

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://unipazmont.xo.je	Checks	9 pruebas
Dominio	unipazmont.xo.je	Hallazgos	44 totales
Fecha	10 de septiembre de 2026 a las 22:22	Problemas	15 detectados

C

61/100

puntos de seguridad



RESUMEN EJECUTIVO

El analisis de ciberseguridad del sitio web ha resultado en una puntuacion de 61/100, lo que otorga una calificacion de grado C. Durante la evaluacion se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios y 3 fallos criticos en la configuracion de seguridad. Aunque el cifrado SSL es correcto, la ausencia total de cabeceras de proteccion y la falta de redireccion automatica a HTTPS debilitan seriamente la infraestructura. Se han detectado rutas de administracion expuestas que aumentan la superficie de ataque para agentes externos. En su estado actual, se concluye que el sitio es vulnerable ante ataques de inyeccion de contenido y suplantacion de identidad.

Resumen de Riesgos

0 CRITICO	5 ALTO	8 MEDIO	2 BAJO	29 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
80 dias restantes (expira: 2026-11-29T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-31T00:00:00.000Z
- 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: openresty — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 200 — No redirige a HTTPS
- 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

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

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
- MEDIO

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

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente

● 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 — 100/100

Estado: OK
No se detecto contenido mixto

● INFO **Contenido mixto**
Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO
Faltan robots.txt y sitemap.xml

● BAJO **robots.txt**
No encontrado (HTTP 404)

● INFO **security.txt**
Presente en /.well-known/security.txt — Buena practica

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 ataques de Cross-Site Scripting (XSS) y la ejecucion de scripts maliciosos.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es vulnerable a ataques de clickjacking que pueden comprometer las acciones del usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo ataques de degradacion de protocolo.

[HIGH] Redireccion HTTPS: El servidor responde por HTTP 200 sin redirigir al puerto seguro, exponiendo los datos en transito a interceptaciones.

[MEDIUM] X-Content-Type-Options: La falta de proteccion contra MIME-type sniffing facilita que el navegador interprete archivos de forma insegura.

[MEDIUM] Referrer-Policy: No se controla la informacion de referencia enviada a otros dominios, lo que podria filtrar rutas internas sensibles.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador a funciones como camara o microfono.

[MEDIUM] Paneles de login expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles publicamente para intentos de fuerza bruta.

[MEDIUM] Archivos de informacion expuestos: Los archivos /readme.html y /README.txt son publicos y pueden revelar detalles tecnicos del sistema.

[LOW] Server header expuesto: El encabezado revela el uso de openresty, informacion util para que un atacante identifique vulnerabilidades especificas.

[LOW] Ausencia de robots.txt: No se encontro el archivo de guia para rastreadores, lo que dificulta el control de indexacion del sitio.