EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://compugraf.cl	Checks	9 pruebas
Dominio	compugraf.cl	Hallazgos	48 totales
Fecha	1 de mayo de 2026 a las 03:55	Problemas	7 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio compugraf.cl arrojó una puntuación de 72/100, lo que resulta en una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 3 advertencias y 1 fallo crítico. La infraestructura presenta debilidades importantes en la configuración del cifrado de tráfico y en la exposición de servicios de red antiguos. Con base en los hallazgos, se concluye que el sitio es actualmente vulnerable a ataques de interceptación de datos y acceso no autorizado a través de puertos inseguros.

Resumen de Riesgos

0	2	2	3	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 29 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 29 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  29 dias restantes (expira: 2026-05-30T05:31:30.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-01T05:31:31.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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

- 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 — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (119 bytes)
- INFO **Reglas robots.txt**
  3 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://compugraf.cl/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- 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
- 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] Redirección HTTP a HTTPS: El servidor permite conexiones por el puerto 80 sin redirigir al protocolo seguro, lo que facilita ataques de interceptación de datos.
[HIGH] Puerto 21 (FTP) ABIERTO: Este servicio permite la transferencia de archivos sin cifrar, exponiendo credenciales y contenido a posibles atacantes en la red.
[MEDIUM] Referrer-Policy ausente: No se ha definido una política para controlar qué información de referencia se envía a otros sitios web.
[MEDIUM] Permissions-Policy ausente: La falta de esta cabecera impide restringir el uso de APIs sensibles del navegador como la cámara o el micrófono.
[LOW] Certificado SSL/TLS por expirar: El certificado actual caduca en 29 días, lo que representa un riesgo de interrupción del servicio y pérdida de confianza del usuario.
[LOW] Server header expuesto: La cabecera revela el uso de LiteSpeed, información que ayuda a potenciales atacantes a buscar vulnerabilidades específicas para esa tecnología.
[LOW] Rutas sensibles en robots.txt: La mención de directorios como admin y config facilita a los atacantes el descubrimiento de paneles de gestión y archivos de configuración.