

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://orion-web-source.vercel.app/https://orion-web-source.vercel.app/	Checks	9 pruebas
Dominio	orion-web-source.vercel.app	Hallazgos	45 totales
Fecha	30 de agosto de 2026 a las 13:51	Problemas	6 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha resultado en una puntuación de 84/100, lo que equivale a una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 8 resultaron satisfactorios y 1 presentó fallos críticos en la configuración de seguridad. Aunque la infraestructura de cifrado y transporte de datos es robusta, el sitio web presenta deficiencias en las cabeceras de respuesta que comprometen la protección del usuario final. En su estado actual, orion-web-source.vercel.app se considera mayoritariamente seguro en su capa de transporte, pero vulnerable a ataques de inyección y manipulación de interfaz. Es necesario corregir los hallazgos técnicos para mitigar riesgos de seguridad de nivel alto y medio.

Resumen de Riesgos

0	2	3	1	39
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	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 89 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
89 dias restantes (expira: 2026-11-27T19:48:08.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-29T19:48:09.000Z
- 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://orion-web-source.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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO

Archivo /readme.html
No accesible (correcto)
- INFO

Archivo /README.txt
No accesible (correcto)
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (80 bytes)
- INFO

Reglas robots.txt
0 Disallow, 1 Allow
- INFO

Sitemap en robots.txt
<https://orionaiproyect.netlify.app/sitemap.xml>
- BAJO

security.txt
No encontrado — Recomendado para politica 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 — 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 esta cabecera fundamental que ayuda a prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de datos.

[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking contra 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, permitiendo la ejecución de scripts maliciosos.

[MEDIUM] Referrer-Policy: No se ha definido una política de referencia, lo que puede causar la filtración accidental de información de navegación privada hacia sitios externos.

[MEDIUM] Permissions-Policy: Falta restringir el acceso a APIs del navegador, dejando abierta la posibilidad de que el sitio acceda a periféricos o funciones sensibles sin control estricto.

[LOW] Server header expuesto: La cabecera revela explícitamente el uso de la tecnología de servidor Vercel, proporcionando información útil para un atacante en fase de reconocimiento.