

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://diferentesnoinferiores.cl/ProgramaAcademico	Checks	9 pruebas
Dominio	diferentesnoinferiores.cl	Hallazgos	44 totales
Fecha	14 de agosto de 2026 a las 21:06	Problemas	11 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación exacta de 72/100, lo que corresponde a una nota C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 1 advertencia y 2 fallos críticos en la configuración del servidor. Aunque el sitio dispone de un cifrado de conexión válido, carece de las protecciones fundamentales contra ataques de inyección y suplantación de identidad. En conclusión, el sitio se considera vulnerable debido a la ausencia total de cabeceras de seguridad esenciales para la protección del usuario final.

Resumen de Riesgos

0 CRITICO	4 ALTO	3 MEDIO	4 BAJO	33 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 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	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 56 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
56 dias restantes (expira: 2026-10-09T22:08:43.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-11T22:08:44.000Z
- 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: Apache — Revela tecnologia del servidor

- BAJO

X-Powered-By expuesto
X-Powered-By: PHP/5.4.45 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://diferentesnoinferiores.cl/
- 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/5.4.45

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 — 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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: No existe protección contra clickjacking, permitiendo que el sitio sea cargado dentro de marcos externos para engañar al usuario.
[HIGH] Strict-Transport-Security: Al no estar configurado HSTS, el sitio no obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación.

[MEDIUM] X-Content-Type-Options: La falta de esta política permite que el navegador realice sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia que se envía a otros sitios, lo que podría filtrar rutas internas de la aplicación.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara o ubicación, aumentando la superficie de riesgo.

[LOW] Server header expuesto: Se detectó la cabecera Server: Apache, la cual revela la tecnología utilizada y facilita la búsqueda de exploits específicos.

[LOW] X-Powered-By expuesto: La cabecera revela el uso de PHP/5.4.45, una versión antigua que informa a posibles atacantes sobre el lenguaje de programación.

[LOW] robots.txt y sitemap.xml: La falta de estos archivos dificulta la correcta gestión del rastreo por parte de buscadores y el control de acceso a rutas.