EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://padrononline.sec.org.ar/consultapadron	Checks	9 pruebas
Dominio	padrononline.sec.org.ar	Hallazgos	48 totales
Fecha	7 de agosto de 2026 a las 02:28	Problemas	16 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web arroja una puntuación de 57/100, lo que corresponde a una calificación de grado D. Se ejecutaron 9 comprobaciones pasivas, de las cuales 4 resultaron correctas, 2 generaron advertencias y 3 fueron identificadas como fallos críticos. El diagnóstico revela carencias graves en la implementación de cabeceras de seguridad y en la protección de las cookies de sesión. Debido a la ausencia de mecanismos básicos de defensa contra ataques de inyección y suplantación, el sitio se considera actualmente vulnerable y requiere intervención inmediata.

Resumen de Riesgos

0	8	5	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 19 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	0	FALLO	HWWAFSESID: falta HttpOnly; HWWAFSESID: falta Se...
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 — 70/100

Estado: AVISO

Certificado expira en 19 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  19 dias restantes (expira: 2026-08-26T13:18:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-30T16:29:13.000Z
- 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: CW — Revela tecnologia del servidor

- 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://padrononline.sec.org.ar/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 455

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

HWWAFSESID: falta HttpOnly; HWWAFSESID: falta Secure; HWWAFSESID: falta SameSite; HWWAFSESTIME: falta HttpOnly; HWWAFSESTIME: falta Secure; HWWAFSESTIME: falta SameSite

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

- BAJO **robots.txt**
  No encontrado (HTTP 455)
- BAJO **sitemap.xml**
  No encontrado (HTTP 455)
- 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 esta cabecera esencial, lo que permite la ejecución de ataques de Cross-Site Scripting (XSS) e inyecciones de datos.
[HIGH] X-Frame-Options: La ausencia de esta directiva expone a los usuarios a ataques de clickjacking, permitiendo que el sitio sea cargado en marcos invisibles.
[HIGH] Strict-Transport-Security: No existe una política HSTS, por lo que el navegador no fuerza conexiones cifradas, facilitando ataques de degradación de protocolo.
[HIGH] Cookie HWWAFSESID (HttpOnly): Esta cookie de sesión carece del flag HttpOnly, permitiendo que scripts maliciosos accedan a ella y roben la sesión.
[HIGH] Cookie HWWAFSESID (Secure): El flag Secure está ausente, lo que significa que la cookie podría enviarse a través de conexiones HTTP no cifradas.
[HIGH] Cookie HWWAFSESTIME (HttpOnly): Falta la protección contra acceso por script en esta cookie de tiempo de sesión, aumentando el riesgo de XSS.
[HIGH] Cookie HWWAFSESTIME (Secure): La falta del flag Secure permite la intercepción de esta cookie en redes no seguras.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros dominios, lo que podría filtrar rutas internas o datos sensibles.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones como la cámara, el micrófono o la geolocalización.
[MEDIUM] Cookies SameSite: Las cookies carecen del atributo SameSite, lo que las hace vulnerables a ataques de Cross-Site Request Forgery (CSRF).
[WARN] Certificado SSL/TLS: El certificado de seguridad actual tiene una fecha de caducidad próxima, restando únicamente 19 días de validez.
[LOW] Server header expuesto: El encabezado del servidor revela la tecnología CW, proporcionando información técnica valiosa para un atacante.
[LOW] Archivos de rastreo ausentes: No se encontraron los archivos robots.txt ni sitemap.xml, devolviendo un código de error 455 no estándar.