WebSecure Pro

REPORTE DE SEGURIDAD WEB

Sitio web analizado: https://example.com/
Fecha de escaneo: 05 de September, 2025
ID de escaneo: 6c42802b-d229-454f-b0bd-a20a2b88d8a6
Duración del escaneo: 188 segundos

■ RIESGO CRÍTICO - Puntuación: 25/10

RESUMEN DE HALLAZGOS:
• Total de vulnerabilidades encontradas: **4**
• Tipos de escaneo realizados: xss, sql_injection, security_headers, ssl_tls, directory_scan
• Estado del escaneo: **COMPLETED**

RESUMEN EJECUTIVO

Este reporte presenta los resultados del análisis de seguridad web realizado en https://example.com/ el 05 de September, 2025. El escaneo se realizó utilizando técnicas automatizadas de detección de vulnerabilidades, enfocándose en las amenazas más comunes según el OWASP Top 10.

HALLAZGOS PRINCIPALES:

• **0** vulnerabilidades CRÍTICAS que requieren atención inmediata
• **3** vulnerabilidades de riesgo ALTO
• **1** vulnerabilidades de riesgo MEDIO
• **0** vulnerabilidades de riesgo BAJO

RECOMENDACIÓN EJECUTIVA:

ACCIÓN INMEDIATA REQUERIDA: Se han identificado vulnerabilidades críticas que exponen el sitio web a ataques severos. Se recomienda suspender operaciones no esenciales hasta que se implementen las correcciones necesarias.

DETALLES DE VULNERABILIDADES

CROSS-SITE SCRIPTING (XSS)

Campo	Valor
Severidad	HIGH
Ubicación	https://example.com/
Descripción	XSS vulnerability detected: Potential XSS Pattern
Recomendación	Sanitizar y validar todas las entradas de usuario. Implementar Content Security Po

SSL/TLS CONFIGURATION ISSUE

Campo	Valor
Severidad	HIGH
Ubicación	https://example.com/
Descripción	Servidor soporta protocolo débil: SSLv2
Recomendación	Deshabilitar SSLv2 y usar solo TLS 1.2+

Campo	Valor
Severidad	HIGH
Ubicación	https://example.com/
Descripción	Servidor soporta protocolo débil: SSLv3
Recomendación	Deshabilitar SSLv3 y usar solo TLS 1.2+

Campo	Valor
Severidad	MEDIUM
Ubicación	https://example.com/
Descripción	HTTP no redirige automáticamente a HTTPS
Recomendación	Configurar redirección automática de HTTP a HTTPS

RECOMENDACIONES DE SEGURIDAD

1. Implementar Content Security Policy (CSP) headers

2. Sanitizar todas las entradas de usuario

3. Usar funciones de escape apropiadas para el contexto HTML

4. Validar y filtrar datos de entrada en el servidor

5. Implementar un programa regular de escaneo de vulnerabilidades

6. Establecer un proceso de gestión de parches y actualizaciones

7. Configurar monitoreo continuo de seguridad

8. Realizar pruebas de penetración periódicas

9. Implementar un Web Application Firewall (WAF)

PRÓXIMOS PASOS SUGERIDOS:

1. **Corto plazo (1-7 días):** Abordar vulnerabilidades críticas y de alto riesgo
2. **Mediano plazo (1-4 semanas):** Implementar medidas preventivas y mejoras de seguridad
3. **Largo plazo (1-3 meses):** Establecer programa de seguridad continua y monitoreo
4. **Seguimiento:** Realizar nuevo escaneo después de implementar correcciones

ANEXO TÉCNICO

Metodología de escaneo:
• Tipos de escaneo: xss, sql_injection, security_headers, ssl_tls, directory_scan
• Duración total: 188 segundos
• Fecha y hora de inicio: 2025-09-05T22:16:19.163844
• Fecha y hora de finalización: 2025-09-05T22:19:27.747318

Herramientas utilizadas:
• WebSecure Pro Scanner v1.0
• Módulos: XSS Scanner, SQL Injection Scanner
• Base de datos de vulnerabilidades: OWASP Top 10 2021

Cobertura del escaneo:
• Análisis de formularios web
• Pruebas de parámetros GET y POST
• Detección de patrones de vulnerabilidad
• Análisis de respuestas del servidor

DETALLES - XSS

• Tiempo de escaneo: 6.7 segundos
• Formularios encontrados: 0
• Parámetros probados: 0
• Vulnerabilidades detectadas: 1
• Estado: Vulnerable

DETALLES - SQL_INJECTION

• Tiempo de escaneo: 51.97 segundos
• Formularios encontrados: 0
• Parámetros probados: 0
• Vulnerabilidades detectadas: 0
• Estado: Seguro

DETALLES - SECURITY_HEADERS

• Tiempo de escaneo: N/A segundos
• Formularios encontrados: N/A
• Parámetros probados: N/A
• Vulnerabilidades detectadas: 9
• Estado: Seguro

DETALLES - SSL_TLS

• Tiempo de escaneo: N/A segundos
• Formularios encontrados: N/A
• Parámetros probados: N/A

• Vulnerabilidades detectadas: 3
• Estado: Seguro

DETALLES - DIRECTORY_SCAN

• Tiempo de escaneo: N/A segundos
• Formularios encontrados: N/A
• Parámetros probados: N/A
• Vulnerabilidades detectadas: 1
• Estado: Seguro

DISCLAIMER

Este reporte ha sido generado mediante herramientas automatizadas de escaneo de vulnerabilidades. Los resultados deben ser verificados por personal técnico calificado antes de implementar cualquier corrección. WebSecure Pro no se hace responsable por daños que puedan resultar del uso de esta información. Se recomienda realizar pruebas adicionales en un ambiente controlado antes de aplicar cambios en producción.