EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mad.es/	Checks	9 pruebas
Dominio	mad.es	Hallazgos	59 totales
Fecha	19 de mayo de 2026 a las 08:41	Problemas	11 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 85/100, lo que equivale a una nota B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, 1 generó una advertencia y 1 fue calificado como fallo. La infraestructura de cifrado es sólida, pero existen carencias importantes en las políticas de seguridad aplicadas a las cabeceras HTTP y en la gestión de cookies. Se concluye que el sitio es generalmente seguro para la navegación, pero presenta vulnerabilidades técnicas que deben ser mitigadas para prevenir ataques dirigidos contra los usuarios.

Resumen de Riesgos

0	3	6	2	48
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 304 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: PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	50	AVISO	debug: falta HttpOnly; debug: falta Secure; debu...
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 304 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  304 dias restantes (expira: 2027-03-18T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-16T00:00:00.000Z
- 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: Apache — 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=31536000; includeSubDomains; preload
- 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://mad.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js

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 — 50/100

Estado: AVISO

debug: falta HttpOnly; debug: falta Secure; debug: falta SameSite; MADSESSID: falta SameSite; PrestaShop-7691f2ae12be10eb29c8442113485ae4: falta SameSite; PrestaShop-7691f2ae12be10eb29c8442113485ae4: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- ALTO **Cookie: debug — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: debug — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: debug — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: MADSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: MADSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: MADSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: PrestaShop-7691f2ae12be10eb29c8442113485ae4 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-7691f2ae12be10eb29c8442113485ae4 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PrestaShop-7691f2ae12be10eb29c8442113485ae4 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: PrestaShop-7691f2ae12be10eb29c8442113485ae4 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-7691f2ae12be10eb29c8442113485ae4 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PrestaShop-7691f2ae12be10eb29c8442113485ae4 — 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 (3968 bytes)
- INFO **Reglas robots.txt**
  91 Disallow, 17 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://mad.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 Seguridad

VULNERABILIDADES DETECTADAS

[ALTA] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de ataques XSS y la inyección de contenido externo no autorizado.
[ALTA] Cookie debug (Flags faltantes): Carece de HttpOnly y Secure, lo que permite que la cookie sea leída por scripts maliciosos y enviada por canales no cifrados.
[MEDIA] Atributo SameSite faltante: Las cookies MADSESSID y de PrestaShop no definen este atributo, aumentando el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIA] Referrer-Policy: No se ha detectado esta cabecera, lo que impide controlar qué información de navegación se comparte con otros dominios.
[MEDIA] Permissions-Policy: La falta de esta configuración permite que el sitio acceda potencialmente a funciones del navegador como la cámara o el micrófono sin restricciones explícitas.
[BAJA] Server header expuesto: El servidor informa que utiliza Apache, revelando la tecnología base a posibles atacantes para buscar exploits específicos.
[BAJA] Ruta sensible en robots.txt: Se expone el directorio config, lo cual facilita la enumeración de rutas internas que deberían permanecer privadas.