EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.gobiernodecanarias.net/	Checks	9 pruebas
Dominio	www.gobiernodecanarias.net	Hallazgos	52 totales
Fecha	10 de abril de 2026 a las 08:58	Problemas	18 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada arroja una puntuacion de 59/100, lo que equivale a una calificacion de grado D. Durante el analisis se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presento advertencias y 3 fallaron criticamente. El sitio presenta deficiencias significativas en la implementacion de cabeceras de seguridad y en el forzado de protocolos seguros. Debido a la presencia de contenido mixto y la exposicion de rutas sensibles, se concluye que el sitio es vulnerable y requiere intervencion inmediata.

Resumen de Riesgos

0	3	10	5	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 186 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	20	FALLO	20 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 186 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  186 dias restantes (expira: 2026-10-13T12:37:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-12T22:31:18.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=0; includeSubDomains
- 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
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=0; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=0 (0 dias) — Recomendado minimo 180 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
- INFO **Tecnologias detectadas**
  Next.js

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

- 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 — 20/100

Estado: FALLO

20 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.gobiernodecanarias.org/principal/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.gobiernodecanarias.org/principal/accesibilidad.ht...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.gobiernodecanarias.net/sesionweb/cgi-bin/cierre.c...
- MEDIO **href (link/stylesheet)**
  ...y 17 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (29037 bytes)
- INFO **Reglas robots.txt**
  631 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "backup" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "\.env" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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] Fallo en redireccion HTTPS: El servidor no redirige automaticamente las peticiones inseguras HTTP a HTTPS.
[HIGH] Ausencia de Content-Security-Policy: No existe una politica que prevenga ataques de inyeccion de codigo o XSS.
[HIGH] X-Frame-Options faltante: La ausencia de esta cabecera permite que el sitio sea cargado en marcos, facilitando ataques de clickjacking.
[MEDIUM] Contenido Mixto detectado: Se han identificado 20 recursos que se cargan mediante HTTP dentro de la pagina segura, comprometiendo el cifrado.
[MEDIUM] HSTS no configurado: La cabecera de seguridad de transporte estricta tiene un valor de cero, lo que anula su proteccion.
[MEDIUM] X-Content-Type-Options ausente: El navegador puede intentar adivinar el tipo de contenido, permitiendo la ejecucion de archivos maliciosos.
[MEDIUM] Archivos informativos expuestos: El acceso publico a /readme.html y /README.txt puede revelar informacion tecnica de la plataforma.
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: No se controla la informacion de origen enviada ni se restringen las APIs del navegador como camara o microfono.
[LOW] Cabecera de servidor expuesta: Se revela que el servidor utiliza Apache, lo que facilita a un atacante la busqueda de exploits especificos.
[LOW] Rutas sensibles en robots.txt: El archivo menciona directorios criticos como admin, backup, .env y config, sirviendo como hoja de ruta para atacantes.
[LOW] Falta de sitemap.xml: No se encuentra el mapa del sitio, lo cual es una advertencia de configuracion incompleta.