EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://dev.aia.es	Checks	9 pruebas
Dominio	dev.aia.es	Hallazgos	27 totales
Fecha	20 de abril de 2026 a las 15:12	Problemas	10 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el dominio evaluado arroja una puntuación de 53/100, lo que resulta en una calificación de nota D. Durante la auditoría se ejecutaron un total de 9 checks pasivos, de los cuales 2 resultaron satisfactorios, 1 generó una advertencia y 2 presentaron fallos críticos de configuración. Se han detectado debilidades significativas en la protección de la capa de transporte y en la configuración de cabeceras defensivas. Debido a la exposición de servicios de transferencia de archivos inseguros y la ausencia de políticas de seguridad modernas, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	4	3	3	17
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 75 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 75 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  75 dias restantes (expira: 2026-07-04T05:03:20.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-05T05:03:21.000Z
- 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.)

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 503)
- BAJO **sitemap.xml**
  No encontrado (HTTP 503)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- 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
- 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] Puerto 21 (FTP) ABIERTO: Este puerto permite la transferencia de archivos sin cifrado, lo que facilita que un atacante intercepte credenciales y datos en tránsito.
[HIGH] Content-Security-Policy Falta: La ausencia de esta cabecera permite la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options Falta: El sitio es vulnerable a ataques de clickjacking al no restringir si la página puede ser cargada en marcos o frames externos.
[HIGH] Strict-Transport-Security Falta: No se fuerza el uso de conexiones seguras HTTPS, dejando a los usuarios expuestos a ataques de degradación de SSL.
[MEDIUM] X-Content-Type-Options Falta: El navegador podría intentar interpretar el contenido de forma distinta a la declarada, facilitando la ejecución de scripts inesperados.
[MEDIUM] Referrer-Policy Falta: No existe control sobre la información de navegación que se envía a terceros cuando se hace clic en un enlace externo.
[MEDIUM] Permissions-Policy Falta: No se restringe el acceso de las APIs del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: La cabecera revela el uso de nginx, lo cual proporciona información valiosa a un atacante sobre la tecnología del servidor.
[LOW] robots.txt y sitemap.xml ausentes: Los archivos devolvieron un error HTTP 503, lo que indica problemas de configuración en el servidor y dificulta la indexación correcta.