EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aulavirtual.anla.gov.co	Checks	9 pruebas
Dominio	aulavirtual.anla.gov.co	Hallazgos	48 totales
Fecha	25 de junio de 2026 a las 17:13	Problemas	16 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web arroja una puntuación de 60/100, lo que se traduce en una calificación de grado C. El análisis consistió en la ejecución de 9 checks pasivos, de los cuales 4 resultaron satisfactorios, se emitió 1 advertencia y 3 finalizaron en fallo. A pesar de contar con un cifrado SSL válido, la carencia casi total de cabeceras de seguridad y la exposición de rutas administrativas elevan el perfil de riesgo. Se concluye que el sitio es vulnerable, principalmente ante ataques de interceptación de tráfico y suplantación de identidad debido a configuraciones deficientes en el servidor y las cookies.

Resumen de Riesgos

0	3	12	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 131 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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	50	AVISO	MoodleSession: falta SameSite; cookiesession1: f...
Contenido Mixto	20	FALLO	5 recursos HTTP en pagina HTTPS
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 131 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  131 dias restantes (expira: 2026-11-03T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-22T00:00:00.000Z
- 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/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- 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.)

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

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
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 50/100

Estado: AVISO

MoodleSession: falta SameSite; cookiesession1: falta Secure; cookiesession1: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: MoodleSession — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: MoodleSession — Secure**
  Flag Secure activo — Solo se envia por HTTPS

- MEDIO **Cookie: MoodleSession — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: cookiesession1 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: cookiesession1 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: cookiesession1 — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

5 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://localhost:8888/moodle/edoo-4.5/course
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://localhost:8888/moodle/edoo-4.5/course
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://localhost:8888/moodle/edoo-4.5/course
- MEDIO **href (link/stylesheet)**
  ...y 2 mas del mismo tipo

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[LOW] Server header expuesto: Se detectó el uso de nginx/1.24.0 (Ubuntu), lo cual facilita a atacantes la búsqueda de exploits específicos para esa versión.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones HTTPS, dejando a los usuarios vulnerables a ataques de degradación de SSL.
[MEDIUM] X-Content-Type-Options: La falta de esta política permite que el navegador realice "MIME-sniffing", pudiendo ejecutar archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No se controla la información de navegación enviada a otros dominios, lo que puede filtrar URLs internas sensibles.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono a través de políticas de seguridad.
[MEDIUM] Archivo /README.txt: Este archivo es accesible públicamente y puede revelar detalles técnicos sobre la estructura y versión del sistema de gestión de contenidos.
[MEDIUM] Ruta /administrator/: El panel de inicio de sesión administrativo está expuesto a Internet, aumentando el riesgo de ataques de fuerza bruta.
[MEDIUM] Ruta /user/login: El punto de acceso para usuarios está visible para cualquier atacante, facilitando intentos de acceso no autorizados.
[MEDIUM] Cookie MoodleSession: La falta del atributo SameSite hace que el identificador de sesión sea susceptible a ataques de Cross-Site Request Forgery (CSRF).
[HIGH] Cookie cookiesession1: No implementa el flag Secure, permitiendo que la cookie de sesión se transmita de forma insegura a través de conexiones HTTP.
[MEDIUM] Contenido Mixto: Se detectaron recursos HTTP que intentan cargar dentro de la página HTTPS, incluyendo enlaces que apuntan erróneamente a localhost.
[FAIL] Robots.txt y Sitemap: La ausencia de estos archivos sugiere una falta de configuración básica de seguridad y control de indexación.