EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://inpropia.com	Checks	9 pruebas
Dominio	inpropia.com	Hallazgos	47 totales
Fecha	21 de abril de 2026 a las 07:41	Problemas	15 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio inpropia.com ha arrojado una puntuación de 61/100, lo que otorga una calificación de C. El análisis se basó en 9 checks pasivos, resultando en 6 verificaciones exitosas, 1 advertencia y 2 fallos críticos en la configuración. Aunque el sitio dispone de un certificado SSL válido, existen deficiencias graves en la protección de la infraestructura, destacando la exposición de la base de datos y la ausencia de cabeceras de seguridad esenciales. Se concluye que el sitio es actualmente vulnerable a ataques de interceptación de datos e intrusiones externas. Es imperativo corregir las configuraciones del servidor para evitar riesgos de pérdida de información.

Resumen de Riesgos

1	6	6	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 34 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS 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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 34 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  34 dias restantes (expira: 2026-05-25T13:48:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-24T13:48:16.000Z
- 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: Apache — Revela tecnologia del servidor

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- 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
- BAJO **Meta generator**
  Expone: IN PROPIA

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 (70 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://www.inpropia.com/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): El puerto de la base de datos está abierto y expuesto a internet, lo que permite intentos de conexión externa y posibles ataques de fuerza bruta o explotación de datos.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y utiliza un protocolo no cifrado, facilitando la interceptación de credenciales y archivos.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: Falta de configuración que protege contra ataques de clickjacking, permitiendo que el sitio sea embebido en marcos maliciosos para engañar a visitantes.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no obliga a utilizar siempre una conexión cifrada HTTPS.
[HIGH] HTTP a HTTPS redireccion: El servidor permite el acceso mediante HTTP sin redirigir automáticamente a la versión segura, exponiendo el tráfico a ataques de intermediario.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido (MIME sniffing), facilitando la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de navegación que se comparte con sitios externos.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como el acceso a la cámara o micrófono, lo que supone un riesgo potencial de privacidad.
[MEDIUM] Rutas de administración expuestas: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles, revelando posibles puntos de entrada a paneles de gestión.
[LOW] Server header expuesto: El servidor responde con la cabecera Server: Apache, revelando la tecnología utilizada y facilitando la búsqueda de vulnerabilidades específicas.
[LOW] Meta generator: La etiqueta meta expone el identificador IN PROPIA, proporcionando información sobre el desarrollo del sitio a posibles atacantes.