EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://snap.vyzo.cloud/	Checks	9 pruebas
Dominio	snap.vyzo.cloud	Hallazgos	43 totales
Fecha	2 de abril de 2026 a las 12:32	Problemas	9 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 72/100, lo que equivale a una nota de grado C. Durante la evaluación, se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas, 2 advertencias y 1 fallo crítico relacionado con la configuración de seguridad. Cabe destacar que no se ejecutó un pentest activo, por lo que los hallazgos se limitan a la configuración superficial y de red. Aunque el sitio cuenta con un cifrado SSL adecuado, la ausencia total de cabeceras de protección lo deja expuesto a ataques convencionales de inyección y suplantación. Se concluye que el sitio es vulnerable y requiere ajustes inmediatos para alcanzar un nivel de seguridad empresarial.

Resumen de Riesgos

0	4	4	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 62 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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 62 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  62 dias restantes (expira: 2026-06-03T01:43:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-05T01:43:04.000Z
- 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/1.29.7 — 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
- 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 302 redirige a https://snap.vyzo.cloud/
- 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

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 — 100/100

Estado: OK

No se encontraron cookies

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

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (147 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 2 Allow
- INFO **Sitemap en robots.txt**
  https://snap.vyzo.cloud/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- 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
- 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: Falta. No se ha definido una política de seguridad de contenido, lo que permite la ejecución de scripts maliciosos y ataques XSS.
[HIGH] X-Frame-Options: Falta. El sitio es susceptible a ataques de clickjacking al permitir que el contenido sea embebido en marcos de sitios externos.
[HIGH] Strict-Transport-Security: Falta. No se obliga al navegador a usar HTTPS mediante HSTS, permitiendo posibles ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Falta. El navegador podría intentar adivinar el tipo de contenido, facilitando la ejecución de archivos maliciosos mediante MIME-sniffing.

[MEDIUM] Referrer-Policy: Falta. No se controla la información de referencia enviada a otros sitios, lo que podría comprometer la privacidad de la navegación.
[MEDIUM] Permissions-Policy: Falta. No hay restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 22 (SSH) abierto: Se detectó que el puerto de administración remota es accesible públicamente, aumentando el riesgo de ataques de fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.29.7, proporcionando información técnica valiosa para un atacante potencial.