EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.moeve.es/es	Checks	9 pruebas
Dominio	www.moeve.es	Hallazgos	52 totales
Fecha	8 de mayo de 2026 a las 09:27	Problemas	15 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar una auditoría técnica en el sitio web, se ha determinado una puntuación de 64/100, lo que otorga una calificación de C. El análisis pasivo ejecutó 9 comprobaciones, de las cuales 4 resultaron satisfactorias, 2 generaron advertencias y 3 fallaron debido a configuraciones de seguridad críticas. Se han detectado puertos de infraestructura sensibles expuestos a internet y una carencia casi total de cabeceras de protección en el servidor. Debido a la exposición de servicios internos y la presencia de contenido mixto, el sitio se considera vulnerable y requiere intervenciones inmediatas para mitigar riesgos de intrusión.

Resumen de Riesgos

3	4	8	0	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	83	AVISO	incap_ses_692_3150111: falta HttpOnly
Contenido Mixto	20	FALLO	9 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	20	FALLO	5 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: 2026-06-17T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-06-18T00:00:00.000Z
- 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

- 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=31536000; 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.moeve.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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

- 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 — 83/100

Estado: AVISO
incap_ses_692_3150111: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: visid_incap_3150111 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: visid_incap_3150111 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: visid_incap_3150111 — SameSite**
  SameSite=none
- ALTO **Cookie: incap_ses_692_3150111 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: incap_ses_692_3150111 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: incap_ses_692_3150111 — SameSite**
  SameSite=none

Contenido Mixto — 20/100

Estado: FALLO
9 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://moeve.es/es/utilidades/catalogo/asfaltos/carretera/li...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://moeve.es/es/utilidades/catalogo/asfaltos/carretera/li...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://moeve.es/es/utilidades/catalogo/asfaltos/carretera/li...
- MEDIO **href (link/stylesheet)**
  ...y 6 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO
Falta robots.txt

- INFO **sitemap.xml**
  Presente, 2523 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO
5 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta

- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — 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
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos está expuesta directamente a internet, permitiendo intentos de conexión externa y fuerza bruta.
[CRITICAL] Puerto 3389 (RDP) abierto: El servicio de escritorio remoto de Windows es visible, lo que representa un riesgo extremo de acceso no autorizado al servidor.
[CRITICAL] Puerto 6379 (Redis) abierto: El motor de caché está expuesto y suele carecer de autenticación por defecto, facilitando el robo de datos en memoria.
[HIGH] Puerto 21 (FTP) abierto: El uso de transferencia de archivos sin cifrar permite la interceptación de credenciales y datos en tránsito.
[HIGH] Content-Security-Policy ausente: La falta de esta cabecera permite ataques de inyección de código como Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options ausente: El sitio no protege contra ataques de clickjacking, permitiendo que la web sea embebida en marcos maliciosos.
[HIGH] Seguridad de Cookies: La cookie incap_ses_692_3150111 carece del atributo HttpOnly, permitiendo su robo mediante scripts maliciosos.
[MEDIUM] Contenido Mixto: Se detectaron 9 recursos cargados mediante HTTP en una página HTTPS, lo que debilita la integridad de la conexión cifrada.
[MEDIUM] X-Content-Type-Options ausente: El servidor no previene el sniffing de tipos MIME, lo que facilita la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un puerto alternativo suele indicar paneles de administración o proxies mal configurados.
[MEDIUM] Referrer-Policy y Permissions-Policy ausentes: Falta control sobre la información de navegación compartida y el uso de APIs del navegador.
[LOW] Robots.txt ausente: No existe un archivo de directrices para rastreadores, afectando la gestión del indexado y la privacidad de rutas.