EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://api.starbucks.mx	Checks	9 pruebas
Dominio	api.starbucks.mx	Hallazgos	47 totales
Fecha	24 de marzo de 2026 a las 19:04	Problemas	20 detectados

D

45/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a la plataforma arroja una puntuación de 45/100, lo que corresponde a una calificación de grado D. De los 9 checks pasivos ejecutados, únicamente 4 resultaron satisfactorios, mientras que se identificaron 5 fallos críticos relacionados con la infraestructura y la configuración de red. La exposición de servicios de base de datos y administración remota representa un riesgo inmediato para la integridad de la información. Tras evaluar los hallazgos técnicos, se concluye que el sitio es actualmente vulnerable y requiere una intervención urgente.

Resumen de Riesgos

3	9	6	2	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 204 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	17	FALLO	visid_incap_2967804: falta Secure; visid_incap_2...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 204 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  204 dias restantes (expira: 2026-10-14T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-14T00:00:00.000Z
- 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

- 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 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 — 17/100

Estado: FALLO

visid_incap_2967804: falta Secure; visid_incap_2967804: falta SameSite; incap_ses_877_2967804: falta HttpOnly; incap_ses_877_2967804: falta Secure; incap_ses_877_2967804: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)

- INFO **Cookie: visid_incap_2967804 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: visid_incap_2967804 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: visid_incap_2967804 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: incap_ses_877_2967804 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: incap_ses_877_2967804 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: incap_ses_877_2967804 — 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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): El servicio de base de datos está expuesto a internet, permitiendo intentos de acceso externo y robo de información sensible.
[CRITICAL] Puerto 3389 (RDP): El protocolo de escritorio remoto de Windows es visible, lo que facilita ataques de fuerza bruta para tomar control del servidor.
[CRITICAL] Puerto 6379 (Redis): Sistema de caché expuesto sin autenticación robusta por defecto, permitiendo la extracción de datos en memoria.
[HIGH] Puerto 21 (FTP): Canal de transferencia de archivos sin cifrado activo, susceptible a la interceptación de credenciales y datos.
[HIGH] Ausencia de Cabeceras de Seguridad: Falta total de protecciones contra ataques XSS, clickjacking e inyección de contenido (CSP, X-Frame-Options).
[HIGH] Fallo en Redirección HTTPS: El sitio no fuerza la conexión cifrada desde el puerto 80, dejando las comunicaciones iniciales vulnerables.
[HIGH] Cookies Inseguras: Las cookies carecen de los flags HttpOnly y Secure, permitiendo su robo mediante scripts maliciosos o redes no cifradas.
[MEDIUM] Puerto 8080 (HTTP-Alt): Puerto de servidor alternativo abierto que incrementa la superficie de ataque disponible para agentes externos.
[MEDIUM] Falta de SameSite en Cookies: La ausencia de este atributo hace que las sesiones sean vulnerables a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[LOW] Ausencia de Robots.txt y Sitemap: La falta de estos archivos dificulta el control sobre el rastreo de buscadores y la indexación del sitio.