EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://terminalserver.es	Checks	9 pruebas
Dominio	terminalserver.es	Hallazgos	47 totales
Fecha	10 de mayo de 2026 a las 20:27	Problemas	3 detectados

A

96/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web arroja una puntuación de 96/100 con una calificación de nota A. Se ejecutaron un total de 9 comprobaciones pasivas, resultando en 8 verificaciones exitosas y 1 advertencia, sin detectarse fallos críticos en la infraestructura analizada. Los resultados demuestran una implementación sólida de protocolos de cifrado y una configuración de cabeceras de seguridad que cumple con los estándares más exigentes. Se han identificado exposiciones menores de información técnica y puertos abiertos que requieren atención inmediata para evitar ataques dirigidos. En conclusión, el sitio se considera seguro bajo los parámetros de este escaneo pasivo, aunque debe mitigar los puntos de exposición identificados.

Resumen de Riesgos

0	0	1	2	44
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 66 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  66 dias restantes (expira: 2026-07-15T16:38:31.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-16T16:38:32.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self' blob:;script-src 'self' 'unsafe-inline' 'unsafe-eval' cdnjs.c...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin, strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(self), microphone=(self), geolocation=(self), payment=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://terminalserver.es/
- 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 403

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, 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (118 bytes)
- INFO **Reglas robots.txt**
  3 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://terminalserver.es/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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

[MEDIO] Puerto 22 (SSH) abierto: El puerto de acceso remoto está expuesto públicamente, lo que facilita intentos de intrusión mediante fuerza bruta contra el servidor.
[BAJO] Cabecera de servidor expuesta: La respuesta del servidor revela el uso de tecnología nginx, proporcionando a posibles atacantes datos útiles para buscar exploits específicos.
[BAJO] Ruta sensible en robots.txt: Se ha detectado una referencia al directorio admin dentro del archivo de rastreo, lo que ayuda a los atacantes a localizar paneles de gestión.
[INFO] Respuesta HTTPS 403: El servidor responde con un estado de acceso prohibido al intentar acceder vía HTTPS, lo cual puede indicar una configuración de permisos restrictiva o un bloqueo de seguridad.