EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ciudadccs.info	Checks	9 pruebas
Dominio	ciudadccs.info	Hallazgos	57 totales
Fecha	29 de agosto de 2026 a las 18:48	Problemas	19 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 53/100, lo que equivale a una nota de D. Se ejecutaron 9 controles pasivos, de los cuales 4 resultaron exitosos, 2 generaron advertencias y 3 fallaron críticamente. La ausencia de cabeceras de seguridad fundamentales y una gestión deficiente del tráfico cifrado comprometen la integridad de la plataforma. Debido a estos hallazgos, se concluye que el sitio es vulnerable y presenta riesgos significativos para la seguridad de los usuarios.

Resumen de Riesgos

0	6	11	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	20	FALLO	300 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 49 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  49 dias restantes (expira: 2026-10-17T09:11:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-19T09:11:53.000Z
- 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: nginx — 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

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
- INFO **Tecnologias detectadas**
  Next.js, 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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: laravel-session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: laravel-session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: laravel-session — SameSite**
  SameSite=lax

Contenido Mixto — 20/100

Estado: FALLO

300 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.ciudadccs.info/assets/img/banner.jpg
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.ciudadccs.info/assets/img/imgdestacados.png
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.ciudadccs.info/assets/img/imgdestacados.png
- MEDIO **src (script/img/iframe)**
  ...y 107 mas del mismo tipo
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ciudadccs.info/publicacion/49337-acuerdos-preven-...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ciudadccs.info/publicacion/49337-acuerdos-preven-...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ciudadccs.info/publicacion/49336-psuv-respalda-fi...
- MEDIO **href (link/stylesheet)**
  ...y 187 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking que pueden engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, facilitando ataques de interceptación.
[HIGH] Redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, dejando las comunicaciones sin cifrar por defecto.
[HIGH] Seguridad de Cookies: La cookie XSRF-TOKEN carece del atributo HttpOnly, permitiendo que sea accesible mediante scripts y aumentando el riesgo de robo de sesión.
[MEDIUM] Contenido Mixto: Se detectaron 300 recursos cargados mediante HTTP en una página HTTPS, lo que degrada la seguridad del cifrado SSL.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que puede llevar a la ejecución de archivos no autorizados.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que puede exponer datos sensibles en las URLs.
[MEDIUM] Permissions-Policy: El sitio no restringe el uso de APIs del navegador como la cámara o el micrófono, aumentando la superficie de ataque.
[LOW] Exposición de Servidor: La cabecera Server revela el uso de nginx, facilitando a posibles atacantes la búsqueda de exploits específicos para esa tecnología.
[LOW] Sitemap: La ausencia del archivo sitemap.xml dificulta la indexación correcta y el monitoreo de la estructura del sitio.