

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://idiazdominguez.es/	Checks	9 pruebas
Dominio	idiazdominguez.es	Hallazgos	51 totales
Fecha	29 de septiembre de 2026 a las 14:44	Problemas	17 detectados

C

65/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 65/100, lo que corresponde a una calificación de C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 5 conformes, 1 advertencia y 3 fallos críticos. La ausencia de cabeceras de seguridad esenciales y la exposición pública de versiones obsoletas del CMS representan riesgos significativos para la integridad del sitio. Aunque el certificado SSL es válido, la presencia de contenido mixto y la falta de HSTS debilitan la protección del usuario final. En conclusión, el sitio se considera vulnerable a ataques de reconocimiento y explotación de vulnerabilidades conocidas.

Resumen de Riesgos

0	4	9	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 81 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.9.9 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 81 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
81 dias restantes (expira: 2026-12-19T07:41:51.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-20T07:41:52.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: hcdn — Revela tecnologia del servidor

- BAJO

X-Powered-By expuesto
X-Powered-By: PHP/8.3.33 — 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)
- 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://idiazdominguez.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: WordPress 6.9.9
- INFO

Tecnologias detectadas
Next.js, PHP/8.3.33

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.9 expuesta, WordPress 2 expuesta

- ALTO

WordPress version
Version 6.9.9 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 — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO

Recurso HTTP (href (link/stylesheet))
http://idiazdominguez.es/wp-content/uploads/elementor/google...
- MEDIO

Recurso HTTP (href (link/stylesheet))
http://idiazdominguez.es/wp-content/uploads/elementor/google...
- MEDIO

Recurso HTTP (href (link/stylesheet))
http://idiazdominguez.es/wp-content/uploads/elementor/google...
- MEDIO

href (link/stylesheet)
...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (118 bytes)
- INFO

Reglas robots.txt
1 Disallow, 1 Allow
- BAJO

Ruta sensible en robots.txt
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO

Sitemap en robots.txt
https://idiazdominguez.es/wp-sitemap.xml
- 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] WordPress version: La versión 6.9.9 se encuentra expuesta públicamente, permitiendo a posibles atacantes buscar y explotar CVEs conocidos para este software.

[HIGH] X-Frame-Options: La falta de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking para engañar a los usuarios.

[HIGH] Strict-Transport-Security: No existe una política HSTS configurada, lo que permite ataques de degradación de protocolo (Downgrade attacks) de HTTPS a HTTP.

[MEDIUM] Contenido Mixto: Se detectaron 4 recursos cargados mediante HTTP en una página protegida por HTTPS, lo que compromete la seguridad global de la sesión.

[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts maliciosos interpretados como otros tipos de archivos.

[MEDIUM] Referrer-Policy: No hay control sobre la información de referencia que se envía a otros dominios al hacer clic en enlaces salientes.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.

[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y puede revelar información técnica detallada sobre la instalación y versión del CMS.

[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, quedando expuesto a intentos de acceso no autorizados por fuerza bruta.

[LOW] Server header expuesto: El servidor revela el uso de la tecnología hcdn, facilitando el perfilamiento del entorno técnico por parte de atacantes.

[LOW] X-Powered-By expuesto: Se expone la versión de PHP/8.3.33, lo que permite a un atacante dirigir ataques específicos contra esa versión del lenguaje.

[LOW] Meta generator: La etiqueta meta en el código fuente confirma explícitamente el uso de WordPress 6.9.9.

[LOW] Ruta sensible en robots.txt: Se hace referencia a directorios administrativos, lo que guía a los rastreadores maliciosos hacia áreas que deberían permanecer privadas.