EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://systemprogramming.servebber.com/s2	Checks	9 pruebas
Dominio	systemprogramming.servebber.com	Hallazgos	15 totales
Fecha	21 de abril de 2026 a las 20:21	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 73/100, lo que corresponde a una calificación de grado C. Durante el proceso se ejecutaron 9 checks pasivos, identificando un cumplimiento correcto únicamente en la gestión de puertos abiertos, mientras que se registraron fallos críticos en la infraestructura de cifrado y archivos de configuración. La imposibilidad de verificar elementos esenciales como los certificados de seguridad y las cabeceras de protección sugiere una configuración de servidor restrictiva o mal implementada. Tras analizar los resultados obtenidos, se concluye que el sitio es actualmente vulnerable debido a la falta de visibilidad sobre sus mecanismos de defensa básicos.

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

[CRITICAL] Conexion SSL: No se pudo establecer una conexion SSL/TLS, lo que impide garantizar la privacidad de los datos transmitidos.
[HIGH] Cabeceras de Seguridad: No se pudieron verificar las directivas de seguridad, dejando al sitio potencialmente expuesto a ataques de inyeccion o clickjacking.
[MEDIUM] Redireccion HTTPS: Existe una falla en la validacion del forzado de trafico cifrado, permitiendo posibles conexiones inseguras bajo HTTP.
[LOW] Robots.txt y Sitemap: El servidor presenta errores al acceder a estos archivos, lo que dificulta la gestion del rastreo y la indexacion adecuada.
[LOW] Seguridad de Cookies: No se pudo confirmar la presencia de atributos de proteccion en las cookies, lo que podria comprometer las sesiones de usuario.
[LOW] Contenido Mixto: La falta de verificacion de elementos cargados mediante fuentes no seguras representa un riesgo para la integridad de la pagina.
[LOW] Deteccion de CMS: El sistema no permite identificar la plataforma de gestion de contenidos ni su version, impidiendo el analisis de parches conocidos.