EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://quixada.ce.gov.br/	Checks	9 pruebas
Dominio	quixada.ce.gov.br	Hallazgos	48 totales
Fecha	27 de abril de 2026 a las 14:43	Problemas	15 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al portal arroja una puntuación de 68/100, lo que resulta en una calificación de grado C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 obtuvieron resultados positivos, 1 generó una advertencia y 2 fallaron significativamente. El análisis revela carencias críticas en la configuración de cabeceras de protección y la presencia de recursos no cifrados. Por estos motivos, se concluye que el sitio es actualmente vulnerable a ataques de inyección y suplantación.

Resumen de Riesgos

0	4	10	1	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 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	20	FALLO	27 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 41 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  41 dias restantes (expira: 2026-06-07T12:21:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-09T12:21:04.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://quixada.ce.gov.br/
- 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

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
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 20/100

Estado: FALLO

27 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://servicos2.speedgov.com.br/quixada/segunda_via/iptu
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://servicos2.speedgov.com.br/quixada/segunda_via/iss
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://servicos2.speedgov.com.br/quixada/segunda_via/itbi
- MEDIO **href (link/stylesheet)**
  ...y 24 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (646 bytes)
- INFO **Reglas robots.txt**
  23 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://quixada.ce.gov.br/sitemap.xml
- 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 facilita la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se fuerza una conexión segura a nivel de navegador, permitiendo posibles ataques de degradación de protocolo.
[HIGH] HSTS: El mecanismo de seguridad de transporte no está configurado, lo que impide que el navegador exija siempre HTTPS.
[MEDIUM] Contenido Mixto: Se detectaron 27 recursos cargados mediante HTTP en una página protegida por SSL, lo que compromete la integridad de la sesión.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos inesperados.
[MEDIUM] Archivos /readme.html y /README.txt: Estos archivos son accesibles públicamente y pueden exponer información técnica sobre la infraestructura interna.
[MEDIUM] Referrer-Policy: No existe control sobre la información que se envía a otros dominios al seguir enlaces salientes.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a componentes sensibles como cámara o geolocalización.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el sitio, lo que podría afectar la visibilidad legítima del portal.
[LOW] Server header expuesto: El encabezado revela el uso de nginx, proporcionando información útil para un atacante sobre la tecnología del servidor.