EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://energyavm.es	Checks	9 pruebas
Dominio	energyavm.es	Hallazgos	49 totales
Fecha	22 de abril de 2026 a las 18:01	Problemas	10 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web energyavm.es ha resultado en una puntuación de 78/100, lo que corresponde a una calificación de nota B. Durante la auditoría se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, una advertencia por puertos abiertos y 2 fallos críticos en la configuración del servidor y el CMS. Aunque el cifrado SSL y la redirección HTTPS son robustos, la exposición de una versión antigua de WordPress y la ausencia de cabeceras de seguridad fundamentales comprometen la integridad del sitio. En su estado actual, se concluye que el sitio es vulnerable a ataques dirigidos de explotación de vulnerabilidades conocidas. Es necesario aplicar medidas correctivas inmediatas para mitigar los riesgos identificados.

Resumen de Riesgos

0	2	4	4	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
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 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	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-06-20T09:48:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-22T08:48:44.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PleskLin — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN;
- INFO **Strict-Transport-Security**
  Presente: max-age=15768000; includeSubDomains
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://energyavm.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15768000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 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: Site Kit by Google 1.168.0
- INFO **Tecnologias detectadas**
  Next.js, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- ALTO **WordPress version**
  Version 2 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)

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 (150 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://www.energyavm.es/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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

- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] WordPress version: La versión 2 de WordPress está expuesta públicamente, lo que facilita a atacantes la búsqueda y explotación de vulnerabilidades conocidas (CVEs).
[HIGH] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de inyección de contenido y scripts maliciosos (XSS).
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó el puerto 8080 abierto, el cual suele utilizarse para servicios de administración o proxies, aumentando la superficie de ataque.
[MEDIUM] Referrer-Policy: La ausencia de esta cabecera impide controlar qué información de navegación se envía a otros sitios web.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono a través de cabeceras de seguridad.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede ser utilizado por atacantes para confirmar la versión exacta y otros detalles del CMS.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando información técnica innecesaria a potenciales atacantes.
[LOW] X-Powered-By expuesto: La cabecera revela el uso de PleskLin, lo que ayuda a identificar el framework y sistema de gestión del servidor.
[LOW] Meta generator: La etiqueta meta expone el uso de Site Kit by Google 1.168.0, revelando detalles adicionales sobre la infraestructura de plugins.
[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.