EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://supermercadosbm.ldcloud.pro/	Checks	9 pruebas
Dominio	supermercadosbm.ldcloud.pro	Hallazgos	39 totales
Fecha	21 de mayo de 2026 a las 23:59	Problemas	13 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el activo arroja una puntuación de 63/100 con una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 1 generó advertencias y 2 terminaron en fallo crítico. A pesar de contar con un cifrado SSL válido, la ausencia total de cabeceras de seguridad y la exposición de puertos administrativos representan un riesgo considerable. Se concluye que el sitio es actualmente vulnerable y requiere intervenciones técnicas inmediatas para mitigar posibles vectores de ataque.

Resumen de Riesgos

0	5	4	4	26
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 300 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 300 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  300 dias restantes (expira: 2027-03-17T22:47:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-13T22:47:27.000Z
- 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: Microsoft-IIS/10.0 — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje

- 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 — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 404 — No redirige a HTTPS

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**
  ASP.NET

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 — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- 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)**
  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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking mediante el uso de marcos o iframes.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS, lo que permite ataques de degradación de protocolo y robo de cookies de sesión.
[HIGH] Redireccion HTTPS: El servidor no redirige el tráfico inseguro al puerto seguro, dejando a los usuarios expuestos en conexiones HTTP.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto que transmite credenciales y datos en texto plano sin cifrado.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador interprete archivos de forma incorrecta mediante el sniffing de tipos MIME.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a otros sitios, lo que puede derivar en la fuga de datos sensibles en la URL.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 22 (SSH): Acceso remoto para administración expuesto públicamente, aumentando la superficie de ataque para fuerza bruta.
[LOW] Server header expuesto: Se revela la versión específica Microsoft-IIS/10.0, lo cual facilita la búsqueda de vulnerabilidades conocidas para ese software.
[LOW] X-Powered-By expuesto: El uso de ASP.NET es visible públicamente, proporcionando información valiosa a un atacante sobre el framework de desarrollo.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 404 para archivos de configuración esenciales de rastreo e indexación.