EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://caminante.cat	Checks	9 pruebas
Dominio	caminante.cat	Hallazgos	47 totales
Fecha	31 de agosto de 2026 a las 16:02	Problemas	13 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 62/100, lo que corresponde a una calificación de grado C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias por configuraciones mejorables y 2 fallos críticos en la infraestructura de seguridad. A pesar de contar con un cifrado de transporte válido, la ausencia de cabeceras de protección y el uso de protocolos de transferencia obsoletos elevan el riesgo operativo. En conclusión, el sitio se considera vulnerable debido a carencias importantes en la gestión de sesiones y en el endurecimiento del servidor.

Resumen de Riesgos

0	7	4	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-11-18T10:06:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-20T10:06:07.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://caminante.cat/
- 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

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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (171 bytes)
- INFO **Reglas robots.txt**
  5 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://caminante.cat/sitemap.php
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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

[ALTA] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos no está cifrado, lo que permite la interceptación de credenciales y datos por parte de terceros.
[ALTA] Cookies de sesión inseguras: La cookie PHPSESSID carece de los atributos HttpOnly y Secure, permitiendo que sea robada mediante scripts maliciosos o interceptada en conexiones no seguras.
[ALTA] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita ataques de inyección de contenido y Cross-Site Scripting (XSS).
[ALTA] Falta de X-Frame-Options: El sitio no previene el enmarcado de su contenido, siendo vulnerable a ataques de secuestro de clics o clickjacking.
[ALTA] Falta de Strict-Transport-Security: No existe una directiva HSTS que obligue al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIA] Falta de X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos maliciosos disfrazados.
[MEDIA] Falta de Referrer-Policy: No se controla la cantidad de información que el navegador envía al navegar hacia otros enlaces.
[MEDIA] Falta de Permissions-Policy: No hay restricciones sobre el acceso a funciones sensibles del navegador como la cámara, el micrófono o la ubicación.
[MEDIA] Cookie sin atributo SameSite: La sesión PHPSESSID es susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[BAJA] Exposición de cabecera Server: El servidor revela que opera bajo Apache, proporcionando información útil para que un atacante busque vulnerabilidades específicas de esa versión.
[BAJA] Ruta sensible en robots.txt: Se ha detectado una referencia directa al directorio admin, facilitando la identificación de áreas de gestión privada.