EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://siopex.com	Checks	9 pruebas
Dominio	siopex.com	Hallazgos	42 totales
Fecha	4 de mayo de 2026 a las 19:34	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada en el sitio web ha arrojado una puntuación de 68/100, lo que equivale a una nota de C. El análisis se basó exclusivamente en la ejecución de 9 checks pasivos, de los cuales 5 resultaron correctos, 2 presentaron advertencias y 2 fallaron de forma crítica. Se han identificado carencias graves en las cabeceras de seguridad y una exposición de puertos de infraestructura que comprometen la integridad del servidor. Debido a la ausencia total de políticas de seguridad en el navegador y la exposición directa de la base de datos, se concluye que el sitio es actualmente vulnerable ante ataques cibernéticos.

Resumen de Riesgos

1	4	4	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 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	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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 65 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  65 dias restantes (expira: 2026-07-08T15:59:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-09T15:59:10.000Z
- 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 — 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://siopex.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

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

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 — 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

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 3306 (MySQL)

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): La base de datos está expuesta directamente a internet, lo que permite ataques de fuerza bruta e intentos de intrusión externa.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de inyección de código como Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: No está configurada, dejando el sitio vulnerable a ataques de clickjacking mediante el uso de frames maliciosos.
[HIGH] Strict-Transport-Security: Falta la directiva HSTS, lo que impide forzar de forma estricta las conexiones cifradas HTTPS en el navegador.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto para administración está abierto, aumentando la superficie de ataque para accesos no autorizados.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios web, comprometiendo la privacidad de la navegación.

[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el uso no autorizado de hardware como cámara o micrófono.
[LOW] Server header expuesto: Se revela el uso del servidor Apache, facilitando a los atacantes la búsqueda de exploits específicos para esa tecnología.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos dificulta la gestión de la indexación y el control de acceso para rastreadores web.