EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://gestoriaareal.es	Checks	9 pruebas
Dominio	gestoriaareal.es	Hallazgos	48 totales
Fecha	20 de marzo de 2026 a las 13:01	Problemas	18 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al dominio gestoriaareal.es ha resultado en una puntuación de 56/100, lo que equivale a una nota de grado D. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 4 resultaron exitosos, 1 generó una advertencia y 4 finalizaron en fallo crítico. Se han detectado deficiencias severas en la configuración de cabeceras de seguridad y la exposición de información técnica sensible. Debido a la falta de protecciones esenciales contra ataques comunes y la visibilidad de versiones desactualizadas, se concluye que el sitio es vulnerable.

Resumen de Riesgos

0	5	9	4	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 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
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-05-29T02:30:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-28T02:30:41.000Z
- 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: OVHcloud — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.3 — Revela framework/lenguaje
- 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://www.gestoriaareal.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: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js, PHP/7.3

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 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://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gestruck.com/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://dfg.es/
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de ataques de inyección de código y XSS.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking mediante marcos externos.
[HIGH] Strict-Transport-Security: La ausencia de HSTS permite que los usuarios realicen conexiones inseguras a través de HTTP.
[HIGH] WordPress version: La versión 6.9.4 se encuentra expuesta públicamente, permitiendo a atacantes identificar vulnerabilidades específicas para este software.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede derivar en la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia que el navegador envía al navegar desde el sitio.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como la cámara o el micrófono, aumentando la superficie de ataque.
[MEDIUM] Archivo /readme.html: Este archivo es accesible y revela detalles internos del CMS WordPress.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es público, facilitando ataques de fuerza bruta.
[MEDIUM] Contenido Mixto: Se detectaron 4 recursos cargados mediante protocolo HTTP inseguro dentro de la página HTTPS, comprometiendo el cifrado.
[LOW] Server header expuesto: Se revela el uso de infraestructura OVHcloud, facilitando el reconocimiento del entorno.
[LOW] X-Powered-By expuesto: La cabecera indica el uso de PHP/7.3, una versión antigua con posibles riesgos asociados.
[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 6.9.4 en el código fuente.
[LOW] sitemap.xml: El archivo no fue encontrado, lo que dificulta la auditoría de rutas y la indexación correcta.