

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://poteasturiano.com/
Dominio poteasturiano.com
Fecha 5 de octubre de 2026 a las 11:53

Checks 9 pruebas
Hallazgos 47 totales
Problemas 14 detectados

C

64/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 64/100, lo que equivale a una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 finalizaron en fallo crítico. A pesar de contar con un cifrado SSL válido, la ausencia total de cabeceras de seguridad y la exposición de versiones de software suponen un riesgo considerable. Debido a estas deficiencias técnicas y a la presencia de contenido mixto, se concluye que el sitio es actualmente vulnerable ante diversos vectores de ataque comunes. No se realizó un pentest activo en esta evaluación.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 76 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 7.1.2 expuesta, WordPress 2 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 76 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
76 dias restantes (expira: 2026-12-20T06:25:42.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-21T06:25:43.000Z
- 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: nginx — Revela tecnologia del servidor

- BAJO

X-Powered-By expuesto
X-Powered-By: PHP/8.4.26, PleskLin — 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://poteasturiano.com/
- 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
- INFO

Tecnologias detectadas
Next.js, PHP/8.4.26, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.1.2 expuesta, WordPress 2 expuesta

- ALTO

WordPress version
Version 7.1.2 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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO

Recurso HTTP (href (link/stylesheet))
http://idearedonda.com
- MEDIO

Recurso HTTP (href (link/stylesheet))
http://www.idearedonda.com

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (118 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://poteasturiano.com/wp-sitemap.xml
- BAJO

security.txt
No encontrado — Recomendado para política 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] WordPress version: La versión 7.1.2 del CMS está expuesta públicamente, facilitando a atacantes la búsqueda de vulnerabilidades conocidas (CVEs).
- [HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de código como Cross-Site Scripting (XSS).
- [HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking para engañar a los usuarios.
- [HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo ataques de degradación de protocolo.
- [MEDIUM] Contenido Mixto: Se detectaron 2 recursos cargados mediante HTTP (idearedonda.com), lo que compromete la integridad de la conexión cifrada.
- [MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.
- [MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y suele revelar información técnica detallada sobre la instalación de WordPress.
- [MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros dominios al hacer clic en enlaces.
- [MEDIUM] Permissions-Policy: La falta de esta cabecera no restringe el acceso de las APIs del navegador a componentes sensibles como cámara o micrófono.
- [LOW] Server header expuesto: El servidor revela que utiliza la tecnología nginx, acotando el trabajo de reconocimiento para un atacante.
- [LOW] X-Powered-By expuesto: Se expone el uso de PHP/8.4.26 y PleskLin, revelando capas críticas de la infraestructura del backend.
- [LOW] Ruta sensible en robots.txt: La mención directa a la ruta de administración permite a los atacantes identificar rápidamente el panel de gestión.