EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://seidor.es	Checks	9 pruebas
Dominio	seidor.es	Hallazgos	47 totales
Fecha	28 de abril de 2026 a las 07:59	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 68/100, lo que resulta en una calificación de nota C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron clasificados como fallos críticos. Aunque la infraestructura base y el cifrado inicial son correctos, se han detectado ausencias graves en las políticas de seguridad del lado del servidor. Debido a la carencia total de cabeceras de protección esenciales, se concluye que el sitio es actualmente vulnerable a ataques de inyección, suplantación de identidad y secuestro de clics.

Resumen de Riesgos

0	4	4	4	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 286 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Drupal
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	__cf_bm: falta SameSite
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 286 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  286 dias restantes (expira: 2027-02-07T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-07T00:00:00.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js — Revela framework/lenguaje
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

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

CMS detectado: Drupal

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

__cf_bm: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __cf_bm — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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

[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera permite la ejecución de scripts maliciosos (XSS) y ataques de inyección de contenido.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a clickjacking, permitiendo que atacantes embeban la web en marcos externos para engañar al usuario.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones HTTPS, permitiendo posibles ataques de degradación de SSL.
[HIGH] HSTS no configurado: El servidor redirige a HTTPS pero no establece la directiva de persistencia de seguridad en el navegador del cliente.
[MEDIUM] X-Content-Type-Options: Falta — Permite que el navegador intente adivinar el tipo de contenido (MIME-sniffing), lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: Falta — No se controla qué información de procedencia se envía a otros sitios, lo que puede filtrar URLs privadas o sensibles.
[MEDIUM] Permissions-Policy: Falta — No se restringen las capacidades del navegador como el acceso a la cámara, micrófono o geolocalización desde el sitio.
[MEDIUM] Cookie __cf_bm: Falta SameSite — Esta cookie de Cloudflare sin el atributo SameSite es susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] Server header expuesto: El valor Server: cloudflare revela detalles de la infraestructura que facilitan el reconocimiento por parte de atacantes.
[LOW] X-Powered-By expuesto: El valor X-Powered-By: Next.js revela el framework utilizado, permitiendo búsquedas dirigidas de exploits específicos.
[LOW] robots.txt: No encontrado — La ausencia de este archivo impide dar instrucciones claras a los rastreadores y puede exponer rutas que no deberían ser indexadas.
[LOW] sitemap.xml: No encontrado — Dificulta la auditoría de contenidos y la correcta indexación de la estructura del sitio por parte de motores de búsqueda.