EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cardsouls.cl/	Checks	9 pruebas
Dominio	www.cardsouls.cl	Hallazgos	65 totales
Fecha	6 de agosto de 2026 a las 02:32	Problemas	13 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad web realizada al sitio ha arrojado una puntuacion de 84/100, lo que otorga una nota B de rendimiento de seguridad. Se ejecutaron 9 checks pasivos de los cuales 5 resultaron correctos y 4 generaron advertencias tecnicas por configuraciones suboptimas. No se detectaron fallos criticos de seguridad de manera inmediata, manteniendo una base solida en la encriptacion de datos. Sin embargo, la presencia de cookies inseguras y contenido mixto indica que el sitio es parcialmente vulnerable a ataques de secuestro de sesion o degradacion de protocolos. En conclusion, el sitio web es funcionalmente seguro para el uso general, pero requiere intervenciones tecnicas para alcanzar un estandar de proteccion robusto.

Resumen de Riesgos

0	6	5	2	52
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Shopify
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	localization: falta HttpOnly; localization: falt...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
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 42 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  42 dias restantes (expira: 2026-09-17T00:17:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-19T00:17:03.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=7889238
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://www.cardsouls.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=7889238
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=7889238 (91 dias) — Recomendado minimo 180 dias
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Shopify

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  Detectado via HTML body
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

localization: falta HttpOnly; localization: falta Secure; _shopify_y: falta HttpOnly; _shopify_y: falta Secure; _shopify_s: falta HttpOnly; _shopify_s: falta Secure

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- ALTO **Cookie: localization — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: localization — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: localization — SameSite**
  SameSite=lax
- ALTO **Cookie: _shopify_y — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: _shopify_y — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: _shopify_y — SameSite**
  SameSite=lax
- ALTO **Cookie: _shopify_s — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: _shopify_s — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: _shopify_s — SameSite**
  SameSite=lax
- INFO **Cookie: _shopify_essential — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_essential — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_essential — SameSite**
  SameSite=lax
- INFO **Cookie: _shopify_analytics — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_analytics — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_analytics — SameSite**
  SameSite=lax
- INFO **Cookie: _shopify_marketing — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_marketing — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_marketing — SameSite**
  SameSite=lax

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://es.shopify.com?utm_campaign=poweredby&utm_medium=...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (3630 bytes)

- INFO **Reglas robots.txt**
  50 Disallow, 35 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.cardsouls.cl/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] Cookies sin flags HttpOnly y Secure: Las cookies localization, _shopify_y y _shopify_s no tienen proteccion contra scripts ni obligan al envio por canales seguros, permitiendo potenciales ataques XSS y robo de sesion.
[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: Se detecto un puerto de servidor web alternativo expuesto, lo que amplia la superficie de ataque y podria revelar servicios internos no protegidos.
[MEDIUM] Contenido Mixto detectado: Un recurso de Shopify se carga mediante HTTP en lugar de HTTPS, lo que compromete la integridad de la navegacion segura y puede ser bloqueado por navegadores modernos.
[MEDIUM] Falta de cabecera Referrer-Policy: El sitio no instruye al navegador sobre cuanta informacion de referencia debe enviarse, lo que podria comprometer la privacidad de los usuarios al navegar hacia enlaces externos.
[MEDIUM] Falta de cabecera Permissions-Policy: No existe una directiva que restrinja el uso de APIs del navegador como la camara o el microfono, permitiendo que potenciales vulnerabilidades de terceros abusen de estas funciones.
[MEDIUM] HSTS con tiempo de vida insuficiente: El parametro max-age esta configurado en 91 dias, cuando el estandar de seguridad recomendado para una proteccion optima es de al menos 180 dias.
[LOW] Exposicion de cabecera Server: Se revela el uso de Cloudflare como tecnologia de servidor, facilitando a posibles atacantes informacion sobre la infraestructura de red utilizada.
[LOW] Ruta administrativa en robots.txt: Se hace referencia directa al directorio admin en el archivo de rastreo, lo que ayuda a recolectar informacion sobre la estructura de gestion del sitio.