

Informe de pentesting

Nimbus Commerce | Demostración ficticia completa

Cliente
Nimbus Commerce (organización ficticia)

Evaluador
Sebastián Latorre Muñoz / iphobiuss · Muestra de report-gen

Fecha
2026-10-02

Versión
1.0

Tabla de contenidos

1. Naturaleza del documento y uso de la muestra	3
2. Control del documento	4
3. Resumen ejecutivo	5
4. Criterios de severidad, prioridad y riesgo residual	6
5. Alcance y objetivos	7
6. Enfoque y metodología	8
7. Resumen de hallazgos	9
8. Hallazgos	10
9. Cadenas de impacto y fronteras de confianza	28
10. Plan de remediación	29
11. Apéndices técnicos y referencias	31
12. Activos evaluados	33
13. Cobertura y limitaciones	34
14. Seguimiento de correcciones y retest	36

1 Naturaleza del documento y uso de la muestra

INFORME FICTICIO DE DEMOSTRACIÓN. Nimbus Commerce es una organización inventada para mostrar las capacidades de report-gen y una forma de documentar una evaluación de seguridad. No es un cliente, una auditoría realizada, una certificación ni un informe de incidente real.

Los hallazgos, activos, personas, fechas de trabajo, evidencias y resultados de retest forman parte de un escenario editorial. Las imágenes técnicas son representaciones sintéticas identificadas como tales. No son capturas de sistemas comprometidos. Las frases que describen acciones o resultados se interpretan dentro de ese escenario.

Qué es verificable en esta entrega

El proyecto estructurado se procesa con report-gen 0.21.2. Las puntuaciones se calculan a partir de los vectores declarados; el informe conserva referencias entre hallazgos, activos y evidencias. El paquete editable permite revisar los campos y volver a exportar el documento con la herramienta. La reproducción del informe no equivale a reproducir un ataque.

Finalidad y límites de publicación

Esta muestra se prepara para el portafolio de Sebastián Latorre Muñoz, iphobiuss, con redacción asistida por IA. Puede presentarse como demostración de la herramienta y de estructura de reportería, manteniendo esta identificación. No debe presentarse como experiencia con un cliente ni como prueba de que las acciones descritas fueron ejecutadas por el titular del portafolio.

Los nombres terminados en `.example`, los identificadores DEMO y los marcadores de credenciales se usan como datos de ejemplo. Ningún secreto del documento es operativo. Las referencias externas corresponden a documentación técnica pública; sus autores no avalan este caso ficticio.

Cómo leerlo

Dirección puede empezar por el resumen ejecutivo, la postura de riesgo y el plan de remediación. Los equipos técnicos encontrarán causa raíz, límites, controles de comparación y criterios de cierre en cada hallazgo. La parte final conserva el inventario, la cobertura del guion y el seguimiento de correcciones.

Fecha de preparación: 2 de octubre de 2026. Versión editorial: 1.0. Clasificación: muestra pública ficticia.

2 Control del documento

Historial de versiones

Versión	Fecha	Autor	Notas
0.1	2026-10-02	Preparación asistida	Definición del escenario, doce hallazgos y activos sintéticos.
0.2	2026-10-02	Preparación asistida	Evidencias didácticas, matriz de cobertura y seis retests ficticios.
1.0	2026-10-02	Generación con report-gen	Edición completa para revisión y publicación como muestra.

Distribución

Fechas del escenario

La ventana ficticia de evaluación es del 21 al 25 de septiembre de 2026. Los retests se sitúan el 30 de septiembre y las fechas objetivo de corrección parten del 2 de octubre. Son fechas narrativas; no acreditan actividad profesional realizada durante ese periodo.

Responsabilidad y procedencia

Elemento	Procedencia y alcance
Organización y activos	Inventados para este documento.
Descripciones y resultados	Escenario didáctico redactado con asistencia de IA.
Imágenes de evidencia	Representaciones sintéticas de controles y resultados.
PDF y proyecto	Generados y validados con report-gen 0.21.2.
Recomendaciones	Análisis del escenario y documentación pública citada.
Aceptación del portafolio	Corresponde al titular antes de publicar la muestra.

Distribución prevista

Lectura pública como ejemplo de informe. Dentro del escenario, los destinatarios serían dirección técnica, responsables de producto, identidad, infraestructura y DevOps. Se usan funciones en lugar de nombres o correos de personas reales.

Los IDs F01 a F12 se mantienen estables aunque cambie el orden de presentación. Una corrección comunicada no se transforma en cierre hasta que exista un retest representado con resultado concluyente. No se incluyen firmas de aceptación ni aprobaciones de personas ficticias.

3 Resumen ejecutivo

Nimbus Commerce representa una plataforma de pedidos con dos organizaciones clientes, servicios de integración y una infraestructura Windows de apoyo. El escenario examina cómo fallos en autorización, recuperación de cuentas, manejo de secretos y delegación de privilegios podrían afectar a los datos y a la operación.

La evaluación ficticia contiene **12 hallazgos iniciales: 2 críticos, 5 altos, 4 medios y 1 bajo**. El riesgo más urgente se concentra en dos rutas públicas hacia datos o cuentas y en una delegación de replicación del dominio. El gráfico del resumen conserva las severidades iniciales; no representa el número de problemas que siguen abiertos tras el retest.

Decisiones que requiere el escenario

1. Contener la búsqueda vulnerable y la recuperación de cuentas hasta verificar sus correcciones. Los retests RT01 y RT02 representan el cierre posterior de esas dos rutas.
2. Priorizar F07, derechos de replicación, aunque su puntuación técnica sea alta y no crítica. Su alcance transversal justifica una prioridad operativa P0.
3. Completar F03 y F05: la autorización de lectura y el bloqueo directo de destinos mejoran, pero quedan rutas alternativas de escritura y redirección.
4. Rotar la credencial de CI y revisar las delegaciones de grupos sin considerar suficiente una limpieza superficial o un aviso de despliegue.

Estado al cierre editorial

Se representan **4 hallazgos corregidos y verificados, 5 en corrección, 1 con corrección comunicada y 2 abiertos**. Se incluyen seis retests ficticios: cuatro completos y dos parciales. Ocho hallazgos, por tanto, carecen todavía de cierre verificado dentro del escenario.

Las consecuencias se explican por activos y permisos. El informe evita convertir una lectura de archivo en ejecución remota, una administración local en compromiso probado del dominio o un encabezado CORS en explotación universal. Donde el impacto depende de una condición, esa condición se declara.

Orientación para dirección

La primera inversión se dirige a fronteras de identidad y permisos: autorización por objeto, recuperación de cuentas y privilegios de servicio. Después se consolida un proceso de entrega que conserve controles de regresión y evidencia de cierre. No se calculan pérdidas monetarias, probabilidad estadística de ataque ni retorno de inversión porque el caso no aporta datos para sostener esas cifras.

Todos los resultados de esta sección son ficticios. Su finalidad es mostrar cómo un informe conecta evidencia, impacto, prioridad y seguimiento.

4 Criterios de severidad, prioridad y riesgo residual

Severidad técnica

Se utiliza **CVSS 3.1 Base** de manera uniforme para que los doce vectores sean comparables dentro de la muestra. Cada puntuación se calcula con report-gen y se acompaña de su vector. No se mezclan puntuaciones 3.1 y 4.0 ni se presentan las métricas Base como un cálculo de riesgo de negocio.

Banda	Intervalo
Crítica	9,0 a 10,0
Alta	7,0 a 8,9
Media	4,0 a 6,9
Baja	0,1 a 3,9
Informativa	0,0

CVSS pertenece a FIRST y se utiliza conforme a su documentación pública. Referencias: <https://www.first.org/cvss/v3.1/specification-document> y <https://www.first.org/cvss/v3.1/user-guide>. Los valores reflejan las condiciones inventadas del caso y requerirían una nueva valoración en un entorno real.

Prioridad operativa del escenario

Prioridad	Criterio y respuesta propuesta
P0	Acceso amplio a datos o identidad transversal. Contención y coordinación inmediata.
P1	Cruce de permisos o privilegios con condiciones identificadas. Corrección prioritaria y retest dirigido.
P2	Exposición condicionada por sesión, interacción o configuración. Corrección planificada y regresión.
P3	Divulgación limitada con privilegios previos altos. Incorporación al ciclo de endurecimiento.

Estos plazos son una propuesta de trabajo ficticia, no un SLA contractual. F07 ejemplifica la diferencia: obtiene 8,8 por sus requisitos técnicos y recibe P0 por afectar al dominio. F12 queda en P3 porque expone datos internos limitados a un rol ya privilegiado.

Riesgo residual y criterio de cierre

La severidad inicial se conserva después de corregir para mantener trazabilidad. El estado de seguimiento indica si la ruta sigue abierta. Un parche anunciado, una respuesta HTTP distinta o una regla que bloquea un único ejemplo no bastan para cerrar el hallazgo.

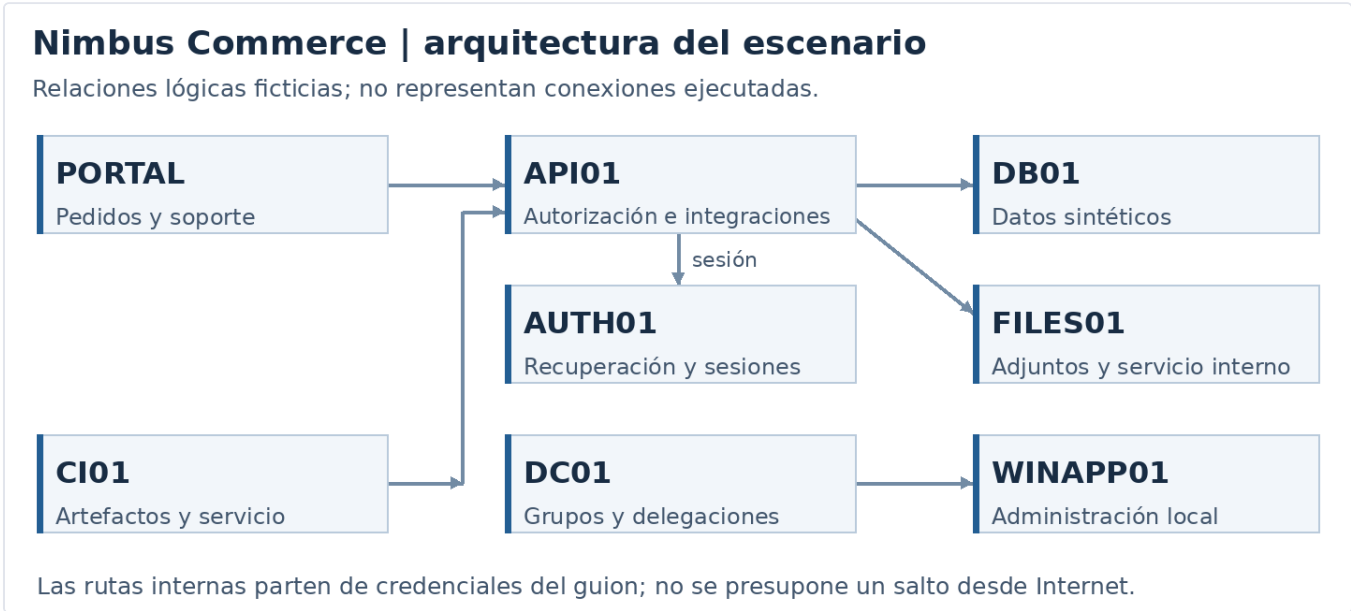
En este documento se exige un control negativo, un control legítimo que siga funcionando y una explicación del alcance probado. Un retest parcial mantiene el hallazgo en corrección. La aceptación de un riesgo, si existiera, necesitaría responsable, justificación, vencimiento y controles compensatorios; no se inventa ninguna aceptación en esta muestra.

5 Alcance y objetivos

Objetivos

Objetivo del escenario

Evaluar cómo una persona sin sesión, una cuenta de cliente o una identidad operativa podrían superar las fronteras de datos y administración. El caso conecta entrada, permiso efectivo, resultado y corrección.



Arquitectura ficticia de Nimbus: portal, API, identidad, datos, archivos e infraestructura.

El inventario final amplía estas relaciones con las funciones y los vínculos a hallazgos.

Supuestos y limitaciones

El guion combina caja gris web/API y revisión interna con dos organizaciones canario. Las comprobaciones de AD parten de credenciales proporcionadas; no se deduce una entrada desde Internet al dominio.

Quedan fuera terceros, producción, datos personales, phishing, carga, persistencia y operaciones destructivas. Nimbus es ficticia y este documento no autoriza pruebas sobre ningún servicio. Una ejecución real exigiría alcance, ventanas, contactos y reglas de enfrentamiento acordados por escrito.

Alcance

Objetivo	Descripción
<code>portal.nimbus.example</code>	Aplicación web y soporte de dos organizaciones sintéticas.
<code>api.nimbus.example</code>	Pedidos, adjuntos y vista previa de integraciones.
<code>auth.nimbus.example</code>	Recuperación de cuentas y ciclo de sesiones.
<code>ci.nimbus.example</code>	Contenido de artefactos e identidad de servicio.
<code>ad.nimbus.example</code>	Delegaciones de DC01 y administración de WINAPP01.

6 Enfoque y metodología

Enfoque

El caso sigue una secuencia de hipótesis, control positivo, variación mínima, comprobación independiente y cierre. Cada hallazgo delimita qué demostraría su evidencia y qué no. Cuando la observación puede tener otra explicación, se añade una comparación: otra identidad, otro objeto, una sesión nueva o un destino de control.

La revisión de configuración y la comprobación de comportamiento se distinguen. Ver un permiso peligroso puede sostener una condición de riesgo; la capacidad atribuida debe contrastarse con la semántica del permiso y las condiciones del escenario. Un resultado aislado de un escáner no se presenta como prueba concluyente.

Estándares y marcos (OWASP, PTES, MITRE ATT&CK)

Se consultan las guías de OWASP para autorización, consultas parametrizadas, recuperación de cuentas, SSRF, sesiones, XSS y gestión de secretos. CWE se usa para clasificar la causa técnica. La documentación de Microsoft ayuda a interpretar las delegaciones de Active Directory y FIRST define la puntuación CVSS.

Estas referencias orientan el análisis; no se afirma cumplimiento integral de OWASP ASVS, ISO 27001, PCI DSS ni otra certificación. Las fuentes específicas aparecen en cada hallazgo y se reúnen en el apéndice.

Recopilación de información

El inventario aporta ocho activos ficticios, responsables funcionales, roles y fronteras de confianza. Antes de variar una entrada se establece la identidad efectiva y el objeto canario. Se conservan identificadores de petición de demostración para vincular el control con su resultado, sin introducir datos de personas reales.

Explotación

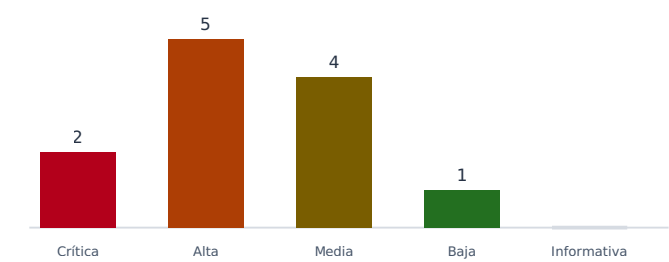
Las evidencias son diagramas de resultados sintéticos, no capturas de ataques. En un ejercicio equivalente, las validaciones descritas se limitarían a objetos canario y cambios reversibles. En este documento no se ejecutan esas acciones. Las métricas de impacto modelan capacidades concretas; las no sustentadas se excluyen o se señalan como consecuencias potenciales.

Limpieza

Cada modificación canario del relato incluye restauración o revocación como parte del criterio de cierre: notas de pedidos, contraseñas, sesiones, membresías y etiquetas de trabajos. Esa limpieza es también ficticia. La preparación real del informe solo crea archivos de proyecto y exportaciones en el entorno de trabajo.

7 Resumen de hallazgos

La evaluación identificó 12 hallazgos con la siguiente clasificación de severidad: 2 crítica, 5 alta, 4 media, 1 baja.



#	Severidad	Hallazgo	Pág.
1	Crítica (9.1)	Inyección SQL en el buscador de pedidos	10
2	Crítica (9.1)	Recuperación de contraseña sin vínculo entre token y cuenta	11
3	Alta (8.1)	Acceso y modificación de pedidos de otra organización	13
4	Alta (7.1)	SSRF en la vista previa de integraciones	16
5	Alta (8.1)	Credencial de servicio publicada en un artefacto de CI	17
6	Alta (8.8)	Derechos de replicación del dominio asignados a una cuenta operativa	19
7	Alta (8.8)	Delegación de membresía sobre un grupo administrador de servidores	20
8	Media (6.5)	Lectura fuera del directorio permitido de adjuntos	14
9	Media (5.4)	XSS almacenado en comentarios del portal de soporte	22
10	Media (6.5)	CORS con credenciales para orígenes no autorizados	23
11	Media (5.4)	Sesión reutilizable después del cierre de sesión	25
12	Baja (2.7)	Diagnósticos internos expuestos en el panel de soporte	26

8 Hallazgos

F01 Inyección SQL en el buscador de pedidos		Crítica 9.1
CWE	CWE-89	
CVSS 3.1	9.1 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	
Descripción (incl. causa raíz)	El buscador público construye una condición SQL concatenando el parámetro <code>q</code> . La cuenta de servicio comparte permisos de lectura y actualización con el módulo de pedidos. En el escenario, una entrada controlada altera la consulta y permite acceder a registros de prueba ajenos al resultado esperado.	
Impacto de seguridad	El modelo contempla lectura y modificación de datos de pedidos sin autenticación. La evidencia didáctica muestra dos registros canario y una actualización reversible en una copia aislada. No se atribuye impacto de disponibilidad ni compromiso del sistema operativo.	
Dominio afectado	portal.nimbus.example; db.nimbus.example	
Remediación	Separar código y datos mediante consultas parametrizadas; usar una cuenta de solo lectura para búsquedas. Aplicar autorización antes de devolver pedidos y conservar pruebas de regresión. Escapar comillas o filtrar palabras SQL no sustituye estas medidas.	
Referencias	- https://cwe.mitre.org/data/definitions/89.html - https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html	

Procedimiento detallado

- Contexto y precondiciones.** El flujo público permite consultar el estado de un envío con una referencia. Se dispone de una copia de datos sintéticos con los pedidos DEMO-1001 y DEMO-1002. El caso se limita a esa copia; no plantea una extracción masiva ni acceso a información de personas.
- Establecer la respuesta de referencia.** Consultar DEMO-1001 y guardar el identificador de petición, el código HTTP y los campos devueltos. Repetir con una referencia inexistente. El primer control devuelve un registro y el segundo ninguno; esta pareja permite separar el comportamiento normal de un fallo de caché.
- Comparar dos condiciones controladas.** En la representación E01 se contrasta una condición verdadera con una falsa. El resultado cambia con la condición SQL y no solamente con el texto visible del buscador. El registro canario del segundo pedido muestra el cruce de la frontera de datos. Las entradas concretas del ensayo se conservan como casos de regresión, sin automatizar enumeraciones.

E01 Cambio de condición y registro canario		CASO FICTICIO
GET /search?q=DEMO-1001	-> 200; filas: 1	
Control booleano verdadero	-> 200; filas: 2	
Control booleano falso	-> 200; filas: 0	
Canario adicional	-> DEMO-1002	
Cambio reversible	-> demo_note: CHECK-F01	
Restauración del dato	-> valor original	
La condición controla la consulta; la prueba se limita a datos canario.		

Figura 1. E01. Evidencia sintética: La condición controla la consulta; la prueba se limita a datos canario. No es una captura de una prueba ejecutada.

4. **Acotar la capacidad de modificación.** El guion de la demostración incluye la modificación reversible del campo interno demo_note en DEMO-1002 sobre la copia aislada. El acceso de escritura se atribuye a los permisos de la cuenta de base de datos, no a una supuesta ejecución de comandos. La operación vuelve a su valor inicial al finalizar.
5. **Interpretar la evidencia y la puntuación.** AV:N y PR:N corresponden al punto de entrada público; AC:L y UI:N reflejan una petición directa. C:H e I:H describen las capacidades modeladas sobre la base de pedidos. A:N evita puntuar una interrupción no representada. Este vector es una valoración del escenario, no una medición de una empresa real.
6. **Activos afectados**
 - portal.nimbus.example
 - db.nimbus.example

Resumen de remediación

Corto plazo

Contener el endpoint de búsqueda y separar sus permisos de escritura. Antes de reabrirlo, conservar los registros técnicos necesarios para investigar solicitudes anómalas, sin almacenar credenciales ni cuerpos completos de pedidos.

Mediano plazo

Reescribir la consulta con parámetros y comprobar todos los filtros dinámicos, incluidos orden y paginación. La prueba negativa debe incluir comillas, expresiones booleanas y referencias de otro cliente. Los resultados normales deben mantenerse para no introducir una regresión funcional.

Largo plazo

Incorporar revisión de acceso a datos en cambios del ORM y de SQL manual. Cerrar el ticket solo si las consultas canario dejan de ampliar resultados, no se aceptan modificaciones desde búsqueda y los controles de autorización siguen funcionando.

F02 Recuperación de contraseña sin vínculo entre token y cuenta		Crítica 9.1
CWE	CWE-640	
CVSS 3.1	9.1 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	
Descripción (incl. causa raíz)	La API comprueba que un token de recuperación exista y no haya expirado, pero utiliza el identificador de cuenta enviado en el cuerpo para seleccionar qué contraseña cambia. Falta comprobar que ambos valores pertenecen a la misma solicitud de recuperación.	
Impacto de seguridad	En el escenario, un token emitido para una cuenta controlada permite cambiar la contraseña de otra cuenta canario, incluida una cuenta administrativa sin segundo factor. Se modela acceso a datos y operaciones del portal; no se presupone acceso a Active Directory.	
Dominio afectado	portal.nimbus.example; auth.nimbus.example	
Remediación	Resolver la cuenta exclusivamente desde el registro de recuperación del servidor. Vincular token, propósito, cuenta y caducidad; consumirlo una sola vez. Invalidar las sesiones afectadas y exigir controles adicionales en la recuperación de cuentas privilegiadas.	
Referencias	• https://cwe.mitre.org/data/definitions/640.html • https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html	

Procedimiento detallado

- 1. Contexto y precondiciones.** Se utilizan las identidades ficticias usuario.a y admin.demo. Ambas pertenecen al escenario y sus buzones son sintéticos. El flujo público de recuperación emite un token para usuario.a; no se necesita una sesión autenticada para enviar la solicitud final.
- 2. Preparar un control legítimo.** Solicitar recuperación para usuario.a y comprobar que el token permite modificar únicamente esa identidad. Registrar su fecha de expiración y propósito. La mera existencia de un token válido no concede autorización para elegir una cuenta distinta.
- 3. Variar solamente la cuenta objetivo.** Mantener el mismo token canario y reemplazar account_id por la identidad administrativa de demostración. E02 representa una respuesta de éxito y el posterior inicio de sesión con la contraseña de prueba. Un 200 aislado no bastaría: el cambio de identidad se acredita con el resultado posterior dentro del guion.

E02 Token válido, identidad incorrecta	CASO FICTICIO
Token emitido para	-> usuario.a
Cuenta enviada al confirmar	-> admin.demo
Respuesta de confirmación	-> 200; password_changed
Sesión posterior	-> subject: admin.demo
Rol de la sesión canario	-> administrator
Limpieza del escenario	-> contraseña y sesiones restauradas
El servidor acepta que el cliente elija una identidad distinta de la del token.	

Figura 2. E02. Evidencia sintética: El servidor acepta que el cliente elija una identidad distinta de la del token. No es una captura de una prueba ejecutada.

- 4. Descartar un cambio aparente.** Comparar el identificador de la sesión nueva, el rol efectivo y una operación canario de administración. Restituir la contraseña inicial y revocar las sesiones del ejercicio. Las contraseñas y tokens se muestran como etiquetas ficticias, no como secretos utilizables.
- 5. Fijar los límites.** C:H e I:H se apoyan en el rol administrativo modelado; A:N evita asumir capacidad de interrupción. Si una instalación real impusiera MFA resistente a la recuperación, la cadena y la valoración requerirían revisión. El problema es el vínculo de identidad, no la longitud del token.
- 6. Activos afectados**
 - portal.nimbus.example
 - auth.nimbus.example

Resumen de remediación

Corto plazo

Restringir la recuperación de cuentas privilegiadas y revisar los registros de cambios de contraseña. Aplicar un control servidor que compare la identidad del token antes de escribir cualquier cambio, sin informar si la cuenta objetivo existe.

Mediano plazo

Eliminar account_id del contrato de confirmación, o rechazar cualquier discrepancia si debe mantenerse por compatibilidad. Probar token caducado, reutilizado, de otra cuenta y de otro propósito. La invalidación debe ser atómica para evitar consumos simultáneos.

Largo plazo

Documentar el ciclo completo de recuperación y sus controles de MFA y sesiones. Una prueba automatizada con dos identidades debe fallar si un token modifica la cuenta equivocada. Registrar el evento con identificadores, nunca el token íntegro.

F03 Acceso y modificación de pedidos de otra organización

Alta 8.1

CWE	CWE-639
CVSS 3.1	8.1 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Descripción (incl. causa raíz)	GET y PATCH de pedidos validan la sesión, pero buscan el objeto por su identificador global sin filtrar por organización. Un miembro de demo-a puede leer y modificar un pedido de demo-b conociendo su identificador.
Impacto de seguridad	Se modela exposición de pedidos y modificación de sus datos de entrega entre organizaciones. La modificación canario afecta solo a una nota de entrega reversible. No se afirma acceso a tarjetas de pago, ejecución de órdenes bancarias ni compromiso del proveedor de pagos.
Dominio afectado	api.nimbus.example
Remediación	Aplicar autorización por objeto en lectura y escritura, usando la organización y el rol resueltos desde la sesión del servidor. Reutilizar la misma política en exportaciones, procesos por lotes y endpoints heredados. Un UUID difícil de adivinar no reemplaza ese control.
Referencias	- https://cwe.mitre.org/data/definitions/639.html - https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/

Procedimiento detallado

- Contexto y precondiciones.** Hay dos organizaciones ficticias, demo-a y demo-b, con dos cuentas de usuario distintas y pedidos propios. La sesión A permanece idéntica durante los controles. Los identificadores se obtienen del conjunto de prueba autorizado; no se utiliza fuerza bruta.
- Confirmar separación de identidades.** Guardar el subject y tenant de cada sesión. Comprobar primero que A accede a su pedido y B al suyo. Evitar reutilizar cookies de la cuenta B al comprobar el acceso cruzado, porque eso produciría una falsa conclusión de BOLA.
- Probar lectura y escritura por separado.** Con la sesión A, pedir el objeto de B y después cambiar su campo delivery_note. La lectura y la modificación son comprobaciones diferentes. E03 representa ambos resultados y la lectura de control con B que confirma el cambio canario.

E03 Matriz de autorización entre organizaciones	CASO FICTICIO
Sesión A -> pedido A / GET	: 200, correcto
Sesión A -> pedido B / GET	: 200, indebido
Sesión A -> pedido B / PATCH	: 200, indebido
Sesión B -> pedido B / GET	: nota CHECK-F03
Objeto canario	: DEMO-B-2001
Cambio al terminar	: restaurado
La identidad está autenticada, pero el objeto no está autorizado para ella.	

Figura 3. E03. Evidencia sintética: La identidad está autenticada, pero el objeto no está autorizado para ella. No es una captura de una prueba ejecutada.

- Comprobar rutas alternativas.** Repetir la matriz en el endpoint de exportación y en el PATCH del recurso. El retest ficticio muestra una corrección parcial: GET aplica la política, pero PATCH sigue permitiendo la escritura cruzada. El ticket permanece abierto aunque una de las rutas ya esté corregida.

5. Interpretar el resultado. La autenticación de A funciona; falla la autorización sobre el objeto. PR:L refleja ese acceso de usuario. C:H e I:H describen el alcance entre organizaciones modelado, y A:N no incorpora denegación de servicio. Deben revisarse también IDs anidados y operaciones por lotes.

6. Activos afectados

- api.nimbus.example

Resumen de remediación

Corto plazo

Deshabilitar las rutas cruzadas identificadas y revisar accesos por tenant. Evitar una respuesta que revele atributos del objeto rechazado. Mantener una forma controlada de atender pedidos legítimos mientras se despliega el cambio.

Mediano plazo

Introducir un punto común de decisión de autorización con tenant, rol, objeto y operación. Añadir una matriz positiva y negativa de dos organizaciones a GET, PATCH, exportación y procesos por lotes. Revisar que tenant_id no pueda sobrescribirse desde el cuerpo del cliente.

Largo plazo

Cerrar solo después de que todas las operaciones cruzadas fallen y las legítimas sigan funcionando. El cambio debe incluir comprobaciones de concurrencia si existe una transferencia de pedido entre organizaciones, y controles de caché que respeten esa separación.

F04

Lectura fuera del directorio permitido de adjuntos

Media 6.5

CWE	CWE-22
CVSS 3.1	6.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Descripción (incl. causa raíz)	La descarga de adjuntos concatena una ruta suministrada por el usuario con la carpeta de almacenamiento. No comprueba que la ruta normalizada permanezca dentro del directorio autorizado ni que el fichero pertenezca al pedido.
Impacto de seguridad	El escenario permite leer un archivo canario fuera de la carpeta de adjuntos. El proceso tiene acceso de lectura a configuraciones internas del servicio. Se modela impacto de confidencialidad; no se representan escritura de archivos, ejecución de código ni acceso ilimitado al host.
Dominio afectado	api.nimbus.example; files.nimbus.example
Remediación	Recibir un identificador de adjunto y resolver su ubicación en el servidor después de autorizar el objeto. Si se manejan rutas, normalizarlas y verificar su pertenencia real al directorio permitido, considerando enlaces simbólicos. Reducir los permisos del proceso.
Referencias	• https://cwe.mitre.org/data/definitions/22.html

Procedimiento detallado

- 1. Contexto y precondiciones.** El servicio FILES01 contiene una carpeta attachments y otra fixtures con un canario llamado outside-marker.txt. Ambos son recursos ficticios. La prueba cruza esa frontera controlada; no depende de leer archivos reales del sistema ni secretos.
- 2. Establecer un adjunto legítimo.** Descargar un documento de la propia organización y registrar su tipo, tamaño y asociación al pedido. Comparar con un identificador inexistente y uno de otro tenant. La validación de ruta y la autorización de objeto son controles complementarios.

3. **Representar el escape de directorio.** E04 contrasta una descarga normal con una ruta que alcanza el archivo canario situado fuera de attachments. Se comparan contenidos, no solo códigos HTTP. La presencia exacta del marcador F04-OUTSIDE diferencia la lectura indebida de una página de error.

E04 Comprobación del directorio de descarga	CASO FICTICIO
Directorio permitido -> /srv/nimbus/attachments	
Archivo de control -> /srv/nimbus/fixtures/outside-marker.txt	
Descarga legítima -> 200; PDF de demostración	
Escape representado -> 200; F04-OUTSIDE	
Enlace a fixtures -> 200; F04-OUTSIDE	
Capacidad modelada -> lectura; sin escritura	
El marcador procede de un recurso exterior al directorio autorizado.	

Figura 4. E04. Evidencia sintética: El marcador procede de un recurso exterior al directorio autorizado. No es una captura de una prueba ejecutada.

4. **Cubrir normalización y enlaces.** El guion contempla segmentos relativos y un enlace simbólico dentro de attachments que apunta a fixtures. Una comprobación puramente textual del prefijo no demuestra contención. Debe validarse el destino efectivo y evitar cambios concurrentes del enlace durante la apertura.
5. **Mantener el alcance de la conclusión.** C:H se basa en la lectura de configuraciones que el modelo concede al proceso; I:N y A:N no atribuyen otras capacidades. En una evaluación real se ajustarían las métricas al conjunto de archivos realmente accesible. El canario prueba la frontera, no la exposición de todos los discos.
6. **Activos afectados**
- api.nimbus.example
 - files.nimbus.example

Resumen de remediación

Corto plazo

Restringir el endpoint y revisar los permisos de lectura del servicio. Sustituir las rutas expuestas por identificadores internos. Conservar un canario de pruebas separado de configuraciones y credenciales para las verificaciones posteriores.

Mediano plazo

Centralizar la resolución de adjuntos y la política de pertenencia al pedido. Probar traversal, enlaces simbólicos, nombres codificados, fichero inexistente y adjunto de otro tenant. La corrección debe rechazar el acceso sin revelar la ruta absoluta en el error.

Largo plazo

Incorporar pruebas de aislamiento del almacenamiento a las actualizaciones del framework y a las migraciones de volumen. Verificar que una descarga normal no cambie y que el usuario del servicio no pueda leer material de otros componentes.

F05 SSRF en la vista previa de integraciones

Alta 7.1

CWE	CWE-918
CVSS 3.1	7.1 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
Descripción (incl. causa raíz)	La función de vista previa solicita una URL indicada por el usuario y devuelve la respuesta. Permite seleccionar método y cuerpo, y sigue redirecciones sin aplicar una política de destino en cada salto. El servicio alcanza una interfaz interna que confía en la red de origen.
Impacto de seguridad	El escenario representa lectura de configuraciones y cambios limitados en un trabajo canario del servicio interno de documentos. No se modela acceso a metadata de un proveedor cloud, obtención de credenciales reales ni ejecución de comandos.
Dominio afectado	api.nimbus.example; files.nimbus.example
Remediación	Sustituir URLs arbitrarias por integraciones predefinidas. Limitar destinos, puertos y métodos, validar la resolución y cada redirección, y aplicar controles de salida de red. Exigir autenticación y autorización propias en la interfaz interna.
Referencias	- https://cwe.mitre.org/data/definitions/918.html - https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

Procedimiento detallado

- Contexto y precondiciones.** La cuenta de integración tiene permisos bajos en la API. La prueba utiliza un receptor canario y un servicio interno ficticio de documentos. Se conocen ambos destinos por el inventario del ejercicio; no se realizan barridos de puertos ni descubrimiento de direcciones ajenas.
- Observar una integración autorizada.** Enviar una URL del receptor canario y comparar el identificador de correlación que recibe con el de la API. El escenario distingue una conexión realizada por el servidor de una petición del navegador. La respuesta visible debe corresponder al mismo identificador.
- Comprobar una frontera interna.** Pedir a la vista previa el recurso canario interno. E05 representa que la API devuelve información de configuración reservada para la red de servicios. El impacto de integridad se limita a cambiar una etiqueta del trabajo DEMO-JOB-05, operación reversible incluida en el modelo.

E05 Destino inicial y destino efectivo	CASO FICTICIO
Origen de la petición	-> servicio de vista previa
Destino autorizado	-> receptor.canario.nimbus.example
Destino interno	-> files.nimbus.example/internal/demo
Respuesta interna	-> configuración canario visible
Operación limitada	-> etiqueta DEMO-JOB-05 modificable
Redirección	-> conserva acceso al destino interno
La confianza en la red interna amplía el alcance de una entrada controlada.	

Figura 5. E05. Evidencia sintética: La confianza en la red interna amplía el alcance de una entrada controlada. No es una captura de una prueba ejecutada.

- Evaluar redirecciones.** El retest ficticio añade un bloqueo de destinos internos directos, pero mantiene redirecciones a ese mismo destino. Esta diferencia explica por qué el hallazgo sigue abierto. Un filtro del primer hostname no protege las resoluciones y destinos efectivos posteriores.

5. Evitar conclusiones excesivas. No se afirma que una SSRF permita alcanzar cualquier red o tomar el control de un host. PR:L refleja la cuenta requerida; C:H e I:L son las capacidades concretas del servicio de documentos representado. La disponibilidad no se prueba ni se puntúa.
6. Activos afectados
 - api.nimbus.example
 - files.nimbus.example

Resumen de remediación

Corto plazo

Desactivar destinos arbitrarios y restringir la salida de red del proceso. Proteger la interfaz interna con identidad de servicio. Mantener únicamente las integraciones necesarias con un contrato explícito de método, ruta y formato de respuesta.

Mediano plazo

Aplicar una política sobre el destino resuelto y cada salto de redirección. Probar IPv4, IPv6, cambios de resolución y rutas indirectas con receptores controlados. Limitar tiempos y tamaños de respuesta para que la vista previa no consuma recursos sin límite.

Largo plazo

Cerrar cuando tanto el acceso directo como el redirigido a recursos fuera de política fallen. Conservar una integración positiva que siga funcionando y una prueba de que el servicio interno rechaza solicitudes sin identidad, incluso desde una red permitida.

F06	Credencial de servicio publicada en un artefacto de CI	Alta 8.1
CWE	CWE-798	
CVSS 3.1	8.1 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N	
Descripción (incl. causa raíz)	El paquete de diagnóstico de una compilación incorpora un archivo de configuración con una credencial reutilizable. Los miembros con lectura de artefactos pueden recuperarla. La identidad de servicio dispone de permisos de lectura y modificación en la API de pedidos.	
Impacto de seguridad	Un usuario de CI con permisos de lectura puede asumir los permisos de una identidad más privilegiada. Se modela consulta y actualización de pedidos canario. La cuenta no administra el sistema operativo ni la facturación del proveedor de infraestructura.	
Dominio afectado	ci.nimbus.example; api.nimbus.example	
Remediación	Revocar y rotar la credencial, retirar el artefacto y revisar sus accesos históricos. Emitir credenciales de corta duración desde un gestor de secretos y limitar los permisos del servicio. Excluir secretos del proceso de empaquetado y detectar regresiones antes de publicar.	
Referencias	• https://cwe.mitre.org/data/definitions/798.html • https://cheatsheetseries.owasp.org/cheatsheets/Secrets_Management_Cheat_Sheet.html	

Procedimiento detallado

1. Contexto y precondiciones. El artefacto build-demo-062 pertenece a un pipeline ficticio. La cadena SECRET-DEMO-NO-VALIDO es un marcador editorial, no una credencial funcional. Las capacidades de svc_order_sync se describen como parte del escenario para explicar la consecuencia del acceso a secretos.

2. **Separar permiso de lectura y permiso de ejecución.** La cuenta de desarrollador puede descargar artefactos, pero no administrar pedidos. Registrar esa diferencia antes de usar la identidad de servicio en el guion. Si ambos actores tuvieran los mismos privilegios, la conclusión sobre elevación requeriría un análisis distinto.
3. **Localizar el origen de la exposición.** E06 identifica el archivo de configuración incluido por una regla de empaquetado demasiado amplia. El error se atribuye al contenido del artefacto y a su distribución, no a la mera existencia de una variable de entorno. El informe conserva una etiqueta sintética en lugar del secreto.

E06 Artefacto de compilación y privilegios		CASO FICTICIO
Artefacto	->	build-demo-062.zip
Archivo incluido	->	diagnostics/service.env
Valor publicado	->	SECRET-DEMO-NO-VALIDO
Acceso al artefacto	->	rol reader de CI
Identidad representada	->	svc_order_sync
Permisos de la identidad	->	pedidos: leer y actualizar
El acceso de lectura al artefacto expone una identidad con mayores permisos.		

Figura 6. E06. Evidencia sintética: El acceso de lectura al artefacto expone una identidad con mayores permisos. No es una captura de una prueba ejecutada.

4. **Modelar una comprobación mínima.** La representación utiliza el servicio para leer y modificar una nota de un pedido canario. No extrae un catálogo completo. Después se restaura el valor. El resultado demuestra los permisos atribuidos al secreto en el ejemplo, sin afirmar que una credencial real haya sido utilizada.
5. **Evaluar la retirada completa.** Borrar el archivo de una compilación posterior no invalida las copias descargadas ni el token anterior. El cierre necesita confirmar revocación, rotación, permisos reducidos y revisión de retención en cachés o almacenes secundarios.
6. **Activos afectados**
 - ci.nimbus.example
 - api.nimbus.example

Resumen de remediación

Corto plazo

Revocar el secreto anterior antes de considerar resuelto el incidente representado. Retirar las copias que controla el pipeline y registrar qué repositorios de artefactos y cachés se revisaron. Coordinar la rotación para evitar una interrupción innecesaria.

Mediano plazo

Separar configuración pública y secretos en tiempo de ejecución. Reducir svc_order_sync a las operaciones y organizaciones que necesita. Impedir la publicación si un análisis de contenido detecta formatos de secreto o archivos prohibidos, con excepciones revisadas y trazables.

Largo plazo

El criterio de cierre exige que el secreto antiguo falle, que el nuevo artefacto no lo contenga y que la identidad limitada mantenga el flujo legítimo. El estado sigue en corrección: este documento no representa todavía un retest concluyente de esa rotación.

F07 **Derechos de replicación del dominio asignados a una cuenta operativa**

Alta 8.8

CWE	CWE-269
CVSS 3.1	8.8 <code>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</code>
Descripción (incl. causa raíz)	La cuenta operativa svc_inventory tiene los derechos de replicación Get-Changes y Get-Changes-All sobre el contexto de nombres del dominio. Esa delegación excede su función de inventario y permite solicitar datos de dominio sensibles mediante replicación.
Impacto de seguridad	El escenario concede una vía hacia secretos de autenticación y compromiso amplio del dominio. La comprobación didáctica se limita a una identidad canario. Las métricas altas de integridad y disponibilidad reflejan el impacto potencial del control del dominio; no representan borrado, parada ni extracción masiva.
Dominio afectado	<code>dc01.ad.nimbus.example</code>
Remediación	Retirar la delegación innecesaria, revisar permisos heredados y grupos que la conceden, y separar inventario de funciones de replicación. Investigar actividad de la identidad y planificar la rotación de secretos según el alcance realmente determinado.
Referencias	https://cwe.mitre.org/data/definitions/269.html https://learn.microsoft.com/en-us/windows/win32/adschema/r-ds-replication-get-changes-all

Procedimiento detallado

- Contexto y precondiciones.** DC01 y el dominio ad.nimbus.example son ficticios. El modelo entrega una cuenta operativa válida y conectividad al controlador de dominio. No se incluyen hashes, contraseñas ni material de autenticación real; la identidad canario solo ilustra el criterio de confirmación.
- Revisar permisos efectivos.** Comprobar tanto las entradas explícitas como la pertenencia transitiva a grupos y la herencia. E07 representa la combinación de los dos derechos sobre la raíz del dominio. Un permiso con nombre parecido sobre una unidad organizativa distinta no demostraría el mismo alcance.
- Distinguir configuración y confirmación.** La revisión de ACL acredita una condición de riesgo. El guion añade una solicitud de replicación limitada a demo-repl-canary para ilustrar cómo se confirmaría la capacidad. Las salidas mostradas son sintéticas; no se ejecutó una extracción de secretos durante la creación de este informe.

E07 Delegación de replicación y alcance		CASO FICTICIO
Principal	->	AD\svc_inventory
Objeto	->	DC=ad,DC=nimbus,DC=example
Derecho efectivo 1	->	DS-Replication-Get-Changes
Derecho efectivo 2	->	DS-Replication-Get-Changes-All
Canario del guion	->	demo-repl-canary
Secretos publicados	->	ninguno
Una identidad de inventario recibe facultades de replicación que no necesita.		

Figura 7. E07. Evidencia sintética: Una identidad de inventario recibe facultades de replicación que no necesita. No es una captura de una prueba ejecutada.

- Acotar la cadena de impacto.** El compromiso del dominio es una consecuencia modelada de la exposición de secretos de autenticación, no un paso adicional ejecutado. No se incluyen persistencia, modificación de políticas ni operaciones destructivas. El equipo tendría que valorar el alcance con su telemetría y procedimientos de respuesta.

5. Justificar la prioridad. La puntuación base es alta con PR:L porque se necesita una identidad de dominio. La prioridad de negocio es P0 por su alcance transversal. Esa diferencia muestra por qué CVSS y prioridad operativa se registran por separado, en lugar de elevar artificialmente el vector.

6. Activos afectados

- dc01.ad.nimbus.example

Resumen de remediación

Corto plazo

Suspender o limitar la identidad comprometible y retirar los derechos injustificados tras comprobar dependencias legítimas. Preservar los registros de autenticación y replicación relevantes. Una rotación aislada no corrige una delegación que sigue existiendo.

Mediano plazo

Inventariar principales con derechos de replicación y documentar excepciones autorizadas. Revisar eventos de acceso a objetos y solicitudes de replicación desde equipos que no son controladores, según la auditoría habilitada y la telemetría realmente disponible.

Largo plazo

Verificar con la misma identidad que la solicitud canario es denegada, mientras la replicación legítima entre controladores continúa. Si se acreditara exposición real de secretos, la recuperación del dominio requeriría un procedimiento adicional; este caso ficticio no afirma haberlo ejecutado.

F08 Delegación de membresía sobre un grupo administrador de servidores		Alta 8.8
CWE	CWE-269	
CVSS 3.1	8.8 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
Descripción (incl. causa raíz)	Helpdesk-L1 puede modificar la membresía de APP-Server-Admins. Este segundo grupo es administrador local en WINAPP01 mediante una política de dominio. La delegación permite elevar una cuenta de soporte a administración del servidor de aplicación.	
Impacto de seguridad	El modelo permite acceso administrativo al host de aplicación y a sus datos y servicios. No se equipara automáticamente esa administración local con control del dominio. La prueba canario solo comprueba el permiso efectivo y una operación administrativa inocua.	
Dominio afectado	dc01.ad.nimbus.example; winapp01.ad.nimbus.example	
Remediación	Retirar el permiso de escritura de membresía y revisar la ruta completa de grupos y políticas. Separar la gestión de soporte de la administración de servidores; aplicar concesiones temporales y aprobadas cuando la operación lo requiera.	
Referencias	• https://cwe.mitre.org/data/definitions/269.html • https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory	

Procedimiento detallado

1. Contexto y precondiciones. La cuenta helpdesk.demo empieza con funciones de soporte limitadas. APP-Server-Admins administra exclusivamente WINAPP01 en este modelo. Se utiliza una identidad canario y una sesión nueva para reflejar correctamente los cambios de token y evitar atribuir privilegios de sesiones anteriores.

2. **Reconstruir la ruta de privilegios.** E08 muestra tres relaciones distintas: permiso sobre member, pertenencia al grupo y asignación de administrador local. Ninguna se deduce únicamente del nombre del grupo. La política aplicada al servidor confirma el último tramo de la cadena.
3. **Representar un cambio reversible.** El guion incorpora demo-helpdesk-canary al grupo y abre una sesión nueva en WINAPP01. La capacidad administrativa se verifica con lectura de un recurso canario restringido, sin instalar servicios ni ejecutar cargas. El cambio se revierte al finalizar.

E08 | Ruta de administración de un servidor

CASO FICTICIO

```
helpdesk.demo -> pertenece a Helpdesk-L1
Helpdesk-L1 -> WriteProperty(member)
Objeto del permiso -> APP-Server-Admins
Política aplicada -> administrador local en WINAPP01
Comprobación canario -> recurso administrativo legible
Estado actual -> corrección comunicada; sin retest

La ruta de delegación termina en administración local, no en control probado del dominio.
```

Figura 8. E08. Evidencia sintética: La ruta de delegación termina en administración local, no en control probado del dominio. No es una captura de una prueba ejecutada.

4. **Revisar herencia y persistencia del permiso.** Comprobar si la entrada procede del objeto, una unidad organizativa o un grupo intermedio. Quitar una membresía canario no elimina la posibilidad de volver a agregarla. El cierre debe corregir la delegación y revisar cambios realizados durante la exposición.
5. **Distintuir corrección comunicada y verificada.** El estado actual del ejemplo es Corrección comunicada: el equipo ficticio informa de una nueva política, pero el retest aún no está representado. No se presenta un aviso de despliegue como evidencia de cierre ni se reduce la severidad original.
6. **Activos afectados**
 - dc01.ad.nimbus.example
 - winapp01.ad.nimbus.example

Resumen de remediación

Corto plazo

Retirar la delegación excesiva y revisar miembros recientes del grupo administrador. Confirmar que el cambio no se vuelve a aplicar desde una plantilla o política de configuración. Documentar las tareas de soporte que necesitan una alternativa legítima.

Mediano plazo

Separar grupos de soporte, cuentas administrativas y ámbitos de servidores. Probar que la cuenta helpdesk.demo ya no puede agregar ni quitar miembros. Verificar los permisos efectivos, además de comparar la configuración deseada.

Largo plazo

Cerrar cuando un retest rechace la modificación y una sesión nueva carezca de administración local, conservando las tareas autorizadas de soporte. El despliegue comunicado no basta: este informe mantiene el estado sin verificar hasta disponer de esa evidencia.

F09 XSS almacenado en comentarios del portal de soporte

Media 5.4

CWE	CWE-79
CVSS 3.1	5.4 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
Descripción (incl. causa raíz)	Los comentarios conservan fragmentos de HTML que se insertan sin un saneado adecuado en el navegador del agente de soporte. Una cuenta de cliente puede guardar contenido activo que se procesa cuando el agente abre el ticket.
Impacto de seguridad	La demostración modifica un marcador visible y accede a información limitada de la página abierta. No representa robo de cookies, acceso total a la cuenta del agente ni extracción de datos hacia un tercero. El impacto depende de que un agente visualice el comentario.
Dominio afectado	portal.nimbus.example
Remediación	Renderizar texto mediante APIs seguras y codificación contextual. Si se necesita HTML enriquecido, aplicar un saneador mantenido con una política reducida. Revisar contenido ya almacenado y usar CSP como defensa complementaria, sin convertirla en la corrección principal.
Referencias	- https://cwe.mitre.org/data/definitions/79.html - https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Procedimiento detallado

- Contexto y precondiciones.** La cuenta cliente.demo crea un ticket y agente.demo lo consulta desde una sesión separada. El marcador de demostración solo cambia un elemento de la página. No abre conexiones externas ni intenta persistir fuera del comentario del caso ficticio.
- Confirmar persistencia del contenido.** Guardar un comentario de texto normal y volver a abrirlo con la segunda identidad. El guion comprueba que el contenido proviene del almacenamiento, no de parámetros del enlace ni de herramientas del navegador utilizadas por el propio agente.
- Diferenciar HTML y ejecución.** E09 representa el marcador XSS-DEMO-ACTIVO en el DOM de la sesión del agente. Mostrar una etiqueta HTML no demuestra por sí solo ejecución de script: el cambio visible del marcador es la observación elegida para esa distinción dentro del escenario.

E09 Comentario persistente y contexto de navegador	CASO FICTICIO
Autor del comentario ->	cliente.demo
Lector del ticket ->	agente.demo
Persistencia ->	comentario recuperado del servidor
Marcador del DOM ->	XSS-DEMO-ACTIVO
Conexiones externas ->	ninguna en el guion
Acceso a cookies HttpOnly ->	no atribuido
El contenido almacenado cruza al contexto de ejecución del navegador del agente.	

Figura 9. E09. Evidencia sintética: El contenido almacenado cruza al contexto de ejecución del navegador del agente. No es una captura de una prueba ejecutada.

4. Acotar contexto y capacidades. El comentario se procesa en el origen del portal. La demostración no atribuye capacidad de leer cookies HttpOnly ni de evitar controles de autorización del servidor. El acceso a datos y las acciones disponibles seguirían limitados por la sesión y las defensas concretas del navegador.

5. **Justificar interacción y alcance.** UI:R refleja la apertura del ticket por la víctima; PR:L, la cuenta necesaria para comentar. S:C representa el paso desde la aplicación vulnerable al contexto de seguridad del navegador del agente. C:L e I:L corresponden a las capacidades limitadas representadas.
6. **Activos afectados**
 - portal.nimbus.example

Resumen de remediación

Corto plazo

Desactivar temporalmente el HTML de comentarios y neutralizar entradas almacenadas que incumplan la política. Conservar el texto útil de los tickets y documentar qué transformaciones se aplicaron para evitar pérdida innecesaria de información.

Mediano plazo

Revisar el renderizado de comentarios en detalle, búsquedas, notificaciones y vistas previas. Incorporar pruebas sobre atributos, URLs y elementos no permitidos en el formato enriquecido. El control debe aplicarse en todos los consumidores del mismo contenido.

Largo plazo

Cerrar cuando los comentarios se muestren como texto o HTML permitido y el marcador no se active en ninguna vista. Mantener un comentario legítimo con formato como control positivo. El escenario todavía no incluye un retest concluyente de esta corrección.

F10 CORS con credenciales para orígenes no autorizados Media 6.5	
CWE	CWE-942
CVSS 3.1	6.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Descripción (incl. causa raíz)	La API refleja el encabezado Origin y permite credenciales sin comprobar una lista de orígenes autorizados. La sesión del escenario utiliza cookies SameSite=None; Secure. Un navegador que admite esas cookies entre sitios puede exponer respuestas autenticadas a un origen ajeno.
Impacto de seguridad	Se modela lectura de datos de pedidos desde una página externa visitada por un usuario autenticado. No se afirma que la presencia de un encabezado CORS, aislada, baste para explotar el fallo ni que todos los navegadores permitan cookies de terceros.
Dominio afectado	api.nimbus.example; auth.nimbus.example
Remediación	Definir una lista exacta de orígenes por entorno y evitar reflejar valores no confiables. Permitir credenciales solo donde sean necesarias; comprobar la política de cookies y caché. No usar comodines de subdominio como sustituto de una lista de aplicaciones autorizadas.
Referencias	• https://cwe.mitre.org/data/definitions/942.html • https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html

Procedimiento detallado

1. **Contexto y precondiciones.** El origen receptor es receptor.canario.nimbus.example y solo contiene datos de demostración. El navegador del guion permite la cookie entre sitios. Esta condición se declara expresamente porque un bloqueo de cookies de terceros puede interrumpir la cadena incluso si la política del servidor es incorrecta.
2. **Verificar la configuración del servidor.** Comparar una petición con el origen legítimo y otra con el receptor canario. E10 muestra que ambos son aceptados con credenciales. La combinación de asterisco y credenciales no se utiliza como prueba: los navegadores no la tratan como una autorización válida de lectura autenticada.

3. **Representar la comprobación en navegador.** La página canario solicita el recurso con credenciales y accede al cuerpo de la respuesta. Ese acceso por JavaScript es la condición relevante; obtener un 200 con una herramienta HTTP no demostraría por sí mismo una vulneración de la política del navegador.

E10 Política CORS y lectura desde otro origen	CASO FICTICIO
Origin enviado	-> receptor.canario.nimbus.example
Allow-Origin devuelto	-> el mismo origen no autorizado
Allow-Credentials	-> true
Cookie del escenario	-> SameSite=None; Secure
Navegador del guion	-> cookies entre sitios permitidas
Lectura por JavaScript	-> cuerpo de pedidos accesible
La lectura autenticada requiere que se cumplan también las condiciones del navegador.	

Figura 10. E10. Evidencia sintética: La lectura autenticada requiere que se cumplan también las condiciones del navegador. No es una captura de una prueba ejecutada.

4. **Mantener una matriz de condiciones.** El guion diferencia sesión presente o ausente y cookies permitidas o bloqueadas. Solo la combinación de sesión válida, envío de cookies y política CORS permisiva representa lectura autenticada. El informe no transforma la configuración en una afirmación universal sobre todos los usuarios.
5. **Definir el alcance de la valoración.** PR:N describe al actor que controla el origen receptor; UI:R refleja que la víctima debe visitarlo. C:H corresponde a la API de pedidos accesible en el modelo. No se representan cambios de estado ni interrupción, por lo que I y A permanecen en N.
6. **Activos afectados**
- api.nimbus.example
 - auth.nimbus.example

Resumen de remediación

Corto plazo

Retirar los orígenes no autorizados y comprobar el funcionamiento de los clientes legítimos. Revisar los encabezados de caché para que una respuesta autorizada para un origen no se reutilice de forma incorrecta para otro.

Mediano plazo

Centralizar la política CORS por entorno. Probar origen exacto permitido, origen ajeno, valor null y subdominios que no correspondan a clientes. Revisar cookies y controles de autorización de cada endpoint sin asumir que CORS sustituye la autenticación.

Largo plazo

Cerrar con una verificación de navegador: el cliente legítimo puede leer la respuesta y el receptor canario no. Las variantes con sesión ausente deben seguir rechazando acceso. El retest ficticio incluido representa esos controles positivos y negativos.

F11 Sesión reutilizable después del cierre de sesión

Media 5.4

CWE	CWE-613
CVSS 3.1	5.4 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
Descripción (incl. causa raíz)	El cierre de sesión borra la cookie del navegador, pero el servidor mantiene válida la sesión anterior hasta su expiración. La misma credencial de sesión permite consultar y modificar preferencias de la cuenta después de cerrar sesión.
Impacto de seguridad	Un actor que ya disponga de esa sesión conserva acceso limitado al perfil y las preferencias. El informe no atribuye al hallazgo una forma de robar el token ni acceso a otras cuentas. La duración restante de la sesión determina la ventana de exposición.
Dominio afectado	auth.nimbus.example; portal.nimbus.example
Remediación	Revocar la sesión en el servidor al cerrar sesión y al realizar cambios sensibles de cuenta. Definir la invalidación de tokens de actualización y las excepciones de sesiones múltiples. Una cookie eliminada en el cliente no acredita revocación del lado servidor.
Referencias	- https://cwe.mitre.org/data/definitions/613.html - https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Procedimiento detallado

- Contexto y precondiciones.** Se conserva una copia sintética de la sesión de usuario.a antes de cerrar sesión en el navegador. Se prueba únicamente esa identidad y un endpoint de preferencias. Las cadenas de sesión se sustituyen por etiquetas no funcionales.
- Confirmar la sesión inicial.** Consultar el perfil con SESSION-DEMO-A y comprobar el identificador del sujeto. Guardar la hora lógica del escenario y la expiración prevista. El control permite distinguir la reutilización del mismo token de una nueva autenticación automática.
- Cerrar sesión y reutilizar la misma credencial.** E11 representa la eliminación de la cookie y una nueva petición con el valor anterior. El servidor devuelve el perfil. No basta con ver la página en la caché del navegador: la evidencia elegida es una respuesta autenticada nueva con su identificador de petición.

E11 Sesión antes y después de logout		CASO FICTICIO
Antes de logout	-> /profile: 200; usuario.a	
Logout en navegador	-> cookie eliminada	
Mismo token después	-> /profile: 200; usuario.a	
Nueva petición	-> request-id: DEMO-F11-02	
Preferencia canario	-> modificable y restaurada	
Nueva autenticación	-> no realizada para la reutilización	
El servidor sigue aceptando la sesión anterior aunque el navegador haya borrado la cookie.		

Figura 11. E11. Evidencia sintética: El servidor sigue aceptando la sesión anterior aunque el navegador haya borrado la cookie. No es una captura de una prueba ejecutada.

- Comprobar una operación limitada.** Modificar una preferencia canario y verificarla desde una sesión nueva legítima. Restaurar el valor. La operación no afecta a credenciales, pedidos ni permisos de otras personas. El alcance limitado explica C:L e I:L.

5. **Separar origen del acceso y persistencia.** PR:L expresa el requisito de poseer una sesión válida del usuario. Este hallazgo describe la persistencia de ese acceso después de logout; no demuestra robo de cookies, phishing ni un bypass de contraseña. El estado permanece abierto en el ejemplo.
6. **Activos afectados**
 - auth.nimbus.example
 - portal.nimbus.example

Resumen de remediación

Corto plazo

Documentar y aplicar la revocación central de sesiones afectadas. Revisar la duración de tokens y el comportamiento de clientes que mantienen varias sesiones. Un plazo de expiración más corto reduce la ventana, pero no cumple por sí solo la semántica de logout.

Mediano plazo

Añadir pruebas de logout, cambio de contraseña, recuperación de cuenta y revocación administrativa. Comprobar tanto tokens de acceso como de actualización. El diseño debe aclarar si una acción revoca una sesión o todas las sesiones del usuario.

Largo plazo

El criterio de cierre exige que el token previo falle en una petición nueva, que no permita actualizar preferencias y que una sesión nueva legítima funcione. Este caso no presenta un retest: la corrección permanece pendiente dentro del escenario.

F12 **Diagnósticos internos expuestos en el panel de soporte**

Baja 2.7

CWE	CWE-209
CVSS 3.1	2.7 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
Descripción (incl. causa raíz)	Un error del panel restringido de soporte devuelve la traza, el nombre interno de base de datos y rutas de despliegue. El rol soporte-admin necesita funciones operativas de la aplicación, pero no acceso a esa información interna del servicio.
Impacto de seguridad	Se modela divulgación limitada de estructura y nombres internos a una cuenta con privilegios altos de aplicación. La respuesta no contiene contraseñas, tokens ni datos de clientes. No se afirma que conocer una versión o una ruta demuestre otra vulnerabilidad.
Dominio afectado	portal.nimbus.example; db.nimbus.example
Remediación	Devolver un error genérico con identificador de correlación y guardar el diagnóstico en registros de acceso restringido. Desactivar el modo de depuración en entregas públicas y sanear los campos que puedan incluir secretos o datos personales.
Referencias	• https://cwe.mitre.org/data/definitions/209.html • https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html

Procedimiento detallado

1. **Contexto y precondiciones.** El fallo aparece en una vista administrativa del panel de soporte. Una cuenta ordinaria no alcanza ese endpoint. La condición evita inflar el riesgo como si fuera una divulgación pública sin autenticación.
2. **Comprobar el requisito de privilegios.** Comparar la respuesta de una cuenta ordinaria con la de soporte-admin. La primera recibe un rechazo de autorización. PR:H registra que se necesita un rol de administración de la aplicación antes de alcanzar el comportamiento vulnerable.

3. **Identificar información adicional.** E12 muestra el tipo de excepción, el nombre de una base y una ruta de aplicación. Se conserva una representación sintética de esos valores. La diferencia frente a un identificador de error es que aporta estructura interna que el cliente no necesita para completar la operación.

E12 Respuesta de error y límite de información		CASO FICTICIO
Cuenta ordinaria	-> 403	
Rol soporte-admin	-> 500 con diagnóstico	
Ruta expuesta	-> /srv/nimbus/app/orders.py	
Base interna	-> nimbus_orders_demo	
Secretos en respuesta	-> ninguno en el escenario	
Identificador útil	-> DEMO-ERR-1201	
La fuga es limitada y requiere un rol privilegiado; no se atribuyen consecuencias adicionales.		

Figura 12. E12. Evidencia sintética: La fuga es limitada y requiere un rol privilegiado; no se atribuyen consecuencias adicionales. No es una captura de una prueba ejecutada.

4. **Evitar encadenamientos no acreditados.** El informe no transforma el nombre de un motor ni su versión en un CVE aplicable. Tampoco atribuye acceso al archivo nombrado. La exposición se valora por sí misma con C:L y sin impacto directo en integridad o disponibilidad.
5. **Definir una corrección verificable.** La respuesta pública debe conservar un identificador utilizable por soporte, mientras la traza queda en un canal autorizado. Las pruebas deben comprobar tanto la ausencia de detalles como la capacidad de correlacionar el error legítimamente.
6. **Activos afectados**
- portal.nimbus.example
 - db.nimbus.example

Resumen de remediación

Corto plazo

Desactivar la devolución de trazas al cliente y mantener un identificador de correlación. Revisar si los registros internos almacenan parámetros sensibles y limitar quién puede consultarlos.

Mediano plazo

Unificar el tratamiento de errores de la API y del panel. Probar fallos de validación, dependencias y excepciones inesperadas. La aplicación debe mantener códigos y mensajes consistentes sin exponer rutas, consultas ni detalles de configuración.

Largo plazo

Cerrar cuando el diagnóstico solo esté disponible en el canal autorizado y el soporte pueda correlacionar el incidente usando DEMO-ERR-1201 como patrón de prueba. El ejemplo mantiene el hallazgo abierto, con prioridad menor que las rutas de acceso a datos y privilegios.

9 Cadenas de impacto y fronteras de confianza

Ruta A: entrada pública y datos de pedidos

F01 modela una entrada pública que altera la consulta de búsqueda. La raíz es la mezcla de código y datos, agravada por una cuenta con permisos de escritura. La lectura y el cambio canario sostienen dos efectos distintos; no se extiende el relato a ejecución en el sistema operativo. RT01 representa la corrección de ambas condiciones relevantes.

F02 ofrece una vía independiente a cuentas del portal: el token de recuperación no queda vinculado a su sujeto. No necesita F01 para funcionar. Separar ambos hallazgos evita presentar una larga cadena artificial que haga parecer dependientes dos problemas con causas y correcciones diferentes.

Ruta B: usuario legítimo y frontera entre organizaciones

En F03, el atacante del escenario ya dispone de una cuenta válida. El fallo aparece al resolver un objeto por ID sin aplicar la política de organización. F04 afecta a otra frontera: la ubicación de un archivo y su pertenencia al pedido. Cambiar IDs por UUIDs no corrige ninguna de esas dos autorizaciones.

F05 amplía las capacidades del mismo tipo de usuario a través de una petición del servidor. La confianza en el origen interno del tráfico contribuye al impacto. El retest que solo bloquea la URL directa deja pendiente el destino efectivo después de una redirección.

Ruta C: identidades operativas y privilegios

F06 relaciona lectura de artefactos con uso de una identidad de servicio más poderosa. El secreto representa un cambio de identidad; eliminar una copia sin revocarlo no corta la ruta.

F07 y F08 parten de identidades internas proporcionadas. No se afirma que el hallazgo web haya permitido alcanzar esas cuentas. F07 modela derechos de replicación del dominio; F08 termina en administración de WINAPP01. El informe mantiene separados el control potencial del dominio y la administración local de un servidor.

Qué conviene cortar primero

La respuesta prioriza las fronteras que concentran permisos: identidad del sujeto, pertenencia del objeto, destino de red y delegación administrativa. Los controles locales ayudan, pero el cierre exige verificar el camino completo. Por ejemplo, corregir GET sin revisar PATCH mejora la lectura y deja abierto el cambio de datos.

Controles positivos conservados

El escenario incluye rechazo de usuarios anónimos en perfil y de usuarios ordinarios en el panel administrativo. Esos resultados muestran que parte de la autenticación y de los roles funciona. No invalidan los fallos de objeto, sesión o recuperación, ni permiten declarar segura toda la plataforma.

Cada ruta aquí descrita es una explicación del modelo ficticio. No representa una intrusión, una prueba de lateralidad ejecutada ni un incidente detectado.

10 Plan de remediación

Resumen del plan

El plan conserva las dependencias entre contención, cambio y verificación. Los responsables y fechas son una propuesta del escenario. Las tareas cerradas permanecen en el registro para explicar qué se verificó; no se eliminan del informe inicial.

ID	Prioridad	Responsable propuesto	Fecha objetivo
F01	P0	Equipo de aplicaciones	2026-10-03
F02	P0	Equipo de identidad	2026-10-03
F03	P1	Equipo de API	2026-10-09
F04	P1	Equipo de API	2026-10-09
F05	P1	Equipo de plataforma	2026-10-09
F06	P1	Equipo de DevOps	2026-10-05
F07	P0	Equipo de identidad	2026-10-03
F08	P1	Equipo de infraestructura	2026-10-09
F09	P2	Equipo de aplicaciones	2026-10-23
F10	P2	Equipo de API	2026-10-23
F11	P2	Equipo de identidad	2026-10-23
F12	P3	Equipo de aplicaciones	2026-11-02

Una fecha objetivo no prueba que un cambio esté realizado. El apartado de seguimiento refleja el estado: cuatro cierres representados, dos correcciones parciales, una corrección comunicada sin retest y cinco casos adicionales sin cierre. La tabla de fechas sirve para gestionar el trabajo; no es un compromiso de una organización real.

Corto plazo

Contener y preservar contexto

Priorizar F07 y confirmar la continuidad de los cierres F01 y F02. La retirada de derechos debe coordinarse con las funciones legítimas de inventario y replicación. Para F06, revocar el secreto anterior y revisar sus permisos antes de dar por concluida la retirada de artefactos.

Designar un responsable de cada cambio y un verificador distinto dentro del modelo organizativo. Registrar versión desplegada, alcance de la corrección y pruebas esperadas. Preservar registros relevantes con minimización de datos; no copiar tokens completos a tickets o documentos.

Salida de esta fase: rutas prioritarias contenidas, responsables asignados y comprobaciones de cierre concretas. Ningún estado se cambia a verificado por el mero envío de un aviso de despliegue.

Mediano plazo

Corregir causas comunes

Completar las matrices de autorización de F03 y la política de destinos de F05. Revisar las demás operaciones que reutilizan el mismo componente. Confirmar F08 con una sesión nueva y permisos efectivos; revisar F09, F10 y F11 como problemas distintos de navegador, origen y ciclo de sesión.

Para cada cambio, conservar una prueba negativa y un flujo legítimo. Un sistema que bloquea toda descarga o toda integración puede detener el caso, pero no demuestra una corrección funcional aceptable. Verificar también paginación, exportaciones y consumidores secundarios de la misma API.

Salida de esta fase: retests completos de las rutas pendientes, regresiones incorporadas y excepciones documentadas. Las correcciones parciales mantienen fecha, responsable y alcance residual visible.

Largo plazo

Mantener y volver a comprobar

Convertir autorización, gestión de secretos y delegación de privilegios en revisiones repetibles del ciclo de cambios. Mantener un inventario de identidades de servicio y de sus permisos; revisar las delegaciones de grupos cuando cambien equipos o funciones.

Usar indicadores que midan resultados: hallazgos sin cierre verificado, correcciones parciales repetidas, antigüedad por prioridad y porcentaje de cambios con prueba de regresión. No se asignan valores de rendimiento a esos indicadores porque no hay una operación real de la que obtenerlos.

Salida de esta fase: un registro sostenible de decisiones, evidencias y responsables. Si un riesgo se acepta, debe tener justificación y vencimiento; la ausencia de tiempo para comprobarlo no debe convertirse automáticamente en aceptación.

11 Apéndices técnicos y referencias

Cambios realizados y limpieza

Registro de cambios del escenario

Caso	Cambio representado	Restitución descrita
F01	Nota interna de pedido canario	Valor anterior restaurado.
F02	Contraseña administrativa de demostración	Restablecimiento y revocación de sesiones.
F03	Nota de entrega de otra organización	Valor restaurado tras control con la segunda cuenta.
F05	Etiqueta de trabajo de documentos	Etiqueta original recuperada.
F08	Miembro canario en grupo administrador	Miembro retirado y sesión de prueba cerrada.
F09	Comentario con marcador de DOM	Comentario de demostración eliminado del relato.
F11	Preferencia de usuario	Valor inicial restaurado.

Esta tabla narra el procedimiento previsto en la ficción. No es un acta de limpieza de sistemas reales. Las pruebas de lectura no se convierten en modificaciones ni se atribuyen acciones adicionales para alargar la cadena.

Herramientas utilizadas

Ejecuciones reales y herramientas del escenario

Ejecutado para producir los archivos: report-gen 0.21.2, su calculadora CVSS, exportadores y validación del proyecto; herramientas locales de inspección y renderizado del PDF. El registro técnico del paquete detalla las comprobaciones realizadas sobre los archivos.

Solo descrito como metodología: proxy HTTP, navegador, cliente de API y revisión de permisos de Active Directory. No se incluyen versiones de escáneres, registros de comandos ni duraciones de pruebas que no se hayan ejecutado. Las imágenes E01 a E12 y RT01 a RT10 incluidas son representaciones didácticas.

Referencias generales

- FIRST, CVSS 3.1, especificación: <https://www.first.org/cvss/v3.1/specification-document>
- FIRST, guía de uso: <https://www.first.org/cvss/v3.1/user-guide>
- OWASP, API Security 2023, autorización por objeto: <https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/>
- Microsoft, derechos de replicación: <https://learn.microsoft.com/en-us/windows/win32/adschema/r-ds-replication-get-changes-all>
- Microsoft, protección de Active Directory: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

Las referencias específicas de prevención y las clasificaciones CWE aparecen en la ficha de cada hallazgo. Son apoyo técnico para interpretar el caso, no una declaración de que las organizaciones citadas revisaron este documento.

Glosario

Término	Uso en este informe
Canario	Objeto o identidad de prueba que permite una comprobación acotada.

Término	Uso en este informe
BOLA	Fallo de autorización al acceder a un objeto mediante su identificador.
Tenant	Organización lógica cuyos datos deben mantenerse separados.
SSRF	Petición realizada por un servidor hacia un destino controlado por una entrada.
ACL	Lista de permisos asociada a un recurso o un objeto.
CVSS Base	Puntuación de severidad técnica para condiciones declaradas.
Prioridad	Orden operativo propuesto según el contexto del caso.
Retest	Nueva comprobación de una corrección y sus límites.
Corrección parcial	Una ruta queda resuelta y otra continúa abierta.
Evidencia sintética	Representación editorial; no una observación de un sistema real.

Reutilización del proyecto

El respaldo editable incluye el YAML y las imágenes vinculadas para importarlo con «Abrir respaldo» en report-gen. El Markdown conserva el contenido para revisión textual. Las modificaciones del proyecto deben exportarse de nuevo para que las tablas, los estados y el informe reflejen la misma versión. Cambiar solamente el PDF rompe esa correspondencia.

12 Activos evaluados

Activo	Objetivo	Tipo	Notas
PORTAL	portal.nimbus.example	Web	Pedidos y soporte; dos organizaciones canario.
API01	api.nimbus.example	API	Pedidos, adjuntos e integraciones; acceso autenticado.
AUTH01	auth.nimbus.example	Identidad	Recuperación de cuentas, sesiones y cookies.
DB01	db.nimbus.example	Base de datos	Copia sintética; permisos y datos canario.
FILES01	files.nimbus.example	Archivos	Adjuntos y servicio interno de documentos.
CI01	ci.nimbus.example	Desarrollo	Artefactos y credenciales de servicio ficticias.
DC01	dc01.ad.nimbus.example	Active Directory	Delegaciones y grupos del dominio ficticio.
WINAPP01	winapp01.ad.nimbus.example	Servidor	Administración local mediante grupo de dominio.

13 Cobertura y limitaciones

Prueba	Activo	Estado	Observaciones
Búsqueda y acceso a datos	portal.nimbus.example	Realizada	Escenario representado: F01; control legítimo y entradas booleanas.
Recuperación de contraseña	auth.nimbus.example	Realizada	Escenario representado: F02; dos identidades y uso único.
Autorización por objeto	api.nimbus.example	Realizada	Escenario representado: F03; lectura y escritura cruzadas.
Aislamiento de adjuntos	files.nimbus.example	Realizada	Escenario representado: F04; ruta canario y enlace simbólico.
Destinos de integraciones	api.nimbus.example	Realizada	Escenario representado: F05; acceso directo y redirección.
Contenido de artefactos	ci.nimbus.example	Realizada	Escenario representado: F06; identidad de servicio excesiva.
Delegaciones de replicación	dc01.ad.nimbus.example	Realizada	Escenario representado: F07; ACL y principal efectivo.
Membresía de grupos	dc01.ad.nimbus.example	Realizada	Escenario representado: F08; ruta hasta administración local.
Aplicación de política local	winapp01.ad.nimbus.example	Realizada	Escenario representado: F08; sesión nueva e identidad canario.
Comentarios enriquecidos	portal.nimbus.example	Realizada	Escenario representado: F09; persistencia y vista del agente.
CORS con credenciales	api.nimbus.example	Realizada	Escenario representado: F10; lectura desde navegador canario.
Revocación de sesiones	auth.nimbus.example	Realizada	Escenario representado: F11; petición nueva después de logout.
Tratamiento de errores	portal.nimbus.example	Realizada	Escenario representado: F12; cuenta ordinaria frente a soporte-admin.
Control positivo de autorización	api.nimbus.example	Realizada	Control representado sin hallazgo: usuario anónimo recibe 401 en perfil.
Separación de rol administrativo	portal.nimbus.example	Realizada	Control representado sin hallazgo: cuenta ordinaria no abre el panel restringido.
Operaciones destructivas	db.nimbus.example	No aplica	Excluidas del guion. No se representan borrados ni interrupción.
Secretos en versiones históricas	ci.nimbus.example	Bloqueada	Pendiente en el escenario por retención incompleta de artefactos.
Respuesta ante compromiso de dominio	dc01.ad.nimbus.example	No aplica	El documento no representa una recuperación real de Active Directory.
Persistencia en servidores	winapp01.ad.nimbus.example	No aplica	Fuera del alcance didáctico; no se instala ningún componente.

Prueba	Activo	Estado	Observaciones
Variedad de navegadores y cookies	auth.nimbus.example	Bloqueada	El escenario CORS representa una configuración; no acredita cobertura universal.
Carga y disponibilidad	api.nimbus.example	No aplica	Excluidas pruebas de estrés y agotamiento de recursos.
Retención de copias externas	files.nimbus.example	Pendiente	El escenario no incluye un inventario completo de copias y respaldos.

Limitaciones

Esta matriz describe el guion ficticio. La etiqueta automática «Realizada» significa que la comprobación está representada documentalmente en el escenario, no que se haya ejecutado contra un sistema. Las filas bloqueadas y pendientes muestran cómo registrar límites sin convertirlos en resultados favorables.

No se desplegó la infraestructura Nimbus, no se enviaron peticiones a los objetivos descritos y no se ejecutaron herramientas de explotación durante la preparación del ejemplo. Las únicas ejecuciones reales corresponden a report-gen y a la validación de los archivos producidos.

No se representa cobertura de aplicaciones móviles, proveedores de pago, nube pública, phishing, seguridad física, denegación de servicio, persistencia ni revisión completa de código. Los controles positivos de la tabla se limitan a las rutas indicadas. No constituyen una certificación global de seguridad.

14 Seguimiento de correcciones y retest

Abierto: 2 · En corrección: 5 · Corrección comunicada: 1 · Corregido y verificado: 4

Hallazgo	Estado	Responsable	Fecha objetivo	Último retest
F01 · Inyección SQL en el buscador de pedidos	Corregido y verificado	Equipo de aplicaciones	2026-10-03	2026-09-30
F02 · Recuperación de contraseña sin vínculo entre token y cuenta	Corregido y verificado	Equipo de identidad	2026-10-03	2026-09-30
F03 · Acceso y modificación de pedidos de otra organización	En corrección	Equipo de API	2026-10-09	2026-09-30
F04 · Lectura fuera del directorio permitido de adjuntos	Corregido y verificado	Equipo de API	2026-10-09	2026-09-30
F05 · SSRF en la vista previa de integraciones	En corrección	Equipo de plataforma	2026-10-09	2026-09-30
F06 · Credencial de servicio publicada en un artefacto de CI	En corrección	Equipo de DevOps	2026-10-05	
F07 · Derechos de replicación del dominio asignados a una cuenta operativa	En corrección	Equipo de identidad	2026-10-03	
F08 · Delegación de membresía sobre un grupo administrador de servidores	Corrección comunicada	Equipo de infraestructura	2026-10-09	
F09 · XSS almacenado en comentarios del portal de soporte	En corrección	Equipo de aplicaciones	2026-10-23	
F10 · CORS con credenciales para orígenes no autorizados	Corregido y verificado	Equipo de API	2026-10-23	2026-09-30
F11 · Sesión reutilizable después del cierre de sesión	Abierto	Equipo de identidad	2026-10-23	
F12 · Diagnósticos internos expuestos en el panel de soporte	Abierto	Equipo de aplicaciones	2026-11-02	

F01 · 2026-09-30 · Corregido

Evaluador: Evaluador ficticio del escenario

Retest ficticio RT01. La búsqueda parametrizada conserva el resultado legítimo y trata las entradas de control como datos. La cuenta de búsqueda ya no puede actualizar demo_note. Los pedidos ajenos no se devuelven. Se representa el cierre de F01, conservando la severidad original para trazabilidad.

RT01 Retest ficticio	CASO FICTICIO
Referencia propia	-> 200; un pedido
Condición de control	-> 200; cero coincidencias
Referencia de otro cliente	-> 404
UPDATE con cuenta de búsqueda	-> permiso denegado
Resultado del escenario	-> corregido
Representación del resultado de retest. No es una ejecución real.	

RT01. Evidencia sintética del retest; sin ejecución contra sistemas reales.

F02 • 2026-09-30 • Corregido

Evaluador: Evaluador ficticio del escenario

Retest ficticio RT02. El servidor obtiene el sujeto desde el token. La combinación cruzada se rechaza; un token válido funciona solo una vez para su cuenta. Los tokens vencidos y reutilizados también fallan. Se representa la invalidación de sesiones anteriores de la cuenta recuperada.

RT02 Retest ficticio		CASO FICTICIO
Token A + cuenta B	-> 400; solicitud inválida	
Token A + cuenta A	-> cambio permitido	
Segundo uso del token A	-> 400	
Token caducado	-> 400	
Sesiones anteriores	-> revocadas	
Representación del resultado de retest. No es una ejecución real.		

RT02. Evidencia sintética del retest; sin ejecución contra sistemas reales.

F03 • 2026-09-30 • Corrección parcial

Evaluador: Evaluador ficticio del escenario

Retest ficticio RT03. GET devuelve 404 para el objeto de otra organización. PATCH todavía admite el cambio de delivery_note y se confirma con la cuenta B. El resultado es parcial y F03 continúa en corrección. La ausencia de lectura cruzada no elimina el impacto de integridad.

RT03 Retest ficticio		CASO FICTICIO
A -> B / GET	-> 404; corregido	
A -> B / PATCH	-> 200; sigue abierto	
B verifica delivery_note	-> CHECK-RT03	
Cambio canario	-> restaurado	
Conclusión	-> corrección parcial	
Representación del resultado de retest. No es una ejecución real.		

RT03. Evidencia sintética del retest; sin ejecución contra sistemas reales.

F04 • 2026-09-30 • Corregido

Evaluador: Evaluador ficticio del escenario

Retest ficticio RT04. La API recibe IDs de adjunto y autoriza pedido y organización antes de resolver el archivo. Los canarios exteriores y el enlace simbólico se rechazan. El adjunto legítimo conserva su contenido y tamaño. El escenario representa el cierre del hallazgo.

RT04 Retest ficticio		CASO FICTICIO
Adjunto propio por ID	-> 200; contenido íntegro	
Canario exterior	-> 404; sin contenido	
Enlace fuera del volumen	-> rechazado	
Adjunto de otro tenant	-> 404	
Ruta absoluta en error	-> ausente	
Representación del resultado de retest. No es una ejecución real.		

RT04. Evidencia sintética del retest; sin ejecución contra sistemas reales.

F05 • 2026-09-30 • Corrección parcial

Evaluador: Evaluador ficticio del escenario

Retest ficticio RT05. La URL interna directa es rechazada, pero una redirección desde el receptor canario vuelve a alcanzar el recurso interno. No se repite el cambio de etiqueta: la lectura del marcador basta para demostrar que la frontera sigue abierta. F05 permanece en corrección.

RT05 Retest ficticio	CASO FICTICIO
Destino interno directo -> bloqueado	
Receptor canario válido -> permitido	
Redirección a interno -> marcador visible	
Cambio de estado en retest -> no representado	
Conclusión -> corrección parcial	
Representación del resultado de retest. No es una ejecución real.	

RT05. Evidencia sintética del retest; sin ejecución contra sistemas reales.

F10 • 2026-09-30 • Corregido

Evaluador: Evaluador ficticio del escenario

Retest ficticio RT10. El origen legítimo conserva la lectura autenticada. El receptor canario y Origin:null no reciben autorización CORS; JavaScript no accede al cuerpo. Las peticiones sin sesión siguen rechazadas. El ejemplo representa una corrección verificada, no solo un cambio de encabezados.

RT10 Retest ficticio	CASO FICTICIO
Origen legítimo + sesión -> respuesta legible	
Origen canario + sesión -> lectura bloqueada	
Origin: null -> lectura bloqueada	
Sin sesión válida -> 401	
Resultado del escenario -> corregido	
Representación del resultado de retest. No es una ejecución real.	

RT10. Evidencia sintética del retest; sin ejecución contra sistemas reales.