

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Tres16.es	Checks	9 pruebas
Dominio	tres16.es	Hallazgos	46 totales
Fecha	17 de julio de 2026 a las 13:14	Problemas	9 detectados

B

80/100

puntos de seguridad



RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio Tres16.es ha resultado en una puntuacion de 80/100, lo que corresponde a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos criticos en la configuracion de seguridad. El sitio presenta una base solida en cuanto a cifrado de datos, pero carece de protecciones esenciales contra ataques de inyeccion y suplantacion. Se concluye que el sitio es seguro en el transporte de datos, pero vulnerable a ataques dirigidos hacia los usuarios finales debido a la configuracion incompleta del servidor.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 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 56 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
56 dias restantes (expira: 2026-09-11T05:40:39.000Z)
- INFO Fecha de emision
Emitido desde: 2026-06-13T05:40:40.000Z
- 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://tres16.es/
- 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
- BAJO

Meta generator
Expone: Astro v5.14.1
- INFO

Tecnologias detectadas
Next.js, Astro

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO

robots.txt
No encontrado (HTTP 404)
- BAJO

sitemap.xml
No encontrado (HTTP 404)
- 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 facilita ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso en el navegador del usuario.

[HIGH] X-Frame-Options: No se detecto esta directiva, lo que permite que el sitio sea cargado en un iframe y lo hace vulnerable a ataques de clickjacking.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podria llevar al navegador a ejecutar archivos con contenido inesperado.

[MEDIUM] Referrer-Policy: No existe una politica definida para el control de informacion de referencia, lo que puede exponer URLs internas a sitios de terceros.

[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente que scripts accedan a funciones como camara o microfono sin control estricto.

[LOW] Server header expuesto: El servidor revela el uso de Vercel, lo que ayuda a un atacante a identificar la infraestructura y buscar exploits especificos.

[LOW] Meta generator expuesto: Se detecto publicamente el uso de Astro v5.14.1, informacion que facilita el reconocimiento de posibles vulnerabilidades en dicha version.

[LOW] robots.txt: El archivo no fue encontrado (404), impidiendo la gestion adecuada de los rastreadores y la privacidad de rutas del sitio.

[LOW] sitemap.xml: La ausencia de este archivo dificulta la auditoria de la estructura del sitio y el analisis de sus endpoints publicos.