EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Kapital.com	Checks	9 pruebas
Dominio	kapital.com	Hallazgos	42 totales
Fecha	18 de abril de 2026 a las 07:30	Problemas	11 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web Kapital.com presenta una postura de seguridad intermedia con una puntuación exacta de 61/100 y una calificación de nota C. El análisis técnico se basó en la ejecución de 9 checks pasivos, donde se obtuvieron 6 resultados satisfactorios y 3 fallos críticos en la configuración del servidor. A pesar de contar con un cifrado SSL robusto, la ausencia total de cabeceras de seguridad y la falta de redirección automática hacia protocolos seguros representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable ante ataques de inyección de contenido y suplantación de identidad en el navegador. Se requiere una intervención técnica inmediata para corregir las deficiencias de hardening detectadas.

Resumen de Riesgos

0	5	3	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 172 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	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 172 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  172 dias restantes (expira: 2026-10-06T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T00:00:00.000Z
- 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: awselb/2.0 — 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 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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)
- 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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- 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 (CSP): Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) y la inyección de scripts maliciosos.
[HIGH] X-Frame-Options: La ausencia de esta protección deja el sitio expuesto a ataques de clickjacking, permitiendo que terceros carguen el sitio en marcos invisibles.
[HIGH] Strict-Transport-Security (HSTS): No se fuerza el uso de conexiones seguras, permitiendo que un atacante degrade la conexión a HTTP mediante ataques de tipo Man-in-the-Middle.
[HIGH] Redirección HTTP a HTTPS: El sitio no redirige el tráfico no cifrado y responde con un código de error 403, lo que impide una transición segura y automática para el usuario.
[MEDIUM] X-Content-Type-Options: Falta la instrucción para evitar el sniffing de tipos MIME, lo que podría permitir al navegador ejecutar archivos con contenido malicioso disfrazado.

[MEDIUM] Referrer-Policy: No existe una política configurada para controlar cuánta información de navegación se comparte con otros sitios web al seguir enlaces.
[MEDIUM] Permissions-Policy: No se restringe el uso de APIs sensibles del navegador como la cámara, el micrófono o la geolocalización desde el contexto del sitio.
[LOW] Server header expuesto: La cabecera del servidor revela el uso de awselb/2.0, facilitando a posibles atacantes información sobre la infraestructura subyacente.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 403 para estos archivos, dificultando la auditoría de contenidos y la indexación controlada por buscadores.