EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://argentina.gridohelado.com/	Checks	9 pruebas
Dominio	argentina.gridohelado.com	Hallazgos	47 totales
Fecha	18 de agosto de 2026 a las 21:55	Problemas	19 detectados

D

45/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 45/100 con una nota final de D. Se ejecutaron un total de 9 checks pasivos, de los cuales 4 resultaron exitosos, 1 presentó advertencias por contenido mixto y 4 fallaron críticamente en áreas de configuración de servidor y cabeceras. La evaluación revela deficiencias severas, incluyendo la exposición de servicios de base de datos y la falta de protecciones contra ataques web comunes. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable y presenta un riesgo significativo para la integridad de los datos y la privacidad de los usuarios.

Resumen de Riesgos

2	7	7	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.0.3 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	4 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-10-20T19:27:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-22T19:27:04.000Z
- 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 — 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 — 0/100

Estado: FALLO
No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 7.0.3
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO
WordPress 7.0.3 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.3 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.intranet.gridohelado.com.ar/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://qr.afip.gob.ar/?qr=oHNAlY6BVHmi56UZ7Sexrg,,

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (35 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

4 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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

[CRITICAL] Puertos de base de datos expuestos: Los puertos 3306 (MySQL) y 5432 (PostgreSQL) se encuentran abiertos, lo que permite ataques de fuerza bruta o explotación directa sobre los datos almacenados.

[HIGH] Falta de Redirección HTTPS y HSTS: El sitio no redirige automáticamente el tráfico HTTP a HTTPS y carece de la cabecera Strict-Transport-Security, permitiendo ataques de interceptación de tráfico.

[HIGH] Ausencia total de Cabeceras de Seguridad: Faltan Content-Security-Policy (XSS), X-Frame-Options (Clickjacking) y otras protecciones esenciales que dejan el sitio expuesto a inyecciones de contenido.

[HIGH] Puerto 21 (FTP) abierto: La presencia de un servicio FTP activo permite la transferencia de archivos y credenciales sin cifrado, facilitando el robo de información sensible.

[HIGH] Exposición de versión de CMS: Se detectó públicamente la versión de WordPress 7.0.3, lo cual facilita a atacantes la búsqueda de vulnerabilidades específicas conocidas para dicha versión.

[MEDIUM] Contenido Mixto detectado: Existen recursos cargándose mediante HTTP (referentes a intranet y AFIP) en una página HTTPS, lo que debilita el cifrado general del sitio.

[MEDIUM] Puerto 22 (SSH) abierto: El acceso remoto seguro está expuesto a internet, aumentando la superficie de ataque para intentos de intrusión no autorizados.

[MEDIUM] Archivos informativos expuestos: El archivo /readme.html es accesible y puede confirmar detalles técnicos de la instalación que facilitan el reconocimiento del sitio.

[LOW] Divulgación de cabecera de servidor: La respuesta HTTP incluye el valor Server: nginx, revelando la tecnología subyacente y ayudando a perfilar el entorno del servidor.

[LOW] Rutas sensibles en robots.txt: El archivo incluye referencias a la ruta "admin", indicando a rastreadores y atacantes posibles puntos de entrada a la administración.