EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sabroso-panama.com/	Checks	9 pruebas
Dominio	sabroso-panama.com	Hallazgos	46 totales
Fecha	1 de julio de 2026 a las 02:24	Problemas	11 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 71/100, lo que corresponde a una calificación de grado C. Se ejecutaron 9 controles pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fallaron críticamente debido a configuraciones deficientes. El análisis revela que, aunque el cifrado base es correcto, existen debilidades importantes en las cabeceras de seguridad y en la exposición de versiones del software. Se concluye que el sitio es actualmente vulnerable ante ataques de reconocimiento y explotación de vulnerabilidades conocidas. Es imperativo aplicar las correcciones detalladas para elevar el nivel de protección de la plataforma.

Resumen de Riesgos

0	5	4	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 55 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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 1.4.11 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 55 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  55 dias restantes (expira: 2026-08-24T23:33:19.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-26T23:33:20.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx — 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)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://sabroso-panama.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
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1.4.11 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 1.4.11 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 (119 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://sabroso-panama.com/wp-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

[ALTA] Versión de WordPress expuesta: Las versiones 1.4.11 y 2 son visibles, permitiendo a atacantes identificar y explotar CVEs específicos del software.
[ALTA] Content-Security-Policy (CSP) ausente: La falta de esta política facilita la ejecución de ataques de inyección de contenido y Cross-Site Scripting (XSS).
[ALTA] X-Frame-Options ausente: El sitio no previene ser cargado dentro de frames externos, lo que lo hace susceptible a ataques de clickjacking.
[ALTA] Strict-Transport-Security (HSTS) ausente: No se obliga al navegador a utilizar exclusivamente conexiones seguras, permitiendo ataques de degradación de SSL.
[MEDIA] Archivo /readme.html accesible: Este archivo público revela información técnica y versiones del CMS que facilitan el reconocimiento por parte de atacantes.
[MEDIA] Panel /wp-login.php expuesto: La ruta de administración es accesible para cualquier usuario, aumentando el riesgo de ataques de fuerza bruta hacia las credenciales.
[MEDIA] Referrer-Policy ausente: No se controla la cantidad de información de referencia enviada a otros sitios web, comprometiendo la privacidad de los usuarios.
[MEDIA] Permissions-Policy ausente: El servidor no restringe el uso de APIs del navegador, como la cámara o el micrófono, en el contexto del sitio.
[BAJA] Cabecera Server expuesta: El encabezado revela el uso de nginx, proporcionando datos específicos sobre la infraestructura que facilitan ataques dirigidos.
[BAJA] Ruta sensible en robots.txt: La referencia directa al directorio "admin" expone la ubicación de áreas sensibles para su indexación o exploración.