EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fuzap.cl	Checks	9 pruebas
Dominio	fuzap.cl	Hallazgos	48 totales
Fecha	5 de mayo de 2026 a las 18:33	Problemas	11 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha arrojado una puntuación de 70/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 checks pasivos, resultando en 5 verificaciones exitosas, 2 advertencias de riesgo medio y 2 fallos de cumplimiento crítico. Aunque el cifrado de datos es robusto, la infraestructura carece por completo de cabeceras de seguridad esenciales para prevenir ataques modernos. En conclusión, el sitio se encuentra en un estado vulnerable debido a configuraciones incompletas en el servidor que podrían comprometer la integridad de los usuarios. Se recomienda una intervención técnica inmediata para elevar los estándares de protección.

Resumen de Riesgos

0	5	3	3	37
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
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 41 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  41 dias restantes (expira: 2026-06-15T19:38:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-17T19:38:02.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://fuzap.cl/public
- 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

- 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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: fuzap_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: fuzap_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: fuzap_session — SameSite**
  SameSite=lax

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

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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 (CSP) faltante: Aumenta radicalmente el riesgo de ataques Cross-Site Scripting (XSS) al no restringir las fuentes de contenido.
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking, permitiendo que sea embebido en marcos de sitios maliciosos.
[HIGH] Strict-Transport-Security (HSTS) faltante: No se obliga al navegador a usar HTTPS en futuras visitas, facilitando ataques de degradación de protocolo.
[HIGH] Cookie XSRF-TOKEN sin atributo HttpOnly: La cookie es accesible mediante scripts del lado del cliente, lo que facilita el robo de sesiones mediante XSS.
[MEDIUM] X-Content-Type-Options faltante: El servidor no previene el MIME-sniffing, lo que podría permitir que archivos cargados se ejecuten como scripts maliciosos.
[MEDIUM] Referrer-Policy faltante: No hay control sobre la información de navegación que se envía a terceros cuando el usuario hace clic en enlaces externos.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: La cabecera revela el uso de LiteSpeed, proporcionando información valiosa a atacantes sobre la tecnología del servidor.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: La falta de estos archivos dificulta la auditoría de indexación y el control de rastreo de motores de búsqueda.