Seguridad de verdad

ASSESSMENT, HARDENING Y PENTEST

Así protejo cada proyecto que construyo — y así trabajo cuando me contratas solo para auditar el tuyo.

Un software que funciona no es lo mismo que un software seguro. La mayoría de las vulnerabilidades no se ven a simple vista: viven en una dependencia desactualizada, una cabecera que falta o un endpoint que nadie revisó a fondo. Este documento explica, sin rodeos, qué hago para encontrarlas, corregirlas y confirmar que ya no están — y qué puedes esperar realmente del servicio.

BAJO QUÉ ESTÁNDARES TRABAJO

OWASP ASVS	**OWASP Top 10**	**CWE Top 25**	**OWASP WSTG**
NIST SP 800-115	**CIS Benchmarks**	**CIS Controls v8**	**Secure Headers**

Cómo trabajo: tres fases, en este orden

No vendo un pentest suelto ni una auditoría genérica. Trabajo en tres fases que se complementan — cada una encuentra o corrige algo distinto, y juntas dan una foto honesta del estado real de tu seguridad.

1

Evaluación de vulnerabilidades (Assessment)

Reviso tu código y tu configuración sin ejecutar ni modificar nada: dependencias desactualizadas, secretos expuestos en el repositorio, errores comunes de programación insegura (inyección, XSS, control de acceso roto) y fallos de configuración. Es una radiografía — diagnostica, no opera.

Estándares: OWASP ASVS, OWASP Top 10 2025, CWE Top 25.

2

Hardening (aplicación de controles)

Con el diagnóstico en mano, aplico un set de controles probado: cabeceras de seguridad, gestión correcta de credenciales, configuración segura de contenedores, permisos mínimos, políticas de acceso. Esta fase sí modifica tu proyecto — y verifico que todo siga compilando y funcionando después de cada cambio.

Estándares: CIS Benchmarks, CIS Controls v8, OWASP Secure Headers, OWASP Proactive Controls.

3

Pentest (prueba de penetración)

Pruebo tu aplicación en vivo, de forma controlada, para confirmar qué vulnerabilidades son realmente explotables y no solo teóricas. Esta fase requiere tu autorización por escrito y un entorno de pruebas —

normalmente tu ambiente de preview, nunca producción sin acuerdo expreso.

Estándares: OWASP WSTG, NIST SP 800-115.

Qué recibes

- ✓ Informe técnico con cada hallazgo: severidad, evidencia, pasos para reproducirlo y cómo corregirlo.
- ✓ Resumen ejecutivo sin jerga técnica, pensado para quien toma la decisión de presupuesto.
- ✓ El nivel de verificación OWASP ASVS (L1, L2 o L3) que tu aplicación alcanza hoy, con lo que falta para subir de nivel.
- ✓ Opcional: un mapeo de los hallazgos hacia NIST CSF, ISO/IEC 27001, SOC 2 o CIS Controls, si lo necesitas para una auditoría propia o de un cliente tuyo.
- ✓ Acompañamiento para aplicar las correcciones, si decides contratarlo.

Lo que este servicio NO es

Prefiero que sepas esto antes de contratarme, no después:

- – No es una certificación. Ni ISO/IEC 27001 ni SOC 2 se obtienen con un assessment o un pentest: esas certifican a toda una organización mediante una auditoría formal independiente. Lo que entrego es evidencia técnica que te acerca a ese estándar, no el certificado en sí.
- – No es una garantía de cero vulnerabilidades futuras. La seguridad no es un estado fijo, es un proceso: cada línea de código nueva, cada dependencia actualizada, puede introducir un riesgo nuevo.
- – El pentest tiene límites claros por diseño. Solo pruebo lo que está autorizado por escrito, en la ventana de tiempo acordada y bajo reglas que evitan tumbar tu sistema o exponer datos reales de tus usuarios.
- – No sustituye asesoría legal. Si necesitas cumplimiento regulatorio formal (protección de datos, normativa sectorial), te entrego hallazgos técnicos — la interpretación legal la debe dar un abogado.

Cómo empezamos

- Conversamos sobre tu proyecto y qué necesitas: solo diagnóstico, solo endurecerlo, solo probarlo en vivo, o las tres fases juntas.
- Firmamos un Acuerdo de Autorización — el marco que me da permiso explícito y por escrito para trabajar sobre tus sistemas, con el alcance y las reglas bien definidas.
- Ejecuto el servicio acordado y te mantengo informado si algo relevante aparece en el camino.
- Te entrego el informe y, si quieres, te acompaño a implementar las correcciones.

Si quieres saber en qué punto está la seguridad de tu producto, hablemos.

[correo / formulario de contacto / web]