EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://oxapampa.com/	Checks	9 pruebas
Dominio	oxapampa.com	Hallazgos	48 totales
Fecha	6 de mayo de 2026 a las 05:00	Problemas	12 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 76/100, lo que representa una calificación de B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, uno presentó advertencias y dos fallaron debido a configuraciones de seguridad insuficientes. Aunque el sitio cuenta con un cifrado de conexión adecuado, la exposición de versiones de software y la falta de cabeceras de protección incrementan el riesgo operativo. Se concluye que el sitio es actualmente funcional pero vulnerable a ataques de reconocimiento y suplantación de interfaz si no se aplican las correcciones recomendadas.

Resumen de Riesgos

0	4	4	4	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 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 6.8.5 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 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-07-18T08:45:49.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-19T08:45:50.000Z
- 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/8.1.34 — 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://oxapampa.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, 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: All in One SEO (AIOSEO) 4.9.4.1
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.1.34

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.5 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.8.5 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 (157 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://oxapampa.com/sitemap.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 la cabecera que impide que el sitio sea cargado en frames, lo que facilita ataques de clickjacking.
[HIGH] Strict-Transport-Security: No existe configuración HSTS, lo que impide que el navegador fuerce conexiones seguras HTTPS de forma permanente.
[HIGH] Versión de WordPress expuesta: La detección de la versión 6.8.5 permite a posibles atacantes identificar vulnerabilidades conocidas (CVE) asociadas a dicho despliegue.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite que los navegadores realicen sniffing de tipos MIME, aumentando el riesgo de ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que puede filtrar información sensible de las URLs a sitios de terceros.
[MEDIUM] Archivo /readme.html accesible: Este archivo público revela información técnica sobre la instalación del CMS que debería ser privada.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso administrativo es visible para cualquier usuario, facilitando ataques de fuerza bruta.
[LOW] Cabecera Server expuesta: Se revela el uso de hcdn como tecnología de servidor, acotando el vector de ataque para intrusos.
[LOW] Cabecera X-Powered-By expuesta: Indica explícitamente el uso de PHP/8.1.34, exponiendo detalles del entorno de ejecución.
[LOW] Meta generator expuesto: La etiqueta revela el uso del plugin All in One SEO 4.9.4.1 y su versión exacta.
[LOW] Rutas sensibles en robots.txt: La mención de directorios como "admin" ofrece pistas directas sobre la estructura interna del sitio a rastreadores maliciosos.