EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.dgt.es	Checks	9 pruebas
Dominio	www.dgt.es	Hallazgos	47 totales
Fecha	27 de mayo de 2026 a las 14:21	Problemas	7 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

Este informe de auditoría detalla el análisis de seguridad realizado sobre el portal dgt.es, el cual ha obtenido una puntuación de 85/100 con una calificación de B. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron exitosos, uno generó una advertencia y uno fue clasificado como fallo crítico. No se ha realizado un pentest activo, por lo que los resultados se limitan a la configuración expuesta del servidor y cabeceras. El sitio presenta una base sólida de cifrado, pero se considera vulnerable a ataques de inyección y manipulación de interfaz debido a la falta de políticas de seguridad modernas.

Resumen de Riesgos

0	2	4	1	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 39 dias
Cabeceras de Seguridad	45	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
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	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 39 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  39 dias restantes (expira: 2026-07-05T10:17:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T10:17:34.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=15768000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- 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://www.dgt.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15768000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 dias)
- 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
- BAJO **Meta generator**
  Expone: DGT, Dirección General Tráfico

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://revista.dgt.es/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.interior.gob.es/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (9401 bytes)
- INFO **Reglas robots.txt**
  220 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.dgt.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 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)**
  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 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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos externos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Al no estar presente, el sitio puede ser cargado dentro de marcos (iframes) en dominios externos, facilitando ataques de clickjacking para engañar a los usuarios.
[MEDIUM] Permissions-Policy: La falta de esta directiva no restringe el acceso de la web a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Contenido Mixto: Se detectaron 2 recursos cargados mediante el protocolo inseguro HTTP (revista.dgt.es y interior.gob.es) dentro de la página HTTPS, lo que debilita la integridad del cifrado.
[MEDIUM] Bloqueo de Indexación: El archivo robots.txt bloquea completamente el acceso a los rastreadores mediante la directiva Disallow: /, lo cual podría ser un error de configuración o una medida de privacidad extrema.
[LOW] Meta generator: El código fuente expone etiquetas que identifican al sitio con la Dirección General de Tráfico, lo que facilita el reconocimiento de la infraestructura por parte de posibles atacantes.