EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.celra.cat/	Checks	9 pruebas
Dominio	www.celra.cat	Hallazgos	53 totales
Fecha	29 de abril de 2026 a las 09:20	Problemas	24 detectados

D

40/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de ciberseguridad realizada arroja una puntuacion de 40/100, lo que equivale a una nota de D. El analisis se baso en 9 checks pasivos, de los cuales solo 2 resultaron satisfactorios, 2 presentaron advertencias y 5 finalizaron en fallo. Se han detectado deficiencias criticas en la configuracion del servidor y una exposicion alarmante de servicios internos. Tras evaluar los resultados, se concluye que el sitio es vulnerable y presenta un riesgo alto para la integridad de los datos y la disponibilidad del servicio.

Resumen de Riesgos

1	10	11	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 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 1.4.33 expuesta
Seguridad de Cookies	0	FALLO	wp_wpfileupload_d68a48e5cabbd9dee5606d1babaefb9a...
Contenido Mixto	20	FALLO	5 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 69 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  69 dias restantes (expira: 2026-07-07T07:00:24.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-08T07:00:25.000Z
- 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: HTTPd — 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 302 redirige a https://www.celra.cat/wp/
- 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

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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1.4.33 expuesta

- ALTO **WordPress version**
  Version 1.4.33 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)

Seguridad de Cookies — 0/100

Estado: FALLO

wp_wpfileupload_d68a48e5cabbd9dee5606d1babaefb9a: falta HttpOnly; wp_wpfileupload_d68a48e5cabbd9dee5606d1babaefb9a: falta Secure;

wp_wpfileupload_d68a48e5cabbd9dee5606d1babaefb9a: falta SameSite; acadp_rand_seed: falta HttpOnly; acadp_rand_seed: falta Secure; acadp_rand_seed: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: wp_wpfileupload_d68a48e5cabbd9dee5606d1babaefb9a — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: wp_wpfileupload_d68a48e5cabbd9dee5606d1babaefb9a — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: wp_wpfileupload_d68a48e5cabbd9dee5606d1babaefb9a — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: acadp_rand_seed — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: acadp_rand_seed — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: acadp_rand_seed — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

5 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://escoladedansa.celra.cat/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://tergavarres.cat/centre-dinterpretacio-del-camp-daviac...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://portaaporta.celra.cat/
- MEDIO **href (link/stylesheet)**
  ...y 2 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (30 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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 esta expuesta directamente a internet, permitiendo ataques de fuerza bruta o explotacion de vulnerabilidades de acceso.
[HIGH] WordPress version 1.4.33 expuesta: El uso de una version obsoleta permite a atacantes identificar y explotar vulnerabilidades conocidas (CVEs) para tomar el control del sitio.
[HIGH] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos no esta cifrado, lo que facilita la interceptacion de credenciales y datos en transito.
[HIGH] Content-Security-Policy falta: La ausencia de esta cabecera permite ataques de inyeccion de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options falta: El sitio no cuenta con proteccion contra Clickjacking, permitiendo que la web sea embebida en marcos maliciosos.
[HIGH] Strict-Transport-Security falta: No se fuerza el uso de HTTPS mediante HSTS, permitiendo ataques de degradacion de conexion.
[HIGH] Cookies sin flags de seguridad: Las cookies wp_wpfileupload y acadp_rand_seed carecen de HttpOnly y Secure, facilitando el robo de sesiones via scripts o redes inseguras.
[MEDIUM] Puerto 22 (SSH) abierto: Aunque es un acceso seguro, su exposicion publica incrementa la superficie de ataque mediante intentos de acceso remoto.
[MEDIUM] Contenido Mixto: Se detectaron 5 recursos cargando via HTTP en una pagina HTTPS, comprometiendo la integridad de la navegacion.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela informacion tecnica sobre la instalacion que ayuda a los atacantes en la fase de reconocimiento.
[MEDIUM] X-Content-Type-Options falta: El navegador puede intentar adivinar el tipo de contenido, lo que facilita ataques de sniffing de MIME-type.
[MEDIUM] Referrer-Policy y Permissions-Policy faltan: No existe control sobre la informacion de procedencia ni sobre el uso de APIs del navegador como la camara o el microfono.
[LOW] Cabecera Server expuesta: Se revela el uso de HTTPd, proporcionando pistas innecesarias sobre la tecnologia de servidor utilizada.
[LOW] sitemap.xml no encontrado: La falta de este archivo dificulta la auditoria de estructura y la indexacion correcta del sitio.