EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://vasco.edu.mx	Checks	9 pruebas
Dominio	vasco.edu.mx	Hallazgos	49 totales
Fecha	1 de mayo de 2026 a las 06:05	Problemas	18 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web arroja una puntuacion de 62/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, resultando en 4 verificaciones correctas, 3 advertencias y 2 fallos criticos detectados. A pesar de contar con un certificado SSL valido, se identificaron deficiencias significativas en la configuracion de cabeceras de seguridad y una exposicion de servicios de infraestructura. Debido a la presencia de contenido mixto y bases de datos accesibles desde el exterior, el sitio se considera actualmente vulnerable ante ataques dirigidos. Es imperativo abordar las debilidades estructurales para proteger la integridad de los datos de la institucion y sus usuarios.

Resumen de Riesgos

1	4	9	4	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-06-15T20:05:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-17T20:05:36.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PleskLin — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://vasco.edu.mx/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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
- BAJO **Meta generator**
  Expone: Incomedia WebSite X5 Pro 2022.2.9 - www.websitex5.com
- INFO **Tecnologias detectadas**
  Astro, PleskLin

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 /wp-login.php**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://vquiroga.sytes.net/moodle/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://vasco.edu.mx/inscripcion.php
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://vasco.edu.mx/contactanos.html
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, 6 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 3306 (MySQL)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): Base de datos MySQL abierta y expuesta a internet, lo que permite ataques de fuerza bruta o extraccion de informacion sensible.
[HIGH] Content-Security-Policy (CSP): Falta esta cabecera esencial para prevenir ataques de inyeccion de codigo y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Cabecera ausente que deja el sitio vulnerable a ataques de clickjacking, permitiendo que el sitio sea embebido de forma maliciosa.
[HIGH] Strict-Transport-Security (HSTS): No esta configurada, lo que impide que el navegador fuerce conexiones seguras permanentemente y facilita ataques de degradacion de SSL.
[MEDIUM] Contenido Mixto: Se detectaron 4 recursos cargados mediante HTTP en una pagina bajo HTTPS, comprometiendo el cifrado total de la sesion.
[MEDIUM] Puerto 22 (SSH): El puerto de administracion remota esta abierto y visible, aumentando la superficie de ataque directa sobre el servidor.
[MEDIUM] Ruta de login expuesta: El panel de acceso /wp-login.php es publico, lo que facilita intentos de acceso no autorizados mediante ataques de diccionario.
[MEDIUM] X-Content-Type-Options: Falta la cabecera que evita que el navegador interprete archivos con tipos MIME incorrectos, previniendo la ejecucion de scripts ocultos.
[MEDIUM] Referrer-Policy: No se ha configurado la politica para controlar que informacion de navegacion se envia a otros sitios cuando el usuario hace clic en un enlace.
[MEDIUM] Permissions-Policy: Ausencia de restricciones para el uso de APIs sensibles del navegador como la camara, microfono o geolocalizacion.
[LOW] Exposicion de tecnologia (Server/X-Powered-By): Se revela el uso de nginx y PleskLin en las cabeceras, informacion que ayuda a un atacante a buscar exploits especificos.
[LOW] Meta generator expuesto: El codigo fuente revela el uso de la herramienta Incomedia WebSite X5 Pro 2022.2.9 para la creacion del sitio.
[LOW] Falta de robots.txt: No se encontro el archivo de instrucciones para rastreadores, lo que dificulta el control de la indexacion en motores de busqueda.