EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://reimaginarte.com.ar	Checks	9 pruebas
Dominio	reimaginarte.com.ar	Hallazgos	36 totales
Fecha	3 de junio de 2026 a las 21:26	Problemas	6 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 85/100, lo que corresponde a una nota B. Se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 1 generó advertencias y 1 se identificó como fallo crítico. Si bien el sitio presenta una base sólida en cuanto a cifrado SSL y cabeceras de seguridad, la exposición de puertos críticos de infraestructura compromete la red interna. Por lo tanto, el sitio se considera vulnerable hasta que se restrinja el acceso a los servicios de base de datos y transferencia de archivos detectados.

Resumen de Riesgos

1	1	0	4	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Deteccion CMS	100	OK	No se detecto un CMS conocido
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-08-13T15:30:45.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-15T15:30:46.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests ...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN

- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=()

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  PHP/8.3.30

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro

- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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] Puerto 3306 (MySQL) ABIERTO: La base de datos está expuesta a internet, lo que permite intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP) ABIERTO: Este protocolo transfiere credenciales y archivos en texto plano, facilitando la interceptación de datos sensibles.
[LOW] Puerto 21 y 3306 expuestos: El acceso externo a estos servicios aumenta significativamente la superficie de ataque del servidor.
[LOW] Server header expuesto: Se revela el uso de LiteSpeed, permitiendo a potenciales atacantes buscar vulnerabilidades específicas para esa tecnología.
[LOW] X-Powered-By expuesto: La cabecera indica el uso de PHP/8.3.30, proporcionando información técnica innecesaria sobre el entorno de ejecución.
[LOW] Faltan robots.txt y sitemap.xml: La ausencia de estos archivos afecta la indexación y revela una falta de configuración en la estructura pública del sitio.