EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.peru21.com	Checks	9 pruebas
Dominio	www.peru21.com	Hallazgos	15 totales
Fecha	31 de julio de 2026 a las 01:53	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio www.peru21.com ha arrojado una puntuación de 73/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 1 resultó satisfactorio y 1 se identificó como un fallo crítico de configuración. La auditoría muestra deficiencias significativas en la validación de protocolos de cifrado y cabeceras de protección esenciales. Debido a la imposibilidad de confirmar parámetros de seguridad básicos en el servidor, se concluye que el sitio es actualmente vulnerable. Se requiere una intervención técnica inmediata para mitigar riesgos de interceptación de datos y mejorar la postura 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

[CRITICO] Conexion SSL/TLS: No se pudo establecer una conexion segura con el servidor, lo cual impide el cifrado de la informacion y expone los datos de los usuarios a ataques de interceptacion.
[ALTO] Cabeceras de Seguridad: No se detectaron ni validaron cabeceras HTTP de proteccion, lo que facilita ataques de Cross-Site Scripting y Clickjacking.
[ALTO] Redireccion HTTPS: El sitio no garantiza la transicion forzosa de trafico inseguro a seguro, dejando sesiones expuestas.
[ALTO] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, aumentando el riesgo de robo de sesiones.
[BAJO] Ausencia de robots.txt y sitemap.xml: El servidor denego el acceso a estos archivos, lo que afecta negativamente al rastreo controlado y a la organizacion del sitio.