EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://uab.cat	Checks	9 pruebas
Dominio	uab.cat	Hallazgos	45 totales
Fecha	19 de mayo de 2026 a las 17:06	Problemas	8 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al dominio uab.cat ha dado como resultado una puntuación de 76/100, lo que equivale a una nota B. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue calificado como fallo. El sitio presenta una base sólida en cuanto a redirecciones HTTPS y protección de rutas, pero muestra debilidades críticas en la configuración de cabeceras y en el mantenimiento del certificado de seguridad. Se concluye que el sitio es actualmente funcional y moderadamente seguro, pero se considera vulnerable a corto plazo debido a la proximidad de la expiración de su certificado TLS. La implementación inmediata de las recomendaciones es necesaria para evitar la pérdida de confianza de los usuarios y posibles ataques de inyección.

Resumen de Riesgos

0	2	4	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	50	AVISO	Certificado expira en 9 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 50/100

Estado: AVISO

Certificado expira en 9 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- ALTO **Dias hasta expiracion**
  9 dias restantes (expira: 2026-05-28T11:03:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-05-28T11:03:03.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age= 31536000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://uab.cat/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age= 31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- 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

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.youtube.com/uabbarcelona?sub_confirmation=1

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (807 bytes)
- INFO **Reglas robots.txt**
  15 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.uab.cat/sitemapindex.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 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)**
  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] Certificado SSL/TLS próximo a expirar: El certificado expira en 9 días (2026-05-28), lo que dejará el sitio inaccesible o marcado como no seguro.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[MEDIUM] X-Content-Type-Options ausente: No se previene el sniffing de tipos MIME, lo que podría permitir que el navegador interprete archivos de forma incorrecta y peligrosa.
[MEDIUM] Referrer-Policy ausente: No se controla qué información de procedencia se envía a terceros al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy ausente: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Contenido Mixto (HTTP sobre HTTPS): Se detectó un enlace a YouTube utilizando el protocolo inseguro http://www.youtube.com/uabbarcelona?sub_confirmation=1.
[LOW] Cabecera Server expuesta: Se revela el uso de Apache, facilitando a un atacante la búsqueda de vulnerabilidades específicas para esa tecnología.
[LOW] Ruta sensible en robots.txt: El archivo menciona la ruta admin, lo que proporciona pistas directas sobre la estructura de gestión del sitio a posibles atacantes.