UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Sistemas

PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web

Curso: *Patrones de Software*

Docente: Ing. Patrick Jose Cuadros Quiroga

Integrantes:

Ccalli Chata, Joel Robert ***(2017057528)***

Jarro Cachi, Jose Luis ***(2020067148)***

Tacna – Perú

2025

CONTROL DE VERSIONES					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	JRCC	JCC	JCC	26/06/2025	Versión Original

PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web
FD05 - Documento de Informe Final

ÍNDICE GENERAL

1. Revisión de Trabajos Relacionados

Se han identificado diversos trabajos de investigación y desarrollo tecnológico que abordan soluciones similares en el ámbito de la ciberseguridad y análisis de vulnerabilidades web. Estos antecedentes proporcionan una base sólida para la conceptualización y desarrollo del sistema *PWASP SCANNER*. A continuación, se describen algunos de los más relevantes:

a. Morales C. Edwin (2021), en su trabajo titulado **"Diseño e Implementación de un Sistema de Recomendación de Equipos Electrónicos Basado en las Preferencias del Usuario"**, desarrolla un sistema web con técnicas de análisis inteligente, aplicando lógica algorítmica orientada a la automatización de decisiones. Si bien el enfoque está orientado a hardware, destaca el uso de algoritmos inteligentes, aplicables en el diseño del motor de análisis de vulnerabilidades.

b. Flores Sánchez, María (2020), en su investigación **"Sistema Web para la Selección de Equipos Informáticos Basado en Análisis de Presupuestos"**, plantea un enfoque que, aunque dirigido a hardware, utiliza un procesamiento basado en parámetros definidos por el usuario, similar al enfoque que adopta *PWASP SCANNER* al recibir configuraciones y parámetros de exploración para personalizar el escaneo.

Estas investigaciones demuestran la viabilidad de diseñar sistemas inteligentes basados en el análisis automatizado y decisiones computacionales, sentando precedentes metodológicos y tecnológicos que inspiran y complementan el desarrollo de *PWASP SCANNER*.

2. Planteamiento del Problema

a. Problema Identificado

En el contexto actual de la transformación digital, los sistemas web se han convertido en pilares fundamentales de operación para empresas, instituciones educativas, y organizaciones gubernamentales. Sin embargo, muchas de estas plataformas son implementadas sin un análisis exhaustivo de seguridad, lo que las expone a múltiples amenazas como inyecciones SQL, Cross-Site Scripting (XSS), ataques CSRF, entre otros. La falta de herramientas automatizadas accesibles para detectar estas vulnerabilidades representa una debilidad crítica que puede ser explotada fácilmente por atacantes.

b. Justificación

El desarrollo de *PWASP SCANNER* surge como una respuesta directa a la creciente necesidad de herramientas accesibles, precisas y eficaces para detectar vulnerabilidades en aplicaciones web. Al integrar funciones de escaneo y análisis automatizado, el sistema permitirá a desarrolladores, auditores y empresas obtener reportes detallados de las posibles debilidades de sus sistemas. Esto contribuirá a fortalecer la seguridad digital desde las etapas tempranas del ciclo de vida del software.

c. Alcance

El sistema *PWASP SCANNER* incluirá las siguientes funcionalidades clave:

- Exploración automática de vulnerabilidades OWASP Top 10.
- Generación de reportes técnicos detallados.
- Configuración personalizada del escaneo (URLs, profundidad, autenticación).
- Interfaz intuitiva y de fácil acceso para usuarios con y sin experiencia técnica.
- Registro de auditorías y recomendaciones de mitigación.
- Panel administrativo para gestión de usuarios y escaneos.

3. Objetivos

a. Objetivo General

Desarrollar un sistema web denominado *PWASP SCANNER*, que permita detectar, registrar y reportar vulnerabilidades en aplicaciones web mediante técnicas de escaneo automatizado, contribuyendo a una mejora significativa en la seguridad digital.

b. Objetivos Específicos

- Analizar e implementar técnicas de escaneo basadas en OWASP Top 10.
- Diseñar una interfaz gráfica clara para facilitar la interacción del usuario con los procesos de escaneo.
- Integrar una base de datos que almacene los resultados de los análisis para seguimiento histórico.
- Desplegar el sistema en la nube para garantizar disponibilidad y accesibilidad.
- Proporcionar reportes técnicos en formatos exportables (PDF, CSV) para su análisis y documentación.

4. Marco Teórico

ASP.NET MVC

Framework de desarrollo que adopta el patrón Modelo-Vista-Controlador, ideal para separar responsabilidades dentro de una aplicación. Favorece la escalabilidad, organización del código y mantenimiento.

SQL Server

Sistema de gestión de bases de datos relacional que permite manejar estructuras complejas de datos, ideal para almacenar los resultados de los escaneos y configuraciones personalizadas.

C#

Lenguaje de programación robusto, orientado a objetos y con amplias capacidades de seguridad, compatible con el entorno .NET, facilitando la lógica del escaneo y procesamiento de reportes.

Somee.com

Servicio de hosting que permite desplegar aplicaciones ASP.NET en la nube, asegurando disponibilidad continua y acceso universal a la herramienta desde cualquier navegador web.

OWASP Top 10

Lista de las 10 vulnerabilidades más críticas para aplicaciones web, publicada por la Open Web Application Security Project (OWASP). Constituye la base del análisis de seguridad de *PWASP SCANNER*.

5. Desarrollo de la Solución

a. Análisis de Factibilidad

- **Técnica**: Se utiliza tecnología ampliamente adoptada como ASP.NET, SQL Server, HTML5 y servicios en la nube, facilitando la implementación.
- **Económica**: El costo estimado es moderado y accesible, con beneficios ampliamente superiores al costo de desarrollo.
- **Operativa**: Las necesidades de los usuarios han sido levantadas en etapas tempranas, permitiendo un diseño adaptado a sus requerimientos.
- **Legal**: Se respetan las normativas de software libre y licenciamiento, así como leyes de protección de datos.
- **Social**: Mejora la cultura de ciberseguridad en organizaciones y usuarios comunes.
- **Ambiental**: Al tratarse de un sistema digital, su impacto ambiental es prácticamente nulo.

b. Tecnologías de Desarrollo

- **Lenguaje de programación**: C#
- **Framework**: ASP.NET MVC
- **Base de datos**: SQL Server
- **Frontend**: HTML5, CSS3, JavaScript
- **Hosting**: Somee.com

c. Metodología de Implementación

Se emplea la metodología **RUP (Rational Unified Process)**, lo que garantiza una estructura iterativa e incremental a lo largo del proyecto. Las fases incluyeron la elaboración de los siguientes documentos:

- FD01 – Carta del Proyecto
- FD02 – Documento de Visión

- FD03 – Especificación de Requisitos (SRS)
- FD04 – Diseño de Arquitectura del Software (SAD)

6. Cronograma de Actividades

El proyecto inició el **21 de septiembre del 2024** y concluyó el **03 de diciembre del 2024**, organizado en las cuatro fases principales de RUP: Inicio, Elaboración, Construcción y Transición.

7. Presupuesto

a. Costos Generales

Concepto	Cantidad	Precio Unitario	Total S/
Impresora	1	600	600
Router	1	80	80
Alquiler Equipos Oficina	2	150	300
Licencias	1	50	50
Cartuchos de Impresora	2	59	118
Marcadores	1	9	9
Papeles	2	30	60
Total			**1.217**

b. Costos Operativos

Elemento	Meses	Precio/Mes	Total
Luz	3	60	63
Internet	3	60	63
Agua	3	35	38
TOTAL			**164**

c. Costos de Ambiente

Descripción	Cantidad	Costo Unitario	Total S/
Licencias Windows	2	57	57
Antivirus (Malware)	2	27	27
Total			**84**

d. Costos de Personal

Rol	Costo/Hora	Horas	Personal	Subtotal S/
Director de Proyecto	5	80	1	1.200
Analista/Diseñador	5	80	1	1.200
Desarrollador	5	80	1	1.200
Total				**3.600**

e. Costos Totales del Proyecto

Categoría	Subtotal (S/)
Costos Generales	1.217
Costos Operativos	164
Costos del Ambiente	84
Costos de Personal	3.600
Total General	**5.065**

8. Conclusión General del Proyecto

El sistema *PWASP SCANNER* representa un avance importante en la detección de vulnerabilidades web de forma automatizada. Su diseño y desarrollo se han sustentado en principios sólidos de ingeniería de software, buenas prácticas de seguridad, y una ejecución organizada bajo la metodología RUP. El sistema está preparado para ser utilizado como herramienta de apoyo en auditorías de seguridad, tanto en entornos educativos como empresariales. Se espera que su implementación contribuya significativamente a la prevención de ciberataques mediante un diagnóstico temprano y detallado de debilidades en sistemas web.