EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://micolegio.com	Checks	9 pruebas
Dominio	micolegio.com	Hallazgos	49 totales
Fecha	5 de septiembre de 2026 a las 20:15	Problemas	22 detectados

D

45/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado ha otorgado una puntuacion de 45/100, lo que corresponde a una nota de D. Se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos y 5 presentaron fallos criticos en la configuracion del servidor y la plataforma. Los hallazgos revelan deficiencias graves en la gestion de puertos, cabeceras de seguridad y manejo de trafico cifrado. Debido a la exposicion de servicios internos y la ausencia de politicas de proteccion basicas, se concluye que el sitio es vulnerable y requiere medidas correctivas urgentes.

Resumen de Riesgos

1	6	12	3	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 83 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	35 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 83 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  83 dias restantes (expira: 2026-11-27T09:03:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-29T09:03:43.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

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

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 20/100

Estado: FALLO

35 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.micolegio.com/img/estachevee60x60.png
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://micolegio.com/template/yam///fast.wistia.net/assets/e...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://micolegio.com/template/yam/./img/twitter.png
- MEDIO **src (script/img/iframe)**
  ...y 11 mas del mismo tipo
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://micolegio.com/template/yam/./css/style.css
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://micolegio.com/template/yam/./css/jquery.fancybox.css
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://micolegio.com/js/introjs/introjs.css
- MEDIO **href (link/stylesheet)**
  ...y 18 mas del mismo tipo

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 — 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): La base de datos se encuentra abierta y expuesta a internet, permitiendo intentos de acceso externo no autorizados.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos esta abierto y opera sin cifrado, facilitando el robo de credenciales de administracion.
[HIGH] Redireccion HTTPS: No existe una redireccion automatica de trafico HTTP a HTTPS, dejando las comunicaciones de los usuarios desprotegidas.
[HIGH] Content-Security-Policy (CSP): La ausencia de esta cabecera facilita la ejecucion de ataques XSS y la inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta configuracion permite ataques de clickjacking al no restringir como se embebe el sitio en marcos externos.
[HIGH] Strict-Transport-Security (HSTS): El servidor no indica a los navegadores que deben usar exclusivamente conexiones seguras de forma permanente.
[MEDIUM] Contenido Mixto: Se detectaron 35 recursos cargados mediante enlaces HTTP inseguros dentro de la pagina protegida, lo que degrada la seguridad SSL.
[MEDIUM] Puerto 22 (SSH): El acceso remoto esta expuesto publicamente, aumentando el riesgo de ataques de fuerza bruta contra el servidor.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite ataques de MIME-type sniffing al no forzar el tipo de contenido definido.
[MEDIUM] Referrer-Policy y Permissions-Policy: No se controla la informacion de navegacion compartida ni se restringen las APIs del navegador como camara o microfono.
[LOW] Server header expuesto: La cabecera revela el uso de Apache, proporcionando informacion tecnica valiosa para la planificacion de exploits dirigidos.
[LOW] Robots.txt y Sitemap: La carencia de estos archivos impide una gestion adecuada del rastreo por parte de motores de busqueda y auditorias de acceso.