

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://reviews.saona.es	Checks	9 pruebas
Dominio	reviews.saona.es	Hallazgos	45 totales
Fecha	16 de julio de 2026 a las 16:36	Problemas	8 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha arrojado una puntuación de 88/100, lo que equivale a una nota B. El análisis se basó en 9 checks pasivos, de los cuales 7 resultaron satisfactorios, uno presentó advertencias y otro fue calificado como fallo. Aunque el cifrado de datos y las redirecciones son correctos, existen carencias en las políticas de seguridad del navegador y exposición de rutas técnicas. En conclusión, el sitio es mayoritariamente seguro pero vulnerable a ataques específicos de inyección y reconocimiento debido a configuraciones incompletas.

Resumen de Riesgos

0	1	6	1	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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 90 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
90 dias restantes (expira: 2026-10-14T10:32:28.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-16T10:32:29.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: nginx/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=31536000
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- 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://reviews.saona.es/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 dias)
- 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

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente

- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente
- 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

- INFO

security.txt
Presente en /.well-known/security.txt — Buena practica

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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido XSS.

[MEDIUM] Permissions-Policy: Falta esta cabecera que restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.

[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles de forma pública y pueden filtrar información sobre la infraestructura interna o versiones del software.

[MEDIUM] Rutas de administración expuestas: Se detectó acceso público a /wp-login.php, /administrator/ y /user/login, lo que facilita ataques de fuerza bruta contra las credenciales.

[LOW] Server header expuesto: La cabecera Server revela el uso de nginx/1.24.0 sobre Ubuntu, proporcionando datos valiosos para que un atacante busque exploits específicos.

[LOW] Ausencia de Robots.txt y Sitemap: El fallo en estos archivos impide una correcta guía de indexación para buscadores y puede exponer áreas que deberían permanecer privadas.