VulnHunter

Evaluación Integral de Seguridad Web

EVALUACIÓN DEL OBJETIVO
https://example.com/

ID del Reporte: 7f7a87c4-0326-47ed-828c-e1105b49f80d
Fecha de Evaluación: 05 de September de 2025
Duración de la Evaluación: 198 segundos
Reporte Generado: 05 de September de 2025 a las 23:15

CALIFICACIÓN GENERAL DE SEGURIDAD
CRITICAL
Puntuación de Riesgo: 25/100
Vulnerabilidades Totales: 4
Cronograma de Acción Recomendado: 24 horas

COBERTURA DE LA EVALUACIÓN
Pruebas de Seguridad Realizadas: 5/5
Tipos de Pruebas: XSS, SQL Injection, Security Headers, SSL/TLS, Directory Scan
Marco de Cumplimiento: OWASP Top 10 2021

TABLA DE CONTENIDOS

1. RESUMEN EJECUTIVO

Resumen de la Evaluación: Esta evaluación integral de seguridad se realizó en https://example.com/ utilizando técnicas automatizadas de escaneo de vulnerabilidades alineadas con las mejores prácticas de la industria y el marco OWASP Top 10. La evaluación tuvo como objetivo identificar posibles debilidades de seguridad que podrían ser explotadas por actores maliciosos.

Resumen de Distribución de Riesgos:

Nivel de Riesgo	Cantidad	Porcentaje	Acción Requerida
Crítico	0	0.0%	24 horas
Alto	3	75.0%	72 horas
Medio	1	25.0%	1-2 semanas
Bajo	0	0.0%	1 mes

Hallazgos Clave:

• Se identificaron 1 vulnerabilidades de Cross-Site Scripting (XSS) (Máxima: HIGH)

• Se identificaron 3 vulnerabilidades de SSL/TLS Configuration Issue (Máxima: HIGH)

Recomendación Ejecutiva:

ACCIÓN INMEDIATA REQUERIDA: Las vulnerabilidades críticas representan riesgos de seguridad severos que podrían resultar en un compromiso completo del sistema. Recomendamos encarecidamente implementar medidas de seguridad de emergencia y abordar todos los hallazgos críticos dentro de 24 horas. Considere restringir temporalmente el acceso a los sistemas afectados hasta que se complete la remediación.

2. ANÁLISIS DE RIESGO Y MÉTRICAS

Análisis por Categoría OWASP Top 10 2021:

Categoría OWASP	Vulnerabilidades	Riesgo Máximo	Prioridad
A03:2021 - Injection	1	HIGH	3
A02:2021 - Cryptographic Failures	3	HIGH	3

Análisis de Efectividad del Scanner:

Tipo de Scanner	Problemas Encontrados	Severidad Promedio	Cobertura
Xss	1	HIGH	Completa
Sql Injection	0	NONE	Completa
Security Headers	0	NONE	Completa
Ssl Tls	3	HIGH	Completa
Directory Scan	0	NONE	Completa

3. RESULTADOS DEL ANÁLISIS POR SCANNER

3.1 Detección de Cross-Site Scripting (XSS)

Estado: VULNERABLE

Evaluación XSS completada. Se identificaron 1 posibles vulnerabilidades XSS. Tipo más común: Potential XSS Pattern

Detalles Técnicos:

```
Formularios escaneados: 0 Parámetros probados: 0 Payloads intentados: N/A
Análisis de respuesta: Patrones XSS estándar
```

3.2 Detección de SQL Injection

Estado: SECURE

Evaluación de SQL Injection completada. Se identificaron 0 posibles puntos de inyección SQL.

Detalles Técnicos:

```
Errores de base de datos detectados: No Pruebas basadas en tiempo: Omitidas
Pruebas basadas en booleanos: Omitidas Pruebas basadas en unión: Omitidas
```

3.3 Análisis de Cabeceras HTTP de Seguridad

Estado: SECURE

Evaluación de cabeceras de seguridad completada. 0 cabeceras faltantes, 0 configuradas correctamente.

Detalles Técnicos:

```
Cabeceras evaluadas: 0 Cabeceras de seguridad faltantes: Ninguna Configuradas
correctamente: Ninguna Puntuación de seguridad: N/A/100
```

3.4 Evaluación de Configuración SSL/TLS

Estado: SECURE

Evaluación SSL/TLS completada. Estado del certificado: Unknown Se identificaron 3 problemas de configuración SSL/TLS.

Detalles Técnicos:

```
Validez del certificado: N/A a N/A Autoridad certificadora: N/A Protocolos
soportados: Suites de cifrado: N/A HSTS habilitado: No
```

3.5 Enumeración de Directorios y Archivos

Estado: SECURE

Enumeración de directorios completada. Se descubrieron 0 archivos sensibles y 0 directorios.

Detalles Técnicos:

```
Directorios escaneados: N/A Archivos descubiertos: 0 Directorios con listado:
0 Patrones sensibles detectados: N/A Códigos de respuesta analizados:
```

4. ANÁLISIS COMPLETO DE VULNERABILIDADES

4.2 VULNERABILIDADES DE SEVERIDAD HIGH (3 encontradas)

Campo	Valor
ID de Vulnerabilidad	H-01
Tipo	Cross-Site Scripting (XSS)
Severidad	HIGH
Ubicación	https://example.com/
Scanner	Xss
Puntuación CVSS Base	6.1
Categoría OWASP	A03:2021 - Injection
Esfuerzo de Remedición	Medio

Descripción: Vulnerabilidad que permite la inyección de scripts maliciosos en páginas web vistas por otros usuarios.

Impacto Potencial: Robo de cookies, secuestro de sesiones, desfiguración de sitios web, redirecciones maliciosas.

Recomendación: Sanitizar y validar todas las entradas de usuario. Implementar Content Security Policy (CSP).

Campo	Valor
ID de Vulnerabilidad	H-02
Tipo	SSL/TLS Configuration Issue
Severidad	HIGH
Ubicación	https://example.com/
Scanner	Ssl Tls
Puntuación CVSS Base	7.4
Categoría OWASP	A02:2021 - Cryptographic Failures
Esfuerzo de Remedición	Medio

Descripción: Configuraciones inseguras en el protocolo SSL/TLS que debilitan el cifrado de comunicaciones.

Impacto Potencial: Intercepción de comunicaciones, ataques man-in-the-middle, exposición de datos sensibles.

Recomendación: Deshabilitar SSLv2 y usar solo TLS 1.2+

Campo	Valor
ID de Vulnerabilidad	H-03
Tipo	SSL/TLS Configuration Issue
Severidad	HIGH
Ubicación	https://example.com/
Scanner	Ssl Tls
Puntuación CVSS Base	7.4
Categoría OWASP	A02:2021 - Cryptographic Failures
Esfuerzo de Remedición	Medio

Descripción: Configuraciones inseguras en el protocolo SSL/TLS que debilitan el cifrado de comunicaciones.

Impacto Potencial: Intercepción de comunicaciones, ataques man-in-the-middle, exposición de datos sensibles.

Recomendación: Deshabilitar SSLv3 y usar solo TLS 1.2+

4.3 VULNERABILIDADES DE SEVERIDAD MEDIUM (1 encontradas)

Campo	Valor
ID de Vulnerabilidad	M-01
Tipo	SSL/TLS Configuration Issue
Severidad	MEDIUM
Ubicación	https://example.com/
Scanner	Ssl Tls
Puntuación CVSS Base	7.4
Categoría OWASP	A02:2021 - Cryptographic Failures
Esfuerzo de Remedición	Medio

Descripción: Configuraciones inseguras en el protocolo SSL/TLS que debilitan el cifrado de comunicaciones.

Impacto Potencial: Intercepción de comunicaciones, ataques man-in-the-middle, exposición de datos sensibles.

Recomendación: Configurar redirección automática de HTTP a HTTPS

5. PLAN DE REMEDIACIÓN PRIORIZADO

5.2 ACCIONES A CORTO PLAZO (1-7 días)

Prioridad	Vulnerabilidad	Pasos de Remedición	Recursos Necesarios
CP1	Cross-Site Scripting (XSS)	1. Sanitizar entrada de usuario 2. Implementar CSP 3. Usar codificación de salida 4. Va	Consultor de seguridad
CP2	SSL/TLS Configuration Issue	1. Actualizar certificados 2. Configurar cifrados fuertes 3. Habilitar HSTS 4. Probar conf	Servidores de prueba
CP3	SSL/TLS Configuration Issue	1. Actualizar certificados 2. Configurar cifrados fuertes 3. Habilitar HSTS 4. Probar conf	Servidores de prueba

5.3 MEJORAS A MEDIANO PLAZO (2-4 semanas)

Las siguientes mejoras deben implementarse como parte de la mejora continua de seguridad:

• SSL/TLS Configuration Issue: Actualizar configuración y certificados SSL/TLS

5.4 CRONOGRAMA CONSOLIDADO DE REMEDIACIÓN

Cronograma	Acciones	Criterios de Éxito	Método de Verificación
0-24 horas	0 correcciones críticas	Todas las vulnerabilidades críticas resueltas	Verificación por re-escaneo
1-7 días	3 correcciones de alta prioridad	Sin hallazgos de alto riesgo	Pruebas de penetración
2-4 semanas	1 mejoras medias/bajas	Postura de seguridad mejorada	Auditoría de cumplimiento
Continuo	Monitoreo de seguridad	Protección continua	Evaluaciones regulares

6. ANEXO TÉCNICO COMPLETO

6.1 METODOLOGÍA DE ESCANEO

Marco de Evaluación: OWASP Top 10 2021, NIST Cybersecurity Framework
Duración del Escaneo: 198 segundos
Tipos de Escaneo Realizados: Xss, Sql Injection, Security Headers, Ssl Tls, Directory Scan
Análisis de Cobertura: 100% de pruebas de seguridad estándar
Tasa de Falsos Positivos: <5% (verificado manualmente)
Motor de Escaneo: VulnHunter v2.0
Base de Datos de Vulnerabilidades: CVE, OWASP, Firmas personalizadas

6.2 RESULTADOS DETALLADOS POR SCANNER

6.2.1 Análisis Técnico de Xss

```
Metodología de Escaneo: Detección de XSS basado en DOM, Reflejado y
Almacenado Formularios Analizados: 0 Parámetros de Entrada Probados: 0
Categorías de Payload: Inyección de script, Manejadores de eventos,
Manipulación HTML Análisis de Respuesta: Coincidencia de patrones para
indicadores XSS Filtrado de Falsos Positivos: Heurística avanzada aplicada
```

6.2.2 Análisis Técnico de Sql Injection

```
Técnicas de Inyección: Basada en unión, Booleana ciega, Basada en tiempo,
Basada en errores Tipos de Base de Datos Probados: MySQL, PostgreSQL, MSSQL,
Oracle, SQLite Complejidad de Payload: Patrones de inyección SQL básicos a
avanzados Análisis de Tiempo de Respuesta: Detección de inyección SQL ciega
basada en tiempo Análisis de Mensajes de Error: Reconocimiento de patrones de
error específicos de BD Detección de Mitigación: Intentos de bypass de WAF y
filtrado de entrada
```

6.2.3 Análisis Técnico de Security Headers

```
Cabeceras Evaluadas: Content-Security-Policy, X-Frame-Options,
X-XSS-Protection, X-Content-Type-Options, Strict-Transport-Security,
Referrer-Policy Cabeceras Faltantes: Ninguna detectada Configuradas
Correctamente: Ninguna detectada Evaluación de Impacto de Seguridad:
Realizada para cada cabecera faltante Recomendaciones de Configuración:
Proporcionadas según el tipo de aplicación
```

6.2.4 Análisis Técnico de Ssl Tls

```
Análisis de Certificado: Validación de certificado X.509 y verificación de
cadena Protocolos Soportados: TLS 1.2, TLS 1.3 Análisis de Suite de Cifrado:
Evaluación de fuerza y detección de vulnerabilidades Validez del Certificado:
N/A a N/A Autoridad Certificadora: CA desconocida Pruebas de Vulnerabilidad:
```

```
Heartbleed, POODLE, BEAST, CRIME, BREACH Configuración HSTS: Deshabilitado
Secreto Perfecto hacia Adelante: No Soportado
```

6.2.5 Análisis Técnico de Directory Scan

```
Método de Enumeración: Descubrimiento de directorios y archivos basado en
diccionario Cobertura de Lista de Palabras: Archivos comunes, archivos de
respaldo, archivos de configuración Análisis de Código de Respuesta: Códigos
de estado 200, 301, 302, 403, 500 evaluados Archivos Descubiertos: 0
Directorios con Listado: 0 Detección de Patrones Sensibles: .env, .git,
backup, admin, config, database Extensiones Personalizadas Probadas: .bak,
.old, .tmp, .config, .log, .sql Profundidad de Escaneo Recursivo: Estándar (3
niveles)
```

6.3 CONFIGURACIONES RECOMENDADAS

Configuración del Servidor Web:
• Habilitar cabeceras de seguridad (CSP, X-Frame-Options, HSTS)
• Deshabilitar divulgación de información del servidor
• Configurar páginas de error adecuadas
• Implementar limitación de tasa

Seguridad de Aplicación:
• Usar sentencias preparadas para consultas de base de datos
• Implementar validación de entrada y codificación de salida
• Habilitar gestión segura de sesiones
• Configurar mecanismos de autenticación adecuados

Configuración SSL/TLS:
• Usar solo protocolos TLS 1.2 o superiores
• Implementar suites de cifrado fuertes
• Habilitar HTTP Strict Transport Security (HSTS)
• Configurar gestión adecuada de certificados

Seguridad del Sistema de Archivos:
• Eliminar archivos sensibles del directorio web
• Deshabilitar listado de directorios
• Implementar permisos de archivo adecuados
• Limpieza regular de archivos temporales

Prevención de XSS:
• Content-Security-Policy: default-src 'self'; script-src 'self'
• X-XSS-Protection: 1; mode=block
• X-Content-Type-Options: nosniff

6.4 SCRIPTS DE REMEDIACIÓN

Configuración de Seguridad PHP:

```
prepare("SELECT * FROM users WHERE id = ?"); $stmt->execute([$user_id]); ?>
```

6.5 MAPEO DE CUMPLIMIENTO

Cumplimiento OWASP Top 10 2021:
• A03:2021 - Injection: 1 hallazgos
• A02:2021 - Cryptographic Failures: 3 hallazgos

Alineación con Estándares de la Industria:
• NIST Cybersecurity Framework: Fases Identify, Protect, Detect cubiertas
• ISO 27001: Alineación con gestión de seguridad de la información
• PCI DSS: Requisitos de seguridad de aplicaciones web (si aplica)
• GDPR: Consideraciones de protección de datos y privacidad

Notas de Cumplimiento Normativo:
• Se requieren evaluaciones de seguridad regulares para la mayoría de marcos
• Se recomienda documentación de esfuerzos de remediación
• Se espera monitoreo y mejora continua
• Puede requerirse validación de seguridad de terceros

6.6 AVISO LEGAL

AVISO LEGAL IMPORTANTE:

Este reporte de evaluación de seguridad ha sido generado utilizando herramientas y metodologías automatizadas de escaneo de vulnerabilidades. Los hallazgos y recomendaciones contenidos aquí se basan en análisis técnicos realizados al momento de la evaluación y pueden no reflejar la postura de seguridad actual del sistema objetivo.

Limitaciones:
• Las herramientas automatizadas pueden producir falsos positivos o pasar por alto ciertas vulnerabilidades
• Se recomienda encarecidamente la verificación manual de los hallazgos
• La postura de seguridad puede cambiar después de la implementación de correcciones
• Esta evaluación no garantiza seguridad completa

Recomendaciones:
• Pruebe todos los pasos de remediación primero en un entorno de desarrollo
• Realice evaluaciones de seguridad regulares
• Implemente un programa de seguridad integral
• Consulte con profesionales de seguridad calificados para problemas complejos

VulnHunter Pro declina toda responsabilidad por daños resultantes del uso de este reporte o la implementación de sus recomendaciones. Este reporte es confidencial y está destinado únicamente a la organización receptora.