EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.plataforma10.com.ar/	Checks	9 pruebas
Dominio	www.plataforma10.com.ar	Hallazgos	63 totales
Fecha	2 de junio de 2026 a las 17:09	Problemas	22 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre plataforma10.com.ar arrojó una puntuación de 65/100, lo que equivale a una calificación de grado C. Se ejecutaron 9 chequeos pasivos que resultaron en 5 verificaciones correctas, 2 advertencias por configuraciones incompletas y 2 fallos críticos en la seguridad de cabeceras y cookies. Aunque el sitio cuenta con un cifrado SSL válido, la ausencia de políticas de seguridad modernas y la exposición de información técnica lo vuelven vulnerable. Se concluye que el sitio es vulnerable ante ataques de interceptación de datos y manipulación de sesiones debido a deficiencias en su configuración de red.

Resumen de Riesgos

0	13	7	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 199 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	33	FALLO	NEXT_LOCALE: falta HttpOnly; NEXT_LOCALE: falta ...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 199 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  199 dias restantes (expira: 2026-12-18T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-20T00:00:00.000Z
- 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

- BAJO **Server header expuesto**
  Server: nginx/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js — Revela framework/lenguaje
- 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://www.plataforma10.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
- INFO **Tecnologias detectadas**
  React, Next.js, Astro, Next.js

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 — 33/100

Estado: FALLO

NEXT_LOCALE: falta HttpOnly; NEXT_LOCALE: falta Secure; NEXT_LOCALE: falta SameSite; source: falta HttpOnly; source: falta Secure; source: falta SameSite; NEXT_COUNTRY: falta HttpOnly; NEXT_COUNTRY: falta Secure; NEXT_COUNTRY: falta SameSite; growthbookId_v2: falta HttpOnly; amp_device_id: falta HttpOnly; p10_initial_date: falta HttpOnly

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- ALTO **Cookie: NEXT_LOCALE — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: NEXT_LOCALE — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: NEXT_LOCALE — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: source — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: source — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: source — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: NEXT_COUNTRY — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: NEXT_COUNTRY — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: NEXT_COUNTRY — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: growthbookId_v2 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: growthbookId_v2 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: growthbookId_v2 — SameSite**
  SameSite=lax
- ALTO **Cookie: amp_device_id — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: amp_device_id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: amp_device_id — SameSite**
  SameSite=lax
- ALTO **Cookie: p10_initial_date — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: p10_initial_date — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: p10_initial_date — SameSite**
  SameSite=lax

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://qr.afip.gob.ar/?qr=eA2ct25tWzDA2wssGl2vrA,,

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (23123 bytes)

- INFO **Reglas robots.txt**
  508 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://www.plataforma10.com.ar/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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 ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking que pueden engañar al usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones HTTPS, facilitando ataques de degradación de protocolo.
[HIGH] Cookie NEXT_LOCALE (HttpOnly/Secure): La falta de estos flags permite el acceso a la cookie mediante scripts y su envío por canales no cifrados.
[HIGH] Cookie source (HttpOnly/Secure): Esta cookie carece de protección básica, exponiendo la sesión a ataques de secuestro y lectura no autorizada.
[HIGH] Cookie NEXT_COUNTRY (HttpOnly/Secure): La ausencia de atributos de seguridad incrementa el riesgo de manipulación de la identidad del usuario.
[HIGH] Cookies growthbookId_v2, amp_device_id, p10_initial_date: Carecen del atributo HttpOnly, siendo accesibles ante cualquier vulnerabilidad de scripts en el navegador.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a terceros, lo que podría filtrar datos de navegación.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como cámara o micrófono, aumentando la superficie de ataque.
[MEDIUM] Contenido Mixto: Se detectó un recurso de AFIP cargando mediante HTTP, lo que debilita la integridad de la página cifrada.
[MEDIUM] Cookies sin SameSite: Las cookies de sesión no tienen protección contra ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.24.0 (Ubuntu), facilitando la búsqueda de exploits específicos para esa versión.
[LOW] X-Powered-By expuesto: Se revela el uso del framework Next.js, proporcionando información valiosa a posibles atacantes sobre la arquitectura interna.