EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://chemdata.nist.gov/dokuwiki/doku.php?id=start	Checks	9 pruebas
Dominio	chemdata.nist.gov	Hallazgos	60 totales
Fecha	21 de julio de 2026 a las 06:57	Problemas	20 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha determinado una puntuación de 70/100, lo que otorga una calificación final de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo como resultado 4 verificaciones correctas, 2 advertencias por configuraciones mejorables y 3 fallos críticos que comprometen la integridad del servidor. A pesar de contar con un cifrado de transporte robusto, la exposición de servicios internos y la falta de cabeceras de protección exponen la plataforma a ataques directos. En conclusión, el sitio se considera vulnerable debido a una superficie de ataque excesivamente amplia y falta de endurecimiento en la configuración del servidor.

Resumen de Riesgos

6	2	8	4	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 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	87	AVISO	DokuWiki: falta SameSite; DWb539d53bcb155331d24d...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	9 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-09-20T12:33:28.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-22T12:33:29.000Z
- 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: cloudflare — 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=31536000; includeSubdomains; preload
- 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://chemdata.nist.gov/
- 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 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: DokuWiki

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 — 87/100

Estado: AVISO

DokuWiki: falta SameSite; DWb539d53bcb155331d24d78dda5feb08e: falta SameSite

- INFO **Cookies detectadas**
  5 cookie(s) encontrada(s)
- INFO **Cookie: DokuWiki — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: DokuWiki — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: DokuWiki — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: DWb539d53bcb155331d24d78dda5feb08e — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: DWb539d53bcb155331d24d78dda5feb08e — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: DWb539d53bcb155331d24d78dda5feb08e — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: FCK_media — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: FCK_media — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: FCK_media — SameSite**
  SameSite=lax
- INFO **Cookie: FCK_NmSp — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: FCK_NmSp — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: FCK_NmSp — SameSite**
  SameSite=lax
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.nist.gov

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 — 20/100

Estado: FALLO

9 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- CRITICO **Puerto 23 (Telnet)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- CRITICO **Puerto 27017 (MongoDB)**
  ABIERTO — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 23 (Telnet) ABIERTO: Permite el acceso remoto mediante un protocolo no cifrado, facilitando la interceptación de credenciales.
[CRITICAL] Puerto 3306 (MySQL) ABIERTO: La base de datos está expuesta a internet, permitiendo ataques de fuerza bruta o explotación de vulnerabilidades del motor.
[CRITICAL] Puerto 3389 (RDP) ABIERTO: El servicio de escritorio remoto de Windows es visible públicamente, siendo un vector principal para ataques de ransomware.
[CRITICAL] Puerto 5432 (PostgreSQL) ABIERTO: Exposición directa de la base de datos PostgreSQL, lo que supone un riesgo de exfiltración de información.
[CRITICAL] Puerto 6379 (Redis) ABIERTO: Servicio de caché expuesto que, por defecto, carece de autenticación fuerte, permitiendo el acceso a datos en memoria.
[CRITICAL] Puerto 27017 (MongoDB) ABIERTO: Base de datos NoSQL accesible desde el exterior, facilitando el robo o manipulación de documentos.
[HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[HIGH] Puerto 21 (FTP) ABIERTO: El protocolo de transferencia de archivos sin cifrar permite que atacantes capturen archivos y contraseñas en tránsito.
[MEDIUM] X-Content-Type-Options faltante: Riesgo de ataques de tipo MIME-sniffing donde el navegador interpreta archivos de forma insegura.
[MEDIUM] Referrer-Policy faltante: No se controla la información de procedencia enviada a otros sitios, lo que puede filtrar URLs privadas.
[MEDIUM] Permissions-Policy faltante: No se restringe el acceso de la web a funciones sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Cookies sin atributo SameSite: Las cookies de DokuWiki carecen de protección contra ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectó un recurso cargado mediante HTTP (nist.gov) dentro de la página HTTPS, lo que degrada la seguridad de la sesión.
[MEDIUM] Puerto 22 (SSH) y 8080 (HTTP-Alt) ABIERTOS: Servicios de administración y servidores alternativos expuestos que aumentan las vías de entrada para intrusos.
[LOW] Cabecera Server expuesta: Indica el uso de Cloudflare, proporcionando información útil para que un atacante planifique su ofensiva.
[LOW] Meta generator DokuWiki expuesto: Revela el software de gestión de contenidos utilizado, facilitando la búsqueda de exploits específicos.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: El servidor responde con errores 404, dificultando la indexación controlada y el rastreo legítimo.