EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://centroaleman.org	Checks	9 pruebas
Dominio	centroaleman.org	Hallazgos	43 totales
Fecha	10 de julio de 2026 a las 02:51	Problemas	11 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio centroaleman.org ha obtenido una puntuación de 68/100, lo que representa una calificación de grado C en su postura de seguridad actual. Los resultados de los 9 checks pasivos ejecutados muestran un desempeño mixto, con 5 validaciones exitosas, 2 advertencias y 1 fallo crítico por tiempo de espera. Aunque el cifrado SSL es robusto, la ausencia total de cabeceras de seguridad y la exposición de puertos innecesarios comprometen la protección del servidor. Se concluye que el sitio es actualmente vulnerable a ataques de suplantación e inyección debido a configuraciones de seguridad incompletas.

Resumen de Riesgos

0	4	4	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 43 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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 43 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  43 dias restantes (expira: 2026-08-22T06:03:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-24T05:03:55.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, 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

- 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
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://centroaleman.org/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

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 7.0
- INFO **Tecnologias detectadas**
  React, Next.js

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 (266 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://centroaleman.org/wp-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 esta cabecera esencial para prevenir ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] X-Frame-Options: La ausencia de esta protección permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se detectó la política HSTS, lo que impide obligar al navegador a usar siempre conexiones seguras.
[HIGH] HSTS (Strict-Transport-Security): El sistema de redirección no fuerza el protocolo HTTPS de manera estricta, permitiendo posibles interceptaciones.
[MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, el sitio es vulnerable a ataques de sniffing de tipo MIME para ejecutar archivos maliciosos.
[MEDIUM] Referrer-Policy: No hay control sobre la información de origen que se envía a otros dominios, lo que puede filtrar datos de navegación.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó el puerto 8080 abierto, lo cual suele indicar un servicio alternativo o proxy expuesto que aumenta la superficie de ataque.
[LOW] Meta generator expuesto: El sitio revela públicamente el uso de WordPress 7.0, facilitando a atacantes la búsqueda de exploits específicos para esa versión.
[LOW] Server header expuesto: Se identifica el uso de Cloudflare, lo que proporciona información técnica sobre la infraestructura de red.
[LOW] Ruta sensible en robots.txt: El archivo incluye una referencia directa a la ruta admin, guiando a posibles atacantes hacia el panel de gestión.