
# 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***

# PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web
# FD01 - Documento de Factibilidad

**Versión *1.0***

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

# ÍNDICE GENERAL

# 1. Descripción del Proyecto

## 1.1 Nombre del proyecto

**PWASP SCANNER: Sistema de Detección de Vulnerabilidades Web**

## 1.2 Duración del proyecto

El proyecto tiene una duración de 5 meses.

## 1.3 Descripción

PWASP SCANNER es una herramienta de seguridad informática desarrollada en Python, diseñada para detectar vulnerabilidades en aplicaciones web, basada en los estándares del OWASP Top 10. El sistema escaneará páginas web específicas identificando fallas de seguridad como inyecciones SQL, XSS, errores de configuración de seguridad, entre otros.

### 1.3.1 Objetivo General

Desarrollar un sistema en Python que permita escanear aplicaciones web y detectar vulnerabilidades comunes según el OWASP Top 10, brindando reportes claros y accionables para mitigarlas.

### Objetivos Específicos

- Implementar un módulo de escaneo automático de URLs.
- Integrar técnicas de detección para cada una de las 10 vulnerabilidades del OWASP.
- Generar reportes técnicos con detalles de vulnerabilidades y recomendaciones.
- Garantizar una interfaz CLI simple y funcional para pentesters y desarrolladores.

# 2. Riesgos

- **Falsos positivos:** El sistema puede reportar errores inexistentes, afectando la confiabilidad.
- **Limitaciones de permisos:** Algunos servidores bloquean los escaneos, reduciendo el alcance de las pruebas.
- **Actualización del OWASP Top 10:** Cambios en las amenazas prioritarias pueden volver obsoletas algunas reglas del sistema.
- **Problemas de compatibilidad con servidores web modernos.**
- **Dificultad de aceptación por parte de usuarios no técnicos.**

# 3. Análisis de la Situación Actual

## 3.1 Planteamiento del problema

Actualmente, muchas aplicaciones web son desplegadas sin un análisis profundo de seguridad, lo cual las expone a ataques cibernéticos. No existen suficientes herramientas accesibles, automatizadas y adaptadas al entorno hispanohablante que realicen escaneos eficientes de vulnerabilidades.

### 3.2 Consideraciones de Hardware y Software

**Hardware:**

- Computadora de escritorio o portátil para desarrollo y pruebas.
- Servidor web local o en la nube para testeo de vulnerabilidades.
- Conexión de red estable.

**Software:**

- Lenguaje de programación: Python 3.x
- Librerías: Requests, BeautifulSoup, Socket, etc.
- Frameworks de soporte: Flask (para posible interfaz web), OWASP ZAP API (como integración opcional).
- Sistema operativo: Windows/Linux.
- Editor de código: Visual Studio Code o PyCharm.

## 4. Estudio de Factibilidad

### 4.1 Factibilidad Técnica

**Software**

| Sistema | Descripción | Operatividad |
|---|---|---|
| **Python 3.x** | Lenguaje principal para desarrollo del scanner. | Portable, versátil y con gran soporte de librerías de seguridad. |
| **VS Code/PyCharm** | IDE para codificación eficiente. | Permite integración de plugins útiles para desarrollo seguro. |
| **Git** | Control de versiones del código fuente. | Permite trabajo colaborativo y backup seguro. |
| **OWASP ZAP API** | Integración opcional para pruebas avanzadas. | Compatible vía REST con el sistema. |

**Hardware**

| Componente | Descripción | Operatividad |
|---|---|---|
| **CPU** | Procesador de al menos 4 núcleos (Intel i5 o similar) | Para escaneos simultáneos eficientes. |
| **Memoria RAM** | Mínimo 8 GB | Para ejecución fluida del sistema. |
| **Almacenamiento** | 500 GB mínimo | Para guardar logs de escaneos y reportes. |
| **Conexión Red** | Mínimo 10 Mbps | Permite pruebas en tiempo real en servidores web. |

### 4.2 Factibilidad Económica

**1. Costos Generales**

| Item | Cantidad | Precio Unitario | Precio Total |
|---|---|---|---|
| **Laptop de desarrollo** | 1 | S/ 1,200 | S/ 1,200 |
| **Router WiFi** | 1 | S/ 80 | S/ 80 |
| **Escritorio + Silla** | 1 | S/ 150 | S/ 150 |
| **Licencia Windows 10** | 1 | S/ 50 | S/ 50 |
| **Antivirus Básico** | 1 | S/ 30 | S/ 30 |
| **Papelería básica** | 1 | S/ 40 | S/ 40 |
| **Total Generales: S/ 1,550** | | | |

**2. Costos Operativos**

| Elemento | Meses | Precio Mensual | Total |
|---|---|---|---|
| **Energía Eléctrica** | 2 | S/ 60 | S/ 120 |
| **Internet** | 2 | S/ 60 | S/ 120 |
| **Agua y saneamiento** | 2 | S/ 30 | S/ 60 |
| **Total Operativos: S/ 300** | | | |

**3. Costos de Ambiente**

| Software | Cantidad | Costo Unitario | Total |
|---|---|---|---|
| **Licencia Windows** | 2 | S/ 50 | S/ 100 |
| **Antivirus** | 2 | S/ 25 | S/ 50 |
| **Total: S/ 150** | | | |

**4. Costos de Personal**

| Rol | Pago/Hora | Horas/Mes | Personal | Subtotal |
|---|---|---|---|---|
| **Jefe de Proyecto** | S/ 5.00 | 80 | 1 | S/ 400 |
| **Desarrollador Python** | S/ 5.00 | 80 | 1 | S/ 400 |
| **Subtotal mensual: S/ 800 x 2 meses = S/ 1,600** | | | | |

**5. Total General: S/ 3,600.00**

### 4.3 Factibilidad Operativa

PWASP SCANNER requiere infraestructura básica, sin mayores requerimientos técnicos. Su interfaz en línea de comandos (CLI) es apta para usuarios técnicos, especialmente en roles de ciberseguridad.

### 4.4 Factibilidad Legal

Cumple con:

- Ley N.º 29733 (Protección de Datos Personales).
- Normativas de ética en pruebas de penetración (solo con autorización).
- Licencias de uso libre de librerías (MIT, GNU GPL).

### 4.5 Factibilidad Social

El proyecto tiene impacto positivo en la comunidad tecnológica, promoviendo el desarrollo seguro de software, fomentando la cultura de pruebas de seguridad preventiva y reduciendo incidentes cibernéticos.

### 4.6 Factibilidad Ambiental

- Operación 100% digital.
- Reducción del uso de papel.
- Bajo consumo energético.
  Compatible con políticas de sostenibilidad y gestión ambiental.

## 5. Análisis Financiero

### 5.1 Justificación de la Inversión

**Beneficios del Proyecto**

**Tangibles:**

- Reducción de ataques web en entornos protegidos.
- Ahorro en consultorías externas de seguridad.
- Automatización del proceso de pruebas de penetración.

**Intangibles:**

- Mayor reputación de seguridad para los usuarios.
- Fomento de una cultura DevSecOps.

### 5.1.2 Criterios de Inversión

**Ingresos Estimados**

| Categoría | Monto | % | Ahorro/Ingreso |
|---|---|---|---|
| **Venta del software** | 5,000 | 40% | 2,000 |
| **Servicios de auditoría** | 3,000 | 50% | 1,500 |

| | | | |
|---|---|---|---|
| **Reducción de incidentes** | 4,000 | 20% | 800 |
| **Total ingresos estimados: S/ 4,300.00** | | | |

**Egresos**

| Servicio | Monto |
|---|---|
| **Hosting y mantenimiento anual** | S/ 1,200 |

**Flujo de caja estimado:**

| Periodo | Ingresos | Egresos | Flujo Neto |
|---|---|---|---|
| **0** | 0 | -3,600 | -3,600 |
| **1** | 4,300 | 1,200 | 3,100 |
| **2-4** | 4,300 | 1,200 | 3,100 (cada año) |

**5.1.2.1 Relación Beneficio/Costo (B/C)**

**B/C = 2.38**

**5.1.2.2 Valor Actual Neto (VAN)**

**VAN ≈ S/ 7,200.00**

**5.1.2.3 Tasa Interna de Retorno (TIR)**

**TIR ≈ 115%**

## 6. Conclusiones

- PWASP SCANNER es factible a nivel técnico, económico, operativo, legal, social y ambiental.
- El equipo puede desarrollar el proyecto eficientemente con recursos mínimos.
- Representa una oportunidad de inversión rentable y de impacto positivo en la ciberseguridad web.
- Se recomienda su implementación inmediata por su alto valor preventivo y formativo.