EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ab-tech.com.ar/	Checks	9 pruebas
Dominio	ab-tech.com.ar	Hallazgos	47 totales
Fecha	28 de agosto de 2026 a las 22:47	Problemas	10 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 65/100, lo que corresponde a una nota C. Se ejecutaron un total de 9 checks pasivos, resultando en 7 verificaciones exitosas y 2 fallos críticos relacionados con la configuración del servidor. El sitio web demuestra una implementación correcta de certificados SSL y gestión de cookies, pero presenta deficiencias graves en la protección contra ataques de inyección y redirecciones seguras. En su estado actual, el sitio se considera vulnerable debido a la ausencia total de cabeceras de seguridad modernas. Se requiere una intervención técnica para corregir los parámetros de red y servidor.

Resumen de Riesgos

0	5	3	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	1 cookies, todas con flags correctos
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 67 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  67 dias restantes (expira: 2026-11-03T19:42:48.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-05T19:42:49.000Z
- 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

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

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 — 100/100

Estado: OK

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: abtech_sess — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: abtech_sess — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: abtech_sess — SameSite**
  SameSite=lax

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 (113 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.ab-tech.com.ar/sitemap.xml
- 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

[HIGH] HTTP a HTTPS redireccion: El servidor responde con un código 200 en conexiones HTTP, lo que significa que no redirige automáticamente a los usuarios hacia la versión segura del sitio.
[HIGH] Strict-Transport-Security (HSTS): Falta la configuración que obliga al navegador a utilizar siempre conexiones HTTPS, permitiendo ataques de degradación de protocolo.
[HIGH] Content-Security-Policy: La ausencia de esta política facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido no autorizado.
[HIGH] X-Frame-Options: No se detectó esta cabecera, lo que deja el sitio expuesto a ataques de clickjacking al permitir que la web sea cargada en marcos externos.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice MIME-type sniffing, aumentando el riesgo de ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de origen enviada a terceros, lo que podría filtrar datos de navegación de los usuarios.
[MEDIUM] Permissions-Policy: El sitio no restringe el uso de APIs del navegador como la cámara o el micrófono, incrementando la superficie de ataque.
[LOW] Server header expuesto: La cabecera revela el uso de nginx, proporcionando a posibles atacantes información sobre la tecnología subyacente del servidor.
[LOW] Ruta sensible en robots.txt: Se menciona una referencia a admin dentro del archivo de configuración para buscadores, revelando posibles rutas de acceso administrativo.