EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://motherboard.es/	Checks	9 pruebas
Dominio	motherboard.es	Hallazgos	46 totales
Fecha	30 de julio de 2026 a las 08:30	Problemas	11 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web motherboard.es arroja una puntuación técnica de 72/100, lo que corresponde a una calificación de grado C. Durante la evaluación, se ejecutaron 9 checks pasivos que resultaron en 6 verificaciones satisfactorias, 2 advertencias por configuraciones mejorables y 1 fallo crítico en la implementación de seguridad. Aunque el sitio web cuenta con un cifrado de transporte robusto, la carencia absoluta de cabeceras de seguridad lo deja vulnerable frente a ataques de inyección y suplantación. En su estado actual, la plataforma se considera vulnerable debido a la exposición de información técnica y la falta de políticas de protección en el navegador.

Resumen de Riesgos

0	4	4	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 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	100	OK	No se encontraron cookies
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): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-10-01T12:09:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-03T12:09:36.000Z
- 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: nginx/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- 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://motherboard.es/
- 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
- BAJO **Meta generator**
  Expone: Ghost 6.54
- INFO **Tecnologias detectadas**
  Next.js, Express

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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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 (213 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://motherboard.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: El sitio no protege contra ataques de clickjacking, permitiendo que la web sea cargada en marcos externos no autorizados.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide forzar conexiones HTTPS y deja la sesión expuesta a ataques de degradación de protocolo.
[HIGH] HSTS no configurado: Aunque existe redirección a HTTPS, la falta de una directiva estricta permite que el navegador intente conexiones inseguras inicialmente.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores realicen MIME-type sniffing, pudiendo ejecutar archivos con tipos de contenido incorrectos.
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información que se envía en el encabezado Referer a otros dominios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición de este puerto facilita intentos de acceso remoto mediante fuerza bruta o explotación de servicios de administración.
[LOW] Server header expuesto: El servidor revela la versión exacta (nginx/1.24.0), lo que ayuda a atacantes a buscar exploits específicos para esa versión.
[LOW] X-Powered-By expuesto: Se identifica el uso del framework Express, proporcionando información valiosa para el reconocimiento de la infraestructura.
[LOW] Meta generator expuesto: La etiqueta meta revela el uso de Ghost 6.54, permitiendo identificar vulnerabilidades conocidas asociadas a dicho software.