EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ctiiles.cl	Checks	9 pruebas
Dominio	ctiiles.cl	Hallazgos	46 totales
Fecha	26 de agosto de 2026 a las 04:42	Problemas	15 detectados

D

55/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el dominio arroja una puntuacion de 55/100, lo que equivale a una calificacion de nota D. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 4 resultaron correctos, 3 presentaron advertencias y 2 fallaron criticamente. El sitio presenta deficiencias severas en la configuracion de cabeceras de seguridad y en la implementacion de protocolos de conexion segura. Se concluye que el sitio es actualmente vulnerable, principalmente debido a la falta de politicas de endurecimiento web y la exposicion de informacion tecnica sensible.

Resumen de Riesgos

0	5	7	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 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	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-11-11T15:39:39.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-13T14:42:23.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.12 — Revela framework/lenguaje
- 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
- INFO **Tecnologias detectadas**
  PHP/8.2.12

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://192.168.50.128:8080/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1836 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- 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

[HIGH] Falta de redireccion HTTPS: El servidor permite conexiones por el puerto 80 sin redirigir al usuario a la version cifrada, dejando los datos expuestos.
[HIGH] Ausencia de Strict-Transport-Security (HSTS): No se instruye al navegador para que utilice exclusivamente conexiones seguras, permitiendo ataques de degradacion de protocolo.
[HIGH] Content-Security-Policy (CSP) faltante: La falta de esta politica facilita la ejecucion de scripts maliciosos y ataques de inyeccion de contenido.
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking al permitir ser cargado dentro de marcos o iframes externos.
[MEDIUM] Contenido Mixto detectado: Se intenta cargar un recurso mediante el protocolo inseguro HTTP desde una direccion IP privada (192.168.50.128:8080).
[MEDIUM] Puerto 8080 abierto: La disponibilidad de este puerto alternativo incrementa la superficie de ataque y sugiere servicios internos mal configurados.
[MEDIUM] Archivo README.txt accesible: La exposicion de este archivo puede revelar informacion sobre la estructura interna o configuraciones del sistema.
[MEDIUM] X-Content-Type-Options faltante: Permite que el navegador realice sniffing de tipos MIME, lo que puede llevar a la ejecucion de archivos maliciosos.
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: No se controla la informacion de navegacion enviada a terceros ni se restringen las APIs del navegador.
[MEDIUM] Configuracion de Robots.txt restrictiva: El archivo bloquea el acceso a todo el sitio, lo que suele ser un error de configuracion en entornos de produccion.
[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare como intermediario, permitiendo a un atacante perfilar la infraestructura de red.
[LOW] X-Powered-By expuesto: El servidor informa explicitamente que utiliza PHP/8.2.12, facilitando la busqueda de exploits para esa version especifica.