EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://carabineros.cl	Checks	9 pruebas
Dominio	carabineros.cl	Hallazgos	15 totales
Fecha	6 de agosto de 2026 a las 02:34	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio web carabineros.cl ha resultado en una puntuacion de 73/100, otorgando una nota de C. El analisis se baso exclusivamente en la ejecucion de 9 checks pasivos, los cuales detectaron una configuracion deficiente en los protocolos de cifrado y la ausencia de archivos de gestion de indexacion. Solo un parametro fue aprobado satisfactoriamente, mientras que el resto de las comprobaciones presentaron fallos criticos de conectividad y configuracion. Debido a la incapacidad de validar la seguridad SSL y las cabeceras de proteccion, se concluye que el sitio es actualmente vulnerable y requiere intervencion inmediata.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

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

[CRITICA] Conexion SSL/TLS: No fue posible establecer una conexion segura, lo que impide garantizar la confidencialidad de los datos transmitidos entre el usuario y el servidor.
[CRITICA] Cabeceras de Seguridad: No se detectaron cabeceras HTTP esenciales, dejando la plataforma expuesta a ataques de clickjacking, inyeccion de codigo y robo de sesiones.
[CRITICA] Redireccion HTTPS: El sitio no fuerza el trafico cifrado, permitiendo potenciales ataques de intermediario (Man-in-the-Middle) al navegar por canales inseguros.
[CRITICA] Seguridad de Cookies: La falta de validacion en las cookies sugiere que informacion sensible de sesion podria ser capturada por terceros.
[BAJA] Ausencia de robots.txt: No existe el archivo de exclusion de rastreadores, lo que compromete el control sobre que partes del servidor son indexadas por buscadores.
[BAJA] Ausencia de sitemap.xml: La falta de un mapa del sitio dificulta la correcta estructuracion de los contenidos y su supervision automatizada.