EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://complejolacteo.eclh.cu	Checks	9 pruebas
Dominio	complejolacteo.eclh.cu	Hallazgos	44 totales
Fecha	20 de abril de 2026 a las 19:38	Problemas	7 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada arroja una puntuacion de 85/100 con una nota final de B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios y 2 fallos relacionados con la configuracion del servidor y politicas de indexacion. Aunque el cifrado de datos es robusto, la ausencia de cabeceras de seguridad fundamentales incrementa el riesgo de ataques contra los usuarios. El sitio se considera mayormente seguro en su transmision de datos, pero vulnerable a nivel de endurecimiento del servidor y proteccion del lado del cliente.

Resumen de Riesgos

0	1	3	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 dias
Cabeceras de Seguridad	45	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, X-C...
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  56 dias restantes (expira: 2026-06-15T23:29:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-17T23:29:56.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

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

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https:; styl...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000;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://complejolacteo.eclh.cu/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000;includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] X-Frame-Options: Falta esta cabecera, lo que permite que el sitio sea cargado en iframes y facilita ataques de secuestro de clic o clickjacking.
[MEDIUM] X-Content-Type-Options: La ausencia de esta directiva permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecucion de scripts maliciosos.

[MEDIUM] Referrer-Policy: No se ha definido una politica de referencia, lo que podria exponer informacion sensible en las URLs al navegar hacia sitios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones del navegador como la camara o el microfono, aumentando la superficie de ataque en el cliente.
[LOW] Server header expuesto: El servidor revela el uso de la tecnologia openresty, proporcionando informacion valiosa a posibles atacantes sobre la infraestructura.
[LOW] robots.txt: El archivo de instrucciones para buscadores no fue encontrado o el acceso esta prohibido, dificultando el control de la indexacion.
[LOW] sitemap.xml: No se localizo el mapa del sitio, lo cual afecta la visibilidad y estructura de los recursos publicos del dominio.
[INFO] Respuesta HTTPS 403: El acceso principal mediante HTTPS devuelve un estado de prohibido, lo que sugiere restricciones de acceso a nivel de directorio.