

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.uac.edu.co/	Checks	9 pruebas
Dominio	www.uac.edu.co	Hallazgos	18 totales
Fecha	16 de abril de 2026 a las 18:54	Problemas	3 detectados

F

37/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio arroja una puntuación crítica de 37/100, lo que conlleva una calificación de nota F. Se ejecutaron un total de 9 comprobaciones pasivas, resultando en solo 1 verificación exitosa, 2 fallos críticos confirmados y varios errores técnicos que impidieron el análisis de otros vectores de ataque. La ausencia de un certificado de seguridad válido y la falta de configuraciones básicas de servidor exponen la infraestructura a riesgos de interceptación de datos. Basándose en estos resultados, el sitio web se clasifica actualmente como vulnerable y no apto para el manejo de información sensible.

Resumen de Riesgos

1 CRITICO	0 ALTO	0 MEDIO	2 BAJO	15 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO Certificado valido
El certificado SSL NO es valido
- INFO Dias hasta expiracion
157 dias restantes (expira: 2026-09-20T14:47:23.000Z)
- INFO Fecha de emision
Emitido desde: 2025-08-19T14:47:23.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO robots.txt
Error al acceder

Puertos Abiertos — 100/100

Estado: OK

1 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 — Envío de correo
	INFO	Puerto 80 (HTTP) Cerrado — 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 autentificacion 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] Certificado SSL no valido: El certificado SSL del sitio no es legitimo o ha expirado, lo que impide establecer una conexion cifrada y segura con los usuarios.

[BAJO] Falta de robots.txt: No se pudo encontrar el archivo de instrucciones para buscadores, lo que dificulta el control de acceso a directorios del sitio.

[BAJO] Falta de sitemap.xml: El archivo de mapa del sitio no esta accesible, afectando la indexacion y la visibilidad de la estructura web.

[ERROR] Cabeceras de seguridad ausentes: No se detectaron cabeceras HTTP de proteccion, lo que facilita ataques de Cross-Site Scripting y Clickjacking.

[ERROR] Redireccion HTTPS no verificada: No se puede confirmar si el trafico inseguro se redirige a una version protegida, permitiendo potenciales ataques de hombre en el medio.

[ERROR] Cookies sin proteccion: Al no poder verificar el estado de las cookies, existe el riesgo de que los datos de sesion viajen sin los atributos Secure o HttpOnly.