EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://multicontas.com.br	Checks	9 pruebas
Dominio	multicontas.com.br	Hallazgos	42 totales
Fecha	20 de julio de 2026 a las 16:18	Problemas	14 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta un nivel de seguridad regular, obteniendo una puntuación exacta de 64/100 con una nota de C. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 fallaron debido a configuraciones críticas de infraestructura. Aunque el cifrado SSL es sólido, la exposición pública de bases de datos y la ausencia total de cabeceras de seguridad representan riesgos significativos. Se concluye que el sitio es actualmente vulnerable a ataques de acceso no autorizado y manipulación de tráfico.

Resumen de Riesgos

2	5	4	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	4 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-09-05T01:31:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-07T01:32:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://multicontas.com.br/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

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 — 20/100

Estado: FALLO

4 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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 MySQL es accesible desde internet, permitiendo ataques de fuerza bruta o explotación directa.
[CRITICAL] Puerto 5432 (PostgreSQL) abierto: La exposición de este puerto facilita la exfiltración de datos sensibles y compromete la integridad del servidor.
[HIGH] Content-Security-Policy (CSP): La falta de esta cabecera permite ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta protección hace que el sitio sea vulnerable a ataques de Clickjacking.
[HIGH] Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS a nivel de navegador, permitiendo ataques de degradación de protocolo.
[HIGH] Puerto 21 (FTP) abierto: El uso de FTP sin cifrar expone credenciales y archivos durante la transferencia en la red.
[MEDIUM] X-Content-Type-Options: El sitio permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a terceros, comprometiendo la privacidad de la navegación.

[MEDIUM] Permissions-Policy: No se restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 22 (SSH) abierto: La interfaz de administración remota está expuesta, aumentando la superficie de ataque para accesos no autorizados.
[LOW] Server header expuesto (LiteSpeed): Revelar el software del servidor ayuda a los atacantes a buscar vulnerabilidades específicas conocidas.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la indexación controlada y revela una gestión deficiente de la estructura web.