

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.theperfumeshop.com/
Dominio www.theperfumeshop.com
Fecha 12 de mayo de 2026 a las 13:37

Checks 9 pruebas
Hallazgos 43 totales
Problemas 8 detectados

C

70/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el dominio theperfumeshop.com ha resultado en una puntuacion exacta de 70/100 y una nota final de C. Durante el analisis se ejecutaron un total de 9 checks pasivos, de los cuales 7 se marcaron como correctos y 2 resultaron en fallos criticos de configuracion. Aunque la infraestructura basica de cifrado es solida, se detectaron deficiencias importantes en las cabeceras de seguridad y en la gestion del trafico cifrado. Debido a la ausencia de mecanismos de proteccion contra ataques de suplantacion y la falta de forzado de conexiones seguras, el sitio se clasifica actualmente como vulnerable ante amenazas comunes de la web.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 93 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	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 93 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
93 dias restantes (expira: 2026-08-13T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2025-08-12T00:00:00.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

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

- INFO **Content-Security-Policy**
Presente: frame-ancestors 'self' *.theperfumeshop.com;
- 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: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (605 bytes)
- INFO **Reglas robots.txt**
21 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
<https://www.theperfumeshop.com/sitemap.xml>
- 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] X-Frame-Options: Falta — Esta cabecera es inexistente, lo que permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.

[HIGH] Strict-Transport-Security: Falta — La ausencia de HSTS impide que el navegador fuerce conexiones cifradas, exponiendo a los usuarios a ataques de degradacion de protocolo.

[HIGH] Redireccion HTTP a HTTPS: Fallida — El servidor no redirige automaticamente las peticiones inseguras a la version protegida, devolviendo un error 403 en su lugar.

[MEDIUM] X-Content-Type-Options: Falta — Al no estar configurada, el navegador podria interpretar archivos de forma incorrecta, permitiendo la ejecucion de scripts maliciosos mediante sniffing de contenido.

[MEDIUM] Referrer-Policy: Falta — No se controla la información de navegación que se envía a terceros cuando un usuario hace clic en un enlace externo.

[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la geolocalización, cámara o micrófono.

[LOW] Server header expuesto: AkamaiGHost — La cabecera revela el uso de tecnología Akamai, lo cual proporciona información valiosa a atacantes potenciales para realizar reconocimiento de infraestructura.