EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://xyz.xkeern.space	Checks	9 pruebas
Dominio	xyz.xkeern.space	Hallazgos	45 totales
Fecha	24 de junio de 2026 a las 08:46	Problemas	6 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio xyz.xkeern.space ha dado como resultado una puntuación de 88/100, obteniendo una calificación final de grado B. El análisis consistió en 9 checks pasivos, de los cuales 7 se completaron con éxito y 2 presentaron fallos que requieren atención inmediata. Se detectó una excelente implementación en la capa de transporte y cabeceras de seguridad, pero existen deficiencias críticas en la configuración de puertos del servidor. Aunque la navegación para el usuario es segura, la infraestructura subyacente se considera vulnerable debido a la exposición de servicios internos. Es imperativo corregir la visibilidad de los puertos de administración para mitigar riesgos de acceso no autorizado.

Resumen de Riesgos

1	0	2	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 87 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 87 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  87 dias restantes (expira: 2026-09-19T17:43:44.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-21T17:43:45.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
  Server: nginx/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self';style-src 'self' https://fonts.googleapis.com;font-src 'self'...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=(), payment=(), usb=(), fullscreen=(self)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://xyz.xkeern.space/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (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
- 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 — 100/100

Estado: OK

No se detecto contenido mixto

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

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

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

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- 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
- 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

[LOW] Server header expuesto: El servidor revela la versión exacta nginx/1.24.0 (Ubuntu), lo cual facilita a potenciales atacantes la búsqueda de vulnerabilidades específicas para dicho software.

[LOW] Falta de archivo robots.txt: La ausencia de este archivo impide dar instrucciones a los rastreadores sobre qué directorios deben ser ignorados, pudiendo exponer rutas sensibles.
[LOW] Falta de archivo sitemap.xml: No se encontró un mapa del sitio, lo que dificulta la correcta indexación y auditoría de la estructura de páginas del dominio.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de acceso remoto está expuesto a Internet, lo que permite intentos de ataques de fuerza bruta contra las credenciales del administrador.
[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos está accesible desde la red pública, lo que representa un riesgo crítico de filtración de datos, ataques de inyección o denegación de servicio.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo aumenta la superficie de ataque, ya que estos servicios suelen tener configuraciones de seguridad menos estrictas.