# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://recoletosconsultores.com | Checks | 9 pruebas |
| Dominio | recoletosconsultores.com | Hallazgos | 49 totales |
| Fecha | 20 de julio de 2026 a las 01:32 | Problemas | 16 detectados |

**D**

55/100

puntos de seguridad

**RESUMEN EJECUTIVO**

La auditoría de seguridad realizada sobre el dominio recoletosconsultores.com arroja una puntuación de 55/100, lo que equivale a una nota de D. De los 9 checks pasivos ejecutados, se obtuvieron 3 resultados satisfactorios, 3 advertencias y 3 fallos críticos. Aunque el sitio cuenta con un certificado SSL válido, la exposición de servicios internos y la ausencia de cabeceras de protección básicas elevan el riesgo de compromiso. Debido a estos hallazgos, el sitio se clasifica actualmente como vulnerable y requiere intervención técnica inmediata.

## Resumen de Riesgos

| 2 | 6 | 6 | 2 | 33 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 35 dias |
| Cabeceras de Seguridad | 15 | FALLO | Solo 1/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 70 | AVISO | HTTP redirige a HTTPS pero falta HSTS |
| Deteccion CMS | 100 | OK | CMS detectado: WordPress |
| Version CMS Expuesta | 20 | FALLO | WordPress 2 expuesta |
| Seguridad de Cookies | 67 | AVISO | pll_language: falta HttpOnly |
| 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 | 20 | FALLO | 3 puertos riesgosos abiertos |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 35 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  35 dias restantes (expira: 2026-08-23T21:12:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-25T21:12:14.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 15/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: nginx — 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)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

## Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://recoletosconsultores.com/
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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, Astro

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

## Seguridad de Cookies — 67/100

Estado: AVISO

pll_language: falta HttpOnly

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: pll_language — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: pll_language — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: pll_language — SameSite**
  SameSite=lax

## Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://mdepablo.es
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.recoletosciudadreal.es

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (591 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 7 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://recoletosconsultores.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 20/100

Estado: FALLO

3 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
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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**

[CRITICAL] Puerto 3306 (MySQL): Base de datos expuesta públicamente, permitiendo ataques de fuerza bruta o explotación directa.
[CRITICAL] Puerto 5432 (PostgreSQL): Servicio de base de datos accesible desde el exterior, aumentando críticamente la superficie de ataque.
[HIGH] Puerto 21 (FTP): Protocolo de transferencia de archivos sin cifrar abierto, lo que facilita la interceptación de credenciales.
[HIGH] Content-Security-Policy: Ausencia de esta cabecera, lo que permite la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta de protección contra clickjacking, permitiendo que el sitio sea embebido en marcos externos fraudulentos.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, dejando a los usuarios vulnerables a ataques de degradación de protocolo.
[HIGH] Cookie pll_language: La cookie carece del atributo HttpOnly, lo que permite que sea robada mediante scripts maliciosos en el navegador.
[MEDIUM] Versión de WordPress expuesta: El archivo readme.html y la ruta wp-login.php son públicos, facilitando la identificación de la tecnología a atacantes.
[MEDIUM] Contenido Mixto: El sitio carga recursos mediante HTTP simple desde dominios externos, rompiendo la cadena de confianza del cifrado SSL.
[MEDIUM] Referrer-Policy y Permissions-Policy: Cabeceras faltantes que derivan en una falta de control sobre la privacidad y las funciones del navegador.
[LOW] Exposición de cabecera Server: El servidor revela el uso de nginx, proporcionando información útil para la fase de reconocimiento de un atacante.
[LOW] Rutas en Robots.txt: Se hace referencia explícita a directorios administrativos, revelando la estructura interna del sitio.