EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://infocar.com.ar/	Checks	9 pruebas
Dominio	infocar.com.ar	Hallazgos	51 totales
Fecha	6 de mayo de 2026 a las 10:30	Problemas	21 detectados

F

39/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 39/100, lo que corresponde a una nota F. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 3 aprobados, 2 advertencias y 3 fallos críticos que comprometen la integridad de la plataforma. La ausencia de un cifrado SSL vigente y la carencia total de cabeceras de seguridad exponen a los usuarios a riesgos severos de interceptación de datos. No se detectó un CMS conocido, lo que sugiere una implementación personalizada que actualmente carece de mantenimiento preventivo. En conclusión, el sitio web es vulnerable y no cumple con los estándares mínimos de seguridad para operar de forma segura en internet.

Resumen de Riesgos

1	12	7	1	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	mac_id: falta HttpOnly; mac_id: falta Secure; ma...
Contenido Mixto	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- ALTO **Dias hasta expiracion**
  -1684 dias restantes (expira: 2021-09-25T16:07:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2020-09-25T16:07:40.000Z
- 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: Apache — 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: ERROR

No se pudo verificar la redireccion HTTPS

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

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**
  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 — 0/100

Estado: FALLO

mac_id: falta HttpOnly; mac_id: falta Secure; mac_id: falta SameSite; PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite; navegadorsoportado: falta HttpOnly; navegadorsoportado: falta Secure; navegadorsoportado: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)

- ALTO **Cookie: mac_id — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: mac_id — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: mac_id — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: navegadorsoportado — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: navegadorsoportado — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: navegadorsoportado — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1315 bytes)
- INFO **Reglas robots.txt**
  30 Disallow, 5 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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

[CRITICAL] Certificado SSL no válido: El certificado SSL ha expirado hace 1684 días, lo que impide establecer conexiones cifradas y seguras con los usuarios.
[HIGH] Ausencia de redirección HTTPS: El sitio responde a través de HTTP (puerto 80) sin redirigir al protocolo seguro, facilitando ataques de hombre en el medio (MITM).
[HIGH] Content-Security-Policy (CSP) faltante: La carencia de esta cabecera permite la ejecución de ataques XSS y la inyección de contenido no autorizado.
[HIGH] X-Frame-Options faltante: El sitio no protege contra ataques de clickjacking, permitiendo que la web sea embebida en marcos externos maliciosos.
[HIGH] Strict-Transport-Security (HSTS) faltante: No se instruye al navegador para usar exclusivamente conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Cookie PHPSESSID sin flags de seguridad: Falta HttpOnly y Secure, lo que permite que la sesión sea robada mediante scripts o interceptada en conexiones no cifradas.
[HIGH] Cookie mac_id sin flags de seguridad: Al carecer de HttpOnly y Secure, esta cookie es vulnerable a ataques de acceso por scripts y captura en tránsito.
[HIGH] Cookie navegadorsoportado sin flags de seguridad: La ausencia de protecciones básicas en esta cookie incrementa la superficie de ataque para el secuestro de información.
[MEDIUM] X-Content-Type-Options faltante: El servidor no previene el sniffing de tipos MIME, lo que podría permitir que archivos cargados se interpreten como scripts ejecutables.
[MEDIUM] Cookies sin atributo SameSite: Las cookies mac_id, PHPSESSID y navegadorsoportado son vulnerables a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy faltante: No se controla la cantidad de información que el navegador envía al seguir enlaces hacia otros sitios web.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Falta de Sitemap en robots.txt: Aunque existe el archivo robots.txt, la ausencia de una ruta de sitemap dificulta la auditoría de rutas y la indexación correcta.
[LOW] Cabecera Server expuesta: El servidor revela que utiliza Apache, información que facilita a un atacante la búsqueda de exploits específicos para esa tecnología.