EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.casarosada.gob.ar/	Checks	9 pruebas
Dominio	www.casarosada.gob.ar	Hallazgos	53 totales
Fecha	19 de mayo de 2026 a las 13:11	Problemas	21 detectados

D

49/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre casarosada.gob.ar ha dado como resultado una puntuación de 49/100, obteniendo una calificación de nota D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 2 generaron advertencias y 4 fueron clasificados como fallos críticos. La ausencia total de cabeceras de seguridad y la gestión deficiente de las cookies de sesión representan un riesgo significativo para la integridad del portal. Por tanto, se concluye que el sitio es vulnerable y requiere intervenciones técnicas inmediatas para alcanzar un estándar de protección aceptable.

Resumen de Riesgos

0	7	11	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 248 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	CMS detectado: Joomla
Version CMS Expuesta	20	FALLO	WordPress 3. expuesta
Seguridad de Cookies	17	FALLO	02c3f1c748d1862712c98c5b6d214031: falta Secure; ...
Contenido Mixto	20	FALLO	13 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 248 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  248 dias restantes (expira: 2027-01-22T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-12T00:00:00.000Z
- 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

- 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 302 redirige a https://www.casarosada.gob.ar
- 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

CMS detectado: Joomla

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  Detectado via HTML body
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Joomla! - Open Source Content Management

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3. expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

Seguridad de Cookies — 17/100

Estado: FALLO

02c3f1c748d1862712c98c5b6d214031: falta Secure; 02c3f1c748d1862712c98c5b6d214031: falta SameSite; TS016e96b4: falta HttpOnly; TS016e96b4: falta Secure; TS016e96b4: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: 02c3f1c748d1862712c98c5b6d214031 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: 02c3f1c748d1862712c98c5b6d214031 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: 02c3f1c748d1862712c98c5b6d214031 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS016e96b4 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS016e96b4 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS016e96b4 — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

13 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.argentina.gob.ar/secretariageneral
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.argentina.gob.ar/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://mapadelestado.jefatura.gob.ar/
- MEDIO **href (link/stylesheet)**
  ...y 10 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (806 bytes)
- INFO **Reglas robots.txt**
  13 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- 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: Falta — Previene XSS y ataques de inyección de contenido.
[HIGH] X-Frame-Options: Falta — Protege contra clickjacking al evitar que el sitio sea embebido en frames.
[HIGH] Strict-Transport-Security: Falta — No se fuerza el uso de conexiones HTTPS a través de HSTS.
[MEDIUM] X-Content-Type-Options: Falta — Evita que el navegador realice MIME-type sniffing y ejecute archivos maliciosos.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de referencia enviada a otros dominios.
[MEDIUM] Permissions-Policy: Falta — No se restringen las APIs del navegador como cámara o micrófono.
[HIGH] HSTS (Strict-Transport-Security): No configurado — El navegador no está obligado a mantener la conexión cifrada.
[LOW] Meta generator: Expone información sobre Joomla como gestor de contenidos facilitando ataques dirigidos.
[MEDIUM] Archivo /README.txt: Archivo accesible públicamente — Puede revelar la versión exacta y detalles técnicos del CMS.
[MEDIUM] Ruta /administrator/: El panel de acceso administrativo es visible para cualquier usuario en internet.
[HIGH] Cookie 02c3f1c748d1862712c98c5b6d214031: Falta flag Secure — La cookie se transmite en conexiones no cifradas.
[MEDIUM] Cookie 02c3f1c748d1862712c98c5b6d214031: Falta SameSite — El sitio es vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[HIGH] Cookie TS016e96b4: Falta HttpOnly — La cookie es accesible mediante scripts, aumentando el riesgo de robo de sesión por XSS.
[HIGH] Cookie TS016e96b4: Falta flag Secure — Los datos de sesión pueden ser interceptados en canales HTTP.
[MEDIUM] Cookie TS016e96b4: Falta SameSite — Riesgo de manipulación de peticiones desde sitios externos.
[MEDIUM] Contenido Mixto: Se detectaron 13 recursos cargados mediante HTTP en una página HTTPS, comprometiendo el cifrado general.
[LOW] Ruta sensible en robots.txt: La referencia a admin expone directorios que deberían permanecer ocultos a los atacantes.
[LOW] sitemap.xml: No encontrado — Dificulta la auditoría de la estructura del sitio y afecta la indexación correcta.