EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://vivialiving.es/	Checks	9 pruebas
Dominio	vivialiving.es	Hallazgos	44 totales
Fecha	27 de mayo de 2026 a las 09:38	Problemas	14 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 60/100, lo que equivale a una calificación de grado C. Durante el análisis se ejecutaron 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, se emitió 1 advertencia y se detectaron 3 fallos críticos en la configuración. Se han identificado deficiencias graves en la protección de la infraestructura, destacando la exposición de bases de datos y la ausencia total de cabeceras de seguridad. Debido a estos hallazgos, el sitio se considera actualmente vulnerable y requiere intervención inmediata para mitigar riesgos de intrusión.

Resumen de Riesgos

2	5	5	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 30 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: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 30 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  30 dias restantes (expira: 2026-06-26T12:17:12.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-28T12:17:13.000Z
- 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: nginx — Revela tecnologia del servidor

- 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://vivialiving.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, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.179.0

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- 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 (172 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://vivialiving.es/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- 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
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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 5432 (PostgreSQL): La base de datos PostgreSQL está expuesta a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[CRITICAL] Puerto 3306 (MySQL): El servicio de base de datos MySQL es accesible públicamente, lo que representa un riesgo extremo de filtración de datos sensibles.
[HIGH] Puerto 21 (FTP): El protocolo de transferencia de archivos está abierto y no utiliza cifrado, facilitando la interceptación de credenciales administrativas.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.

[HIGH] X-Frame-Options: El sitio carece de protección contra clickjacking, permitiendo que atacantes embeban la web en marcos externos para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide obligar a los navegadores a utilizar conexiones cifradas de forma permanente.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera hace que el sitio sea vulnerable a ataques de sniffing de tipos MIME por parte del navegador.
[MEDIUM] Referrer-Policy: No existe control sobre la información de procedencia enviada a otros dominios, lo que puede filtrar URLs privadas.
[MEDIUM] Permissions-Policy: Las APIs del navegador como la cámara o el micrófono no están restringidas, comprometiendo la privacidad potencial del visitante.
[MEDIUM] Archivo /readme.html y /wp-login.php: Estos archivos son accesibles públicamente, facilitando el reconocimiento de la versión del CMS y ataques dirigidos al panel de acceso.
[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando información técnica valiosa para que un atacante busque exploits específicos.
[LOW] Meta generator: La etiqueta meta expone el uso de Site Kit by Google 1.179.0, revelando herramientas internas de la web.