EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.duoc.cl/	Checks	9 pruebas
Dominio	www.duoc.cl	Hallazgos	42 totales
Fecha	14 de julio de 2026 a las 17:27	Problemas	5 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 86/100, lo que corresponde a una calificación de grado B. Durante el proceso se ejecutaron 9 procesos de revisión pasiva, resultando en 6 verificaciones exitosas, 1 advertencia y 1 fallo crítico. El sistema presenta una base sólida en cifrado y cabeceras de seguridad, pero se han detectado deficiencias importantes en la exposición de versiones del CMS y la gestión de redirecciones. En su estado actual, el sitio se considera mayoritariamente seguro, aunque vulnerable a ataques dirigidos debido a la divulgación de información técnica sensible.

Resumen de Riesgos

0	1	2	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 187 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.8.1 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 187 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  187 dias restantes (expira: 2027-01-17T21:05:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-24T15:32:02.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://*.is...

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubdomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: clipboard-write=(self "https://e.issuu.com"),geolocation=(),midi=(),sync-xhr=(),...

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.8.1
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.1 expuesta

- ALTO **WordPress version**
  Version 6.8.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

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://observatorio.duoc.cl/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (112 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.duoc.cl/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 puerto(s) abierto(s), todos esperados

- 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)**
  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 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] WordPress version: La versión 6.8.1 se encuentra expuesta públicamente, lo que facilita a atacantes la búsqueda de exploits específicos para este motor.
[MEDIUM] Contenido Mixto: El recurso http://observatorio.duoc.cl/ se carga mediante HTTP en una página protegida, lo que compromete la integridad de la conexión.
[MEDIUM] Archivo /readme.html: Este archivo es accesible para cualquier usuario y revela información técnica interna del gestor de contenidos.
[LOW] Redirección HTTPS: El sistema no pudo verificar una redirección automática forzada hacia el protocolo seguro, lo que podría permitir conexiones no cifradas.
[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 6.8.1 en el código fuente del sitio.
[LOW] Rutas sensibles en robots.txt: La mención directa a rutas como "admin" ofrece pistas sobre la estructura de directorios privados a posibles atacantes.