EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sublimebp.com.ar/	Checks	9 pruebas
Dominio	sublimebp.com.ar	Hallazgos	49 totales
Fecha	16 de abril de 2026 a las 23:27	Problemas	14 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al dominio sublimebp.com.ar arroja una puntuacion de 78/100, lo que corresponde a una calificacion de Grado B. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 presento fallos criticos relacionados con la configuracion del servidor. El sitio web demuestra una implementacion solida de cifrado SSL y redirecciones seguras, pero presenta carencias importantes en la proteccion contra ataques de inyeccion y clickjacking debido a la ausencia de cabeceras de seguridad. En su estado actual, el sitio se considera mayormente seguro para la navegacion, pero es vulnerable a ataques dirigidos contra el cliente y a la exposicion de informacion tecnica innecesaria.

Resumen de Riesgos

0	2	10	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-07-14T21:56:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-15T21:56:56.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: openresty — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000;includeSubDomains; preload
- 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 — 100/100

Estado: OK
HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://sublimebp.com.ar/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000;includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- 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

- 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

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 60/100

Estado: AVISO
Falta sitemap.xml

- INFO **robots.txt**
  Presente (198 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO
1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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

[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera permite la ejecucion de scripts no autorizados, facilitando ataques de XSS e inyeccion de contenido.
[HIGH] X-Frame-Options: Falta — El sitio puede ser cargado dentro de frames externos, lo que lo hace vulnerable a ataques de clickjacking para engañar a los usuarios.
[MEDIUM] X-Content-Type-Options: Falta — No se previene el MIME-type sniffing, permitiendo que el navegador interprete archivos de forma incorrecta y potencialmente peligrosa.
[MEDIUM] Referrer-Policy: Falta — No existe control sobre la informacion de procedencia enviada en las peticiones, lo que podria filtrar rutas internas a dominios externos.
[MEDIUM] Permissions-Policy: Falta — No se restringe el acceso a APIs sensibles del navegador como camara o microfono desde el contexto de la web.
[MEDIUM] Archivo /readme.html y /README.txt: Detectados — Estos archivos son accesibles publicamente y suelen contener informacion sobre la infraestructura o versiones del software.
[MEDIUM] Paneles de login expuestos: Rutas /wp-login.php, /administrator/ y /user/login accesibles — La visibilidad de estas rutas facilita ataques de fuerza bruta contra las credenciales administrativas.
[MEDIUM] Puerto 22 (SSH) abierto: Detectado — Este puerto de administracion remota es visible publicamente, lo que aumenta la superficie de ataque para intentos de intrusion.
[MEDIUM] Robots.txt restrictivo y con rutas sensibles: Advertencia — El archivo bloquea el rastreo total y menciona explicitamente la palabra admin, revelando areas de interes para atacantes.
[LOW] Server header expuesto: Server: openresty — El servidor revela publicamente la tecnologia que utiliza, facilitando la busqueda de exploits especificos.