EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.redclinica.cl	Checks	9 pruebas
Dominio	www.redclinica.cl	Hallazgos	62 totales
Fecha	1 de septiembre de 2026 a las 18:59	Problemas	15 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio redclinica.cl arroja una puntuación de 81/100, obteniendo una nota de B. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue calificado como fallo crítico. Si bien la base de cifrado y conectividad es robusta, la ausencia de cabeceras de seguridad y la configuración deficiente de las cookies representan un riesgo significativo. Por lo tanto, se concluye que el sitio es vulnerable a ataques específicos de interceptación de datos y suplantación.

Resumen de Riesgos

0	7	6	2	47
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	.ASPXANONYMOUS: falta Secure; .ASPXANONYMOUS: fa...
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): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-11-26T23:20:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-28T22:21:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- 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=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.redclinica.cl/
- 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**
  Astro, ASP.NET

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 — 33/100

Estado: FALLO

.ASPXANONYMOUS: falta Secure; .ASPXANONYMOUS: falta SameSite; Analytics_VisitorId: falta Secure; Analytics_VisitorId: falta SameSite; Analytics: falta Secure; Analytics: falta SameSite; language: falta Secure; language: falta SameSite; __RequestVerificationToken: falta Secure; __RequestVerificationToken: falta SameSite

- INFO **Cookies detectadas**
  5 cookie(s) encontrada(s)
- INFO **Cookie: .ASPXANONYMOUS — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: .ASPXANONYMOUS — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: .ASPXANONYMOUS — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: Analytics_VisitorId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: Analytics_VisitorId — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: Analytics_VisitorId — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: Analytics — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: Analytics — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: Analytics — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: language — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: language — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: language — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: __RequestVerificationToken — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __RequestVerificationToken — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __RequestVerificationToken — 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 (99 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow

- INFO **Sitemap en robots.txt**
  https://www.redclinica.cl/SiteMap.aspx
- 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] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar presente, el sitio queda expuesto a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.
[HIGH] Cookie Secure Flag: Las cookies .ASPXANONYMOUS, Analytics_VisitorId, Analytics, language y __RequestVerificationToken no tienen el flag Secure, permitiendo su transmisión por conexiones no cifradas.
[MEDIUM] Cookie SameSite: Diversas cookies de sesión y analítica carecen del atributo SameSite, lo que incrementa el riesgo de ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto, lo que podría exponer servicios alternativos o interfaces de administración no deseadas.
[LOW] Server header expuesto: El encabezado revela el uso de Cloudflare, lo que proporciona información técnica sobre la infraestructura de red a posibles atacantes.
[LOW] X-Powered-By expuesto: El servidor indica explícitamente el uso de ASP.NET, permitiendo a terceros conocer el framework de desarrollo utilizado.