EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cin.cat/	Checks	9 pruebas
Dominio	www.cin.cat	Hallazgos	50 totales
Fecha	21 de abril de 2026 a las 19:57	Problemas	21 detectados

F

39/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al sitio web ha arrojado una puntuacion de 39/100, lo que equivale a una calificacion de grado F. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales unicamente 3 resultaron satisfactorios, mientras que se detectaron 1 advertencia y 5 fallos criticos. El sitio presenta deficiencias graves en la implementacion de cabeceras de seguridad, gestion de cookies y cifrado de recursos internos. Debido a la ausencia de redireccion automatica a HTTPS y la exposicion de servicios de transferencia de archivos inseguros, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	8	10	3	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	20	FALLO	489 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-07-08T06:59:00.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-09T06:59:01.000Z
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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: 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**
  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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

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

Contenido Mixto — 20/100

Estado: FALLO

489 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://apps.hexderp.com/HexCookies/hexcookies.php
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.cin.cat/lang-ca/pag/clients/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.cin.cat/lang-ca/pag/contact/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.cin.cat/lang-ca/pag/contact/
- MEDIO **href (link/stylesheet)**
  ...y 485 mas del mismo tipo

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- 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
- 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] Ausencia de Content-Security-Policy: Facilita ataques de XSS e inyeccion de contenido malicioso al no restringir las fuentes de scripts permitidas.
[HIGH] Ausencia de X-Frame-Options: Permite que el sitio sea cargado en marcos externos o iframes, aumentando el riesgo de ataques de clickjacking.
[HIGH] Falta de Strict-Transport-Security (HSTS): El navegador no fuerza la conexion cifrada, dejando a los usuarios vulnerables a ataques de degradacion de protocolo.
[HIGH] Fallo en Redireccion HTTP a HTTPS: La web responde por canales no cifrados bajo el protocolo HTTP, exponiendo datos sensibles durante el transito.
[HIGH] Cookies de sesion inseguras (PHPSESSID): Carece de los flags HttpOnly y Secure, permitiendo su robo mediante scripts maliciosos o intercepcion en redes.
[HIGH] Puerto 21 (FTP) Abierto: El uso de FTP implica la transferencia de credenciales y archivos en texto plano, lo cual es facilmente interceptable por terceros.
[MEDIUM] Contenido Mixto Masivo: Se detectaron 489 recursos cargados via HTTP dentro de una pagina HTTPS, comprometiendo la integridad y privacidad del cifrado SSL.
[MEDIUM] Ausencia de X-Content-Type-Options: Expone al sitio a ataques de sniffing de MIME-type donde el navegador podria interpretar archivos de forma incorrecta y peligrosa.
[MEDIUM] Falta de SameSite en Cookies: La ausencia de este atributo en la cookie de sesion incrementa la superficie de ataque para vulnerabilidades de Cross-Site Request Forgery (CSRF).
[MEDIUM] Puerto 22 (SSH) Abierto: Representa un vector de ataque para intentos de acceso remoto si no cuenta con una politica de endurecimiento estricta.
[LOW] Server Header Expuesto: La cabecera revela especificamente el uso de Apache, facilitando a posibles atacantes la busqueda de exploits conocidos para esa tecnologia.
[LOW] Faltan archivos robots.txt y sitemap.xml: Dificulta la indexacion correcta y el control sobre que areas del sitio deben ser rastreadas por los motores de busqueda.