CIBERSEGURIDAD · HACKING ÉTICO AUTORIZADO

Informe de muestra: *así se ve el trabajo.*

Un extracto real de un encargo completo — evaluación, endurecimiento, pentest y re-test — para que sepas exactamente qué documento recibes antes de contratar nada.

Qué es y qué no es este documento.

Es una **demostración metodológica sobre un sistema propio de AT Solutions**: un bot de WhatsApp que captura facturas y las vuelca en un panel. No es el informe de un cliente y no se presenta como caso de éxito de nadie. Se publica porque enseña el proceso y el formato del entregable — que es justo lo que no se puede evaluar leyendo una lista de estándares.

Referencia	AUD-MUESTRA-2026-08 (extracto)
Alcance	Aplicación web + API + base de datos + canal de mensajería
Ciclo cubierto	Assessment → Hardening → Pentest → Hardening → Re-test
Estándares	OWASP ASVS · OWASP Top 10 2025 · OWASP WSTG · NIST SP 800-115 · CIS · CWE Top 25
Consultor	AT Solutions — Alex Turcios · atsolutions.com.sv

Resumen ejecutivo

Qué se omitió. Un informe de seguridad es un mapa de cómo atacar el sistema que describe: el original circula cifrado y solo entre quienes el cliente autoriza. De este extracto público se retiraron nombres de cliente y de sistema, URLs de entornos, identificadores de proyecto, variables de entorno propietarias y proveedores de infraestructura. Las rutas de archivo del hallazgo de ejemplo *sí* se conservan —el sistema auditado es propio— porque son justo lo que distingue un hallazgo útil de una advertencia genérica.

37/100	21	12/100
RIESGO INICIAL	HALLAZGOS	RIESGO RESIDUAL

SEVERIDAD	CONFIRMADOS	PLAUSIBLES	TOTAL
Crítica	0	0	0
Alta	1	0	1
Media	6	0	6
Baja	6	6	12
Informativa	1	1	2
Total	**14**	**7**	**21**

Nivel OWASP ASVS al inicio: por debajo de L1, con seis capítulos en fallo (V3 sesiones, V4 control de acceso, V5 validación, V7 registro, V12 ficheros, V14 configuración).

Qué hacer primero

Un informe que no ordena las prioridades obliga al cliente a decidir con información que no tiene. Estas son las tres cosas que movían la aguja, en orden.

El hallazgo que manda sobre todos los demás

Los arreglos de endurecimiento existían **solo en el equipo del desarrollador**. La plataforma despliega desde el repositorio, y el último commit publicado seguía declarando la versión vieja del framework —con nueve CVEs conocidas, una de ellas un salto del middleware que era la única capa de autorización del panel—. Traducción operativa: **el sistema en producción no tenía aplicado ninguno de los arreglos**. El trabajo estaba hecho; faltaba publicarlo.

Top 3 acciones prioritarias

1. Publicar los manifiestos de dependencias en un solo commit y desplegar. Cierra dos hallazgos de golpe.
2. Endurecer las cookies de sesión: sin `HttpOnly`, sin `Secure` y con 400 días de vida, el token del administrador era legible desde el navegador y duraba más de un año.
3. Unificar la lista blanca de administradores en una sola fuente de verdad. Había dos listas sin sincronizar: dar de baja a alguien en una no lo revocaba en la otra.

Lo que ya estaba sólido

Un informe honesto también dice qué está bien: firma del webhook correcta y fallando cerrado; las acciones del panel revalidaban autorización en el servidor además del middleware (defensa en profundidad real); control de acceso a nivel de fila bien construido y bucket privado; cero inyección SQL, cero XSS, cero XXE; y ningún secreto en el historial de git, verificado sobre todas las ramas.

Anatomía de un hallazgo

Así se documenta cada uno de los 21. Sin este nivel de detalle, un hallazgo no es accionable: es una preocupación.

CN-006 · Inyección de fórmulas en el CSV exportado MEDIA

Veredicto	CONFIRMADO (CVSS ~6.0)
CWE	CWE-1236 — neutralización incorrecta de elementos de fórmula en un CSV
OWASP	A03:2025 (Inyección) · ASVS V5 Validación y codificación, L1
Ubicación	`src/components/dashboard/gastos-table.tsx:211`
Origen del dato	`src/lib/conversation/state.ts:255`

Descripción. La función que escapa celdas protege comillas y separadores —correcto para el formato CSV— pero no neutraliza los caracteres que Excel, LibreOffice y Google Sheets interpretan como inicio de fórmula (`=` `+` `-` `@`, tabulador, retorno de carro). Los campos exportados «proveedor» y «concepto» los escribe directamente el empleado desde WhatsApp, y se guardan sin ninguna validación.

Escenario de fallo. Un empleado con número autorizado envía una foto y luego responde por WhatsApp con un valor de proveedor que empieza por `=HYPERLINK(...)` apuntando a un servidor externo, y confirma. El valor se guarda tal cual. El administrador entra al panel, pulsa «Exportar CSV» y abre el archivo en Excel: la celda se evalúa como fórmula y, al hacer clic, filtra el contenido de la hoja —montos, proveedores, empleados— al servidor del atacante. Con la variante DDE se llega a ejecución de comandos en la máquina del administrador.

Evidencia — código vulnerable:

```
/** Escapa un campo para CSV (comillas y separadores). */
function csvCell(value: string | number): string {
  const s = String(value);
  if (/[",\r\n]/.test(s)) return `"${s.replace(/"/g, '""')}"`;
  return s;
}
```

Remediación — código propuesto:

```
function csvCell(value: string | number): string {
  let s = String(value);
  // Neutraliza fórmulas: Excel/Sheets evalúan campos que empiezan
  // por = + - @ TAB CR, incluso dentro de comillas.
  if (/^[=+\-@\t\r]/.test(s)) s = `'${s}`;
  if (/[",\r\n]/.test(s)) return `"${s.replace(/"/g, '""')}"`;
  return s;
}
```

Complementario: acotar longitud y rechazar caracteres de control en los dos campos antes de guardarlos.

Del hallazgo a la decisión: tú decides qué se toca

Entre el informe y el endurecimiento hay un paso que casi nadie formaliza. Cada hallazgo vuelve al cliente con la corrección propuesta y el riesgo de que esa corrección afecte a lo que hoy funciona. El cliente marca una sola casilla por fila.

ID	HALLAZGO	SEV.	ARREGLAR	POSPONER	ASUMO RIESGO
CN-004	Lista blanca de administradores duplicada sin sincronizar	Media	☑	☐	☐
CN-006	Inyección de fórmulas en el CSV exportado	Media	☑	☐	☐
CN-010	Teléfonos de empleados (PII) escritos en los registros	Baja	☑	☐	☐
CN-016	La política de contenido permite scripts en línea	Media	☐	☐	☑
–	Validación de formato de fecha en un campo de entrada	Baja	☐	☑	☐

La regla que protege a las dos partes

Si una fila queda sin marcar, no se aplica ningún cambio sobre ese hallazgo: **el silencio no se interpreta como autorización**. Y cuando el cliente elige «asumo el riesgo», queda constancia escrita de que fue informado del hallazgo, de su severidad y de su escenario de fallo. Nadie descubre seis meses después que se tocó algo que no debía tocarse, ni que se dejó algo abierto sin avisar.

Ejemplo real de riesgo aceptado, con condición de reactivación

CN-016 · La política de contenido permite scripts en línea MEDIA RIESGO ACEPTADO

Por qué se aceptó. Solo es explotable si existe un XSS, y el pentest no encontró ninguno: hoy no hay ninguna ruta que renderice HTML controlado por el usuario. El arreglo correcto obliga a un render dinámico que choca con las páginas estáticas y con la librería de gráficos del panel.

Condición de reactivación. Si se introduce una ruta que renderice HTML controlado por el usuario, este hallazgo pasa a **crítico** y hay que migrar antes de desplegarla.

Advertencia incluida en el informe. No aplicar el paliativo habitual: en el nivel 3 de la especificación hace que el navegador ignore la directiva permisiva y, sin el resto del trabajo hecho, bloquearía los scripts que hoy funcionan.

Pentest: qué resultó explotable de verdad

El análisis estático dice qué *podría* fallar. El pentest dice qué *falla*. Se ejecutó sobre un entorno de preview con base de datos separada y datos ficticios; producción quedó excluida por decisión del cliente. La salida de mensajería se desactivó a propósito para que ninguna prueba pudiera escribirle a una persona real.

CN-022 · El bot respondía a cualquier número MEDIA

El destino de los mensajes salientes se tomaba del mensaje entrante y no de la lista de remitentes autorizados. Confirmado en vivo: el sistema intentó responder a un número fuera de la lista.

Corrección: enfriamiento de 12 h por número más límite de tasa global. **Cierre:** arreglado y re-testeado.

CN-023 · El webhook no tenía límite de tasa MEDIA

Treinta peticiones seguidas se atendieron sin una sola respuesta de «demasiadas peticiones».

Corrección: límite con estado en base de datos, global (300/min) y por IP (120/min), aplicado sobre peticiones ya firmadas. **Cierre:** arreglado y re-testeado.

CN-024 · Sin protección contra reenvío (replay) BAJA

Un mismo cuerpo firmado, reenviado, se procesaba de nuevo.

Corrección: deduplicación por identificador de evento con estado en base de datos y limpieza automática. **Cierre:** arreglado y re-testeado.

CN-018 · Eco del parámetro de verificación NO EXPLOTABLE

Un informe honesto también cierra hallazgos en falso: se probó y se confirmó que la respuesta viaja como texto plano con la cabecera que impide reinterpretarla. No es XSS. Queda documentado como **confirmado no explotable**, no como «pendiente».

El resultado que buscaba el cliente

El pentest **no encontró forma de leer datos del panel sin ser un administrador autorizado**. La autorización se aplica ahora en la base de datos, no solo en la aplicación, y resistió el ataque directo a la API saltándose la capa web.

Re-test: la prueba de que quedó cerrado

Aquí es donde la mayoría de los trabajos de seguridad terminan sin terminar. Cada corrección se vuelve a probar contra el sistema en ejecución, no se marca como hecha en una hoja.

PRUEBA	RESULTADO MEDIDO
Control positivo	Evento firmado válido de número autorizado → **procesado**. Descarta el falso aprobado de «rechaza absolutamente todo».
Límite de tasa (CN-023)	140 peticiones firmadas → **27 respuestas 429** y motivo registrado en el log.
Anti-replay (CN-024)	Cuerpo firmado idéntico enviado dos veces → **procesado una sola vez**.
Enfriamiento (CN-022)	Primer aviso enviado, **segundo suprimido** por cooldown.
Autorización (CN-004)	Anónimo → **401**. Administrador legítimo → **entra**.

Por qué existe el control positivo

Un sistema que rechaza todo pasa cualquier prueba de seguridad y no sirve para nada. Por eso cada tanda de pruebas incluye un caso legítimo que *debe* funcionar. Sin él, no se puede distinguir «el control funciona» de «lo rompimos».

Cómo terminó

ESTADO	HALLAZGOS
Arreglados y verificados en la primera pasada	11
Confirmados en pentest, corregidos y re-testeados	4
Higiene adicional aplicada	3
Confirmados no explotables	1
Omitidos por decisión documentada del cliente	2
Riesgo aceptado por el cliente, con condición de reactivación	1
Recomendaciones futuras de baja prioridad	2

Riesgo: de 37/100 (medio) a 12/100 (bajo). Nivel base OWASP ASVS L1 alcanzado. Durante el encargo, el escáner volcó en claro una clave de API de un proveedor externo: se avisó, el cliente la rotó, se verificó el sistema con la clave nueva y se revocó la anterior. También eso va en el informe.

Descargo de responsabilidad

Este informe refleja el estado del sistema en la fecha indicada. Una evaluación de seguridad reduce el riesgo, pero no garantiza la ausencia de vulnerabilidades futuras. **No constituye una certificación ISO/IEC 27001 ni SOC 2**, que requieren una auditoría formal e independiente de la organización. AT Solutions no es entidad certificadora: lo que entrega es una evaluación técnica independiente, útil como base para una auditoría formal si se necesita. Recomendación de re-auditoría: tras el próximo cambio grande y, en cualquier caso, en 6–12 meses.

¿Quieres saber qué tan expuesto estás?
Escribe por WhatsApp al +503 6308 7389 o entra en atsolutions.com.sv/seguridad. Definimos el alcance por escrito antes de tocar nada.