EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://dev.yoump3.app/es9	Checks	9 pruebas
Dominio	dev.yoump3.app	Hallazgos	44 totales
Fecha	9 de mayo de 2026 a las 10:37	Problemas	10 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web ha arrojado una puntuacion de 68/100, lo que equivale a una nota de C. Durante la auditoria se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, 3 generaron advertencias y 1 fue calificado como fallo critico. Aunque el cifrado SSL es solido, la ausencia total de cabeceras de seguridad y la exposicion de puertos alternativos comprometen la integridad de la plataforma. Se concluye que el sitio es vulnerable y requiere intervenciones inmediatas para alcanzar un nivel de proteccion profesional.

Resumen de Riesgos

0	4	5	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 74 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	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 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-07-21T22:57:25.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-22T21:59:41.000Z
- 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: 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
- 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://dev.yoump3.app
- 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
- INFO **Tecnologias detectadas**
  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 — 100/100

Estado: OK

No se encontraron cookies

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

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://windows.microsoft.com/es-es/windows7/how-to-manage-co...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (64 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://yoump3.app/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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de Clickjacking donde un atacante puede cargar la web en un marco invisible.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce siempre conexiones seguras, permitiendo posibles degradaciones de protocolo.
[HIGH] HSTS (Strict-Transport-Security): No configurado en la redireccion, lo que debilita la seguridad de la conexion HTTPS.
[MEDIUM] X-Content-Type-Options: Al faltar, el navegador podria intentar interpretar el contenido de forma distinta al tipo MIME declarado, facilitando la ejecucion de scripts.

[MEDIUM] Referrer-Policy: No se controla la informacion de navegacion enviada a terceros al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones como camara o microfono ante posibles vulnerabilidades.
[MEDIUM] Contenido Mixto: Se detecto un recurso (stylesheet de Microsoft) cargando mediante protocolo HTTP inseguro dentro de la pagina HTTPS.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto, lo que representa un vector de ataque si no se utiliza para un servicio especifico y protegido.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando informacion tecnica que podria ser aprovechada por un atacante.