EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.hipotecario.com.ar/	Checks	9 pruebas
Dominio	www.hipotecario.com.ar	Hallazgos	49 totales
Fecha	19 de mayo de 2026 a las 13:02	Problemas	12 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web hipotecario.com.ar arroja una puntuación de 62/100, otorgando una calificación de nota C. Se han realizado 9 verificaciones pasivas, de las cuales 4 resultaron exitosas, 2 presentaron advertencias y 3 fallaron en criterios de seguridad esenciales. El escaneo revela deficiencias importantes en la configuración de cabeceras, la gestión de redirecciones seguras y la exposición de metadatos técnicos. Debido a la visibilidad de versiones de software y la falta de cifrado forzado, el sitio se clasifica actualmente como vulnerable frente a ataques dirigidos. Es imperativo abordar estas brechas para garantizar la integridad de la plataforma y la confianza de sus usuarios.

Resumen de Riesgos

0	3	7	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 113 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.4.5 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 113 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  113 dias restantes (expira: 2026-09-09T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-12T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(),midi=(),sync-xhr=(),microphone=(),camera=(),magnetometer=(),gyros...

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 404 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.4.5
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.4.5 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.4.5 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- 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
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ucu.org.ar
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.bcra.gov.ar/BCRAyVos/Comparacion_de_Comisiones.as...
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, ? URLs
- 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

[ALTA] Content-Security-Policy: Falta la cabecera CSP, lo que facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[ALTA] Redirección HTTP a HTTPS: El sitio no redirige automáticamente el tráfico inseguro a una conexión cifrada, devolviendo un error 404 en el proceso.
[ALTA] Versión de WordPress expuesta: La versión 6.4.5 es visible públicamente, lo que permite a atacantes buscar vulnerabilidades conocidas (CVE) para esta versión específica.
[MEDIA] Archivos técnicos accesibles: Los archivos /readme.html y /README.txt están expuestos, revelando detalles sobre la arquitectura interna del CMS.
[MEDIA] Panel de administración expuesto: La ruta /wp-login.php es accesible de forma pública, aumentando el riesgo de ataques de fuerza bruta contra las credenciales.
[MEDIA] Contenido mixto: Se detectaron 4 recursos cargados mediante el protocolo inseguro HTTP dentro de una página cifrada por HTTPS.
[BAJA] Meta generator: La etiqueta meta en el código fuente expone explícitamente el uso de WordPress 6.4.5 y referencias a PrestaShop.
[BAJA] Robots.txt ausente: No se encontró el archivo robots.txt, lo que dificulta la gestión del rastreo por parte de los motores de búsqueda.