EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://getweb.cl	Checks	9 pruebas
Dominio	getweb.cl	Hallazgos	42 totales
Fecha	27 de mayo de 2026 a las 14:10	Problemas	13 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio getweb.cl ha resultado en una puntuación de 61/100, lo que otorga al sitio una calificación de grado C. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 finalizaron con éxito, no se registraron advertencias y 3 resultaron en fallos críticos de configuración. A pesar de contar con un cifrado SSL robusto, el sitio presenta carencias importantes en la implementación de cabeceras de seguridad y en la gestión de redirecciones de tráfico. Debido a la ausencia de políticas de protección contra ataques de inyección y suplantación, el sitio se concluye como vulnerable frente a amenazas web comunes.

Resumen de Riesgos

0	5	7	1	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-08-25T10:10:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-27T10:10:52.000Z
- 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: LiteSpeed — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

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
- 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 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Ausencia de redirección HTTP a HTTPS: El sitio permite conexiones a través de HTTP sin cifrar, lo que facilita la interceptación de datos.
[HIGH] Content-Security-Policy (CSP) faltante: No existe una política definida para prevenir ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options faltante: La ausencia de esta cabecera permite que el sitio sea cargado en marcos (iframes), facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS) faltante: El navegador no recibe instrucciones para forzar siempre una conexión segura, permitiendo ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options faltante: El sitio es vulnerable al sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy faltante: No se controla la cantidad de información que el navegador envía a otros sitios web al seguir un enlace.

[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o la geolocalización.
[MEDIUM] Archivos técnicos expuestos (/readme.html, /README.txt): El acceso público a estos archivos puede revelar detalles sobre la infraestructura interna y posibles debilidades.
[MEDIUM] Paneles de acceso públicos (/administrator/, /user/login): La exposición de estas rutas facilita los intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Cabecera Server expuesta: Se revela el uso del servidor LiteSpeed, lo que ayuda a un atacante a buscar vulnerabilidades específicas para esa tecnología.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta el control sobre el rastreo de bots y la indexación del contenido.