EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pipilacha.es	Checks	9 pruebas
Dominio	pipilacha.es	Hallazgos	50 totales
Fecha	25 de abril de 2026 a las 19:00	Problemas	8 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica del sitio web ha resultado en una puntuación de 79/100, lo que equivale a una nota de B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 fueron satisfactorios, 1 generó una advertencia y 2 resultaron en fallo crítico. Aunque el cifrado de datos es robusto, se han identificado carencias importantes en las políticas de seguridad de las cabeceras y en la protección de las cookies. Debido a la falta de defensas contra ataques de inyección, el sitio se considera vulnerable a pesar de tener una base de infraestructura estable.

Resumen de Riesgos

0	2	4	2	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Squarespace
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	crumb: falta HttpOnly; crumb: falta SameSite
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
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 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-07-08T03:56:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-09T03:56:15.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://www.pipilacha.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Squarespace

- 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**
  Detectado via HTML body
- INFO **Tecnologias detectadas**
  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 — 33/100

Estado: FALLO

crumb: falta HttpOnly; crumb: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: crumb — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: crumb — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: crumb — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://static1.squarespace.com/static/68905151cfadb270466a04...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1507 bytes)
- INFO **Reglas robots.txt**
  27 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.pipilacha.es/sitemap.xml
- 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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
El análisis de seguridad técnica del sitio web ha resultado en una puntuación de 79/100, lo que equivale a una nota de B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 fueron satisfactorios, 1 generó una advertencia y 2 resultaron en fallo crítico. Aunque el cifrado de datos es robusto, se han identificado carencias importantes en las políticas de seguridad de las cabeceras y en la protección de las cookies. Debido a la falta de defensas contra ataques de inyección, el sitio se considera vulnerable a pesar de tener una base de infraestructura estable.

---VULNERABILITIES---
[HIGH] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] Cookie HttpOnly: La cookie denominada crumb no tiene el atributo HttpOnly, permitiendo que scripts de terceros accedan a ella y faciliten el robo de sesiones.
[MEDIUM] Cookie SameSite: La cookie crumb carece de la instrucción SameSite, dejando el sitio expuesto a ataques de falsificación de petición en sitios cruzados o CSRF.
[MEDIUM] Referrer-Policy: Ausencia de una política que controle cuánta información de procedencia se envía a otros dominios al navegar.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de funciones del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Contenido Mixto: Se detectó un recurso de hoja de estilo cargándose a través de una conexión HTTP no segura dentro de la página HTTPS.
[LOW] Server header expuesto: La cabecera del servidor revela explícitamente el uso de Squarespace, ayudando a posibles atacantes en la fase de reconocimiento.
[LOW] Ruta sensible en robots.txt: El archivo robots.txt menciona la ruta config, lo cual puede orientar a actores malintencionados hacia áreas administrativas.