EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://jrygyn.ceos.digital	Checks	9 pruebas
Dominio	jrygyn.ceos.digital	Hallazgos	15 totales
Fecha	12 de mayo de 2026 a las 15:22	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web jrygyn.ceos.digital ha arrojado una puntuación exacta de 73/100 con una calificación de nota C. Durante la evaluación de seguridad, se realizaron 9 checks pasivos, de los cuales 1 resultó satisfactorio y 1 se registró como fallo crítico de configuración. La imposibilidad de establecer conexiones seguras y la falta de archivos de optimización básica indican una infraestructura inestable. Por lo tanto, se concluye que el sitio es actualmente vulnerable y no cumple con los estándares mínimos de seguridad web.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar 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 — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

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

[CRITICA] Error de conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide el cifrado de datos y expone la comunicación.
[CRITICA] Ausencia de Cabeceras de Seguridad: El servidor no permite verificar protecciones contra ataques XSS o Clickjacking debido a errores de respuesta.
[CRITICA] Fallo en Redirección HTTPS: No se ha podido validar que el tráfico inseguro se redirija automáticamente a una versión cifrada.
[BAJA] Falta de archivo robots.txt: No se encontró el archivo de directrices para rastreadores, lo que dificulta el control sobre la indexación del sitio.
[BAJA] Ausencia de sitemap.xml: El mapa del sitio no está disponible, afectando la visibilidad técnica y la estructura de navegación profesional.
[INFORMATIVA] Error de análisis CMS: No fue posible detectar la plataforma de gestión de contenidos ni su versión debido a bloqueos en el escaneo.