EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://skin.club/es	Checks	9 pruebas
Dominio	skin.club	Hallazgos	59 totales
Fecha	11 de abril de 2026 a las 23:39	Problemas	10 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web arroja una puntuación de 86/100 con una calificación de grado B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 generaron advertencias, sin detectarse fallos críticos de seguridad. Los resultados indican una infraestructura base sólida, especialmente en el cifrado de comunicaciones y la configuración del servidor de nombres. Sin embargo, se han identificado debilidades en la protección de la capa de aplicación y en la configuración de las cookies de sesión. En conclusión, el sitio se considera mayoritariamente seguro, aunque presenta vulnerabilidades de severidad alta y media que requieren atención inmediata para mitigar riesgos de suplantación y robo de datos.

Resumen de Riesgos

0	3	5	2	49
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	70	AVISO	4/6 presentes. Faltan: X-Frame-Options, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	58	AVISO	ld.context-key: falta SameSite; lang: falta Http...
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 65 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  65 dias restantes (expira: 2026-06-15T19:46:36.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-17T18:46:49.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 70/100

Estado: AVISO

4/6 presentes. Faltan: X-Frame-Options, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self' 'unsafe-inline' data: https: wss:; img-src 'self' data: blob:...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://skin.club/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 dias)
- 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
- INFO **Tecnologias detectadas**
  Nuxt

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 — 58/100

Estado: AVISO

ld.context-key: falta SameSite; lang: falta HttpOnly; lang: falta Secure; lang: falta SameSite; __cf_bm: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- INFO **Cookie: ld.context-key — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ld.context-key — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ld.context-key — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: lang — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: lang — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __cf_bm — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: _cfuvid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _cfuvid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _cfuvid — 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 (376 bytes)
- INFO **Reglas robots.txt**
  14 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://skin.club/sitemap_index.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

[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, lo que facilita a un atacante identificar la tecnología de protección empleada.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en iframes, exponiendo a los usuarios a ataques de clickjacking.
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, lo que podría permitir el acceso no autorizado a funciones como la cámara o el micrófono.
[MEDIUM] Cookie ld.context-key: Falta el atributo SameSite, lo que hace a la cookie vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[HIGH] Cookie lang (HttpOnly): La falta de este flag permite que la cookie sea accesible mediante scripts, aumentando el riesgo de robo de sesión a través de ataques XSS.
[HIGH] Cookie lang (Secure): La ausencia del flag Secure permite que la cookie sea transmitida por canales no cifrados, comprometiendo su integridad.
[MEDIUM] Cookie lang (SameSite): La falta de esta restricción facilita vectores de ataque para el secuestro de acciones del usuario.
[MEDIUM] Cookie __cf_bm: No define una política SameSite, incrementando la superficie de ataque para peticiones no autorizadas.
[LOW] Ruta sensible en robots.txt: La referencia directa al directorio admin en el archivo robots.txt revela rutas de gestión interna a posibles atacantes.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, lo cual puede exponer servicios administrativos o proxies no destinados al acceso público.