# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://extremiana.com/ | Checks | 9 pruebas |
| Dominio | extremiana.com | Hallazgos | 47 totales |
| Fecha | 17 de mayo de 2026 a las 17:32 | Problemas | 16 detectados |

C

60/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 60/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fueron calificados como fallos críticos. Se han identificado riesgos significativos relacionados con la falta de cabeceras de seguridad y el uso de una versión de software obsoleta. Debido a la exposición de servicios sensibles y la falta de protecciones modernas, el sitio se considera vulnerable frente a ataques dirigidos. Es imperativo realizar tareas de actualización y endurecimiento de la configuración para mejorar la postura de seguridad.

## Resumen de Riesgos

| 0 | 6 | 7 | 3 | 31 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 183 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, PrestaShop |
| Version CMS Expuesta | 20 | FALLO | WordPress 5.4.4 expuesta, WordPress 2 expuesta |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 60 | AVISO | 1 recurso(s) HTTP en pagina HTTPS |
| Robots.txt y Sitemap | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 60 | AVISO | 2 puerto(s) potencialmente riesgoso(s): 21 (FTP)... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 183 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  183 dias restantes (expira: 2026-11-16T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-03T00:00:00.000Z
- 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: 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
- 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://extremiana.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, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 5.4.4
- INFO **Tecnologias detectadas**
  Next.js

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.4.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 5.4.4 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://html5shim.googlecode.com/svn/trunk/html5.js

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] WordPress version: La versión 5.4.4 está expuesta públicamente, lo que permite a atacantes buscar y explotar CVEs conocidos para este software desactualizado.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: No está configurada, dejando el sitio vulnerable a ataques de clickjacking donde se puede superponer contenido malicioso.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, aumentando el riesgo de ataques Man-in-the-Middle.
[HIGH] Puerto 21 (FTP): Se encuentra abierto, lo que implica que la transferencia de archivos y credenciales se realiza sin cifrado de extremo a extremo.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que puede llevar a que archivos de texto sean ejecutados como scripts.
[MEDIUM] Referrer-Policy: No hay control sobre la información de referencia enviada a otros sitios, lo que podría filtrar rutas internas o datos de navegación.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono mediante políticas de seguridad.
[MEDIUM] Recurso HTTP: Se detectó contenido mixto debido a que un script de googlecode.com se carga a través de una conexión HTTP no segura dentro de la web HTTPS.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y puede revelar detalles técnicos específicos sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible, facilitando ataques de fuerza bruta contra las credenciales de gestión.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto está abierto, representando un vector de ataque si no se cuenta con una política estricta de llaves criptográficas.
[LOW] Server header expuesto: La cabecera revela el uso de servidor Apache, facilitando a los atacantes el reconocimiento de la infraestructura tecnológica.
[LOW] Meta generator: El código fuente expone explícitamente la versión WordPress 5.4.4, agilizando la fase de recolección de información del atacante.
[LOW] Ruta sensible en robots.txt: Se hace referencia a directorios de administración que deberían permanecer ocultos para evitar el mapeo de áreas críticas.