

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://software-center.vercel.app/
Dominio software-center.vercel.app
Fecha 14 de agosto de 2026 a las 15:21

Checks 9 pruebas
Hallazgos 43 totales
Problemas 6 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 82/100, lo que corresponde a una calificación de grado B. Se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, no hubo advertencias y se registró 1 fallo crítico relacionado con la configuración de cabeceras. La infraestructura presenta una base sólida en cuanto a cifrado y redirecciones, pero carece de protecciones esenciales contra ataques de inyección y suplantación de identidad. Aunque el sitio muestra un nivel de seguridad aceptable, se considera vulnerable a ataques específicos del lado del cliente debido a la ausencia de políticas de seguridad en el servidor. Es imperativo corregir las omisiones en las cabeceras HTTP para alcanzar un estado de protección óptimo.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 43 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
Seguridad de Cookies	100	OK	No se encontraron cookies
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 43 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
43 dias restantes (expira: 2026-09-26T13:27:56.000Z)
- INFO Fecha de emision
Emitido desde: 2026-06-28T13:27:57.000Z
- 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: Vercel — 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 308 redirige a https://software-center.vercel.app/
- 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
- INFO

Tecnologias detectadas
Next.js

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt

Presente (184 bytes)
- INFO

Reglas robots.txt

0 Disallow, 0 Allow
- INFO

Sitemap en robots.txt

https://software-center.vercel.app/sitemap.xml
- BAJO

security.txt

No encontrado — Recomendado para política de divulgacion

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 — Envío 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

Análisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta esta cabecera, lo cual deja al sitio desprotegido ante ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Su ausencia permite que el sitio sea cargado en frames de dominios externos, facilitando ataques de clickjacking para engañar a los usuarios.

[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría intentar interpretar el contenido de forma distinta al tipo MIME declarado, abriendo la puerta a ataques de sniffing.

[MEDIUM] Referrer-Policy: La falta de esta política impide controlar qué información de navegación se envía a otros sitios al seguir enlaces salientes.

[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la cámara o el micrófono, lo que supone un riesgo potencial de privacidad.

[LOW] Server header expuesto: El encabezado revela explícitamente el uso de la tecnología Vercel, proporcionando información técnica útil para un posible atacante.