EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://conductoresprofesionales.es	Checks	9 pruebas
Dominio	conductoresprofesionales.es	Hallazgos	50 totales
Fecha	17 de agosto de 2026 a las 13:49	Problemas	11 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha resultado en una puntuación de 89/100, lo que otorga una calificación de grado B. El análisis se basó en 9 comprobaciones pasivas, de las cuales 6 finalizaron correctamente y 3 generaron advertencias de seguridad, sin detectarse fallos críticos de denegación de servicio o certificados inválidos. Aunque la base del cifrado es sólida, existen riesgos considerables en la configuración de la infraestructura del servidor. Por lo tanto, se concluye que el sitio es generalmente seguro para el usuario final, pero presenta vulnerabilidades técnicas en el backend que deben ser subsanadas para evitar intrusiones.

Resumen de Riesgos

1	1	4	5	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 43 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Drupal
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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 43 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  43 dias restantes (expira: 2026-09-29T22:31:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-01T22:31:35.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=1000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- 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://conductoresprofesionales.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=1000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=1000 (0 dias) — Recomendado minimo 180 dias
- 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**
  PHP/8.3.30

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)
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (2027 bytes)
- INFO **Reglas robots.txt**
  34 Disallow, 18 Allow
- 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 500)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): La base de datos está abierta a conexiones externas, permitiendo intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos activo sin cifrado, lo que permite la interceptación de credenciales y datos en la red.
[MEDIUM] Referrer-Policy: Falta esta cabecera de seguridad, lo que puede provocar la filtración involuntaria de información de navegación a sitios externos.
[MEDIUM] Permissions-Policy: Cabecera ausente, lo que impide restringir el acceso del navegador a funciones sensibles como la geolocalización o la cámara.
[MEDIUM] HSTS max-age: El valor de duración está configurado en cero, invalidando la protección de transporte estricto de HTTP frente a ataques de degradación.
[MEDIUM] Ruta /user/login: El panel de acceso administrativo de Drupal es visible públicamente, aumentando la superficie de ataque para accesos ilícitos.
[LOW] Server header expuesto: El servidor revela el uso de LiteSpeed, facilitando a un atacante la búsqueda de exploits específicos para esa tecnología.
[LOW] X-Powered-By expuesto: Se muestra la versión exacta de PHP/8.3.30, lo que permite perfilar el entorno de ejecución del sitio.
[LOW] Rutas sensibles en robots.txt: El archivo menciona directorios como admin y config, guiando potencialmente a un atacante hacia áreas restringidas.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado (HTTP 500), lo que sugiere un error de configuración interna en el CMS.