EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.buinzoo.cl	Checks	9 pruebas
Dominio	www.buinzoo.cl	Hallazgos	50 totales
Fecha	12 de mayo de 2026 a las 18:50	Problemas	19 detectados

F

39/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 39/100, lo que resulta en una calificación de nota F. Se realizaron 9 comprobaciones pasivas, de las cuales 3 resultaron satisfactorias, 2 generaron advertencias y 4 fallaron de forma crítica. El escaneo revela deficiencias severas en la configuración de cabeceras de seguridad y en la protección de los mecanismos de sesión. Se han detectado versiones de software expuestas y una falta de redirección forzada a protocolos seguros. Debido a la acumulación de estos hallazgos, el sitio se considera actualmente vulnerable y con un riesgo elevado de compromiso.

Resumen de Riesgos

0	8	7	4	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 81 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 6.8.2 expuesta, WordPress 2 expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 81 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  81 dias restantes (expira: 2026-08-02T04:55:45.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-04T03:58:02.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.29 — Revela framework/lenguaje
- 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 6.8.2
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.2.29

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.2 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.8.2 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)

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.buinzoo.cl/wp-content/themes/bioparque/img/biopar...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (114 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**
  http://www.buinzoo.cl/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Ausencia de Cabeceras de Seguridad: Faltan CSP, X-Frame-Options, HSTS y otras cabeceras esenciales, facilitando ataques de XSS y Clickjacking.
[HIGH] Redirección HTTPS Inexistente: El sitio no redirige el tráfico HTTP a HTTPS de forma automática, permitiendo conexiones no cifradas.
[HIGH] Exposición de Versión CMS: Se detectó públicamente el uso de WordPress 6.8.2, lo cual facilita a atacantes la búsqueda de exploits específicos para esa versión.
[HIGH] Cookies de Sesión Inseguras: La cookie PHPSESSID carece de los atributos HttpOnly y Secure, lo que permite su robo mediante scripts o interceptación de tráfico.
[MEDIUM] Falta de SameSite en Cookies: La ausencia de este atributo en la sesión de PHP aumenta el riesgo de ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto Detectado: Existe un recurso cargado mediante el protocolo inseguro HTTP dentro de la página protegida por SSL.
[MEDIUM] Puerto 8080 Abierto: El puerto de servidor web alternativo está accesible, lo que incrementa la superficie de ataque del servidor.
[MEDIUM] Archivo readme.html Expuesto: Este archivo permite confirmar detalles técnicos y versiones del sistema de gestión de contenidos a terceros.
[LOW] Exposición de Información del Servidor: Se revelan tecnologías específicas en las cabeceras, incluyendo el uso de Cloudflare y la versión de PHP 8.2.29.
[LOW] Rutas Sensibles en Robots.txt: Se mencionan rutas administrativas que podrían guiar a un atacante hacia directorios de gestión del sitio.