EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://phptravels.net/	Checks	9 pruebas
Dominio	phptravels.net	Hallazgos	45 totales
Fecha	6 de julio de 2026 a las 17:19	Problemas	9 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio phptravels.net arrojo una puntuacion de 68/100, lo que corresponde a una calificacion de grado C. El analisis se baso en 9 checks pasivos, de los cuales 4 resultaron exitosos, 3 generaron advertencias y 2 fueron clasificados como fallos. Aunque el cifrado de transporte es correcto, se detectaron deficiencias criticas en la configuracion de cabeceras de seguridad y en la gestion de cookies de sesion. La falta de politicas contra ataques de inyeccion y la exposicion de puertos adicionales incrementan la superficie de ataque. Se concluye que el sitio es moderadamente vulnerable y requiere medidas correctivas para proteger la integridad de sus usuarios.

Resumen de Riesgos

0	5	3	1	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-09-16T01:45:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-18T00:47:33.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

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

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- 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://phptravels.net/
- 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
- INFO **Tecnologias detectadas**
  React, Next.js

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)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, 41 URLs
- 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] Content-Security-Policy: Falta esta cabecera, lo cual es peligroso porque permite la ejecucion de ataques XSS y la inyeccion de contenido malicioso.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce siempre conexiones seguras, facilitando ataques de degradacion de protocolo.

[HIGH] Cookie PHPSESSID - HttpOnly: La cookie de sesion carece del flag HttpOnly, permitiendo que sea accesible mediante scripts, lo que facilita el robo de sesiones.
[HIGH] Cookie PHPSESSID - Secure: La falta del flag Secure permite que la cookie de sesion sea transmitida a traves de conexiones HTTP no cifradas.
[MEDIUM] Cookie PHPSESSID - SameSite: La ausencia de este atributo deja el sitio vulnerable a ataques de falsificacion de peticion en sitios cruzados (CSRF).
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente el acceso no autorizado a perifericos como camara o microfono.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y expone un servidor web alternativo o proxy, aumentando los puntos de entrada posibles.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, lo que entrega informacion sobre la infraestructura tecnologica a posibles atacantes.
[LOW] Robots.txt y Sitemap: El archivo robots.txt no fue encontrado, dificultando la gestion de rastreo y revelando falta de mantenimiento en politicas de indexacion.