EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://senorial.com.ar	Checks	9 pruebas
Dominio	senorial.com.ar	Hallazgos	38 totales
Fecha	24 de abril de 2026 a las 12:29	Problemas	8 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web senorial.com.ar arroja una puntuación de 72/100, lo que corresponde a una calificación de grado C. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias y 2 presentaron fallos críticos. Aunque la infraestructura base de cifrado es sólida, el sitio carece por completo de políticas de endurecimiento en el servidor. Debido a la ausencia de cabeceras de seguridad esenciales y problemas de redirección, el sitio se considera actualmente vulnerable ante ataques de inyección y suplantación. No se realizó un pentest activo, por lo que podrían existir vulnerabilidades lógicas adicionales no detectadas.

Resumen de Riesgos

0	3	3	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-07-15T03:36:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-16T02:45:09.000Z
- 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

- 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.)

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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

[ALTA] Content-Security-Policy: Esta cabecera está ausente, lo que permite la ejecución de scripts no autorizados y aumenta drásticamente el riesgo de ataques Cross-Site Scripting (XSS).
[ALTA] X-Frame-Options: La falta de esta configuración hace que el sitio sea susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.
[ALTA] Strict-Transport-Security: Al no estar presente, el servidor no obliga al navegador a usar conexiones HTTPS cifradas, facilitando ataques de degradación de protocolo.
[MEDIA] X-Content-Type-Options: La ausencia de esta cabecera permite el MIME-type sniffing, lo que podría llevar al navegador a interpretar archivos de forma incorrecta y ejecutar código malicioso.
[MEDIA] Referrer-Policy: No se ha definido una política de referencia, lo que provoca que información sensible sobre la procedencia de la navegación pueda filtrarse a terceros.
[MEDIA] Permissions-Policy: No se restringe el acceso a funciones del navegador como la cámara o el micrófono, dejando expuesta la privacidad del usuario ante posibles scripts maliciosos.
[BAJA] Robots.txt y Sitemap: Ambos archivos devolvieron un error HTTP 403, lo que impide una indexación correcta y sugiere configuraciones de permisos de archivos deficientes.