EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Www.ukukhome.com	Checks	9 pruebas
Dominio	www.ukukhome.com	Hallazgos	54 totales
Fecha	10 de mayo de 2026 a las 16:30	Problemas	12 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ukukhome.com ha arrojado una puntuación de 77/100 con una calificación de nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue calificado como fallo crítico. Aunque el cifrado SSL y la gestión de cookies son correctos, la exposición de servicios internos y la ausencia de cabeceras de seguridad representan riesgos significativos. Se concluye que el sitio es actualmente vulnerable a ataques dirigidos contra su infraestructura de base de datos y ataques de interceptación de tráfico.

Resumen de Riesgos

1	4	5	2	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	3 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-06-16T04:50:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-18T04:50:17.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://www.ukukhome.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

CMS detectado: PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

3 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PHPSESSID — SameSite**
  SameSite=lax
- INFO **Cookie: PrestaShop-5bda53068fd4da6a246f69ca9cbc16ab — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-5bda53068fd4da6a246f69ca9cbc16ab — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PrestaShop-5bda53068fd4da6a246f69ca9cbc16ab — SameSite**
  SameSite=lax
- INFO **Cookie: PrestaShop-5bda53068fd4da6a246f69ca9cbc16ab — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PrestaShop-5bda53068fd4da6a246f69ca9cbc16ab — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PrestaShop-5bda53068fd4da6a246f69ca9cbc16ab — SameSite**
  SameSite=lax

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 (4260 bytes)
- INFO **Reglas robots.txt**
  142 Disallow, 8 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.ukukhome.com/1_index_sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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

- 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
- 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

[CRITICAL] Puerto 3306 (MySQL): La base de datos MySQL se encuentra abierta y expuesta a Internet, lo que permite intentos de acceso externo y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos activo sin cifrar, lo que permite la captura de credenciales de administración en texto plano.
[HIGH] X-Frame-Options: Cabecera ausente, lo que hace al sitio vulnerable a ataques de clickjacking donde un atacante puede camuflar la interfaz.
[HIGH] Strict-Transport-Security: Falta de configuración HSTS, lo que permite que un atacante intente degradar la conexión del usuario de HTTPS a HTTP.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el sniffing de tipos MIME, facilitando la ejecución de scripts maliciosos disfrazados de otros archivos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros dominios, lo que puede filtrar URLs privadas de la administración.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador, permitiendo potencialmente el acceso no autorizado a funciones como la cámara o geolocalización.
[MEDIUM] Archivos README expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, facilitando información técnica sobre la instalación de PrestaShop.
[LOW] Server header expuesto: El servidor revela el uso de LiteSpeed, permitiendo a los atacantes buscar vulnerabilidades específicas para esa tecnología.
[LOW] Ruta sensible en robots.txt: Se hace referencia a la carpeta config, lo que orienta a los atacantes hacia áreas restringidas del sistema de archivos.