EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aol.com	Checks	9 pruebas
Dominio	aol.com	Hallazgos	51 totales
Fecha	21 de julio de 2026 a las 19:55	Problemas	5 detectados

A

92/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio aol.com ha resultado en una puntuación de 92/100, lo que otorga al sitio una calificación de Nota A. Durante la evaluación se ejecutaron un total de 9 checks pasivos, obteniendo 8 resultados satisfactorios y 1 advertencia relacionada con la configuración de cabeceras. La infraestructura presenta una robustez significativa en su cifrado y gestión de identidades digitales. Se concluye que el sitio es altamente seguro, aunque existen vectores de riesgo residuales en la capa de políticas de seguridad del navegador que deben ser atendidos.

Resumen de Riesgos

0	1	2	2	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 141 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 141 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  141 dias restantes (expira: 2026-12-09T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-26T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://aol.com:443/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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**
  React, Next.js, Astro

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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: plid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: plid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: plid — SameSite**
  SameSite=lax

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2207 bytes)
- INFO **Reglas robots.txt**
  60 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.aol.com/products/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)**
  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] Content-Security-Policy: Esta cabecera no se encuentra implementada, lo que es peligroso porque deja al sitio vulnerable ante ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[MEDIUM] Permissions-Policy: La ausencia de esta política impide restringir el acceso a APIs del navegador como la cámara o el micrófono, aumentando el riesgo de privacidad.
[MEDIUM] Configuración de Robots.txt: El archivo bloquea la indexación total mediante "Disallow: /" y expone la ruta "config", lo cual puede revelar directorios sensibles a atacantes.
[LOW] Exposición de cabecera Server: El servidor revela el uso de la tecnología "ATS", lo que facilita a un atacante potencial la búsqueda de exploits específicos para ese software.