EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://dibs.bancocaroni.com.ve/DIBS_CARONI_VNZ/pages/login	Checks	9 pruebas
Dominio	dibs.bancocaroni.com.ve	Hallazgos	44 totales
Fecha	11 de junio de 2026 a las 16:01	Problemas	10 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web presenta una puntuación de 64/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron correctos, 2 generaron advertencias y 2 fallaron debido a configuraciones críticas ausentes. Si bien el cifrado de datos es válido, la carencia de políticas de seguridad modernas y la falta de redirección forzada a HTTPS elevan el riesgo de ataques. Por tanto, el sitio se considera vulnerable y requiere correcciones técnicas para alcanzar un nivel de protección aceptable.

Resumen de Riesgos

0	4	4	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 170 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 170 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  170 dias restantes (expira: 2026-11-28T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-28T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: same-origin
- 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 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- 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. La ausencia de esta cabecera facilita la ejecución de ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] Strict-Transport-Security: Falta. Al no estar configurada, el sitio no instruye al navegador para usar exclusivamente conexiones seguras, permitiendo ataques de degradación de SSL.

[HIGH] Redirección HTTP a HTTPS: Fallida. El sitio no redirige automáticamente el tráfico inseguro al canal cifrado, exponiendo los datos de los usuarios en tránsito.
[MEDIUM] X-Content-Type-Options: Falta. Esto permite que el navegador intente adivinar el tipo de contenido, lo que puede ser explotado mediante ataques de MIME-sniffing.
[MEDIUM] Permissions-Policy: Falta. No se restringe el acceso del navegador a funcionalidades sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: Se detectó un puerto alternativo accesible que amplía la superficie de ataque y puede exponer servicios internos.
[MEDIUM] Configuración de robots.txt: El archivo bloquea el rastreo de todo el sitio, lo cual es inusual y puede esconder configuraciones por defecto o directorios sensibles.
[LOW] Server header expuesto: El servidor revela el uso de la tecnología Cloudflare, proporcionando información técnica útil para un posible atacante.
[LOW] sitemap.xml: No encontrado. La ausencia de este archivo dificulta la auditoría de la estructura del sitio y la indexación legítima.