EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aemifesa.online	Checks	9 pruebas
Dominio	aemifesa.online	Hallazgos	48 totales
Fecha	22 de abril de 2026 a las 20:38	Problemas	16 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio ha resultado en una puntuación de 60/100, lo que otorga al sitio una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 3 resultaron exitosos, 3 generaron advertencias y 3 fallaron críticamente. Aunque el cifrado de transporte es correcto, la ausencia casi total de cabeceras de seguridad y la exposición de servicios obsoletos representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable ante ataques de interceptación y manipulación de sesiones.

Resumen de Riesgos

0	5	7	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	33	FALLO	MoodleSession: falta HttpOnly; MoodleSession: fa...
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
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 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-06-07T05:43:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-09T05:43:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PleskLin — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: sameorigin
- 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 303 redirige a https://aemifesa.online
- 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
- INFO **Tecnologias detectadas**
  Next.js, PleskLin

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 33/100

Estado: FALLO

MoodleSession: falta HttpOnly; MoodleSession: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: MoodleSession — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: MoodleSession — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: MoodleSession — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.aemifesa.org/es/el-gremi/qui-som
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.aemifesa.org/es/el-gremi/qualificacions

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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): El puerto está abierto, permitiendo la transferencia de archivos mediante un protocolo no cifrado propenso a la captura de credenciales.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles degradaciones de conexión.
[HIGH] Cookie MoodleSession (HttpOnly): La falta de este atributo permite que la cookie de sesión sea accesible mediante scripts, aumentando el riesgo de robo de identidad.
[MEDIUM] Cookie MoodleSession (SameSite): La carencia de esta directiva hace que la sesión sea vulnerable a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron 2 recursos cargados mediante HTTP en una página protegida por SSL, lo que debilita la integridad de la conexión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría llevar a la ejecución de archivos no confiables.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a sitios externos mediante el campo referer.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso del navegador a funciones sensibles como la cámara o el micrófono.
[MEDIUM] Archivo /README.txt: Este archivo es accesible públicamente y puede revelar detalles técnicos internos del sistema de gestión.
[LOW] Server header expuesto: El encabezado revela el uso de nginx, facilitando el reconocimiento de objetivos para atacantes.
[LOW] X-Powered-By expuesto: Se detectó el uso de PleskLin, exponiendo información sobre el framework o panel de control utilizado.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos dificulta la auditoría de rutas y la correcta indexación de seguridad por buscadores.