EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://adira.es	Checks	9 pruebas
Dominio	adira.es	Hallazgos	57 totales
Fecha	28 de marzo de 2026 a las 19:33	Problemas	24 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio adira.es ha arrojado una puntuación de 61/100, lo que corresponde a una calificación de grado C. El análisis consistió en 9 procesos de inspección pasiva, resultando en 4 verificaciones correctas, 2 advertencias y 3 fallos críticos detectados en la infraestructura. Se han identificado brechas de seguridad importantes relacionadas con la obsolescencia del software base y la configuración deficiente de las cabeceras de respuesta del servidor. Debido a la exposición de una versión de WordPress antigua y la falta de mecanismos de protección contra ataques web comunes, se concluye que el sitio es actualmente vulnerable y requiere una intervención correctiva inmediata.

Resumen de Riesgos

0	5	15	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 283 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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 4.1.1 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	22 recursos 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 283 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  283 dias restantes (expira: 2027-01-05T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-15T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Apache/2.4.66 (Unix) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.19 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;, upgrade-insecure-requests;
- 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://adira.es/
- 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: Powered by LayerSlider 7.12.3 - Build Heros, Sliders, and Popups. Create Animations and Beautiful, Rich Web Content as Easy as Never Before on WordPress.
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.4.19

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.1.1 expuesta

- ALTO **WordPress version**
  Version 4.1.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- 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

22 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.adira.es/wp-content/uploads/2015/02/Adira.png
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.adira.es/wp-content/uploads/2015/02/Adira.png
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.adira.es/wp-content/uploads/2015/02/Adira.png
- MEDIO **src (script/img/iframe)**
  ...y 9 mas del mismo tipo
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.adira.es/aviso-legal/
- MEDIO **Recurso HTTP (CSS url())**
  http://demo.select-themes.com/stockholm8/wp-content/uploads/...
- MEDIO **Recurso HTTP (CSS url())**
  http://www.adira.es/wp-content/uploads/2015/02/banner_works....
- MEDIO **Recurso HTTP (CSS url())**
  http://www.adira.es/wp-content/uploads/2015/02/eleccion-estr...
- MEDIO **CSS url()**
  ...y 5 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (113 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 en robots.txt**
  https://www.adira.es/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 8080 (HTTP-Alt)

- 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
- 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
- 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

[HIGH] WordPress version: Se detectó la versión 4.1.1, la cual es extremadamente antigua y cuenta con múltiples vulnerabilidades públicas conocidas (CVEs) que permiten el compromiso total del sitio.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos se encuentra abierto y expuesto, permitiendo el envío de credenciales en texto plano, lo cual facilita la interceptación de datos.
[HIGH] HSTS (Strict-Transport-Security): La ausencia de esta cabecera impide que el navegador fuerce conexiones seguras, permitiendo ataques de degradación de HTTPS a HTTP.
[HIGH] X-Frame-Options: La falta de esta directiva hace que el sitio sea susceptible a ataques de Clickjacking, donde un atacante puede cargar la web en un marco invisible para engañar al usuario.
[MEDIUM] Contenido Mixto: Se localizaron 22 recursos cargados mediante protocolo HTTP inseguro dentro de una página HTTPS, lo que debilita el cifrado de la sesión y genera advertencias en el navegador.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de scripts maliciosos disfrazados de otros archivos.
[MEDIUM] Puerto 8080 (HTTP-Alt): La exposición de este puerto alternativo puede revelar paneles de administración o servicios secundarios no protegidos adecuadamente.
[MEDIUM] Ruta /wp-login.php: El panel de acceso a la administración está disponible públicamente, facilitando ataques de fuerza bruta contra las credenciales del sitio.
[MEDIUM] Referrer-Policy y Permissions-Policy: La ausencia de estas cabeceras permite la fuga de información sobre la procedencia del tráfico y no restringe el acceso del navegador a funciones sensibles.
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.66, facilitando a los atacantes el reconocimiento de vulnerabilidades específicas de esa versión.
[LOW] X-Powered-By expuesto: Se muestra el uso de PHP/8.4.19, lo que proporciona información adicional sobre el entorno de ejecución para ataques dirigidos.
[LOW] Meta generator: La etiqueta revela el uso y versión de LayerSlider, exponiendo la superficie de ataque de los complementos instalados.
[LOW] Ruta sensible en robots.txt: Se hace referencia explícita a rutas de administración, guiando a posibles atacantes hacia áreas restringidas.