EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://afa.ad	Checks	9 pruebas
Dominio	afa.ad	Hallazgos	40 totales
Fecha	28 de abril de 2026 a las 08:00	Problemas	6 detectados

A

91/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al portal ha resultado en una puntuación de 91/100, obteniendo una calificación de grado A. Se ejecutaron un total de 9 comprobaciones pasivas, logrando 5 resultados satisfactorios, 1 advertencia y 1 fallo en los parámetros evaluados. Aunque la infraestructura base muestra robustez, se han identificado fugas de información en las cabeceras y errores en la configuración de archivos de indexación. En conclusión, el sitio se considera seguro bajo estándares actuales, pero presenta vulnerabilidades menores que deben ser mitigadas para prevenir técnicas de reconocimiento por parte de atacantes.

Resumen de Riesgos

0	0	1	5	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 251 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	0	ERROR	No se pudo verificar contenido mixto
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 251 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  251 dias restantes (expira: 2027-01-03T23:59:59.000Z)
- 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 — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- BAJO **Server header expuesto**
  Server: waitress — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Zope (www.zope.dev), Python (www.python.org) — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: frame-ancestors afa.ad www.afa.ad
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000;includeSubDomains;preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

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
- BAJO **Meta generator**
  Expone: Plone - http://plone.com
- INFO **Tecnologias detectadas**
  Zope (www.zope.dev), Python (www.python.org)

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- 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

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

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

[MEDIUM] Permissions-Policy: Falta esta cabecera, la cual es necesaria para restringir el acceso a APIs sensibles del navegador como la cámara, el micrófono o la ubicación.
[LOW] Server header expuesto: Se detectó la cabecera Server: waitress, lo que revela la tecnología específica del servidor y facilita ataques dirigidos.
[LOW] X-Powered-By expuesto: Se exponen las tecnologías Zope y Python, permitiendo a un atacante buscar exploits específicos para dichos frameworks.
[LOW] Meta generator: La etiqueta meta expone el uso de Plone, proporcionando información valiosa sobre la arquitectura interna del sitio.
[LOW] robots.txt: No se pudo acceder o no existe el archivo, lo que dificulta el control sobre qué partes del sitio deben ser rastreadas.
[LOW] sitemap.xml: El archivo de mapa del sitio no está disponible, afectando la visibilidad y estructura de la plataforma ante auditorías externas.