EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://locosdewallstreet.com/financial-research/fr_posts/resultados-q1-2026-semapa	Checks	9 pruebas
Dominio	locosdewallstreet.com	Hallazgos	48 totales
Fecha	21 de mayo de 2026 a las 07:36	Problemas	11 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha arrojado una puntuación de 72/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se generó 1 advertencia y se detectaron 2 fallos críticos. Aunque la plataforma cuenta con una base sólida en cuanto a cifrado, la exposición de información técnica y la ausencia de cabeceras defensivas representan un riesgo importante. No se realizó un pentest activo, por lo que el análisis se limita a la superficie de exposición pública. En su estado actual, el sitio se considera vulnerable ante ataques de inyección y reconocimiento avanzado.

Resumen de Riesgos

0	3	6	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.5.8 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-07-21T09:51:54.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-22T09:51:55.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=15724800; includeSubDomains
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 308 redirige a https://locosdewallstreet.com
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15724800; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15724800 (182 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.5.8
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.5.8 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.5.8 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 (130 bytes)
- INFO **Reglas robots.txt**
  3 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://locosdewallstreet.com/sitemap_index.xml
- 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 — Previene XSS y ataques de inyeccion de contenido.
[HIGH] X-Frame-Options: Falta — Protege contra clickjacking al evitar que el sitio sea embebido en frames externos.
[HIGH] WordPress version: Version 6.5.8 expuesta publicamente — Permite a atacantes buscar y explotar CVEs conocidos especificos para esta version.
[MEDIUM] X-Content-Type-Options: Falta — Evita que el navegador realice MIME-type sniffing, mitigando la ejecucion de archivos maliciosos.
[MEDIUM] Referrer-Policy: Falta — Controla la informacion de navegacion que se envia a traves de la cabecera referer.
[MEDIUM] Permissions-Policy: Falta — No restringe el acceso a APIs sensibles del navegador como la camara, microfono o geolocalizacion.
[MEDIUM] Puerto 22 (SSH): ABIERTO — El acceso remoto esta expuesto, lo que permite intentos de intrusion por fuerza bruta si no esta debidamente protegido.
[MEDIUM] Archivo /readme.html: Accesible publicamente — Este archivo revela informacion interna y versiones del CMS que facilitan el reconocimiento.
[MEDIUM] Ruta /wp-login.php: Accesible publicamente — El panel de administracion esta expuesto a ataques de fuerza bruta directos.
[LOW] Meta generator: Expone explicitamente WordPress 6.5.8 en el codigo fuente.
[LOW] Ruta sensible en robots.txt: Referencia a la palabra admin, lo que orienta a posibles atacantes hacia directorios de gestion.