EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://davidsmh.es/	Checks	9 pruebas
Dominio	davidsmh.es	Hallazgos	48 totales
Fecha	5 de agosto de 2026 a las 12:10	Problemas	7 detectados

A

94/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 94/100 con una calificación de nota A. Se ejecutaron 9 procesos de revisión pasiva, resultando en 7 evaluaciones satisfactorias y 2 advertencias relacionadas con la exposición de información y puertos. El sitio web demuestra una implementación robusta de protocolos de cifrado y cabeceras de protección. Se concluye que el sitio es seguro en sus fundamentos de comunicación, aunque presenta vectores de información pública que deben ser mitigados para evitar ataques de reconocimiento.

Resumen de Riesgos

0	0	3	4	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	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 65 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  65 dias restantes (expira: 2026-10-09T21:45:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-11T20:46:35.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'none'; script-src 'nonce-z7bIQIk4bm9cuQlYbFcc97' 'unsafe-eval' http...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://davidsmh.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 (17223 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[MEDIUM] Archivo /README.txt: El archivo es accesible públicamente, lo cual es peligroso porque puede revelar versiones de software e información técnica interna del servidor.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: La presencia de un servidor web alternativo o proxy abierto puede ser utilizada para evadir controles de seguridad o exponer servicios administrativos.
[MEDIUM] Bloqueo total en robots.txt: La directiva Disallow: / intenta ocultar todo el sitio, lo cual suele atraer la atención de atacantes hacia contenido que se pretende proteger.
[LOW] Cabecera de servidor expuesta: Se identifica el uso de Cloudflare en la cabecera Server, lo cual facilita a un atacante el reconocimiento de la infraestructura tecnológica.
[LOW] Referencia a rutas sensibles en robots.txt: Se mencionan explícitamente rutas como admin y config, exponiendo posibles puntos de entrada críticos a actores maliciosos.
[LOW] Ausencia de sitemap.xml: El mapa del sitio no fue encontrado (error 403), lo que impide una auditoría clara de las rutas legítimas del servidor.