EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.ehdonorione.edu.ar/	Checks	9 pruebas
Dominio	www.ehdonorione.edu.ar	Hallazgos	57 totales
Fecha	26 de agosto de 2026 a las 06:35	Problemas	13 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio ehdonorione.edu.ar arroja una puntuación de 75/100, lo que corresponde a una calificación de grado B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 falló debido a la ausencia de cabeceras de seguridad críticas. El portal presenta una base sólida en cuanto a cifrado SSL y redirección HTTPS, pero muestra debilidades significativas en la configuración de cookies y protección contra ataques de inyección. En conclusión, el sitio es moderadamente seguro, aunque se considera vulnerable a ataques de clickjacking y robo de sesiones si no se aplican las correcciones recomendadas.

Resumen de Riesgos

0	5	6	2	44
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Wix
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	56	AVISO	XSRF-TOKEN: falta HttpOnly; ssr-caching: falta H...
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): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-11-16T01:57:07.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-18T01:57:08.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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=31556952
- 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.ehdonorione.edu.ar/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556952
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556952 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Wix

- 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**
  Detectado via HTML body
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Wix.com Website Builder
- INFO **Tecnologias detectadas**
  React, 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 — 56/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; ssr-caching: falta HttpOnly; ssr-caching: falta Secure; ssr-caching: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=none
- ALTO **Cookie: ssr-caching — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ssr-caching — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ssr-caching — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.hermanasdedonorione.org.ar/comocolaborar.php

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (496 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.ehdonorione.edu.ar/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[ALTA] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[ALTA] X-Frame-Options: La ausencia de esta política permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[ALTA] Cookies sin flag HttpOnly: Las cookies XSRF-TOKEN y ssr-caching son accesibles mediante scripts del navegador, aumentando el riesgo de robo de identidad.
[ALTA] Cookie ssr-caching sin flag Secure: Esta cookie se transmite a través de conexiones no cifradas, lo que permite su intercepción por terceros.
[MEDIA] Falta de Referrer-Policy y Permissions-Policy: No se controla la información de navegación enviada a otros sitios ni se restringen APIs sensibles del navegador.
[MEDIA] Cookie ssr-caching sin flag SameSite: La falta de este atributo hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIA] Contenido Mixto: Se detectó un recurso stylesheet cargado vía HTTP (hermanasdedonorione.org.ar/comocolaborar.php), lo que compromete la integridad de la página HTTPS.
[MEDIA] Puerto 8080 abierto: El puerto de servidor web alternativo está expuesto, representando un vector potencial para servicios no autorizados.
[MEDIA] Configuración de robots.txt: El archivo bloquea la indexación de todo el contenido mediante la directiva Disallow: /, afectando la visibilidad legítima del sitio.
[BAJA] Server header expuesto: La cabecera revela el uso de tecnología Cloudflare, proporcionando información técnica útil para atacantes.
[BAJA] Meta generator expuesto: El código fuente del sitio confirma el uso de Wix.com Website Builder como herramienta de creación.