EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://enamoradosdealicante.es	Checks	9 pruebas
Dominio	enamoradosdealicante.es	Hallazgos	52 totales
Fecha	27 de julio de 2026 a las 11:37	Problemas	11 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada sobre el sitio web ha dado como resultado una puntuación de 75/100, lo que equivale a una calificación de grado B. El análisis pasivo ejecutó un total de 9 comprobaciones, logrando 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos en la configuración. A pesar de contar con una base sólida en el cifrado de datos, se han detectado debilidades severas relacionadas con la obsolescencia del software y la gestión de sesiones. El sitio se considera actualmente vulnerable debido a la exposición de una versión de WordPress antigua y brechas en la seguridad de las cookies. Es imperativo abordar estos hallazgos para mitigar el riesgo de intrusiones o robo de información.

Resumen de Riesgos

0	5	2	4	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: X-Frame-Options
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 3.1.2 expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-10-23T09:09:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-25T09:09:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: X-Frame-Options

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PleskLin — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(self), camera=(), microphone=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://enamoradosdealicante.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 dias)
- 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: Powered by WPBakery Page Builder - drag and drop page builder for WordPress.
- INFO **Tecnologias detectadas**
  Next.js, Astro, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3.1.2 expuesta

- ALTO **WordPress version**
  Version 3.1.2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (124 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://enamoradosdealicante.es/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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 3.1.2 está expuesta públicamente, lo que facilita a atacantes la explotación de múltiples vulnerabilidades conocidas y documentadas (CVEs).
[HIGH] X-Frame-Options: La falta de esta cabecera de seguridad permite ataques de clickjacking, donde un tercero puede cargar el sitio en un marco invisible para engañar al usuario.
[HIGH] Cookie PHPSESSID (HttpOnly): La ausencia de este flag permite que la cookie sea accesible mediante scripts de navegador, elevando el riesgo de robo de sesión vía XSS.
[HIGH] Cookie PHPSESSID (Secure): La falta de este atributo permite que la cookie de sesión se envíe a través de conexiones no cifradas, exponiéndola a intercepciones.
[HIGH] Puerto 21 (FTP): Este puerto está abierto y utiliza un protocolo de transferencia de archivos que no cifra las credenciales ni los datos enviados.
[MEDIUM] Cookie PHPSESSID (SameSite): La configuración carece de esta protección, lo que deja a los usuarios vulnerables a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Puerto 22 (SSH): Se detectó un puerto de acceso remoto abierto que, de no estar correctamente securizado, representa un vector de entrada para ataques de fuerza bruta.
[LOW] Server header expuesto: El encabezado revela el uso de nginx, proporcionando información técnica útil para que un atacante perfile el servidor.
[LOW] X-Powered-By expuesto: La cabecera indica el uso de PleskLin, lo que ayuda a identificar el entorno de ejecución y posibles vectores específicos.
[LOW] Meta generator: La etiqueta revela el uso de WPBakery Page Builder, lo que permite identificar complementos específicos y sus posibles fallos.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a la ruta admin, lo que orienta a los atacantes hacia los paneles de gestión del sitio.