EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://interior.gob.cl/	Checks	9 pruebas
Dominio	interior.gob.cl	Hallazgos	50 totales
Fecha	9 de septiembre de 2026 a las 15:01	Problemas	14 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 65/100, lo que corresponde a una calificación de grado C. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios y 4 presentaron fallos significativos en la configuración. Aunque el cifrado de transporte es adecuado, existen carencias críticas en las cabeceras de seguridad y en la protección de las cookies de sesión. No se llevó a cabo un pentest activo, por lo que la evaluación se limita a la superficie de exposición pública. Se concluye que el sitio es vulnerable debido a configuraciones deficientes que facilitan ataques de inyección y robo de identidad digital.

Resumen de Riesgos

0	3	8	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 137 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
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	0	FALLO	TS014e623b: falta HttpOnly; TS014e623b: falta Se...
Contenido Mixto	20	FALLO	12 recursos HTTP en pagina HTTPS
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 137 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  137 dias restantes (expira: 2027-01-24T20:41:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-09T20:41:29.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15768000; includeSubdomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.interior.gob.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15768000; includeSubdomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 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

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 — 0/100

Estado: FALLO

TS014e623b: falta HttpOnly; TS014e623b: falta Secure; TS014e623b: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: TS014e623b — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS014e623b — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS014e623b — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

12 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://agendapublica.interior.gob.cl
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://subinterior.gob.cl/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.subdere.gov.cl/
- MEDIO **href (link/stylesheet)**
  ...y 9 mas del mismo tipo

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 no autorizados y ataques de inyección de código XSS.
[HIGH] Cookie sin flag HttpOnly: La cookie TS014e623b es accesible a través de scripts del navegador, lo que permite el robo de sesiones mediante ataques maliciosos.
[HIGH] Cookie sin flag Secure: La cookie TS014e623b puede ser transmitida a través de conexiones no cifradas, exponiéndola a intercepciones en la red.
[MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, el navegador podría interpretar archivos de forma incorrecta, permitiendo ataques de sniffing de tipos MIME.
[MEDIUM] Referrer-Policy: La falta de control sobre la información del referer puede filtrar URLs privadas a sitios de terceros.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador, como la geolocalización o la cámara, aumentando la superficie de ataque.
[MEDIUM] Cookie sin flag SameSite: La omisión de este atributo hace que el sitio sea susceptible a ataques de falsificación de peticiones en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron 12 recursos cargados mediante conexiones HTTP inseguras dentro de la página cifrada, comprometiendo la integridad del sitio.
[LOW] Server header expuesto: El servidor revela el valor Minterior, lo que facilita a un atacante identificar la tecnología específica y buscar exploits conocidos.
[LOW] Archivos de indexación faltantes: No se encontraron robots.txt ni sitemap.xml, lo que dificulta la gestión correcta del rastreo por parte de buscadores.