

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.zukkly.com/login
Dominio www.zukkly.com
Fecha 2 de mayo de 2026 a las 07:21

Checks 9 pruebas
Hallazgos 46 totales
Problemas 4 detectados

A

96/100

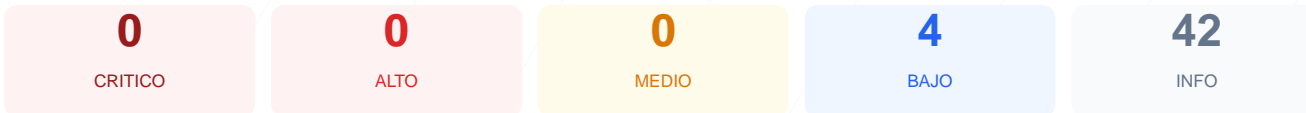
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 96/100 con una calificación de nota A. Se han ejecutado 9 comprobaciones pasivas, de las cuales 8 resultaron satisfactorias y solo una presentó fallos relacionados con la configuración de metadatos. El sitio demuestra un manejo de cifrado y cabeceras de protección de alto nivel, lo que garantiza la integridad de los datos transmitidos. A pesar de las omisiones en los archivos de indexación, la arquitectura base se muestra robusta frente a intentos de intrusión comunes. En conclusión, el sitio web se considera seguro y confiable para su uso operativo actual.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 66 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
66 dias restantes (expira: 2026-07-07T15:00:08.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-08T15:00:09.000Z
- 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: Vercel — Revela tecnologia del servidor

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: Next.js — Revela framework/lenguaje
- **INFO** **Content-Security-Policy**
Presente: default-src 'self'; script-src 'self' 'nonce-j4prgsgmoAwFnAAX+2055Q==' 'strict-d...
- **INFO** **X-Frame-Options**
Presente: SAMEORIGIN
- **INFO** **Strict-Transport-Security**
Presente: max-age=63072000; includeSubDomains; preload
- **INFO** **X-Content-Type-Options**
Presente: nosniff
- **INFO** **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- **INFO** **Permissions-Policy**
Presente: camera=(), microphone=(), geolocation=(), payment=(), usb=(), bluetooth=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 308 redirige a https://www.zukkly.com/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=63072000; includeSubDomains; preload
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=63072000 (730 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**
React, Next.js, 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 — 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 autentificacion 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

[LOW] Información del servidor expuesta: La cabecera Server revela el uso de Vercel, permitiendo a potenciales atacantes conocer la infraestructura para buscar vulnerabilidades específicas del proveedor.

[LOW] Framework tecnológico expuesto: La cabecera X-Powered-By indica el uso de Next.js, lo que facilita el reconocimiento de la pila tecnológica y posibles vectores de ataque dirigidos al framework.

[LOW] Ausencia de archivo de directivas de rastreo: No se encontró el archivo robots.txt (Error 404), lo cual impide gestionar correctamente qué áreas del sitio deben o no ser indexadas por motores de búsqueda.

[LOW] Ausencia de mapa del sitio: No se detectó el archivo sitemap.xml (Error 404), dificultando la auditoría de rutas del sitio y la correcta navegación de los indexadores automáticos.