Manual del Usuario

Sistema de Auditoría de Seguridad Web

Versión 1.0

Fecha: Julio 2025

Tabla de Contenidos

Introducción

El Sistema de Auditoría de Seguridad Web es una herramienta diseñada para evaluar y mejorar la calidad del código y la seguridad de aplicaciones web existentes. Permite realizar auditorías automatizadas, pruebas de vulnerabilidades y aplicar buenas prácticas de desarrollo seguro.

Objetivo Principal

Proporcionar una solución integral para identificar vulnerabilidades de seguridad en aplicaciones web y generar reportes detallados con recomendaciones de mejora.

Características Principales

- Análisis estático de código
- Detección de vulnerabilidades OWASP Top 10
- Pruebas de penetración automatizadas
- Generación de reportes detallados
- Interfaz intuitiva y fácil de usar

Requisitos del Sistema

Requisitos Mínimos

- **Sistema Operativo**: Windows 10/11, macOS 10.14+, Linux Ubuntu 18.04+
- **Memoria RAM**: 4 GB mínimo, 8 GB recomendado
- **Espacio en disco**: 2 GB de espacio libre
- **Procesador**: Intel Core i3 o equivalente
- **Conexión a Internet**: Requerida para actualizaciones de base de datos

Requisitos de Software

- Python 3.8 o superior
- Node.js 14.0 o superior
- Navegador web moderno (Chrome, Firefox, Safari, Edge)

Instalación

Paso 1: Descarga

1. Descarga el archivo `sistema-auditoria-web.rar` desde el enlace proporcionado
2. Extrae el contenido en una carpeta de tu elección

Paso 2: Instalación de Dependencias

```bash
# Navega al directorio del proyecto
cd sistema-auditoria-web

# Instala las dependencias de Python
pip install -r requirements.txt

# Instala las dependencias de Node.js
npm install
```

Paso 3: Configuración Inicial

1. Ejecuta el archivo `setup.py` para configurar la base de datos
2. Configura las variables de entorno en el archivo `.env`
3. Ejecuta la aplicación con `python app.py`

Interfaz de Usuario

Panel Principal

La interfaz principal consta de las siguientes secciones:

1. **Barra de Navegación Superior**
   - Menú de proyectos
   - Configuración
   - Ayuda
2. **Panel Lateral Izquierdo**
   - Lista de proyectos
   - Historial de auditorías
   - Configuraciones rápidas
3. **Área de Trabajo Central**
   - Formulario de nueva auditoría
   - Resultados de análisis
   - Gráficos y estadísticas
4. **Panel de Estado Inferior**
   - Progreso de análisis
   - Notificaciones
   - Información del sistema

Funcionalidades Principales

1. Análisis de Código Estático

- Escaneo automático de archivos fuente
- Detección de patrones inseguros
- Análisis de dependencias
- Verificación de configuraciones

2. Pruebas de Vulnerabilidades

- Inyección SQL
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Autenticación y autorización
- Gestión de sesiones

3. Generación de Reportes

- Reportes en PDF y HTML

- Resumen ejecutivo
- Detalles técnicos
- Recomendaciones de seguridad

4. Panel de Monitoreo

- Dashboard en tiempo real
- Métricas de seguridad
- Tendencias y estadísticas
- Alertas automáticas

Guía de Uso

Crear Nueva Auditoría

1. **Acceso al Sistema**
   - Inicia la aplicación
   - Haz clic en "Nueva Auditoría"
2. **Configuración del Proyecto**
   - Nombre del proyecto
   - URL o ruta del código fuente
   - Tipo de aplicación web
   - Seleccionar pruebas a realizar
3. **Configuración de Parámetros**
   - Nivel de profundidad del análisis
   - Tipos de vulnerabilidades a buscar
   - Exclusiones y filtros
4. **Ejecutar Auditoría**
   - Haz clic en "Iniciar Análisis"
   - Monitorea el progreso en la barra de estado
   - Espera a que termine el proceso

Visualizar Resultados

1. **Resumen de Resultados**
   - Número total de vulnerabilidades encontradas
   - Clasificación por severidad
   - Tiempo de análisis

2. **Detalles de Vulnerabilidades**
   - Descripción detallada
   - Ubicación en el código
   - Nivel de riesgo
   - Recomendaciones de solución
3. **Generar Reporte**
   - Selecciona el formato deseado
   - Personaliza el contenido
   - Descarga o envía por email

Gestión de Proyectos

1. **Crear Proyecto**
   - Nombre y descripción
   - Configuración de parámetros
   - Asignación de responsables
2. **Editar Proyecto**
   - Modificar configuraciones
   - Actualizar información
   - Cambiar responsables
3. **Eliminar Proyecto**
   - Confirmación de eliminación
   - Respaldo de datos
   - Limpieza de archivos

Interpretación de Resultados

Niveles de Severidad

Crítico 🔴

- Vulnerabilidades que permiten compromiso completo
- Requieren atención inmediata
- Pueden resultar en pérdida de datos o control del sistema

Alto 🟠

- Vulnerabilidades significativas

- Pueden llevar a acceso no autorizado
- Requieren corrección prioritaria

Medio 🟡

- Vulnerabilidades moderadas
- Pueden facilitar otros ataques
- Requieren corrección planificada

Bajo 🟢

- Vulnerabilidades menores
- Impacto limitado
- Corrección recomendada

Tipos de Vulnerabilidades Comunes

1. **Inyección SQL**
   - Descripción: Permite ejecutar comandos SQL maliciosos
   - Impacto: Acceso a base de datos, modificación de datos
   - Solución: Usar consultas parametrizadas
2. **Cross-Site Scripting (XSS)**
   - Descripción: Ejecución de scripts maliciosos en el navegador
   - Impacto: Robo de cookies, sesiones hijacking
   - Solución: Validación y escape de datos
3. **Configuración Insegura**
   - Descripción: Configuraciones por defecto inseguras
   - Impacto: Exposición de información sensible
   - Solución: Hardening de configuraciones

Solución de Problemas

Problemas Comunes

Error: "No se puede conectar a la base de datos"

Causa: Configuración incorrecta de la base de datos **Solución**:

1. Verificar credenciales en archivo `.env`
2. Comprobar que el servidor de BD esté ejecutándose
3. Verificar permisos de conexión

Error: "Análisis interrumpido"

Causa: Falta de recursos o archivos corruptos **Solución**:

1. Verificar espacio en disco disponible
2. Comprobar integridad de archivos fuente
3. Reiniciar el análisis

Error: "Reporte no se genera"

Causa: Permisos insuficientes o error en plantillas **Solución**:

1. Verificar permisos de escritura
2. Comprobar plantillas de reporte
3. Revisar logs de error

Diagnóstico y Logs

Ubicación de Logs

- Logs de aplicación: `logs/app.log`
- Logs de errores: `logs/error.log`
- Logs de auditoría: `logs/audit.log`

Niveles de Log

- DEBUG: Información detallada para desarrollo
- INFO: Información general de funcionamiento
- WARNING: Advertencias que no interrumpen el funcionamiento
- ERROR: Errores que requieren atención
- CRITICAL: Errores críticos que detienen la aplicación

Mejores Prácticas

Preparación del Análisis

1. Asegurar que el código fuente esté completo
2. Incluir archivos de configuración
3. Documentar dependencias externas
4. Realizar respaldo antes del análisis

Interpretación de Resultados

1. Priorizar vulnerabilidades críticas
2. Verificar falsos positivos
3. Documentar decisiones de corrección
4. Establecer plan de remedición

Seguimiento y Monitoreo

1. Realizar auditorías periódicas
2. Mantener registro de correcciones
3. Actualizar configuraciones de seguridad
4. Capacitar al equipo de desarrollo

Actualizaciones y Mantenimiento

Actualizaciones Automáticas

- Base de datos de vulnerabilidades
- Reglas de detección
- Plantillas de reporte

Actualizaciones Manuales

- Versión de la aplicación
- Dependencias de sistema
- Configuraciones personalizadas

Mantenimiento Preventivo

- Limpieza de archivos temporales
- Optimización de base de datos
- Revisión de logs y rendimiento

Soporte Técnico

Información de Contacto

- **Email**: soporte@auditoria-web.com
- **Teléfono**: +593-4-XXX-XXXX
- **Horario**: Lunes a Viernes 8:00 AM - 6:00 PM (GMT-5)

Recursos Adicionales

- **Documentación Online**: https://docs.auditoria-web.com
- **Foro de Usuarios**: https://forum.auditoria-web.com
- **Base de Conocimiento**: https://kb.auditoria-web.com
- **Video Tutoriales**: https://youtube.com/auditoria-web

Información de Versión

- **Versión Actual**: 1.0.0
- **Fecha de Lanzamiento**: Julio 2025
- **Última Actualización**: Julio 14, 2025

Este manual ha sido desarrollado para facilitar el uso del Sistema de Auditoría de Seguridad Web. Para obtener la información más actualizada, consulte la documentación online.