EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kapylarcenter.es	Checks	9 pruebas
Dominio	kapylarcenter.es	Hallazgos	44 totales
Fecha	13 de septiembre de 2026 a las 17:43	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a la plataforma arroja una puntuación de 72/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 comprobaciones pasivas, resultando en 6 verificaciones satisfactorias, 2 advertencias y 1 fallo crítico en la configuración de cabeceras. Aunque la base de cifrado es sólida, la ausencia total de políticas de seguridad en el servidor y la exposición de puertos adicionales elevan el riesgo. En conclusión, el sitio se considera actualmente vulnerable ante ataques de inyección y suplantación. Se requiere una intervención técnica inmediata para alcanzar niveles de protección aceptables.

Resumen de Riesgos

0	4	5	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 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	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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-12-05T00:02:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-05T23:02:56.000Z
- 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: cloudflare — 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://kapylarcenter.es/
- 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

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 — 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 (2074 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://kapylarcenter.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de Cross-Site Scripting (XSS) e inyección de datos maliciosos.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No existe una política HSTS configurada, lo que permite ataques de degradación de protocolo de HTTPS a HTTP.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó este puerto abierto, lo cual suele ser un vector de ataque si aloja servicios de administración o proxies desprotegidos.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando la ejecución de scripts maliciosos.
[MEDIUM] Bloqueo total en robots.txt: El archivo configurado con Disallow: / impide la indexación legítima, pero también revela una estructura que intenta ocultarse sin seguridad real.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que podría filtrar URLs privadas o datos sensibles.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando el riesgo de privacidad para el usuario.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando información valiosa a posibles atacantes para realizar ataques dirigidos.