EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.doble-k.com/	Checks	9 pruebas
Dominio	www.doble-k.com	Hallazgos	42 totales
Fecha	7 de mayo de 2026 a las 07:59	Problemas	20 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el activo digital presenta una puntuación de 53/100, lo que otorga una calificación de grado D. Se han ejecutado 9 comprobaciones pasivas, resultando en 5 verificaciones correctas y 4 fallos de seguridad significativos. Aunque el cifrado de transporte es válido, la infraestructura presenta debilidades críticas en la configuración del servidor y una exposición alarmante de servicios internos. Se concluye que el sitio es actualmente vulnerable y presenta un riesgo elevado de compromiso de datos debido a la visibilidad pública de sus bases de datos y herramientas de administración.

Resumen de Riesgos

6	6	5	3	22
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 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	100	OK	No se detecto contenido mixto
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 41 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  41 dias restantes (expira: 2026-06-17T10:40:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-19T10:40:19.000Z
- 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

- 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

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 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 27017 (MongoDB) Abierto: Base de datos NoSQL expuesta que permite intentos de acceso externo y posible exfiltración de información.
[CRITICAL] Puerto 6379 (Redis) Abierto: El motor de caché es accesible desde internet, lo que suele implicar acceso a datos temporales sin autenticación.
[CRITICAL] Puerto 5432 (PostgreSQL) Abierto: La exposición directa de este motor de base de datos facilita ataques de fuerza bruta contra las credenciales de administración.
[CRITICAL] Puerto 3389 (RDP) Abierto: El servicio de escritorio remoto de Windows es visible, siendo uno de los vectores principales para el despliegue de ransomware.
[CRITICAL] Puerto 3306 (MySQL) Abierto: Base de datos relacional accesible públicamente, lo que aumenta drásticamente la superficie de ataque del servidor.

[CRITICAL] Puerto 23 (Telnet) Abierto: Protocolo de administración remota obsoleto que transmite toda la información, incluyendo contraseñas, en texto plano.
[HIGH] Ausencia de Redirección HTTPS: El servidor no fuerza el tráfico seguro, permitiendo que las conexiones se realicen por el puerto 80 sin cifrado.
[HIGH] Content-Security-Policy (CSP) Faltante: No existe una política que restrinja el origen de los recursos, facilitando ataques de inyección y XSS.
[HIGH] X-Frame-Options Faltante: La ausencia de esta cabecera permite que el sitio sea embebido en marcos externos, habilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS) Faltante: No se instruye al navegador para que use siempre HTTPS, permitiendo ataques de degradación de protocolo.
[MEDIUM] Puertos de Gestión Abiertos (21, 22, 8080): La visibilidad de FTP, SSH y puertos alternativos proporciona puntos de entrada adicionales para atacantes.
[MEDIUM] Cabeceras de Seguridad Secundarias Faltantes: La falta de X-Content-Type-Options, Referrer-Policy y Permissions-Policy debilita la privacidad y seguridad del cliente.
[LOW] Cabecera Server Expuesta: El servidor informa explícitamente el uso de tecnología OVHcloud, ayudando a los atacantes a perfilar la infraestructura.
[LOW] Archivos de Indexación Faltantes: No se han encontrado robots.txt ni sitemap.xml, lo cual afecta a la visibilidad controlada en motores de búsqueda.