EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://centerltda.cl	Checks	9 pruebas
Dominio	centerltda.cl	Hallazgos	25 totales
Fecha	7 de mayo de 2026 a las 04:41	Problemas	7 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de ciberseguridad realizado sobre el sitio web ha dado como resultado una puntuación de 71/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 3 resultaron satisfactorios y 1 presentó fallos críticos de configuración, mientras que el resto no pudo completarse por tiempo de espera. Aunque el cifrado de datos es correcto, la ausencia de múltiples capas de protección en las cabeceras de respuesta compromete la robustez del sitio. Se concluye que el sitio es vulnerable a ataques de inyección y suplantación de identidad debido a estas carencias en las políticas de seguridad del servidor. Es necesario implementar las medidas correctivas detalladas para mitigar los riesgos de explotación activa.

Resumen de Riesgos

0	2	3	2	18
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Seguridad de Cookies	100	OK	No se encontraron cookies
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-07-14T08:03:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-15T08:03:33.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.20 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking

- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubdomains;
- 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.)

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Content-Security-Policy: La ausencia de esta cabecera permite que el sitio sea susceptible a ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] X-Frame-Options: Al no estar presente, el sitio carece de protección contra ataques de clickjacking, permitiendo que atacantes embeban el sitio en marcos maliciosos.
[MEDIUM] X-Content-Type-Options: La falta de esta instrucción impide que el navegador bloquee intentos de sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que puede provocar la filtración involuntaria de información de navegación hacia dominios de terceros.
[MEDIUM] Permissions-Policy: La carencia de esta cabecera permite que el navegador mantenga acceso a APIs sensibles del dispositivo del usuario sin restricciones impuestas por el servidor.
[LOW] Server header expuesto: El servidor responde con la cabecera Server: Apache, lo que facilita a los atacantes identificar el software base y buscar exploits específicos.
[LOW] X-Powered-By expuesto: La cabecera revela el uso de PHP/8.4.20, exponiendo la tecnología y versión exacta del lenguaje de programación utilizado en el backend.