

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://vaultlicen.tecnoelerd.com
Dominio vaultlicen.tecnoelerd.com
Fecha 23 de abril de 2026 a las 11:16

Checks 9 pruebas
Hallazgos 47 totales
Problemas 12 detectados

D

59/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 59/100, lo que equivale a una nota de D. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 terminaron en fallo crítico. La infraestructura presenta debilidades significativas en la configuración del servidor y en la implementación de políticas de seguridad para el navegador. Debido a la ausencia total de cabeceras de protección y la falta de redirección forzada a protocolos seguros, se concluye que el sitio es vulnerable ante ataques de interceptación y suplantación.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 87 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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	100	OK	1 cookies, todas con flags correctos
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 87 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
87 dias restantes (expira: 2026-07-19T18:15:54.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-20T18:15:55.000Z
- 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 — 0/100

Estado: **FALLO**

No hay redireccion HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redireccion**
HTTP 302 — 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 — 100/100

Estado: **OK**

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
- INFO **Cookie: session — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: session — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: 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 (1738 bytes)
- INFO **Reglas robots.txt**
9 Disallow, 1 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 autentificacion 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: Falta la cabecera encargada de prevenir ataques de inyección de scripts y Cross-Site Scripting.
- [HIGH] X-Frame-Options: Ausencia de protección contra ataques de clickjacking, lo que permitiría a un atacante embeber el sitio en marcos maliciosos.
- [HIGH] Strict-Transport-Security: El servidor no ordena al navegador el uso exclusivo de conexiones cifradas, facilitando ataques de degradación de protocolo.
- [HIGH] Redirección HTTP: No existe un salto automático de tráfico inseguro hacia HTTPS, dejando las sesiones iniciales expuestas.
- [MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando la ejecución de archivos maliciosos ocultos.
- [MEDIUM] Referrer-Policy: No hay control sobre cuánta información de origen se envía a otros dominios al navegar por enlaces externos.
- [MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la ubicación o periféricos.
- [MEDIUM] Puerto 8080 abierto: Se detectó un puerto de servidor web alternativo expuesto que incrementa la superficie de ataque externa.
- [MEDIUM] Bloqueo total en robots.txt: La configuración actual impide que cualquier buscador indexe el contenido de forma legítima.
- [LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando pistas tecnológicas a potenciales atacantes.
- [LOW] sitemap.xml ausente: El archivo de mapa del sitio no fue localizado, afectando la estructura de auditoría de contenidos.