EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://topayuda.es	Checks	9 pruebas
Dominio	topayuda.es	Hallazgos	48 totales
Fecha	12 de mayo de 2026 a las 12:37	Problemas	6 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web arroja una puntuación técnica de 83/100, lo que representa una calificación de nota B. El análisis se basó en 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue identificado como fallo de seguridad. Se observa una implementación robusta en el cifrado de datos y la configuración del servidor, aunque existen debilidades críticas en la gestión de sesiones y cabeceras de protección. A pesar de los resultados positivos en infraestructura, el sitio se considera vulnerable a ataques dirigidos contra los usuarios debido a la falta de políticas de seguridad aplicadas al navegador.

Resumen de Riesgos

0	4	2	0	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 75 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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	33	FALLO	locale: falta HttpOnly; locale: falta Secure; _t...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 75 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  75 dias restantes (expira: 2026-07-26T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-27T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

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

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-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://topayuda.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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

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 — 33/100

Estado: FALLO

locale: falta HttpOnly; locale: falta Secure; _top_assmat_session: falta Secure; _top_assmat_session: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: locale — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: locale — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: locale — SameSite**
  SameSite=lax
- INFO **Cookie: _top_assmat_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: _top_assmat_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: _top_assmat_session — 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 — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, ? URLs
- 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] Content-Security-Policy: Falta — La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] Cookie: locale (HttpOnly): Falta — Al no tener el flag HttpOnly, la cookie es accesible mediante scripts, facilitando el robo de información en caso de vulnerabilidad XSS.
[HIGH] Cookie: locale (Secure): Falta — La cookie puede enviarse a través de conexiones no cifradas, exponiendo datos en redes inseguras.
[HIGH] Cookie: _top_assmat_session (Secure): Falta — Los identificadores de sesión se transmiten sin el flag de seguridad, lo que permite su interceptación en tránsito.
[MEDIUM] Permissions-Policy: Falta — No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, aumentando la superficie de ataque.
[MEDIUM] Cookie: _top_assmat_session (SameSite): Falta — La carencia de este atributo hace que el sitio sea susceptible a ataques de falsificación de solicitudes entre sitios o CSRF.
[LOW] Robots.txt: Falta — La inexistencia de este archivo impide gestionar correctamente el rastreo de los motores de búsqueda sobre el contenido del sitio.