

Escanear Vulnerabilidades

Informe de Seguridad Web

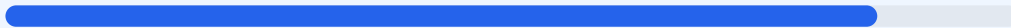
URL https://cultbeauty.co.uk
Dominio cultbeauty.co.uk
Fecha 12 de mayo de 2026 a las 02:00

Checks 9 pruebas
Hallazgos 60 totales
Problemas 11 detectados

B

86/100

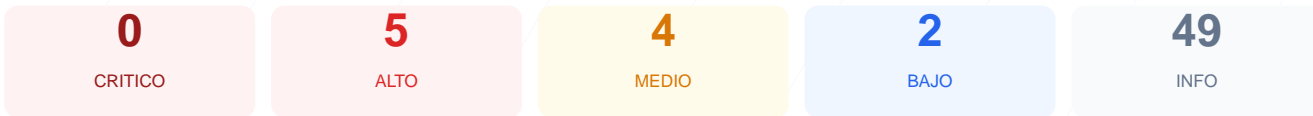
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado a la plataforma arroja una puntuación de 86/100, lo que otorga una calificación de nota B. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias, se registró 1 advertencia y se detectó 1 fallo crítico en la configuración de seguridad. Aunque el cifrado de datos y la redirección segura son impecables, existen debilidades importantes en la protección del navegador y la gestión de sesiones. El sitio presenta una base técnica sólida pero se mantiene vulnerable a ataques de secuestro de sesión y manipulación de interfaz. En conclusión, el estado general es aceptable, pero requiere intervenciones inmediatas para alcanzar un nivel de seguridad empresarial óptimo.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 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 44 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
44 dias restantes (expira: 2026-06-25T07:47:57.000Z)
- INFO Fecha de emision
Emitido desde: 2026-03-27T07:47:58.000Z
- 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://cultbeauty.co.uk/
- 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 (5489 bytes)
- INFO **Reglas robots.txt**
135 Disallow, 0 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
https://www.cultbeauty.co.uk/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] Cookies sin flag HttpOnly: Las cookies chumewe_user y chumewe_sess son accesibles vía scripts, lo que permite a un atacante robar sesiones de usuario mediante ataques XSS.

[HIGH] X-Frame-Options: La ausencia de esta cabecera de seguridad permite que el sitio sea embebido en marcos maliciosos, facilitando ataques de Clickjacking.

[MEDIUM] X-Content-Type-Options: Al faltar esta protección, el navegador podría interpretar archivos de forma incorrecta, permitiendo la ejecución de código no deseado.

[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que puede exponer información sensible de la URL al navegar hacia enlaces externos.

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

[MEDIUM] Bloqueo total en Robots.txt: El archivo de rastreo prohíbe el acceso a todo el contenido del sitio, lo cual puede ser un error de configuración o una medida de ofuscación inusual.

[LOW] Server header expuesto: El servidor revela que utiliza la tecnología Cloudflare, proporcionando información útil para que un atacante profile la infraestructura.

[LOW] Meta generator expuesto: Se identifica públicamente el uso de Astro v5.15.8, permitiendo la búsqueda de vulnerabilidades específicas asociadas a dicha versión del framework.