EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://carerit.com	Checks	9 pruebas
Dominio	carerit.com	Hallazgos	45 totales
Fecha	21 de abril de 2026 a las 08:50	Problemas	25 detectados

D

49/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el dominio carerit.com ha dado como resultado una puntuación de 49/100, obteniendo una calificación de grado D. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, de las cuales 4 resultaron satisfactorias, 1 generó una advertencia y 4 fueron fallos críticos. Los hallazgos revelan una infraestructura con una superficie de exposición alarmante debido a la apertura de múltiples puertos de bases de datos y servicios de gestión remota. En su estado actual, el sitio se considera vulnerable y presenta riesgos significativos para la confidencialidad y disponibilidad de la información alojada.

Resumen de Riesgos

6	6	11	2	20
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 48 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	No se encontraron cookies
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 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-06-07T23:26:30.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-09T23:26:31.000Z
- 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: OVHcloud — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4 — Revela framework/lenguaje
- 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 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
- INFO **Tecnologias detectadas**
  PHP/8.4

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
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://localhost:8080/realms/carerit/protocol/openid-connect...

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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: Este protocolo transmite información en texto plano y permite el acceso remoto, siendo extremadamente vulnerable a la interceptación de credenciales.

[CRITICAL] Puerto 3306 (MySQL) abierto: La exposición directa de la base de datos a internet facilita ataques de fuerza bruta y posibles brechas de datos.
[CRITICAL] Puerto 3389 (RDP) abierto: El servicio de escritorio remoto de Windows es un vector crítico utilizado frecuentemente para el despliegue de ransomware.
[CRITICAL] Puerto 5432 (PostgreSQL) abierto: Los motores de bases de datos no deben ser accesibles desde redes públicas sin túneles seguros.
[CRITICAL] Puerto 6379 (Redis) abierto: Redis suele carecer de autenticación por defecto, permitiendo que un atacante externo acceda a los datos almacenados en caché.
[CRITICAL] Puerto 27017 (MongoDB) abierto: Exposición de base de datos NoSQL que permite consultas externas si no cuenta con políticas de red restrictivas.
[HIGH] Redirección HTTPS ausente: El servidor no fuerza el uso de conexiones cifradas, permitiendo el acceso mediante el protocolo inseguro HTTP.
[HIGH] Content-Security-Policy faltante: Ausencia de directivas para prevenir ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking al permitir ser embebido en marcos de otras webs.
[HIGH] Strict-Transport-Security faltante: No se implementa la política HSTS, lo que deja a los usuarios vulnerables a ataques de degradación de SSL.
[HIGH] Puerto 21 (FTP) abierto: Protocolo de transferencia de archivos obsoleto que envía credenciales y datos sin ningún tipo de cifrado.
[MEDIUM] Contenido mixto detectado: Se intenta cargar un recurso mediante HTTP (localhost:8080) en una página segura, lo que compromete la integridad de la sesión.
[MEDIUM] Rutas de administración expuestas: Se detectó visibilidad pública en rutas sensibles como /wp-login.php, /administrator/ y /user/login.
[MEDIUM] Archivos de información accesibles: Los archivos /readme.html y /README.txt están disponibles y pueden revelar detalles específicos de la tecnología utilizada.
[MEDIUM] X-Content-Type-Options faltante: Riesgo de que el navegador interprete archivos de forma incorrecta, facilitando la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy faltante: No se controla qué información de origen se comparte con sitios de terceros al navegar.
[MEDIUM] Permissions-Policy faltante: No se restringe el acceso de la web a funciones sensibles del dispositivo del usuario como cámara o ubicación.
[MEDIUM] Puerto 22 (SSH) abierto: El acceso remoto seguro está expuesto, requiriendo un endurecimiento de contraseñas y monitorización constante.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo puede ocultar servicios vulnerables o paneles de desarrollo sin protección.
[LOW] Cabecera Server expuesta: Se identifica el uso de OVHcloud, lo que ayuda a potenciales atacantes a perfilar la infraestructura.
[LOW] Cabecera X-Powered-By expuesta: Revela el uso de PHP/8.4, permitiendo la búsqueda de vulnerabilidades específicas para esa versión del lenguaje.