EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://lasrozasinnova.es	Checks	9 pruebas
Dominio	lasrozasinnova.es	Hallazgos	49 totales
Fecha	6 de julio de 2026 a las 06:47	Problemas	8 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta un nivel de seguridad aceptable, obteniendo una puntuación técnica de 84/100 y una calificación de grado B. Tras realizar 9 checks pasivos, se determinó que 6 operan correctamente, 2 presentan advertencias y 1 se considera un fallo crítico. La infraestructura destaca por una implementación impecable de cifrado SSL y cabeceras de protección, pero muestra debilidades significativas en la exposición de información técnica y servicios de red. Aunque la plataforma no presenta una intrusión inminente, la visibilidad de versiones de software y puertos inseguros la hace vulnerable a ataques dirigidos. En conclusión, el sitio es generalmente seguro para el usuario final, pero requiere endurecimiento técnico en su configuración de servidor.

Resumen de Riesgos

0	2	3	3	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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 7.0 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
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 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-09-24T10:05:19.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-26T10:05:20.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.31, PleskLin — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;, upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000, max-age=63072000
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin, strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(), autoplay=(), camera=(), cross-origin-isolated=(), display-capt...

Redireccion HTTPS — 100/100

Estado: OK
HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://lasrozasinnova.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000, max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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: WordPress 7.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.31, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO
WordPress 7.0 expuesta

- ALTO **WordPress version**
  Version 7.0 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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.lasrozas.es
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.lasrozas.es

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (218 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://lasrozasinnova.es/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 7.0 de WordPress se encuentra expuesta públicamente, permitiendo a atacantes identificar y explotar vulnerabilidades conocidas (CVEs).
[HIGH] Puerto 21 (FTP): El puerto de transferencia de archivos está abierto y no utiliza cifrado, lo que permite la interceptación de credenciales y datos en tránsito.
[MEDIUM] Recurso HTTP (Mixed Content): Existen dos referencias a hojas de estilo mediante el protocolo inseguro HTTP desde el dominio lasrozas.es, lo que degrada la integridad de la conexión.
[MEDIUM] Puerto 22 (SSH): El servicio de acceso remoto seguro está expuesto, representando un vector potencial de ataque por fuerza bruta si no está debidamente restringido.
[LOW] Server header expuesto: La cabecera revela el uso de Nginx, proporcionando pistas sobre la tecnología del servidor a posibles atacantes.
[LOW] X-Powered-By expuesto: Se revela el uso de PHP/8.3.31 y PleskLin, facilitando el perfilado de la infraestructura interna.
[LOW] Meta generator: La etiqueta meta del código fuente confirma explícitamente el uso de WordPress 7.0.