EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.coursera.org/programs/62-10-colegio-nacional-ciudad-nueva-6572-ciencias-sociales-tarde-a-ciudad-del-este-xr153	Checks	9 ejecutados
Dominio	www.coursera.org	Hallazgos	56 totales
Fecha	19 de mayo de 2026 a las 21:41	Problemas	13 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 79/100, lo que equivale a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron exitosos, 1 presenta advertencias y 2 han fallado debido a configuraciones críticas ausentes. El sitio muestra una base sólida en cuanto al cifrado de conexión, pero presenta debilidades importantes en la gestión de cabeceras de seguridad y la configuración de cookies. Se concluye que el sitio es moderadamente seguro, aunque vulnerable a ataques de inyección y secuestro de sesión si no se corrigen las deficiencias detectadas.

Resumen de Riesgos

0	4	7	2	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 140 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	CSRF3-Token: falta HttpOnly; __204u: falta HttpO...
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 140 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  140 dias restantes (expira: 2026-10-06T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://www.coursera.org/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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**
  React, Next.js, Astro, Express

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

Seguridad de Cookies — 33/100

Estado: FALLO

CSRF3-Token: falta HttpOnly; __204u: falta HttpOnly; __204u: falta Secure; __204u: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: CSRF3-Token — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: CSRF3-Token — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: CSRF3-Token — SameSite**
  SameSite=none
- ALTO **Cookie: __204u — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: __204u — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __204u — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://play.google.com/store/apps/details?id=org.coursera.an...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://play.google.com/store/apps/details?id=org.coursera.an...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1253 bytes)
- INFO **Reglas robots.txt**
  30 Disallow, 5 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.coursera.org/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] Cookie CSRF3-Token: Falta el flag HttpOnly, permitiendo que la cookie sea accesible mediante scripts de cliente, aumentando el riesgo de robo de sesión.
[HIGH] Cookie __204u (HttpOnly): La carencia del atributo HttpOnly expone el identificador al acceso por JavaScript.
[HIGH] Cookie __204u (Secure): La cookie no tiene el flag Secure, lo que permite que sea enviada a través de conexiones HTTP no cifradas.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que podría filtrar información sensible sobre la procedencia del tráfico a dominios externos.
[MEDIUM] Permissions-Policy: La falta de esta cabecera permite que el navegador acceda a APIs potencialmente invasivas sin restricciones específicas del servidor.
[MEDIUM] Ruta /user/login: El panel de acceso administrativo es accesible de forma pública, facilitando intentos de fuerza bruta.
[MEDIUM] Cookie __204u (SameSite): Al no tener definido el atributo SameSite, el sitio es vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron recursos cargando por el protocolo inseguro HTTP dentro de la página protegida por HTTPS.
[MEDIUM] Bloqueo total robots.txt: El archivo bloquea la indexación de todo el sitio, lo cual puede ser un error de configuración o una medida de seguridad excesiva.
[LOW] Server header expuesto: El valor envoy revela la tecnología de balanceo o servidor utilizada.
[LOW] X-Powered-By expuesto: El valor Express revela el framework de desarrollo utilizado, facilitando el reconocimiento para un atacante.