EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pac.bcn.cat/login	Checks	9 pruebas
Dominio	pac.bcn.cat	Hallazgos	45 totales
Fecha	29 de abril de 2026 a las 13:49	Problemas	9 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre pac.bcn.cat arroja una puntuación de 78/100 con una calificación de nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se detectaron 2 fallos críticos. Aunque el cifrado SSL es excelente, la ausencia de cabeceras de seguridad y la configuración deficiente de las cookies presentan riesgos importantes. En conclusión, el sitio web muestra una postura de seguridad aceptable, pero permanece vulnerable ante ataques de inyección y secuestro de sesiones.

Resumen de Riesgos

0	2	4	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 260 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	50	AVISO	JSESSIONID: falta SameSite; c2dbd8019f46277257ee...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 260 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  260 dias restantes (expira: 2027-01-14T09:27:19.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-14T09:27:20.000Z
- 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000 ; includeSubDomains
- 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.)

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

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

JSESSIONID: falta SameSite; c2dbd8019f46277257ee01526c9c7fa3: falta Secure; c2dbd8019f46277257ee01526c9c7fa3: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: JSESSIONID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: c2dbd8019f46277257ee01526c9c7fa3 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript

- ALTO **Cookie: c2dbd8019f46277257ee01526c9c7fa3 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: c2dbd8019f46277257ee01526c9c7fa3 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 401)
- BAJO **sitemap.xml**
  No encontrado (HTTP 401)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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] Cookie Secure Flag: La cookie c2dbd8019f46277257ee01526c9c7fa3 carece del atributo Secure, lo que permite que sea enviada a través de conexiones no cifradas.
[MEDIUM] Referrer-Policy: No está configurada, lo que puede filtrar información sensible de navegación a dominios externos.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso del navegador a funciones de hardware como la cámara o el micrófono.
[MEDIUM] Cookies SameSite Flag: Las cookies JSESSIONID y c2dbd8019f46277257ee01526c9c7fa3 no tienen definido el atributo SameSite, exponiendo al usuario a ataques de Cross-Site Request Forgery (CSRF).

[LOW] Server Header: Se expone la versión del servidor (Apache), facilitando a atacantes la búsqueda de vulnerabilidades específicas para esa tecnología.
[LOW] Archivos de indexación: No se encontraron los archivos robots.txt ni sitemap.xml tras recibir un error de autorización HTTP 401.