EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://horacioquiroga.horacioquiroga.edu.uy.uy	Checks	9 pruebas
Dominio	horacioquiroga.horacioquiroga.edu.uy.uy	Hallazgos	15 totales
Fecha	13 de agosto de 2026 a las 17:12	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web arrojo una puntuacion exacta de 73/100, lo que le otorga una nota C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo como resultado 1 check correcto y 1 fallo critico detectado. Debido a la imposibilidad de establecer una conexion cifrada y la ausencia de configuraciones basicas de seguridad, el sitio web se clasifica actualmente como vulnerable. Es imperativo solucionar los problemas de conectividad SSL para proteger la integridad de los usuarios.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  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

[CRITICO] Conexion SSL/TLS: No se pudo establecer una conexion segura con el servidor, lo que impide el cifrado de la informacion y expone los datos a interceptaciones.
[BAJO] Archivos robots.txt y sitemap.xml: El sitio carece de estos archivos o presenta errores de acceso, lo que dificulta la gestion del rastreo por parte de buscadores.
[CRITICO] Cabeceras de Seguridad: No se detectaron cabeceras HTTP esenciales, dejando el sitio expuesto a ataques de intermediario y ejecucion de scripts no autorizados.
[CRITICO] Redireccion HTTPS: El servidor no fuerza el uso de conexiones seguras, permitiendo que el trafico viaje de forma insegura a traves de HTTP.