EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://seguridad.evidenciainformarica.com.ec	Checks	9 pruebas
Dominio	seguridad.evidenciainformarica.com.ec	Hallazgos	15 totales
Fecha	22 de abril de 2026 a las 16:09	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el dominio ha resultado en una puntuación de 73/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 1 resultado exitoso y 1 fallo crítico identificado, mientras que el resto de los parámetros no pudieron ser validados debido a errores de respuesta del servidor. La ausencia de una conexión cifrada verificable y la falta de archivos de configuración básica comprometen la integridad del sitio. En conclusión, el sitio web se considera vulnerable debido a fallas graves en su infraestructura de seguridad básica.

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] Conexión SSL/TLS: No se pudo establecer una conexión segura con el servidor, lo que impide el cifrado de la información y expone los datos a intercepciones.
[HIGH] Cabeceras de Seguridad: No se detectaron cabeceras HTTP de seguridad, dejando el sitio expuesto a ataques de inyección, clickjacking y robo de sesiones.
[HIGH] Redirección HTTPS: El servidor no fuerza el uso de conexiones seguras, permitiendo que los usuarios naveguen a través de protocolos vulnerables.
[MEDIUM] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, lo que podría facilitar el secuestro de sesiones.
[LOW] Archivos de Indexación (robots.txt y sitemap.xml): Los archivos no están accesibles o no existen, lo que dificulta el control de rastreo por parte de motores de búsqueda.
[LOW] Detección de CMS: La configuración del servidor impide identificar la tecnología base, lo que si bien oculta información, también indica problemas de visibilidad para auditorías.