EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://wow-peru.lat	Checks	9 pruebas
Dominio	wow-peru.lat	Hallazgos	46 totales
Fecha	31 de agosto de 2026 a las 05:47	Problemas	7 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web wow-peru.lat ha obtenido una puntuación de 77/100, lo que representa una nota de grado B en la auditoría de seguridad. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 presentó fallos críticos de configuración. Si bien el sitio posee un certificado de cifrado robusto, carece de mecanismos básicos para forzar la navegación segura y expone información técnica que facilita el reconocimiento externo. En conclusión, el sitio se considera vulnerable a ataques de intermediario y exposición de datos por configuraciones incorrectas en el servidor y políticas de transporte.

Resumen de Riesgos

0	3	2	2	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 69 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  69 dias restantes (expira: 2026-11-08T00:50:07.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-09T23:50:18.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' https://code.jquery.com https://challenges...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=()

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
- INFO **Tecnologias detectadas**
  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 — 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 (2148 bytes)
- INFO **Reglas robots.txt**
  20 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "\.env" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://wow-peru.lat/sitemap.xml
- 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] HTTP a HTTPS redirección: El servidor responde con éxito en el puerto 80 sin redirigir al usuario hacia la versión segura, permitiendo capturar datos en texto plano.

[HIGH] HSTS (Strict-Transport-Security) ausente: Al no configurar esta cabecera, el navegador no está obligado a usar HTTPS en visitas futuras, permitiendo ataques de degradación de protocolo.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto alternativo aumenta la superficie de ataque, ya que suele albergar servicios de administración o proxies menos protegidos.
[MEDIUM] Bloqueo total en robots.txt: Se ha configurado una instrucción que prohíbe el rastreo de todo el sitio, lo cual puede indicar una falta de refinamiento en la política de visibilidad pública.
[LOW] Referencia a .env en robots.txt: Mencionar archivos de variables de entorno en el archivo de robots expone la posible ubicación de secretos, contraseñas y claves de API ante un atacante.
[LOW] Server header expuesto: El encabezado revela el uso de Cloudflare, lo que permite a un actor malicioso centrar sus esfuerzos en vectores de ataque específicos para esta infraestructura.