validez. Deben rechazarse sin datos. Comprobar renovación, sesiones paralelas y reincorporación. Mantener un usuario autorizado como control positivo.

07 / Entrega y control documental

Seguimiento de correcciones

AZ-001 | Ingeniería de aplicación/API
Aplicar acceso por objeto vinculado a empresa y revisar rutas relacionadas. Estado: ilustrativo / no verificado.

AZ-002 | Ingeniería de identidad/API
Invalidar acceso tras la baja y comprobar sesiones simultáneas. Estado: ilustrativo / no verificado.

Una entrega real incluye

Resumen ejecutivo, alcance y límites confirmados, hallazgos técnicos reproducibles, justificación del riesgo, correcciones prácticas y un canal para aclaraciones. Alcance, fechas y condiciones comerciales de verificación se acuerdan en la propuesta.

Control documental

Versión 1.0 | 6 de noviembre de 2026
Ejemplo público para demostrar el estilo de informes de Azacus.io. Sin información de clientes ni resultados reales de proyectos.

Distribución
Ejemplo público. Los informes reales se entregan por el canal confidencial acordado.

Hablemos de tu evaluación

Azacus.io
ping [at] azacus.io
https://azacus.io

Pentesting sénior de aplicaciones, APIs e infraestructura.