

Escanear Vulnerabilidades

Informe de Seguridad Web

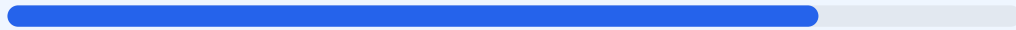
URL https://psb-cv.netlify.app/#experiencia
Dominio psb-cv.netlify.app
Fecha 18 de mayo de 2026 a las 02:28

Checks 9 pruebas
Hallazgos 45 totales
Problemas 11 detectados

B

80/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha arrojado una puntuación de 80/100, lo que equivale a una nota B. Esta evaluación se basó en la ejecución de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos en la configuración de seguridad. Se observa una implementación sólida en cuanto a cifrado de datos y transporte seguro, pero existen carencias importantes en la protección contra ataques de inyección y suplantación. En su estado actual, el sitio se considera mayoritariamente seguro para el usuario final, aunque presenta una superficie de exposición innecesaria que lo hace vulnerable ante atacantes específicos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 306 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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 306 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
306 dias restantes (expira: 2027-03-19T23:59:00Z)
- INFO **Fecha de emision**
Emitido desde: 2026-02-16T00:00:00Z
- 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: Netlify — 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=31536000; 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://psb-cv.netlify.app/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains; preload
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=31536000 (365 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO** security.txt
Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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 impide prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking, permitiendo que sea cargado dentro de marcos externos no autorizados.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría llevar al navegador a interpretar archivos de forma incorrecta y peligrosa.

[MEDIUM] Referrer-Policy: No existe un control sobre la información de navegación que se envía a terceros al seguir enlaces externos.

[MEDIUM] Permissions-Policy: La configuración no restringe el acceso de las APIs del navegador a componentes sensibles como la cámara, el micrófono o la ubicación.

[MEDIUM] Archivos informativos expuestos: El acceso público a /readme.html y /README.txt puede revelar metadatos técnicos y detalles de la infraestructura interna.

[MEDIUM] Rutas administrativas accesibles: Se detectaron endpoints activos como /wp-login.php y /administrator/ que, aunque no corresponden a un CMS detectado, aumentan el ruido de ataques de fuerza bruta.

[LOW] Server header expuesto: La cabecera revela el uso de Netlify como servidor, lo que facilita la fase de reconocimiento de un atacante para buscar exploits específicos.

[LOW] Ausencia de Robots.txt y Sitemap: El sitio carece de instrucciones para rastreadores, lo que dificulta la indexación correcta y la gestión del tráfico de bots.