# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://economicas.uba.ar/ | Checks | 9 pruebas |
| Dominio | economicas.uba.ar | Hallazgos | 47 totales |
| Fecha | 19 de mayo de 2026 a las 13:27 | Problemas | 15 detectados |

**D**

57/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad del sitio web arroja una puntuación de 57/100, lo que resulta en una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 fallaron con criticidad alta. La infraestructura presenta debilidades significativas en la configuración del servidor y en la protección contra ataques de inyección. Con base en estos resultados, se concluye que el sitio es actualmente vulnerable ante diversos vectores de ataque comunes en la web. La falta de medidas preventivas básicas compromete la integridad y la privacidad de los usuarios que interactúan con la plataforma.

## Resumen de Riesgos

| 0 | 6 | 6 | 3 | 32 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 150 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, PrestaShop |
| Version CMS Expuesta | 20 | FALLO | WordPress 6.9.4 expuesta, WordPress 2 expuesta |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 100 | OK | No se detectaron puertos abiertos |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 150 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  150 dias restantes (expira: 2026-10-16T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-15T00:00:00.000Z
- 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: Apache/2.4.62 (Debian) — 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, 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 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (445 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://economicas.uba.ar/sitemap_index.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 — 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**

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta configuración hace al sitio susceptible a ataques de clickjacking, permitiendo que sea cargado en marcos externos.
[HIGH] Strict-Transport-Security: No se implementa HSTS, lo que impide obligar al navegador a usar conexiones cifradas de forma exclusiva.
[HIGH] Redirección HTTP a HTTPS: El sitio responde por el puerto 80 sin redirigir al tráfico seguro, permitiendo la interceptación de datos en tránsito.
[HIGH] Versión de WordPress expuesta: Se detecta públicamente WordPress 6.9.4, lo que permite a atacantes buscar vulnerabilidades específicas para esa versión.
[MEDIUM] X-Content-Type-Options: La carencia de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos inesperados.
[MEDIUM] Referrer-Policy: No hay control sobre la información de origen que se envía a enlaces externos, pudiendo filtrar datos privados.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Archivos readme expuestos: Los archivos /readme.html y /README.txt son accesibles, revelando detalles técnicos internos del gestor de contenidos.
[MEDIUM] Panel de administración accesible: La ruta /wp-login.php está expuesta, facilitando intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Cabecera Server expuesta: Se revela el uso de Apache/2.4.62 (Debian), lo que ayuda a los atacantes a perfilar el entorno del servidor.
[LOW] Meta generator: La etiqueta meta expone la versión exacta del CMS, simplificando la fase de reconocimiento de un ataque.
[LOW] Rutas en robots.txt: El archivo referencia directorios administrativos, orientando a posibles atacantes hacia secciones restringidas.