

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://studiorp.net/	Checks	9 pruebas
Dominio	studiorp.net	Hallazgos	44 totales
Fecha	1 de octubre de 2026 a las 10:43	Problemas	6 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio studiorp.net arroja una puntuación de 82/100, lo que corresponde a una calificación de nota B. Se ejecutaron un total de 9 checks pasivos, obteniendo 7 resultados satisfactorios, 1 advertencia y 1 fallo crítico en la configuración de seguridad. El sitio demuestra una implementación sólida en cuanto a cifrado de datos y transporte mediante SSL/TLS. Sin embargo, la ausencia casi total de cabeceras de seguridad críticas incrementa el riesgo de ataques dirigidos a los usuarios finales. En su estado actual, el sitio se considera mayormente seguro en su infraestructura de red, pero vulnerable en su capa de aplicación web.

Resumen de Riesgos

0 CRITICO	2 ALTO	3 MEDIO	1 BAJO	38 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 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 robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
61 dias restantes (expira: 2026-12-01T01:38:13.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-02T01:38:14.000Z
- 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
- 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://studiorp.net/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=63072000
- BAJO

HSTS includeSubDomains
HSTS no 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
React, Next.js

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 — 60/100

Estado: AVISO
Falta robots.txt

● INFO **sitemap.xml**
Presente, 29 URLs

● 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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido como Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: Al no estar definida, la web es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen el sitio en marcos invisibles para engañar al usuario.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores realicen "MIME-type sniffing", lo que podría derivar en la ejecución de archivos con contenido malicioso.

[MEDIUM] Referrer-Policy: No existe control sobre la información que el navegador envía en el encabezado Referer, lo que podría exponer datos de navegación sensibles a terceros.

[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente que el sitio o scripts externos accedan a funciones como la cámara, el micrófono o la geolocalización.

[LOW] Server header expuesto: El servidor revela el uso de la tecnología Vercel, proporcionando información técnica valiosa a posibles atacantes para buscar vulnerabilidades específicas.

[LOW] Falta de robots.txt: No se detectó el archivo de instrucciones para motores de búsqueda, lo que dificulta la gestión del rastreo y la indexación del contenido.