EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.idrive.com/idrive/sh/sh?k=h0l6q3c0i8 www.idrive.com	Checks	9 pruebas
Dominio	www.idrive.com	Hallazgos	49 totales
Fecha	23 de abril de 2026 a las 20:38	Problemas	8 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio www.idrive.com arroja una puntuación de 84/100 con una calificación de nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios, se detectó 1 advertencia y 1 fallo crítico relacionado con la seguridad de cabeceras. La infraestructura presenta una excelente implementación de cifrado SSL/TLS y redirecciones seguras, aunque muestra debilidades en la protección contra ataques de inyección y gestión de sesiones. El sitio se considera mayoritariamente seguro, pero presenta vulnerabilidades específicas que deben ser corregidas para mitigar riesgos de seguridad intermedios. Por lo tanto, la postura de seguridad es robusta pero requiere ajustes técnicos inmediatos.

Resumen de Riesgos

0	1	5	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 291 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	67	AVISO	JSESSIONID: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 291 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  291 dias restantes (expira: 2027-02-08T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-16T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15768000
- 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 301 redirige a https://www.idrive.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15768000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 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

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
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: JSESSIONID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: JSESSIONID — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (888 bytes)
- INFO **Reglas robots.txt**
  20 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "backup" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.idrive.com/sitemap.xml
- 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: Falta esta cabecera esencial, lo que aumenta significativamente el riesgo de ataques XSS y de inyección de contenido.
[MEDIUM] Cookie JSESSIONID: El parámetro SameSite no está configurado, dejando la sesión del usuario vulnerable a ataques de falsificación de petición en sitios cruzados o CSRF.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite que los navegadores realicen sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No se ha definido una política de referente, lo que puede filtrar información sensible de la URL a sitios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono a través de políticas de seguridad.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y podría ser utilizado para obtener detalles técnicos sobre la tecnología subyacente.
[LOW] Server header expuesto: La cabecera Server revela el uso de nginx, proporcionando información útil a posibles atacantes sobre el software del servidor.
[LOW] Ruta sensible en robots.txt: Se menciona una ruta relacionada con backup en el archivo de rastreo, lo que expone directorios que deberían ser privados.