EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aplitech.cl	Checks	9 pruebas
Dominio	aplitech.cl	Hallazgos	47 totales
Fecha	8 de mayo de 2026 a las 19:42	Problemas	14 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio web arrojo una puntuacion de 64/100, lo que equivale a una nota de calificacion C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 finalizaron en fallo critico. Aunque el cifrado de conexion es correcto, la ausencia total de cabeceras de seguridad y la exposicion de versiones de software desactualizadas representan un riesgo significativo. Debido a estos hallazgos, se concluye que el sitio es vulnerable ante ataques de inyeccion y explotacion de vulnerabilidades conocidas.

Resumen de Riesgos

0	5	6	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 5.8.13 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
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 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-07-18T20:02:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-19T20:02:15.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://aplitech.cl/
- 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 5.8.13
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.8.13 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 5.8.13 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)

- 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://es.wordpress.org/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (112 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://aplitech.cl/wp-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] Content-Security-Policy: Falta — Previene XSS y ataques de inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Falta — Protege al sitio contra ataques de clickjacking que suplantan la interfaz.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones HTTPS, permitiendo degradacion de seguridad.
[HIGH] WordPress version: Version 5.8.13 expuesta publicamente — Permite a posibles atacantes identificar y explotar CVEs especificos de esta version.
[MEDIUM] X-Content-Type-Options: Falta — Evita que el navegador interprete archivos de forma incorrecta mediante MIME-type sniffing.
[MEDIUM] Referrer-Policy: Falta — No se controla la informacion de navegacion que el sitio comparte con enlaces externos.
[MEDIUM] Permissions-Policy: Falta — No se restringen las APIs del navegador como la camara o el microfono desde el servidor.
[MEDIUM] Archivo /readme.html: Accesible publicamente — Este archivo revela informacion tecnica y versiones del CMS a terceros.
[MEDIUM] Ruta /wp-login.php: Panel de acceso expuesto — Facilita intentos de intrusion mediante ataques de fuerza bruta.
[MEDIUM] Recurso HTTP: Vinculo a es.wordpress.org — Genera contenido mixto al cargar elementos mediante protocolos no seguros dentro de un sitio HTTPS.
[LOW] Server header expuesto: Apache — Revela la tecnologia y el tipo de servidor web utilizado, facilitando el reconocimiento.
[LOW] Meta generator: Expone WordPress 5.8.13 — Divulga la version exacta del motor del sitio en el codigo fuente.
[LOW] Ruta sensible en robots.txt: Referencia a admin — Sugiere la ubicacion de directorios de administracion a los motores de busqueda y atacantes.