EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kejati-kaltim.kejaksaan.go.id/	Checks	9 pruebas
Dominio	kejati-kaltim.kejaksaan.go.id	Hallazgos	46 totales
Fecha	1 de septiembre de 2026 a las 10:36	Problemas	12 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al portal institucional arroja una puntuación de 64/100, lo que representa una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron clasificados como fallos críticos. Aunque la infraestructura de cifrado base es sólida, la ausencia total de políticas de seguridad en las cabeceras del servidor y la exposición de versiones de software comprometen la integridad de la plataforma. En su estado actual, el sitio se considera vulnerable a ataques de clickjacking, inyección de código y reconocimiento dirigido.

Resumen de Riesgos

0	5	4	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 113 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.7.7 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 113 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  113 dias restantes (expira: 2026-12-22T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-21T00:00:00.000Z
- 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: nginx — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://kejati-kaltim.kejaksaan.go.id/
- 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

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.7.7
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.7.7 expuesta

- ALTO **WordPress version**
  Version 6.7.7 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (130 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://kejati-kaltim.kejaksaan.go.id/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de cross-site scripting (XSS).
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea embebido en marcos de sitios externos.
[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a mantener una conexión segura, facilitando ataques de degradación de protocolo (SSL Stripping).
[HIGH] Versión de WordPress expuesta: La visibilidad pública de la versión 6.7.7 permite a posibles atacantes identificar vulnerabilidades específicas y CVEs conocidos para este CMS.
[MEDIUM] Falta de X-Content-Type-Options: La configuración actual permite el MIME-type sniffing, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Falta de Referrer-Policy: No se controla la cantidad de información enviada en las peticiones salientes, lo que podría filtrar datos de navegación.
[MEDIUM] Falta de Permissions-Policy: El servidor no restringe el acceso a funciones sensibles del navegador como geolocalización o periféricos.
[MEDIUM] Contenido mixto detectado: Se identificó un recurso cargado mediante el protocolo inseguro HTTP, comprometiendo la seguridad total de la página cifrada.
[LOW] Cabecera de servidor expuesta: El sistema revela el uso de nginx, proporcionando información técnica que facilita el perfilado del servidor por parte de terceros.
[LOW] Ruta sensible en robots.txt: El archivo incluye referencias directas a directorios de administración, ayudando a los atacantes a mapear áreas restringidas.