EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://saladillocuida.ar/	Checks	9 pruebas
Dominio	saladillocuida.ar	Hallazgos	44 totales
Fecha	16 de agosto de 2026 a las 20:30	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio saladillocuida.ar arrojó una puntuación de 59/100, lo que equivale a una calificación de nota D. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fallaron críticamente. El sitio presenta una configuración deficiente en cuanto a la protección del transporte de datos y la implementación de cabeceras de seguridad esenciales. Debido a la falta de redirección forzada a HTTPS y la ausencia total de políticas de seguridad en el servidor, el sitio se considera vulnerable ante ataques de interceptación y suplantación.

Resumen de Riesgos

0	5	5	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 35 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 35 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  35 dias restantes (expira: 2026-09-20T23:56:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-22T23:56:47.000Z
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- 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

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 — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1836 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] Falta de redirección HTTPS: El servidor permite conexiones inseguras a través de HTTP sin redirigir automáticamente al protocolo cifrado.
[HIGH] Falta de Strict-Transport-Security: No se informa al navegador que debe usar exclusivamente HTTPS, facilitando ataques de degradación de conexión.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.

[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea embebido en marcos externos sin restricciones.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de un puerto alternativo incrementa la superficie de ataque y revela posibles servicios internos o proxies.
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Bloqueo total en robots.txt: El archivo de configuración bloquea el acceso a todos los rastreadores, lo que impide la indexación legítima del sitio.
[MEDIUM] Falta de Referrer-Policy: No se controla qué información de origen se envía cuando el usuario navega hacia enlaces externos.
[MEDIUM] Falta de Permissions-Policy: El servidor no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono.
[LOW] Cabecera de servidor expuesta: El sitio revela que utiliza tecnología Cloudflare, lo que asiste a un atacante en la fase de reconocimiento.
[LOW] Falta de sitemap.xml: La ausencia de este archivo dificulta la auditoría de la estructura del sitio y su correcta visibilidad técnica.