# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://shieldaudit.es | Checks | 9 pruebas |
| Dominio | shieldaudit.es | Hallazgos | 48 totales |
| Fecha | 14 de mayo de 2026 a las 12:31 | Problemas | 14 detectados |

**C**

72/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio shieldaudit.es ha arrojado una puntuación de 72/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos de seguridad. Los hallazgos principales indican deficiencias en la configuración de cabeceras de seguridad y una exposición de puertos críticos en el servidor. Debido a la visibilidad de la versión del CMS y servicios de base de datos, el sitio se considera actualmente vulnerable ante ataques dirigidos.

## Resumen de Riesgos

| 1 | 5 | 4 | 4 | 34 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 82 dias |
| Cabeceras de Seguridad | 40 | FALLO | Solo 2/6 presentes. Faltan: X-Frame-Options, Str... |
| Redireccion HTTPS | 70 | AVISO | HTTP redirige a HTTPS pero falta HSTS |
| Deteccion CMS | 100 | OK | CMS detectado: WordPress |
| Version CMS Expuesta | 20 | FALLO | WordPress 3 expuesta, WordPress 2 expuesta |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 60 | AVISO | 2 puerto(s) potencialmente riesgoso(s): 21 (FTP)... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-08-04T18:54:36.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-06T18:54:37.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://shieldaudit.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: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.178.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.30

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 3 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

## 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (498 bytes)
- INFO **Reglas robots.txt**
  5 Disallow, 7 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- 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) abierto: La base de datos es accesible desde internet, lo que permite intentos de intrusión y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP) abierto: Servicio de transferencia de archivos sin cifrar que facilita la captura de credenciales en la red.
[HIGH] WordPress version expuesta: La visibilidad de la versión del CMS permite a atacantes identificar vulnerabilidades conocidas y explotarlas fácilmente.
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera de seguridad hace que el sitio sea vulnerable a ataques de clickjacking.
[HIGH] Falta de Strict-Transport-Security: No se fuerza la conexión segura mediante HSTS, permitiendo posibles ataques de degradación de HTTPS a HTTP.
[MEDIUM] Archivo /readme.html accesible: Este archivo público revela información técnica y versiones del sistema que deberían ser privadas.
[MEDIUM] Ruta /wp-login.php accesible: El panel de acceso administrativo está expuesto públicamente a cualquier usuario o bot.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de navegación que se envía a otros sitios web al hacer clic en enlaces.
[MEDIUM] Falta de Permissions-Policy: Ausencia de restricciones sobre el acceso del navegador a funciones como cámara, micrófono o geolocalización.
[LOW] Server header expuesto: El encabezado revela que el servidor utiliza tecnología LiteSpeed, ayudando al reconocimiento del atacante.
[LOW] X-Powered-By expuesto: El encabezado revela el uso exacto de PHP/8.2.30, facilitando la búsqueda de exploits específicos.
[LOW] Meta generator expuesto: Se detecta la etiqueta que indica el uso de Site Kit by Google 1.178.0.
[LOW] Ruta sensible en robots.txt: El archivo de indexación menciona rutas administrativas que dan pistas sobre la estructura interna.