EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://siiac.junaeb.cl/siiac/com.siiac.formulario	Checks	9 pruebas
Dominio	siiac.junaeb.cl	Hallazgos	49 totales
Fecha	9 de mayo de 2026 a las 23:45	Problemas	14 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma ha otorgado una puntuación de 71/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 controles pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 finalizaron con errores críticos. A pesar de contar con un cifrado de transporte robusto, se identificaron deficiencias importantes en las cabeceras de seguridad y en la gestión de sesiones de usuario. Por estos motivos, el sitio web se considera vulnerable ante ataques de interceptación y suplantación de identidad. Es imperativo corregir las configuraciones del servidor para alcanzar un nivel de protección adecuado.

Resumen de Riesgos

0	6	7	1	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 211 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 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	33	FALLO	GX_CLIENT_ID: falta Secure; GX_CLIENT_ID: falta ...
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 211 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  211 dias restantes (expira: 2026-12-06T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-24T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://siiac.junaeb.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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 33/100

Estado: FALLO

GX_CLIENT_ID: falta Secure; GX_CLIENT_ID: falta SameSite; GX_SESSION_ID: falta Secure; GX_SESSION_ID: falta SameSite; JSESSIONID: falta Secure; JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- INFO **Cookie: GX_CLIENT_ID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: GX_CLIENT_ID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: GX_CLIENT_ID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: GX_SESSION_ID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: GX_SESSION_ID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: GX_SESSION_ID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: JSESSIONID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: JSESSIONID — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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 facilita la ejecución de ataques Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[HIGH] Strict-Transport-Security: Al no tener configurado HSTS, el sitio no obliga al navegador a usar conexiones HTTPS, permitiendo posibles degradaciones de seguridad.
[HIGH] Cookie Secure Flag: Las cookies GX_CLIENT_ID, GX_SESSION_ID y JSESSIONID no tienen el atributo Secure, lo que permite que viajen a través de conexiones HTTP no cifradas.
[HIGH] HSTS (Strict-Transport-Security): Aunque existe redirección a HTTPS, la falta de la cabecera HSTS deja una ventana de vulnerabilidad en el primer contacto del usuario con el servidor.
[MEDIUM] Cookie SameSite Flag: Las cookies de sesión carecen del atributo SameSite, lo que expone a los usuarios a ataques de falsificación de peticiones en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que puede causar la filtración involuntaria de información de navegación hacia dominios externos.
[MEDIUM] Permissions-Policy: La falta de esta cabecera permite que el navegador acceda a APIs sensibles (cámara, micrófono, geolocalización) sin restricciones de seguridad adicionales.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo cual podría revelar detalles técnicos sobre la infraestructura o versiones del software.
[LOW] Server header expuesto: El servidor responde con la cabecera "Server: nginx", revelando la tecnología subyacente y facilitando la búsqueda de exploits específicos para esa versión.