EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nas.gottsynology.com/d/s/18Fj3A4mNLiqqGG0BgXAQ0JbyhH2Vdpl/4fSoO6iV7f_-ELDO0d-JgoJMAdxHhaIm-7rvA9mC9Mg0	Duracion	3 minutos
Dominio	nas.gottsynology.com	Hallazgos	47 totales
Fecha	15 de mayo de 2026 a las 16:37	Problemas	14 detectados

D

54/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha resultado en una puntuación de 54/100, obteniendo una nota final de D. Durante el análisis, se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fallaron de forma crítica. El sistema presenta deficiencias importantes en la implementación de cabeceras de seguridad, protección de cookies y políticas de redirección de tráfico cifrado. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable ante ataques comunes de interceptación de datos y manipulación de sesiones.

Resumen de Riesgos

0	6	6	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	0	FALLO	drive-sharing-4fSoO6iV7f_-ELDO0d-JgoJMAdxHhaIm-7...
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 42 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  42 dias restantes (expira: 2026-06-26T06:22:00.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-28T06:22:01.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: base-uri 'self'; connect-src data: ws: wss: http: https:; default-src 'self' 'u...
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

- 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 — 0/100

Estado: FALLO

drive-sharing-4fSoO6iV7f_-ELDO0d-JgoJMAdxHhaIm-7rvA9mC9Mg0: falta HttpOnly; drive-sharing-4fSoO6iV7f_-ELDO0d-JgoJMAdxHhaIm-7rvA9mC9Mg0: falta Secure; drive-sharing-4fSoO6iV7f_-ELDO0d-JgoJMAdxHhaIm-7rvA9mC9Mg0: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: drive-sharing-4fSoO6iV7f_-ELDO0d-JgoJMAdxHhaIm-7rvA9mC9Mg0 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: drive-sharing-4fSoO6iV7f_-ELDO0d-JgoJMAdxHhaIm-7rvA9mC9Mg0 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: drive-sharing-4fSoO6iV7f_-ELDO0d-JgoJMAdxHhaIm-7rvA9mC9Mg0 — SameSite**
  Falta SameSite — Vulnerable a CSRF

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: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] Redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP al puerto seguro HTTPS, permitiendo conexiones no cifradas.
[HIGH] X-Frame-Options: Falta esta cabecera crítica, lo que permite que el sitio sea cargado en iframes y facilita ataques de clickjacking.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones seguras de forma permanente.
[HIGH] Cookie sin flag HttpOnly: La cookie drive-sharing es accesible a través de scripts de cliente, aumentando el riesgo de robo de sesión mediante XSS.
[HIGH] Cookie sin flag Secure: La cookie de sesión se envía a través de conexiones HTTP no cifradas, exponiéndola a ataques de escucha (eavesdropping).
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría realizar MIME-type sniffing, facilitando la ejecución de archivos maliciosos.
[MEDIUM] Cookie sin flag SameSite: La falta de este atributo hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy: No existe una política configurada para controlar cuánta información de referencia se envía a otros dominios.
[MEDIUM] Permissions-Policy: Falta la restricción de APIs del navegador, permitiendo potencialmente el uso no autorizado de funciones como cámara o micrófono.
[MEDIUM] Puerto 8080 abierto: Se detectó el puerto HTTP alternativo abierto, lo cual aumenta la superficie de exposición del servidor.
[MEDIUM] Bloqueo en robots.txt: El archivo bloquea el acceso total al sitio (Disallow: /), lo cual puede ser un error de configuración o una medida de ocultación ineficiente.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando pistas sobre la infraestructura tecnológica subyacente.
[LOW] sitemap.xml: No se encontró el mapa del sitio, lo que dificulta la auditoría de contenidos y la indexación correcta.