

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kalysoboard.com/	Checks	9 pruebas
Dominio	kalysoboard.com	Hallazgos	45 totales
Fecha	5 de octubre de 2026 a las 15:19	Problemas	8 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha otorgado una puntuación de 81/100 con una nota de B, reflejando un estado de seguridad aceptable pero con deficiencias técnicas que deben subsanarse. Durante la auditoría se ejecutaron 9 controles pasivos, obteniendo 7 resultados satisfactorios, 1 advertencia y 1 fallo crítico en la configuración de cabeceras. Aunque la base de cifrado es sólida, la ausencia de políticas de seguridad en el servidor expone a los usuarios a riesgos de interceptación y manipulación de contenido. En conclusión, el sitio se considera moderadamente seguro, aunque presenta vulnerabilidades de configuración que podrían ser explotadas en ataques dirigidos.

Resumen de Riesgos

0	4	3	1	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 174 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 174 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
174 dias restantes (expira: 2027-03-28T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-29T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, Permissions-Policy

- BAJO Server header expuesto
Server: IONOS Webserver — 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)
- INFO

X-Content-Type-Options
Presente: nosniiff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- 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://kalysoboard.com/
- 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)
- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente
- 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 (101 bytes)
- INFO

Reglas robots.txt
2 Disallow, 1 Allow
- INFO

Sitemap en robots.txt
https://kalyso.com/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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.

[HIGH] X-Frame-Options: La falta de esta directiva permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.

[HIGH] Strict-Transport-Security: No se ha configurado el mecanismo HSTS, lo que permite que un atacante intente degradar la conexión de HTTPS a HTTP.

[MEDIUM] Paneles de login expuestos: Se detectó acceso público a las rutas /administrator/ y /user/login, lo que aumenta la superficie de ataque para intentos de fuerza bruta.

[MEDIUM] Permissions-Policy: El servidor no restringe el uso de APIs del navegador como la cámara o el micrófono, dejando la privacidad del usuario menos protegida.

[LOW] Server header expuesto: La cabecera revela el uso de IONOS Webserver, proporcionando información técnica valiosa para la fase de reconocimiento de un atacante.