EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ikasistemas.com	Checks	9 pruebas
Dominio	ikasistemas.com	Hallazgos	53 totales
Fecha	22 de abril de 2026 a las 17:57	Problemas	25 detectados

D

41/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio ikasistemas.com ha arrojado una puntuación de 41/100, lo que corresponde a una calificación de grado D. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 4 resultaron exitosas y 5 presentaron fallos críticos en la configuración. Los resultados revelan una superficie de ataque considerable debido a la exposición de servicios de infraestructura y la ausencia de políticas de seguridad en el navegador. Concluimos que el sitio es actualmente vulnerable y requiere una intervención inmediata para mitigar riesgos de compromiso de datos.

Resumen de Riesgos

1	7	14	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 40 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.0.11 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	23 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 40 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  40 dias restantes (expira: 2026-06-01T07:55:50.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-03T07:55:51.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: HTTPd — 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)
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.0.11

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.0.11 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.0.11 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 20/100

Estado: FALLO

23 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://ikasistemas.com/wp-content/uploads/2012/07/Logo_small...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://ikasistemas.com/wp-content/uploads/2012/04/IPB_Slide_...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://ikasistemas.com/wp-content/uploads/2012/04/IPB2_Slide...
- MEDIO **src (script/img/iframe)**
  ...y 14 mas del mismo tipo
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://twitter.com/iksistemas
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.facebook.com/pages/IK-Sistemas/173313582772914
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.bilbonet.net
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (113 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://ikasistemas.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- 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) abierto: La base de datos es accesible desde internet, lo que permite ataques directos de fuerza bruta o explotación de servicios.
[HIGH] Puerto 21 (FTP) abierto: El uso de este protocolo transfiere credenciales y archivos en texto plano, facilitando la interceptación de datos.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] Falta de X-Frame-Options: El sitio no protege contra ataques de clickjacking, permitiendo que la interfaz sea embebida en marcos externos maliciosos.
[HIGH] Falta de Strict-Transport-Security: No se implementa HSTS, lo que deja a los usuarios vulnerables a ataques de degradación de protocolo SSL/TLS.
[HIGH] Ausencia de redirección HTTPS: El servidor permite conexiones HTTP sin cifrar en el puerto 80, exponiendo la comunicación del usuario.
[HIGH] Versión de WordPress 6.0.11 expuesta: Revelar la versión exacta del CMS facilita a los atacantes el uso de exploits para vulnerabilidades conocidas.
[MEDIUM] Contenido Mixto: Se detectaron 23 recursos cargados mediante HTTP dentro de la navegación cifrada, comprometiendo la integridad de la sesión.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de administración es accesible públicamente, aumentando el riesgo de ataques automatizados de acceso.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administración remota está expuesto, ampliando los vectores de ataque hacia el servidor.
[MEDIUM] X-Content-Type-Options faltante: Facilita ataques basados en la interpretación incorrecta de tipos MIME por parte del navegador.
[MEDIUM] Archivo /readme.html accesible: Expone información técnica y versiones del sistema que deberían permanecer ocultas por seguridad.
[LOW] Server header expuesto: El servidor revela el software HTTPd, proporcionando datos valiosos para la fase de reconocimiento de un ataque.
[LOW] Ruta sensible en robots.txt: Se referencia el directorio admin, indicando a los rastreadores y atacantes la ubicación de áreas privadas.