

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://Lookfantastic.com
Dominio lookfantastic.com
Fecha 11 de mayo de 2026 a las 04:33

Checks 9 pruebas
Hallazgos 60 totales
Problemas 11 detectados

B

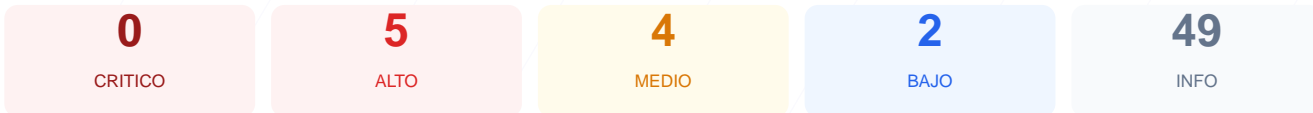
86/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al dominio ha resultado en una puntuación de 86/100 con una calificación de grado B. De los 9 checks pasivos ejecutados, 7 resultaron satisfactorios, mientras que se identificó 1 advertencia y 1 fallo crítico relacionado con la configuración de seguridad. Aunque el cifrado de datos es robusto, la ausencia de cabeceras de protección y la gestión insegura de cookies de sesión presentan riesgos de seguridad. Se concluye que el sitio es generalmente seguro en su transporte de datos, pero vulnerable a ataques de manipulación de interfaz y robo de sesiones.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 dias
Cabeceras de Seguridad	45	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, X-C...
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	67	AVISO	chumewe_user: falta HttpOnly; chumewe_user_versi...
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 45 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
45 dias restantes (expira: 2026-06-25T07:53:00.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-27T07:53:01.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
Presente: child-src 'self' https://insight.adsrvr.org https://match.adsrvr.org https://*.j...
- ALTO **X-Frame-Options**
Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
Presente: max-age=31557600
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://lookfantastic.com/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31557600
- BAJO **HSTS includeSubDomains**
HSTS no cubre subdominios
- INFO **HSTS max-age**
max-age=31557600 (365 dias)
- 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
- BAJO **Meta generator**
Expone: Astro v5.15.8
- INFO **Tecnologias detectadas**
Next.js, Astro

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 — 67/100

Estado: AVISO

chumewe_user: falta HttpOnly; chumewe_user_version: falta HttpOnly; chumewe_sess: falta HttpOnly; chumewe_sess_version: falta HttpOnly

- INFO **Cookies detectadas**
4 cookie(s) encontrada(s)
- ALTO **Cookie: chumewe_user — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: chumewe_user — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: chumewe_user — SameSite**
SameSite=none
- ALTO **Cookie: chumewe_user_version — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: chumewe_user_version — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: chumewe_user_version — SameSite**
SameSite=none
- ALTO **Cookie: chumewe_sess — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: chumewe_sess — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: chumewe_sess — SameSite**
SameSite=none
- ALTO **Cookie: chumewe_sess_version — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: chumewe_sess_version — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: chumewe_sess_version — 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 (5619 bytes)
- INFO **Reglas robots.txt**
139 Disallow, 0 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
https://www.lookfantastic.com/sitemapindex-product.xml.gz
- INFO **security.txt**
Presente en /.well-known/security.txt — Buena practica

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 — Envío 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 autenticación 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: La ausencia de esta cabecera permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking para engañar a los usuarios.

[HIGH] Cookies sin atributo HttpOnly: Las cookies chumewe_user, chumewe_user_version, chumewe_sess y chumewe_sess_version carecen de esta bandera, permitiendo que sean accesibles mediante JavaScript y aumentando el riesgo de robo de identidad en ataques XSS.

[MEDIUM] X-Content-Type-Options: Falta la directiva para evitar el sniffing de tipos MIME, lo que podría permitir al navegador ejecutar contenido malicioso disfrazado de archivos legítimos.

[MEDIUM] Referrer-Policy: No existe una política definida, lo que provoca que información sensible de la URL pueda filtrarse a dominios externos al navegar.

[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.

[MEDIUM] Bloqueo total en robots.txt: El archivo robots.txt contiene una directiva Disallow que impide el rastreo completo del sitio, lo cual puede ser un error de configuración administrativa.

[LOW] Exposición de tecnología del servidor: La cabecera Server revela el uso de Cloudflare, facilitando la fase de reconocimiento a un atacante.

[LOW] Versión de tecnología expuesta: La etiqueta meta generator revela el uso de Astro v5.15.8, permitiendo a potenciales atacantes buscar vulnerabilidades específicas para esa versión.