EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://oregons.duckdns.org/tienda_oregon/?fbclid=IwVEREWARx97xleHRuA2FlbQIxMABzcnRjBmFwcF9pZAo2NjI4NTY4Mzc5AAEelkV9C97nxYbW2mfDQHRcEp-KJ18XLq3MR6HVfmFbf8e7NLoe1N4lNsw3v3E_aem_a6HF1LtRf34oIqKk9rmJIg	Checks	9 pruebas
Dominio	oregons.duckdns.org	Hallazgos	46 totales
Fecha	14 de mayo de 2026 a las 00:52	Problemas	14 detectados

D

58/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad, el sitio web ha obtenido una puntuación de 58/100 con una calificación de grado D. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 4 resultaron exitosas, 2 generaron advertencias y 3 finalizaron en fallo crítico. A pesar de contar con un certificado de cifrado válido, la ausencia total de cabeceras de protección y la falta de seguridad en las sesiones representan un riesgo elevado. En su estado actual, el sitio web se considera vulnerable y requiere correcciones técnicas inmediatas para proteger la integridad de sus visitantes.

Resumen de Riesgos

0	6	5	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 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	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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 72 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  72 dias restantes (expira: 2026-07-24T20:31:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-25T20:31:35.000Z
- 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/2.4.58 (Ubuntu) — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://oregons.duckdns.org/
- 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 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Content-Security-Policy: Falta esta cabecera que previene ataques de inyección de código y scripts maliciosos XSS.

[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de Clickjacking.
[HIGH] Strict-Transport-Security: No se detectó configuración HSTS, lo que impide que el navegador fuerce conexiones seguras de forma persistente.
[HIGH] Cookie PHPSESSID - Flag HttpOnly: La cookie de sesión es accesible mediante scripts, lo que permite el robo de identidad en caso de XSS.
[HIGH] Cookie PHPSESSID - Flag Secure: La sesión puede ser transmitida por canales no cifrados, exponiendo las credenciales del usuario en redes públicas.
[MEDIUM] X-Content-Type-Options: Falta la protección contra MIME-sniffing, permitiendo que el navegador interprete archivos de forma incorrecta y peligrosa.
[MEDIUM] Cookie PHPSESSID - Flag SameSite: La ausencia de este flag incrementa el riesgo de ataques de falsificación de petición en sitios cruzados CSRF.
[MEDIUM] Puerto 22 (SSH) abierto: El puerto de administración remota está expuesto públicamente, lo que aumenta la superficie de ataque para intentos de intrusión.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se comparte con sitios externos al hacer clic en enlaces.
[MEDIUM] Permissions-Policy: No se restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la ubicación.
[LOW] Server header expuesto: El servidor revela que utiliza Apache/2.4.58 en Ubuntu, información útil para que un atacante busque vulnerabilidades específicas.
[LOW] Archivos de estructura faltantes: No se encontraron los archivos robots.txt ni sitemap.xml, esenciales para la gestión de rastreo y visibilidad.