EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nexusdeploy.nexusdigitalsolutions.group/login	Checks	9 pruebas
Dominio	nexusdeploy.nexusdigitalsolutions.group	Hallazgos	49 totales
Fecha	25 de julio de 2026 a las 05:31	Problemas	13 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 68/100, lo que corresponde a una calificación de grado C. Se completaron un total de 9 checks pasivos, resultando en 4 verificaciones exitosas, 4 advertencias y 1 fallo crítico en la configuración global. A pesar de contar con un certificado SSL válido, la ausencia total de cabeceras de seguridad y la gestión deficiente de cookies comprometen la integridad de la plataforma. Debido a estos hallazgos, el sitio se considera actualmente vulnerable ante ataques de inyección y suplantación de identidad.

Resumen de Riesgos

0	5	7	1	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-10-18T20:32:05.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-20T19:46:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://nexusdeploy.nexusdigitalsolutions.group/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: coolify_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: coolify_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: coolify_session — SameSite**
  SameSite=lax

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 sitemap.xml

- INFO **robots.txt**
  Presente (26 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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

- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: No está configurada, lo que permite que el sitio sea embebido en marcos externos facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: Falta la configuración HSTS, por lo que el navegador no fuerza de forma automática la conexión cifrada.
[HIGH] Cookie XSRF-TOKEN: Carece del atributo HttpOnly, permitiendo que scripts de terceros accedan al token y aumenten el riesgo de robo de sesión.
[MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-type sniffing, lo que podría permitir la ejecución de archivos con tipos de datos mal interpretados.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que podría exponer servicios administrativos o proxies no protegidos.
[MEDIUM] Archivos informativos expuestos: La presencia de readme.html y README.txt puede revelar detalles técnicos sobre la infraestructura interna.
[MEDIUM] Referrer-Policy: La falta de esta política puede filtrar información sensible de la URL a sitios de terceros durante la navegación.
[MEDIUM] Permissions-Policy: No se restringe el uso de APIs del navegador como la cámara o el micrófono a nivel de servidor.
[MEDIUM] Robots.txt y Sitemap: El archivo de rastreo bloquea todo el contenido y carece de un mapa del sitio, dificultando la indexación correcta.
[LOW] Server header: Se expone la firma del servidor cloudflare, revelando información tecnológica útil para un atacante.