EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aula.coopdgii.com	Checks	9 pruebas
Dominio	aula.coopdgii.com	Hallazgos	49 totales
Fecha	25 de septiembre de 2026 a las 17:45	Problemas	11 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio aula.coopdgii.com arroja una puntuación de 71/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos en la configuración. Aunque la transferencia de datos está cifrada correctamente, se detectaron deficiencias graves en la protección del servidor y en las cabeceras de seguridad web. La exposición de servicios internos y la ausencia de políticas de seguridad en el navegador incrementan significativamente el riesgo de ataques. En su estado actual, el sitio se considera vulnerable debido a la visibilidad pública de su base de datos y la falta de protecciones modernas contra inyecciones de código.

Resumen de Riesgos

1	3	4	3	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 40 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	100	OK	2 cookies, todas con flags correctos
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	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 40 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  40 dias restantes (expira: 2026-11-04T15:01:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-06T15:01:17.000Z
- 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: Apache/2.4.52 (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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://aula.coopdgii.com/
- 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

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

2 cookies, todas con flags correctos

- 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
- INFO **Cookie: MoodleSession — SameSite**
  SameSite=lax
- INFO **Cookie: MoodleSession — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: MoodleSession — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: MoodleSession — 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 — 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

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 3306 (MySQL)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos es accesible desde cualquier punto de internet, lo que expone la información a ataques de fuerza bruta y exfiltración de datos.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] Falta de Strict-Transport-Security: No se obliga al uso de conexiones seguras mediante HSTS, facilitando ataques de interceptación de tráfico.
[MEDIUM] Puerto 22 (SSH) abierto: El puerto de administración remota está expuesto, aumentando la superficie de ataque para intentos de acceso no autorizado al sistema operativo.
[MEDIUM] Falta de X-Content-Type-Options: El sitio es vulnerable al "MIME-sniffing", permitiendo que el navegador interprete archivos de forma incorrecta y ejecute código malicioso.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de navegación que se envía a otros dominios, lo que podría filtrar datos sensibles de los usuarios.
[MEDIUM] Falta de Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador como la cámara o el micrófono, dejando esta seguridad a merced del cliente.
[LOW] Cabecera de servidor expuesta: Se revela el uso de Apache/2.4.52 en Ubuntu, proporcionando detalles técnicos precisos que un atacante puede usar para buscar exploits específicos.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 404 para estos archivos, dificultando la gestión de indexación y el control de acceso para rastreadores.