EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://secretaria@seen.es	Checks	9 pruebas
Dominio	seen.es	Hallazgos	22 totales
Fecha	10 de agosto de 2026 a las 10:14	Problemas	3 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada otorga al sitio una puntuacion exacta de 77/100, lo que corresponde a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resulto correcto, 3 generaron advertencias y no se registraron fallos criticos inmediatos. El analisis revela una base solida en cuanto a cifrado basico, aunque persisten deficiencias en la configuracion avanzada del servidor. En conclusion, el sitio se considera moderadamente seguro, pero presenta vectores de riesgo que requieren atencion para evitar interceptaciones de datos.

Resumen de Riesgos

0	2	0	1	19
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 136 dias
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 136 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  136 dias restantes (expira: 2026-12-23T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-08T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.seen.es/

- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, 202 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] HSTS (Strict-Transport-Security): Esta cabecera no esta configurada, lo que impide que el navegador fuerce conexiones HTTPS y permite ataques de degradacion de SSL.
[ALTA] Puerto 21 (FTP): El puerto se encuentra abierto, lo que es peligroso porque este protocolo transfiere archivos y credenciales en texto plano sin cifrar.
[BAJA] robots.txt: No se encontro el archivo en el servidor, lo que dificulta el control sobre que partes del sitio deben o no ser indexadas por buscadores.