EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tappers.pe/	Checks	9 pruebas
Dominio	tappers.pe	Hallazgos	47 totales
Fecha	31 de marzo de 2026 a las 23:07	Problemas	5 detectados

A

95/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web arroja una puntuacion exacta de 95/100 con una nota final de A. Se ejecutaron un total de 9 checks pasivos, de los cuales 8 resultaron exitosos y solo uno presento advertencias menores. No se detectaron fallos de seguridad criticos ni brechas abiertas durante el proceso de evaluacion. Basandonos en estos resultados, se concluye que el sitio es seguro y mantiene estandares de proteccion elevados. Sin embargo, existen oportunidades de endurecimiento en las cabeceras de comunicacion para mitigar riesgos residuales.

Resumen de Riesgos

0	0	3	2	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-06-25T15:14:00.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-27T15:14:01.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'none'
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://tappers.pe/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 dias
- 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: Weblium, effortless website builder
- INFO **Tecnologias detectadas**
  React, 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 — 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 (100 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://tappers.pe/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 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 — 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

[MEDIUM] Referrer-Policy: La ausencia de esta cabecera impide controlar que informacion de procedencia se envia a terceros al hacer clic en enlaces.
[MEDIUM] Permissions-Policy: El sitio no define restricciones sobre que funciones del navegador (como camara o geolocalizacion) pueden activarse, lo que podria ser abusado.
[MEDIUM] HSTS max-age: La politica de transporte seguro tiene una duracion de solo 30 dias, cuando el estandar de la industria recomienda un minimo de 180 dias.
[LOW] Server header expuesto: El servidor responde con la cabecera openresty, revelando la tecnologia subyacente y facilitando el reconocimiento a atacantes.
[LOW] Meta generator: Se detecto informacion que identifica a Weblium como el constructor del sitio, lo cual ayuda a potenciales atacantes a buscar vulnerabilidades especificas de esa plataforma.