EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://invotecsa.com	Checks	9 pruebas
Dominio	invotecsa.com	Hallazgos	41 totales
Fecha	23 de junio de 2026 a las 21:38	Problemas	10 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad para el dominio evaluado ha resultado en una puntuación de 71/100 con una calificación de nota C. Los checks pasivos ejecutados identificaron un total de 9 validaciones, de las cuales 5 resultaron satisfactorias, 1 generó advertencias y 1 falló críticamente. Aunque el sitio cuenta con cifrado de tráfico activo, existen deficiencias importantes en las cabeceras de seguridad y exposición de información técnica. Se concluye que el sitio es vulnerable ante ataques de inyección y suplantación de identidad debido a una configuración de servidor incompleta.

Resumen de Riesgos

0	3	4	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 dias
Cabeceras de Seguridad	10	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  56 dias restantes (expira: 2026-08-19T04:13:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-21T03:14:45.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 10/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33 — Revela framework/lenguaje

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.8.5
- INFO **Tecnologias detectadas**
  Next.js, PHP/7.4.33

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1831 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 2 Allow

- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://invotecsa.com/index.php/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta — Previene XSS y ataques de inyección de contenido al restringir fuentes permitidas.
[HIGH] X-Frame-Options: Falta — Protege contra ataques de clickjacking al evitar que el sitio se cargue en iframes externos.
[HIGH] Strict-Transport-Security: Falta — No fuerza conexiones seguras mediante HSTS, permitiendo posibles ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Falta — Evita que el navegador realice MIME-type sniffing y ejecute archivos maliciosos.
[MEDIUM] Permissions-Policy: Falta — No restringe el uso de APIs sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Puerto 8080 (HTTP-Alt): ABIERTO — El acceso a un puerto de servidor alternativo o proxy aumenta la superficie de ataque.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el sitio, lo que sugiere una posible mala configuración de visibilidad.
[LOW] Server header expuesto: Revela el uso de Cloudflare, permitiendo a atacantes dirigir vectores específicos contra esta infraestructura.
[LOW] X-Powered-By expuesto: Revela el uso de PHP/7.4.33, lo cual facilita la búsqueda de vulnerabilidades conocidas para esa versión.
[LOW] Meta generator: Expone la versión WordPress 6.8.5, facilitando el reconocimiento de versiones de CMS por parte de atacantes.