EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.xvz.cl/	Checks	9 pruebas
Dominio	www.xvz.cl	Hallazgos	51 totales
Fecha	28 de abril de 2026 a las 00:32	Problemas	10 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web xvz.cl arroja una puntuación de 77/100 con una calificación de grado B. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de cabeceras y cookies. La evaluación muestra una base sólida en cuanto a cifrado SSL y redireccionamiento HTTPS, pero identifica debilidades importantes en la protección contra ataques de inyección y secuestro de sesión. En conclusión, el sitio web es parcialmente seguro, pero se considera vulnerable debido a la ausencia de políticas de seguridad modernas que protejan la integridad de la navegación de sus usuarios.

Resumen de Riesgos

0	4	4	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Wix
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	0	FALLO	ssr-caching: falta HttpOnly; ssr-caching: falta ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-07-04T13:02:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-05T13:03:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Pepyaka — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31556952
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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.xvz.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556952
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556952 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Wix

- 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**
  Detectado via HTML body
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Wix.com Website Builder
- INFO **Tecnologias detectadas**
  React, 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 — 0/100

Estado: FALLO

ssr-caching: falta HttpOnly; ssr-caching: falta Secure; ssr-caching: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: ssr-caching — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ssr-caching — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ssr-caching — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (484 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.xvz.cl/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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: Falta esta cabecera crítica, lo que deja al sitio vulnerable a ataques de Cross-Site Scripting (XSS) y ataques de inyección de contenido.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite ataques de clickjacking, permitiendo que el sitio sea cargado dentro de marcos maliciosos.
[HIGH] Cookie ssr-caching (Falta HttpOnly): La cookie de sesión es accesible mediante scripts del navegador, facilitando el robo de identidad en caso de una vulnerabilidad XSS.
[HIGH] Cookie ssr-caching (Falta Secure): El flag Secure no está presente, lo que significa que la información de la cookie podría ser enviada a través de conexiones no cifradas.
[MEDIUM] Referrer-Policy: No se detectó una política de referencia, lo que puede provocar la filtración involuntaria de información de navegación a terceros.
[MEDIUM] Permissions-Policy: Falta esta cabecera para restringir el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Cookie ssr-caching (Falta SameSite): La ausencia de este atributo hace que el sitio sea susceptible a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Bloqueo en Robots.txt: El archivo robots.txt contiene una instrucción Disallow: / que bloquea el rastreo de todo el sitio, afectando negativamente la indexación.
[LOW] Server header expuesto: El servidor responde con la cabecera Server: Pepyaka, revelando información técnica que ayuda a los atacantes en la fase de reconocimiento.
[LOW] Meta generator: Se expone públicamente el uso de Wix.com Website Builder, revelando la tecnología de construcción del sitio.