

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://insumac.vercel.app/
Dominio insumac.vercel.app
Fecha 28 de agosto de 2026 a las 20:14

Checks 9 pruebas
Hallazgos 45 totales
Problemas 3 detectados

A

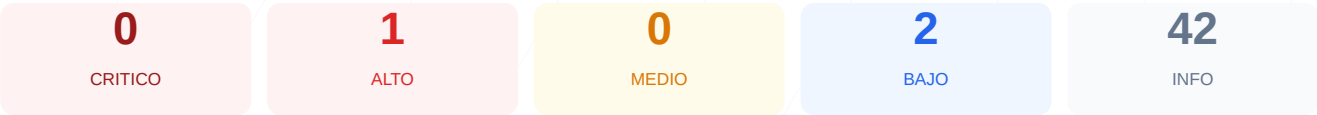
95/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta un nivel de seguridad sobresaliente, obteniendo una puntuacion de 95/100 y una nota A. Durante la auditoria se ejecutaron 9 checks pasivos, resultando 7 de ellos exitosos y 2 con advertencias menores. No se detectaron fallos criticos ni vulnerabilidades de alta severidad que pongan en riesgo inmediato la operacion. El analisis concluye que el sitio es seguro, aunque requiere ajustes puntuales en las cabeceras de seguridad y configuracion de archivos de rastreo. Se recomienda aplicar las medidas correctivas para mitigar riesgos potenciales de reconocimiento y ataques de clickjacking.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: X-Frame-Options
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
90 dias restantes (expira: 2026-11-26T14:14:16.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-28T14:14:17.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: X-Frame-Options

- BAJO Server header expuesto
Server: Vercel — Revela tecnologia del servidor

- BAJO

X-Powered-By expuesto
X-Powered-By: Next.js — Revela framework/lenguaje
- INFO

Content-Security-Policy
Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https://www.googletagmanag...
- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- INFO

Strict-Transport-Security
Presente: max-age=63072000; includeSubDomains; preload
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 308 redirige a https://insumac.vercel.app/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=63072000 (730 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado
- INFO

Tecnologias detectadas
React, Next.js, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO

Archivo /readme.html
No accesible (correcto)

- INFO

Archivo /README.txt

No accesible (correcto)
- INFO

Version CMS

No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO

Cookies detectadas

El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO

Contenido mixto

Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO

sitemap.xml

Presente, 168 URLs
- BAJO

security.txt

No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- INFO

Puerto 21 (FTP)

Cerrado — Transferencia de archivos sin cifrar
- INFO

Puerto 22 (SSH)

Cerrado — Acceso remoto seguro
- INFO

Puerto 23 (Telnet)

Cerrado — Acceso remoto sin cifrar
- INFO

Puerto 25 (SMTP)

Cerrado — Envio de correo
- INFO

Puerto 80 (HTTP)

Abierto (esperado) — Servidor web
- INFO

Puerto 443 (HTTPS)

Abierto (esperado) — Servidor web seguro
- INFO

Puerto 3306 (MySQL)

Cerrado — Base de datos MySQL expuesta
- INFO

Puerto 3389 (RDP)

Cerrado — Escritorio remoto Windows
- INFO

Puerto 5432 (PostgreSQL)

Cerrado — Base de datos PostgreSQL expuesta
- INFO

Puerto 6379 (Redis)

Cerrado — Cache Redis sin autenticacion por defecto
- INFO

Puerto 8080 (HTTP-Alt)

Cerrado — Servidor web alternativo / proxy
- INFO

Puerto 27017 (MongoDB)

Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en iframes de dominios maliciosos, facilitando ataques de clickjacking.

[LOW] Server header expuesto: El encabezado Server revela el uso de Vercel, proporcionando informacion tecnica sobre la infraestructura que puede ser utilizada en fases de reconocimiento.

[LOW] X-Powered-By expuesto: Se expone el uso del framework Next.js, lo que permite a un atacante identificar posibles vectores de ataque especificos para dicha tecnologia.

[LOW] Robots.txt faltante: La falta de este archivo impide definir reglas de indexacion para motores de busqueda, lo que podria resultar en el rastreo de areas no deseadas.