EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://web2.colegiosantamartacoquimbo.cl	Checks	9 pruebas
Dominio	web2.colegiosantamartacoquimbo.cl	Hallazgos	48 totales
Fecha	28 de abril de 2026 a las 21:16	Problemas	11 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio web2.colegiosantamartacoquimbo.cl arroja una puntuacion de 70/100 con una nota final de C. El analisis se baso en 9 checks pasivos, de los cuales 4 resultaron exitosos, 3 generaron advertencias y 1 fue calificado como fallo critico. Aunque la implementacion del cifrado SSL es correcta, se detectaron deficiencias significativas en la configuracion de cabeceras de seguridad y exposicion de servicios innecesarios. Se concluye que el sitio es vulnerable ante ataques de interceptacion de datos y manipulacion de contenido debido a estas omisiones tecnicas.

Resumen de Riesgos

0	3	5	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 54 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	67	AVISO	ep_session_id: falta SameSite
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 54 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  54 dias restantes (expira: 2026-06-21T13:09:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T13:09:41.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubdomains;
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://web2.colegiosantamartacoquimbo.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubdomains;
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Seguridad de Cookies — 67/100

Estado: AVISO

ep_session_id: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: ep_session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript

- INFO **Cookie: ep_session_id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ep_session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (134 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://web2.colegiosantamartacoquimbo.cl/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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

[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos se encuentra abierto y opera sin cifrado, permitiendo la captura de credenciales en transito.

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecucion de ataques de inyeccion de codigo malicioso y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: No se detecto esta directiva, lo que hace al sitio susceptible a ataques de clickjacking para engañar a los usuarios.
[MEDIUM] Cookie ep_session_id: Falta el atributo SameSite, lo que expone la sesion del usuario a ataques de falsificacion de peticion en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se identifico un recurso stylesheet cargado mediante protocolo HTTP inseguro dentro de la pagina HTTPS.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice sniffing de tipos MIME, pudiendo ejecutar archivos no ejecutables.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de procedencia enviada a sitios de terceros durante la navegacion.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como camara, microfono o geolocalizacion.
[LOW] Meta generator: El codigo fuente expone explicitamente el uso de WordPress 6.9.4, facilitando la busqueda de exploits para esa version.
[LOW] Server header expuesto: La cabecera revela el uso de servidor Apache, brindando informacion valiosa a posibles atacantes sobre la infraestructura.
[LOW] Ruta sensible en robots.txt: Se menciona una ruta relativa a administracion, lo que orienta a atacantes sobre la ubicacion de paneles de gestion.