# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://theoxeniapalace.com/theoxenia-palace/ | Checks | 9 pruebas |
| Dominio | theoxeniapalace.com | Hallazgos | 48 totales |
| Fecha | 26 de septiembre de 2026 a las 07:55 | Problemas | 18 detectados |

**D**

56/100

puntos de seguridad

**RESUMEN EJECUTIVO**

Tras completar la auditoría de seguridad, el sitio web ha obtenido una puntuación técnica de 56/100, lo que se traduce en una nota de grado D. El análisis de los checks pasivos revela un estado de seguridad precario, habiéndose ejecutado 9 comprobaciones con un resultado de 4 satisfactorias, 1 advertencia y 4 fallos críticos. Se han detectado deficiencias graves en la configuración de cabeceras de seguridad, exposición de versiones de software y presencia de contenido mixto. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable y presenta riesgos significativos para la integridad de los datos y la navegación de los usuarios.

## Resumen de Riesgos

| 0 | 5 | 9 | 4 | 30 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 55 dias |
| Cabeceras de Seguridad | 0 | FALLO | Solo 0/6 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 7.1.2 expuesta, WordPress 2 expuesta |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 20 | FALLO | 6 recursos HTTP en pagina HTTPS |
| Robots.txt y Sitemap | 20 | FALLO | Faltan robots.txt y sitemap.xml |
| Puertos Abiertos | 100 | OK | No se detectaron puertos abiertos |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 55 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  55 dias restantes (expira: 2026-11-20T01:37:28.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-22T01:37:29.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, 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)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://theoxeniapalace.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
- BAJO **Meta generator**
  Expone: WordPress 7.1.2
- INFO **Tecnologias detectadas**
  Next.js, Astro

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.1.2 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.1.2 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)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

## 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

6 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://theoxeniapalace.com/theoxenia-house
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://theoxeniapalace.com/piraeus-theoxenia
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://theoxeniapalace.com/theoxenia-residence
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

## Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de inyección de código y XSS.
[HIGH] X-Frame-Options: La ausencia de esta política permite ataques de clickjacking, poniendo en riesgo las acciones del usuario.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide forzar conexiones seguras y permite ataques de degradación de protocolo.
[HIGH] Versión de WordPress expuesta: La versión 7.1.2 es visible públicamente, facilitando a los atacantes la búsqueda de vulnerabilidades conocidas (CVE).
[MEDIUM] Contenido Mixto: Se detectaron 6 recursos cargados mediante HTTP dentro de una página segura HTTPS, lo que rompe la cadena de cifrado.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice sniffing de tipos MIME, aumentando el riesgo de ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información que se envía a otros sitios web al navegar desde la página actual.
[MEDIUM] Permissions-Policy: No se restringen las APIs sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Archivos sensibles expuestos: El archivo readme.html y la ruta de administración wp-login.php son accesibles, revelando información técnica.
[LOW] Server header expuesto: El encabezado revela el uso de tecnología nginx, facilitando la fase de reconocimiento de un atacante.
[LOW] Meta generator visible: El código fuente expone directamente la versión de WordPress utilizada.
[LOW] Ausencia de archivos de control: No se encontraron los archivos robots.txt ni sitemap.xml, lo que indica una gestión de rastreo deficiente.