

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://www.cemex.com/
Dominio www.cemex.com
Fecha 7 de octubre de 2026 a las 17:57

Checks 9 pruebas
Hallazgos 51 totales
Problemas 15 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio cemex.com ha resultado en una puntuación de 72/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias por configuraciones incompletas y 2 fallos críticos en la exposición de servicios. Aunque el sitio implementa correctamente el cifrado de transporte, presenta deficiencias severas en la protección de la capa de aplicación y la visibilidad de infraestructura interna. En su estado actual, el sitio se considera vulnerable debido a la exposición de puertos críticos que podrían permitir accesos no autorizados.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 75 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	83	AVISO	incap_ses_612_1922095: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 75 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
75 dias restantes (expira: 2026-12-21T09:54:35.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-22T09:54:35.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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
- 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://www.cemex.com/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 días)
- 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

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO

Archivo /README.txt
No accesible (correcto)
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente
- MEDIO

Ruta /administrator/
Panel de login accesible publicamente

- MEDIO

Ruta /user/login
Panel de login accesible publicamente
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

incap_ses_612_1922095: falta HttpOnly

- INFO

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

Cookie: visid_incap_1922095 — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: visid_incap_1922095 — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: visid_incap_1922095 — SameSite
SameSite=none
- ALTO

Cookie: incap_ses_612_1922095 — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO

Cookie: incap_ses_612_1922095 — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: incap_ses_612_1922095 — SameSite
SameSite=none

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 robots.txt

- INFO

sitemap.xml
Presente, ? URLs
- 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): Base de datos expuesta directamente a internet, permitiendo intentos de intrusión o ataques de fuerza bruta.
- [CRITICAL] Puerto 3389 (RDP): Protocolo de escritorio remoto de Windows abierto, un vector de ataque principal para el secuestro de servidores.
- [CRITICAL] Puerto 6379 (Redis): Servicio de caché expuesto que suele carecer de autenticación, permitiendo la extracción de datos en memoria.
- [HIGH] Puerto 21 (FTP): Transferencia de archivos sin cifrar que permite la interceptación de credenciales y datos sensibles en la red.
- [HIGH] Content-Security-Policy: Ausencia de política de seguridad, lo que facilita ataques de inyección de contenido y XSS.
- [HIGH] X-Frame-Options: Falta de cabecera de protección, dejando el sitio vulnerable a ataques de clickjacking.
- [HIGH] Cookie incap_ses_612_1922095: Carece del atributo HttpOnly, permitiendo que la cookie de sesión sea accesible mediante scripts maliciosos.
- [MEDIUM] Puerto 8080 (HTTP-Alt): Servidor web alternativo activo que puede exponer servicios internos o interfaces de administración.
- [MEDIUM] X-Content-Type-Options: Ausencia de protección contra la interpretación incorrecta de tipos MIME por parte del navegador.
- [MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones salientes.
- [MEDIUM] Permissions-Policy: Falta de restricción en el uso de APIs del navegador como cámara, micrófono o geolocalización.
- [MEDIUM] Rutas administrativas expuestas: Los paneles /wp-login.php, /administrator/ y /user/login son accesibles desde internet.
- [MEDIUM] Archivo /readme.html: Presencia de archivos técnicos que pueden revelar detalles específicos sobre la configuración del servidor.
- [MEDIUM] Robots.txt: No se detectó el archivo de gestión de rastreo, dificultando el control sobre qué partes del sitio indexan los buscadores.