EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.universaldecauchos.com	Checks	9 pruebas
Dominio	www.universaldecauchos.com	Hallazgos	43 totales
Fecha	29 de abril de 2026 a las 19:56	Problemas	12 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el sitio arroja una puntuacion exacta de 64/100, lo que resulta en una nota C. Los resultados de los checks pasivos indican que, de 9 pruebas ejecutadas, 5 resultaron exitosas, 1 presenta advertencias y 3 fallaron de forma critica. Aunque el servidor posee un cifrado de datos activo, la ausencia total de politicas de seguridad en las cabeceras debilita la proteccion de los usuarios. Debido a estas omisiones tecnicas en la configuracion, se concluye que el sitio es actualmente vulnerable a ataques de inyeccion y suplantacion.

Resumen de Riesgos

0	4	4	4	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 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	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 58 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  58 dias restantes (expira: 2026-06-26T19:57:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-28T19:57:47.000Z
- 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: LiteSpeed — 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://universaldecauchos.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

- INFO **WordPress**
  Detectado via HTML body
- 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: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 500)
- BAJO **sitemap.xml**
  No encontrado (HTTP 500)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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 faltante: La ausencia de esta cabecera permite ataques de inyeccion de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea cargado en marcos externos no autorizados.
[HIGH] Strict-Transport-Security faltante: No se obliga al navegador a utilizar conexiones HTTPS, permitiendo posibles ataques de degradacion de seguridad.
[MEDIUM] X-Content-Type-Options faltante: Facilita ataques basados en MIME-type sniffing, permitiendo que el navegador interprete archivos de forma incorrecta.
[MEDIUM] Referrer-Policy faltante: No se controla la cantidad de informacion de navegacion que se envia a otros sitios web al seguir enlaces.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el uso de APIs sensibles del navegador como la camara, el microfono o la geolocalizacion.

[MEDIUM] Archivo /readme.html accesible: Este archivo publico revela informacion tecnica sobre la instalacion del CMS que puede ser aprovechada por atacantes.
[LOW] HSTS no configurado: El servidor redirige a HTTPS pero no establece una instruccion permanente de seguridad para el navegador.
[LOW] Server header expuesto: Se revela el uso de LiteSpeed como tecnologia de servidor, facilitando la busqueda de exploits especificos.
[LOW] Meta generator expuesto: El codigo fuente muestra publicamente el uso de WordPress 6.9.4, exponiendo la version exacta ante posibles vulnerabilidades conocidas.
[LOW] Archivos robots.txt y sitemap.xml no encontrados: El servidor devuelve errores HTTP 500 al intentar acceder a estos archivos de gestion de indexacion.