

Escanear Vulnerabilidades

Informe de Seguridad Web

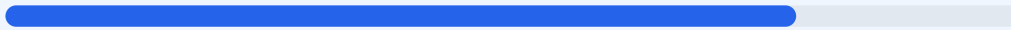
URL https://cazanga.com.br/
Dominio cazanga.com.br
Fecha 5 de junio de 2026 a las 13:02

Checks 9 pruebas
Hallazgos 47 totales
Problemas 8 detectados

B

78/100

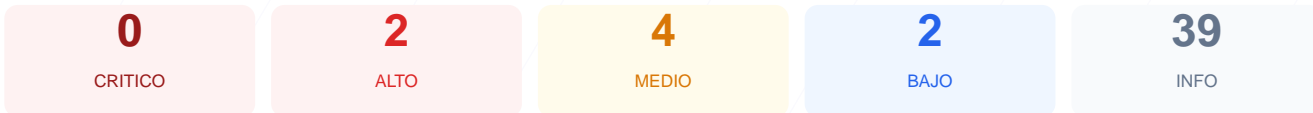
puntos de seguridad



RESUMEN EJECUTIVO

El sitio web analizado ha obtenido una puntuacion de 78/100 con una calificacion de grado B, lo que indica un nivel de seguridad aceptable pero con margenes de mejora importantes. Durante la auditoria se ejecutaron 9 checks pasivos, de los cuales 6 resultaron exitosos, 1 genero una advertencia y 2 fallaron debido a configuraciones incorrectas. Aunque la base de cifrado y transporte es solida, la exposicion de informacion tecnica y la falta de cabeceras de proteccion modernas son puntos criticos. Se concluye que el sitio es parcialmente vulnerable a ataques de reconocimiento y ataques de inyeccion de contenido.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 48 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 8 expuesta, WordPress 2 expuesta
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 48 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
48 dias restantes (expira: 2026-07-23T01:50:25.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-24T01:50:26.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: cloudflare — Revela tecnologia del servidor

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyeccion de contenido
- **INFO** **X-Frame-Options**
Presente: SAMEORIGIN
- **INFO** **Strict-Transport-Security**
Presente: max-age=31557600
- **INFO** **X-Content-Type-Options**
Presente: nosniiff
- **MEDIO** **Referrer-Policy**
Falta — Controla la informacion de referer enviada
- **MEDIO** **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://cazanga.com.br/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31557600
- **BAJO** **HSTS includeSubDomains**
HSTS no cubre subdominios
- **INFO** **HSTS max-age**
max-age=31557600 (365 dias)
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- **INFO** **WordPress**
Detectado via HTML body
- **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
- **BAJO** **Meta generator**
Expone: Elementor 4.1.1.1; features: additional_custom_breakpoints; settings: css_print_method-external, google_font-enabled, font_display-auto
- **INFO** **Tecnologias detectadas**
Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 8 expuesta, WordPress 2 expuesta

- **ALTO** **WordPress version**
Version 8 expuesta publicamente — Permite a atacantes buscar CVEs conocidos

- MEDIO** Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO** Archivo /README.txt
No accesible (correcto)

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 (172 bytes)
- INFO** Reglas robots.txt
1 Disallow, 0 Allow
- INFO** Sitemap en robots.txt
https://cazanga.com.br/sitemap_index.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 esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyeccion de datos.
- [HIGH] WordPress version: La version 8 del CMS se encuentra expuesta publicamente, facilitando la busqueda de exploits conocidos por atacantes.
- [MEDIUM] Referrer-Policy: No se detecto esta cabecera, lo que impide controlar que informacion de origen se envia a otros sitios.
- [MEDIUM] Permissions-Policy: Ausencia de restricciones para APIs del navegador como camara o microfono, aumentando el riesgo de privacidad.
- [MEDIUM] Archivo /readme.html: Este archivo es accesible de forma publica y puede revelar detalles tecnicos especificos de la instalacion.
- [MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, funcionando como un servidor web alternativo que amplia la superficie de ataque.
- [LOW] Server header expuesto: Se detecto la cabecera Server: cloudfare, revelando detalles sobre la infraestructura de red utilizada.
- [LOW] Meta generator: Se exponen metadatos de Elementor 4.1.1 y configuraciones de fuentes, lo que ayuda en el perfilado del sitio por parte de terceros.