

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://ventasonline.comercialmultimas.cl/	Checks	9 pruebas
Dominio	ventasonline.comercialmultimas.cl	Hallazgos	49 totales
Fecha	2 de junio de 2026 a las 16:34	Problemas	8 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio ventasonline.comercialmultimas.cl arrojó una puntuación de 82/100, lo que equivale a una nota de calificación B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 se marcó como fallo crítico. Si bien el sitio presenta una base sólida en cuanto a su certificado SSL y la ausencia de puertos innecesarios expuestos, existen deficiencias importantes en la configuración de cabeceras y gestión de sesiones. Se concluye que el sitio es generalmente estable pero vulnerable a ataques de secuestro de sesión y degradación de protocolo debido a configuraciones de cookies incompletas.

Resumen de Riesgos

0	6	2	0	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 142 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	0	FALLO	flash-old: falta HttpOnly; flash-old: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 142 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
142 dias restantes (expira: 2026-10-22T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2025-09-23T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- INFO Content-Security-Policy
Presente: frame-ancestors 'none'

- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: no-referrer
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), autoplay=(), fullscreen=()

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://ventasonline.comercialmultimas.cl:443/
- 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
- INFO

Tecnologias detectadas
Next.js

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 — 0/100

Estado: FALLO

flash-old: falta HttpOnly; flash-old: falta Secure; flash-old: falta SameSite; session-v1.2: falta HttpOnly; session-v1.2: falta Secure; session-v1.2: falta SameSite

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)
- ALTO

Cookie: flash-old — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO

Cookie: flash-old — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: flash-old — SameSite
Falta SameSite — Vulnerable a CSRF
- ALTO

Cookie: session-v1.2 — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO

Cookie: session-v1.2 — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: session-v1.2 — SameSite
Falta SameSite — Vulnerable a CSRF

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (107 bytes)
- INFO

Reglas robots.txt
3 Disallow, 0 Allow
- INFO

sitemap.xml
Presente, 745 URLs
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)
Abierto (esperado) — Servidor web
- INFO

Puerto 443 (HTTPS)
Abierto (esperado) — 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] Strict-Transport-Security: La ausencia de la cabecera HSTS permite que un atacante pueda forzar la comunicación a través de HTTP, facilitando ataques de interceptación de datos.

[HIGH] Cookie flash-old - HttpOnly: Esta cookie carece del flag HttpOnly, lo que la hace accesible mediante scripts de JavaScript y eleva el riesgo de robo de identidad en ataques XSS.

[HIGH] Cookie flash-old - Secure: Al no tener el flag Secure, la cookie puede ser transmitida a través de conexiones no cifradas, exponiendo información sensible en redes inseguras.

[HIGH] Cookie session-v1.2 - HttpOnly: El identificador de sesión es vulnerable a ser extraído por scripts maliciosos al no tener activa la protección HttpOnly.

[HIGH] Cookie session-v1.2 - Secure: La sesión del usuario podría ser interceptada si se transmite por un canal HTTP debido a la falta del flag de seguridad obligatorio.

[MEDIUM] Cookie flash-old - SameSite: La falta de este atributo permite que la cookie sea enviada en peticiones de terceros, lo que facilita ataques de falsificación de petición en sitios cruzados (CSRF).

[MEDIUM] Cookie session-v1.2 - SameSite: Sin el flag SameSite, la sesión del usuario queda desprotegida ante acciones no autorizadas iniciadas desde sitios web externos.