EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://academiaonline.clinicachinita.com/plataforma/	Checks	9 pruebas
Dominio	academiaonline.clinicachinita.com	Hallazgos	47 totales
Fecha	13 de abril de 2026 a las 22:13	Problemas	16 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras el análisis de seguridad realizado, el sitio web ha obtenido una puntuación de 56/100, lo que resulta en una calificación de grado D. Los resultados de los 9 checks pasivos ejecutados muestran un balance preocupante con 4 pruebas superadas, 2 advertencias y 3 fallos críticos en áreas fundamentales. Se han detectado deficiencias graves en la configuración de cabeceras de seguridad y una exposición de servicios de infraestructura que no deberían ser públicos. Por tanto, se concluye que el sitio es actualmente vulnerable y requiere una intervención técnica inmediata para mitigar riesgos de intrusión.

Resumen de Riesgos

1	7	5	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-06-22T22:40:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-24T22:40:21.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- 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://academiaonline.clinicachinita.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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, PHP/7.4.33

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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 500)
- INFO **sitemap.xml**
  Presente, 1 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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 internet, lo que permite ataques de fuerza bruta o explotación de vulnerabilidades del motor de datos.
[HIGH] Cabecera Content-Security-Policy faltante: La ausencia de CSP facilita la ejecución de ataques Cross-Site Scripting (XSS) e inyecciones de contenido.
[HIGH] Cabecera X-Frame-Options faltante: El sitio no previene el clickjacking, permitiendo que atacantes carguen la web en marcos externos para engañar usuarios.
[HIGH] HSTS (Strict-Transport-Security) no configurado: No se fuerza al navegador a usar siempre HTTPS, dejando la conexión vulnerable a ataques de degradación de cifrado.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: La sesión es accesible mediante scripts del lado del cliente, aumentando el riesgo de robo de identidad en caso de XSS.
[HIGH] Cookie PHPSESSID sin flag Secure: El identificador de sesión puede ser transmitido a través de canales no cifrados si el usuario accede por error vía HTTP.
[HIGH] Puerto 21 (FTP) abierto: Se permite la transferencia de archivos mediante un protocolo inseguro que envía credenciales en texto plano.
[MEDIUM] Cabecera X-Content-Type-Options faltante: Facilita ataques de MIME-type sniffing, permitiendo que el navegador interprete archivos de forma incorrecta y peligrosa.
[MEDIUM] Cabecera Referrer-Policy faltante: No se controla qué información de origen se envía a otros dominios, lo que podría filtrar rutas internas sensibles.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: El sitio carece de protección nativa en cookies contra ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Puerto 22 (SSH) abierto: La interfaz de gestión remota está expuesta al público, lo que supone un vector de ataque para accesos no autorizados.
[LOW] Exposición de cabecera Server: El servidor revela el uso de Apache, proporcionando información útil para que un atacante busque exploits específicos.
[LOW] Exposición de cabecera X-Powered-By: Se revela el uso de PHP/7.4.33, informando sobre la tecnología y versión exacta utilizada en el backend.
[LOW] Archivo robots.txt no encontrado: El servidor responde con un error 500 al buscar este archivo, lo que impide gestionar el rastreo de buscadores adecuadamente.