EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.facesbeauty.cl/checkout/?socialselling=on#/payment	Checks	9 pruebas
Dominio	www.facesbeauty.cl	Hallazgos	50 totales
Fecha	29 de abril de 2026 a las 21:53	Problemas	14 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación técnica de 71/100, lo que corresponde a una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron correctos, 3 generaron advertencias y 1 fue calificado como fallo crítico. Se han detectado deficiencias importantes en la implementación de cabeceras de seguridad y en la protección de cookies de sesión. Debido a estas omisiones técnicas y a la exposición de rutas administrativas, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación y manipulación de datos.

Resumen de Riesgos

0	4	8	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 74 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	67	AVISO	VtexWorkspace: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-07-12T16:08:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-13T16:08:28.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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://www.facesbeauty.cl/
- 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

VtexWorkspace: falta HttpOnly

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: VtexWorkspace — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: VtexWorkspace — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: VtexWorkspace — SameSite**
  SameSite=none

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 (3815 bytes)
- INFO **Reglas robots.txt**
  47 Disallow, 30 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.facesbeauty.cl/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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

MEDIO **Puerto 8080 (HTTP-Alt)**

ABIERTO — 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 ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: Al no contar con HSTS, el sitio no obliga al navegador a usar conexiones HTTPS, permitiendo posibles degradaciones de seguridad.
[HIGH] Cookie VtexWorkspace: El atributo HttpOnly no está configurado, lo que permite que la cookie de sesión sea robada mediante scripts maliciosos.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera expone a los usuarios a ataques de MIME-type sniffing.
[MEDIUM] Referrer-Policy: No se controla la información que el navegador envía a otros sitios cuando se hace clic en un enlace saliente.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador, como el acceso a la cámara o el micrófono, aumentando el riesgo de privacidad.
[MEDIUM] Archivos técnicos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, pudiendo revelar versiones internas del software.
[MEDIUM] Ruta /wp-login.php: Se detectó un panel de acceso administrativo expuesto, lo cual facilita ataques de fuerza bruta.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y podría alojar servicios alternativos sin la debida protección.
[MEDIUM] Configuración de robots.txt: El archivo bloquea el acceso total al sitio y revela rutas sensibles bajo el término admin.
[LOW] Server header expuesto: El servidor responde con la cabecera Server: cloudflare, revelando información sobre la arquitectura tecnológica utilizada.