EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://elosnus.es	Checks	9 pruebas
Dominio	elosnus.es	Hallazgos	48 totales
Fecha	23 de marzo de 2026 a las 23:15	Problemas	12 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 76/100, lo que corresponde a una calificación de grado B. Durante el proceso se ejecutaron 9 comprobaciones pasivas, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos en la configuración de seguridad. Aunque la plataforma cuenta con un cifrado de transporte sólido, presenta deficiencias importantes en la implementación de cabeceras de protección y en la exposición de información técnica sensible. Se concluye que el sitio es actualmente vulnerable a ataques de clickjacking y reconocimiento de software por parte de terceros malintencionados.

Resumen de Riesgos

0	4	4	4	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 55 dias
Cabeceras de Seguridad	40	FALLO	Solo 2/6 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 6.9.4 expuesta, 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 55 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  55 dias restantes (expira: 2026-05-18T00:05:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-17T00:05:27.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.27 — 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://elosnus.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 6.9.4
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.27

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 — 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 (511 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://elosnus.es/sitemap_index.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] X-Frame-Options: Falta esta cabecera, lo que permite que el sitio sea embebido en marcos externos facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones HTTPS de manera permanente y segura.
[HIGH] WordPress version: Se detectó la versión 6.9.4 expuesta públicamente, lo que permite a atacantes identificar y explotar CVEs conocidos para dicha versión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, pudiendo ejecutar scripts maliciosos disfrazados de otros archivos.
[MEDIUM] Referrer-Policy: No está configurada, lo que provoca la fuga de información de navegación hacia sitios externos mediante el campo referer.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y revela información técnica detallada sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, quedando expuesto a intentos de fuerza bruta.
[LOW] Server header expuesto: La cabecera revela el uso de hcdn, facilitando el reconocimiento de la infraestructura del servidor.
[LOW] X-Powered-By expuesto: Revela el uso de PHP/8.3.27, proporcionando datos específicos sobre el lenguaje de programación y su versión.
[LOW] Meta generator: La etiqueta meta expone la versión 6.9.4 de WordPress directamente en el código fuente.
[LOW] Ruta sensible en robots.txt: Se hace referencia a rutas tipo admin, lo que orienta a los atacantes sobre la estructura interna del sitio.