

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pagosnet.provincianet.com.ar/pagosnet/public/application	Checks	9 pruebas
Dominio	pagosnet.provincianet.com.ar	Hallazgos	42 totales
Fecha	14 de agosto de 2026 a las 00:55	Problemas	12 detectados

C

62/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación técnica de 62/100, lo que se traduce en una calificación de grado C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presentó advertencias y 3 fallaron críticamente. El sitio carece de todas las cabeceras de seguridad fundamentales y presenta configuraciones de sesión inseguras que comprometen la integridad de los datos del usuario. Debido a estas omisiones en la configuración del servidor, el sitio se considera vulnerable a ataques de interceptación y suplantación. Es imperativo aplicar medidas correctivas inmediatas para elevar los estándares de protección de la plataforma.

Resumen de Riesgos

0	6	6	0	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 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	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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 45 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
45 dias restantes (expira: 2026-09-27T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-03-13T00:00:00.000Z
- 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 301 redirige a https://pagosnet.provincianet.com.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

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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)

- ALTO

Cookie: PHPSESSID — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO

Cookie: PHPSESSID — Secure
Falta flag Secure — Cookie se envía en conexiones HTTP
- MEDIO

Cookie: PHPSESSID — 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 — Envío 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: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo posibles degradaciones de HTTPS a HTTP.

[HIGH] Cookie PHPSESSID - HttpOnly: La cookie de sesión es accesible mediante scripts de cliente, lo que facilita el robo de sesiones a través de XSS.

[HIGH] Cookie PHPSESSID - Secure: La sesión puede ser enviada a través de conexiones no cifradas, exponiendo los datos a interceptación en la red.

[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos con extensiones falsas.

[MEDIUM] Referrer-Policy: No hay control sobre la información de referencia enviada a otros sitios, lo que puede filtrar URLs privadas.

[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones como la cámara o el micrófono sin control explícito.

[MEDIUM] Cookie PHPSESSID - SameSite: La falta de este atributo hace que la sesión sea vulnerable a ataques de falsificación de solicitud en sitios cruzados (CSRF).

[MEDIUM] Archivos readme.html y README.txt: Estos archivos son accesibles públicamente y pueden revelar información técnica sobre la infraestructura interna.

[LOW] Robots.txt y Sitemap: La ausencia de estos archivos dificulta la auditoría de rutas permitidas y la indexación correcta de la estructura web.