EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cetrencada.cat	Checks	9 pruebas
Dominio	cetrencada.cat	Hallazgos	47 totales
Fecha	11 de agosto de 2026 a las 08:47	Problemas	16 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre cetrencada.cat ha otorgado una puntuación de 60/100, lo que resulta en una nota de grado C. Se han ejecutado 9 checks pasivos, de los cuales 5 han sido satisfactorios, 1 ha generado una advertencia y 3 han resultado en fallo crítico. La evaluación revela carencias significativas en la configuración del servidor y una exposición peligrosa de servicios internos. Debido a la visibilidad de puertos de bases de datos y la ausencia total de cabeceras de protección, el sitio se considera actualmente vulnerable. Se requiere una intervención inmediata para mitigar los riesgos de intrusión y robo de datos.

Resumen de Riesgos

1	6	7	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0.3 expuesta, WordPress 2 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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-10-11T08:09:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-13T08:09:15.000Z
- 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://cetrencada.cat/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 500

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 7.0.3
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.3 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.3 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 (194 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **sitemap.xml**
  Presente, 1754 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos está expuesta directamente a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options ausente: El sitio permite ser cargado en marcos externos, lo que lo hace vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS) no configurado: No se obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Puerto 21 (FTP) abierto: Este protocolo transmite información sin cifrar, lo que pone en riesgo las credenciales de acceso al servidor.
[HIGH] Versión de WordPress 7.0.3 expuesta: Revelar la versión específica permite a atacantes buscar vulnerabilidades conocidas (CVE) para este software.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de acceso remoto está visible, incrementando la superficie de ataque para accesos no autorizados.
[MEDIUM] X-Content-Type-Options ausente: El servidor no previene el sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts camuflados.
[MEDIUM] Referrer-Policy ausente: No se controla la información de procedencia enviada a terceros, comprometiendo la privacidad de los usuarios.
[MEDIUM] Permissions-Policy ausente: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela información técnica interna sobre el CMS que facilita el reconocimiento del sistema.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de administración es accesible públicamente, facilitando ataques dirigidos contra las cuentas de administrador.
[MEDIUM] Robots.txt con bloqueo total: El archivo impide el rastreo de todo el sitio, lo cual puede ser un indicio de configuraciones erróneas o contenido oculto.
[LOW] Server header expuesto: Se revela el uso de Apache, permitiendo a los atacantes perfilar mejor la infraestructura del servidor.
[LOW] Meta generator expuesto: La etiqueta meta confirma el uso de WordPress 7.0.3, asistiendo en la fase de reconocimiento de un ataque.